NEC

GVT-159429-001-00 1.7

QX-S5100G シリーズ

Ethernet スイッチ オペレーションマニュアル

改版履歴

版数	日付	改版内容
1.0	2021/04	初版発行
1.1	2021/07	・01-はじめにの 15 章 装置管理に locator blink コマンドに関する記載を追加しました。 ・09-セキュリティの 16 章 ARP アタックプロテクションに arp scan コマンドに関する記載を追加しました。 ・11- システム管理の 13 章 NetMeister にプロキシ関連の記載、ゼロタッチプロビジョニングに関する記載、トラブルシューティングを追加しました。
1.2	2022/03	・09-セキュリティの 3 章 802.1X に 802.1 X ユニキャストトリガーサイレント機能を追加しました。 ・09-セキュリティの 7 章ポートセキュリティに 7.12 ポートでの認証方式のトリガー順序の設定を追加しました。
1.3	2022/06	・11- システム管理の 13 章 NetMeister に IRF 対応に関する記載を追加しました。
1.4	2023/03	・01-はじめにの 15 章 装置管理の「CPU 使用率のモニタリングの設定」にメモを追加しました。 ・01-はじめにの 15 章 装置管理の「トランシーバの診断」を削除しました。 ・03-アクセスの 8 章 STP の「BPDU ガードの有効化」に検出の間隔についての設定コマンドを追加しました。 ・03-アクセスの 12 章 VoiceVLAN に「12.12 Voice VLAN を配信する CDP の設定」を追加しました。 ・03-アクセスの 14 章 VLAN マッピングの重要に追記をしました。 ・03-アクセスの 15 章 LLDP の「15.5 CDP 互換モードの設定」に cdp voice-vlan コマンドの設定方法を追加しました。 ・04-IP サービスの 1 章 ARP の「1.3.1 装置で学習できるダイナミック ARP エントリの最大数の設定」の設定手順に追記をしました。 ・04-IP サービスの 7 章 DHCP サーバの設定の「カスタマイズ DHCP オプションの設定」にオプショングループでのカスタマイズ DHCP オプションの設定手順を追記しました。 ・09-セキュリティの 7 章ポートセキュリティの port-security port-mode コマンドに mac-and-userlogin-secure-ext オプションを追加しました。 ・09-セキュリティの 7 章ポートセキュリティに port-security mac-move bypass-vlan-check コマンドに関する記載を追加しました。 ・11-システム管理の 13 章 NetMeister に親機モード運用時の設定を追加しました。

版数	日付	改版内容
1.5	2025/05	・表紙ロゴ色、配置の変更 ・01-はじめに 5 章 CLI によるログインの「5.2 コンソールポートからのローカルログイン」を更新しました。 ・03-アクセス の 8 章 STP の「8.28.6. BPDU ドロップ機能の有効化」 に、制限とガイドラインを追加しました。 ・04-IP サービス の 2 章 Gratuitous ARP に「2.4. デバイスの MAC アドレス変更に対する gratuitous ARP パケット再送信の設定」を追加しました。 ・08-ACL and QoS の 1 章 ACL の「1.5.2 拡張 IPv6 ACL の設定」 にポイントを追加しました。 ・08-ACL and QoS の 8 章 プライオリティマーキング の「8.2. 設定手順」を誤記修正しました。 ・09-セキュリティ 17 章 uRPF 「17.2 グローバルでの uRPF の有効化」について、以下の誤記を修正しました。 ・設定手順 2 から、 ・loose パラメータを削除 ・strict パラメータのオプションを削除 ・10-高可用性 3 章 DLPP の「3.2 設定の制限とガイドライン」を更新しました。 ・10-高可用性 の 4 章 RRPP の「4.2. RRPP の設定作業リスト」の注意に追記をしました。 ・10-高可用性の 9 章 Track の「9.4Track 設定作業リスト」に、PoE との関連付けを追加しました。 ・11-システム管理 4 章 PoE 行頭メモに poe high-inrush に対応していることを記載しました。 「4.4 PD による突入電力の許容（high-inrush のやり方）」を追加しました。
1.6	2025/07	・02 IRFスタック1章 IRFスタックの「1.1.2 ソフトウェア要件」 に設定に関する注意を追加しました。 ・12-謝辞を更新しました。
1.7	2026/11	・QX-S5100Gシリーズ Ethernet スイッチマニュアル訂正資料9.0版を反映しました。

Copyright © NEC Corporation 2021-2026

All Rights Reserved

事前に NEC の書面による許可なく、本マニュアルをいかなる形式または方法で複製または配布することを禁止します。

商標

本マニュアルに記載されているその他の商標は、各社が保有します。

注意

- 本装置は *QX-S5100G シリーズ Ethernet スイッチ コマンドマニュアル*に記載されているコマンドのみ使用することができます。*QX-S5100G シリーズ Ethernet スイッチ コマンドマニュアル*に記載されていないコマンドを使用した場合の動作については保証しません。
- 本マニュアルの内容は、予告なく変更されることがあります。本マニュアルのすべての記述、情報、および推奨事項は、明示的か暗黙的かにかかわらず、いかなる種類の保証の対象になりません。

本マニュアルについて

バージョン

本マニュアルに対応する製品バージョンは Version 7.1.X を含む以降のソフトウェアです。

関連マニュアル

次のマニュアルには、QX-S5100G シリーズ Ethernet スイッチに関する詳細な説明があります。

マニュアル	内容
QX-S5100G シリーズ Ethernet スイッチ インスタレーションマニュアル	システムのインストールについて説明しています。
QX-S5100G シリーズ Ethernet スイッチ オペレーションマニュアル	機能の設定について説明しています。
QX-S5100G シリーズ Ethernet スイッチ コマンドマニュアル	機能に関するコマンドについて説明しています。
QX-S5100G シリーズ Ethernet スイッチ Web コンソール操作マニュアル	Web コンソールからの装置設定、状態確認等についての操作を記述しています。

マニュアルの構成

このオペレーションマニュアルは以下のセクションで構成されます。

- **はじめに**

  Ethernet スイッチへのアクセス方法、ファイルシステム管理、設定ファイル管理、ソフトウェア管理、装置管理といった、Ethernet スイッチの管理の設定について説明します。

- **IRF スタック**

  IRF スタックの設定について説明します。

- **アクセス**

  Ethernet ポート、リンクアグリゲーション、VLAN、STP といった、レイヤ 2 機能の設定について説明します。

- **IP サービス**

  ARP、IP アドレス（IPv4＆IPv6）、DHCP 関連機能、IP パフォーマンスといった、ネットワークプロトコルの設定について説明します。

- **ルーティングプロトコル**

各種ルーティングプロトコル（IPv4＆IPv6）の設定について説明します。

- **マルチキャスト**

  各種マルチキャストプロトコル（IPv4＆IPv6）の設定について説明します。

- **MCE**

  MCE の設定について説明します。

- **ACL and QoS**

  QoS、ACL の設定について説明します。

- **セキュリティ**

  AAA、RADIUS、802.1X、MAC アドレス認証、SSH 等の設定について説明します。

- **高可用性**

  Ethernet OAM、CFD、DLDP、RRPP、BFD 等の設定について説明します。

- **システム管理**

  システム保守、ネットワーク管理の設定といった、Ethernet スイッチのシステム管理および保守について説明します。

- **謝辞**

表記規則

本マニュアルでは、次の表記規則を使用しています。

I. コマンド表記規則

表記規則	説明
太字体	コマンドラインを示すキーワードには**太字体**を使用します。
イタリック体	コマンドの引数は*イタリック体*を使用します。
[ ]	大カッコに囲まれた項目(キーワード、引数)はオプションです。
{ x | y | ... }	選択する項目は、中カッコに入れて縦線で区切ってあります。1 つを選択します。
[x | y | ...]	オプションの選択項目は､大カッコに入れて縦線で区切ってあります。1 つまたは複数を選択します。
{ x | y | ... }*	選択する項目は、中カッコに入れて縦線で区切ってあります。少なくとも 1 つ選択できます。
[x | y | ...]*	オプションの選択項目は、大カッコに入れて、縦線で区切ってあります。1 つあるいは複数選択することも、何も選択しないこともできます。
&<1-n>	&の前のキーワードと引数を組み合わせます。引数で指定した数までキーワードを繰り返し指定できます。
#	#で始まる行はコメントを示します。

II. GUI 表記規則

表記規則	説明
< >	ボタン名は三角カッコに入っています。例えば、<OK>ボタンをクリックします。
[ ]	ウィンドウ名、メニュー項目、データ表、およびフィールド名は大カッコに入っています。例えば、[New User]ウィンドウが表示されます。
/	複数レベルのメニューはスラッシュで区切ってあります。例えば、[File/Create/Folder]。

III. キーボード操作

表記規則	説明
<KEY>	KEY のキーを押します。例えば、 <Enter>は Enter キーを押します。
<KEY1 + KEY2>	複数のキーを同時に押します。例えば、<Ctrl+Alt+A>は 3 つのキーを同時に押すことを表します。
<KEY1, KEY2>	複数のキーを順番に押します。例えば、 <Alt, A>は 2 つのキーを順に押すことを表します。

IV. マウス操作

表記規則	説明
クリック	マウスのボタンを素早く押します。特に指定がない場合は左ボタンを押します。
ダブルクリック	マウスの左ボタンを素早く 2 回押します。
ドラッグ	マウスの左ボタンを押したまま移動します。

V. 記号

表記規則	説明
⚠ **警告**	表示を無視したり指示に従わない場合、利用者が怪我などをする恐れのある重要な情報を示します。
⚠ **注意**	表示を無視したり指示に従わない場合、データの損失や破損、ハードウェアやソフトウェアの損傷などが発生する恐れのある重要な情報を示します。
⚠ **重要**	注意を払う必要がある情報を示します。
🕮 **メモ**	追加または補足となる情報を示します。
🕮 **ポイント**	参考となる情報を示します。

VI. ネットワークアイコン

表記規則	説明
	ルータ、スイッチ、またはファイアウォールなどの一般的なネットワークデバイスを表しています。
	ルータまたはレイヤ 3 スイッチなどのルーティング対応のデバイスを表しています。
	レイヤ 2、レイヤ 3 スイッチまたはレイヤ 2 転送機能に対応したルータなどの一般的なスイッチデバイスを表しています。

VII. 設定例

本マニュアルの設定例は各機能での代表的な設定例を示します。インタフェース番号、システム名の表記、display コマンドで表示される情報は、ご使用の装置と異なることがあります。

VIII. セキュリティ強化

セキュリティ強化のため、simple で設定されたパスワードも cipher や hash で登録されます。

本マニュアルは以下に示す 12 個のセクションで構成されています。

01 - はじめに

02 - IRF スタック

03 - アクセス

04 - IP サービス

05 - ルーティングプロトコル

06 - マルチキャスト

07 - MCE

08 - ACL and QoS

09 - セキュリティ

10 - 高可用性

11 - システム管理

12 - 謝辞

QX-S5100G シリーズ Ethernet スイッチ

オペレーションマニュアル

1. はじめに

本マニュアルは以下に示す章で構成されています。

01-CLI
02-RBAC
03-ログイン
04-コンソールポートによる最初のログイン
05-CLI によるログイン
06-Web コンソールによるログイン
07-SNMP によるログイン
08-RESTful
09-ログインユーザの制御
10-FTP
11-TFTP
12-ファイルシステム管理
13-コンフィグレーションファイル管理
14-ソフトウェアのアップグレード
15-装置管理
16-Python
17-Comware 7 python 拡張 API
18-Auto Config

目次

このセクションのページは**1-x-x**です。

1章 CLI 1-1
1.1 CLI viewの記述 1-1
1.1.1 user viewからsystem viewへの移行 1-2
1.1.2 各viewから上位viewへの戻り 1-2
1.1.3 user viewへの戻り 1-2
1.2 コマンドラインを使ったオンラインヘルプ 1-2
1.3 コマンドのundo 1-3
1.4 コマンドの実行 1-4
1.4.1 コマンドラインの編集 1-4
1.4.2 引数の文字列あるいはテキストタイプ値の入力 1-5
1.4.3 インタフェースタイプの入力 1-5
1.4.4 コマンドの補完 1-6
1.4.5 コマンドエイリアスの設定と使用方法 1-6
1.4.6 ホットキーを使用した設定と使用方法 1-7
1.4.7 情報の同期出力 1-9
1.5 コマンドラインのエラーメッセージ 1-9
1.6 履歴コマンドの保存 1-9
1.7 CLI表示の管理 1-10
1.7.1 出力のスクリーンの休止 1-10
1.7.2 表示コマンドの各出力ラインの番号表示 1-11
1.7.3 出力のフィルタリング 1-12
1.7.4 displayコマンドのファイルへの保存 1-14
1.7.5 displayコマンドからの出力の有効的な表示、管理 1-15
1.8 稼働中の設定の保存 1-16

1章 CLI

Command-Line Interface （CLI）は、装置とユーザ間の相互運用ユーザインタフェースです。装置の設定、管理、モニタリングを行うため、CLI からコマンドを入力します。

```
<Switch> system-view
System View: return to User View with Ctrl+z.

[Switch]
```

CLI にはコンソールポートを使用する以外にも、Telnet、SSH などを使用してログインすることができます。

1.1 CLI viewの記述

コマンドは機能によって異なる view にグループ分けされています。コマンドを使用する場合、その view に入る必要があります。

CLI view は図 1-1に示すような階層構造となっています。各 view は、どこで何を行うのかを一意に示すプロンプトとなります。たとえば[Switch-vlan100]という view は、VLAN100 view で、その VLAN の属性を設定することができます。

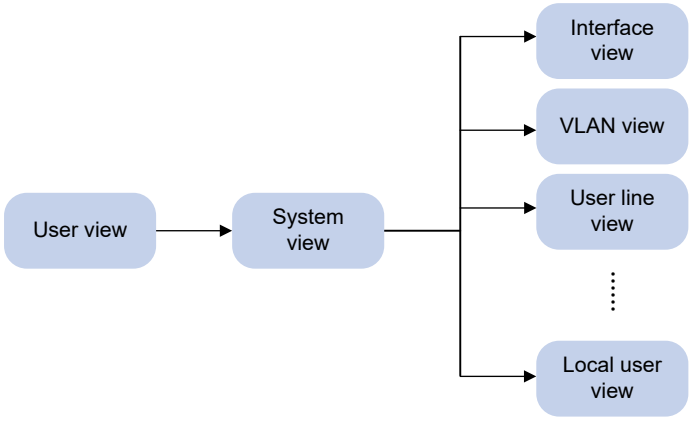


図 1-1 CLI view

CLI でログインした後、最初に user view に入ります。user view のプロンプトは <*Device-name*>で、*Device-name* は装置名を示します。デフォルトは装置名で、**sysname** コマンドを使用して変更することができます。

user view では以下の操作を行うことができます。

- 表示、デバッグ、ファイル管理、FTP、Telnet、日時の設定、再起動などの基本的な操作を行うことができます。
- user view から system view に移行することができます。system view のプロンプトは [*Device-name*]です。

system view では以下の操作を行うことができます。

- グローバルの設定（時間の設定、バナー、ショートカットキーなど）といくつかの機能を行うことができます。
- system view からさらに、異なる view に移行することができます。たとえば、以下の操作を行うことができます。
  - interface view に移行し、インタフェースパラメータの設定ができます。
  - VLAN view に移行し、VLAN にポートを追加することができます。
  - user line view に移行し、ログインユーザの属性を設定することができます。

view プロンプトでクエスチョン“?”を入力することで、その view で利用できるすべてのコマンドを表示します。

1.1.1 user view から system view への移行

操作	コマンド
system viewに移行する	**system-view**

1.1.2 各 view から上位 view への戻り

操作	コマンド
各viewから上位viewに戻る	**quit**

user view で **quit** コマンドを実行することで、装置の接続を終了します。

public key view で **peer-public-key end** コマンドを実行することで、system view へ戻ります。

1.1.3 user view への戻り

return コマンドあるいはホットキー**Ctrl+Z** を実行することで直接 user view に戻ることができます。あるいは **quit** コマンドを繰り返すことで user view に戻ることができます。

以下の手順で、他の view から user view へ戻ります。

操作	コマンド
user viewに戻る	**return**

1.2 コマンドラインを使ったオンラインヘルプ

CLI オンラインヘルプは状況に応じてヘルプ情報が異なります。すべてのプロンプトで“?”を入力し、その view で利用できるコマンドを表示するか、コマンドのいずれかの位置で、すべての有効なオプションを表示することができます。

CLI オンラインヘルプにアクセスするには以下の方法を行います。

- 各 view で “?” を入力することで、その view で利用できるすべてのコマンドの最初のキーワードを表示します。

```
<Switch> ?
User view commands:
archive             Archive configuration
  arp                 Address Resolution Protocol (ARP) module
  backup              Backup operation
...
```

- コマンドキーワードの後ろにスペースを空けて”?”を入力することで、設定可能なキーワードかパラメータが表示されます。
  - □ キーワードの場所にスペースを空けて”?”を入力したとき、設定可能なキーワードの概要が表示されます。

```
<Switch> terminal ?
  debugging  Enable to display debugging logs on the current terminal
  logging    Display logs on the current terminal
  monitor    Enable to display logs on the current terminal
```

  - □ パラメータの場所にスペースを空けて”?”を入力したとき、設定可能なパラメータの概要が表示されます。

```
<Switch> system-view
[Switch] interface vlan-interface ?
  <1-4094>  Vlan-interface interface number
[Switch] interface vlan-interface 1 ?
  <cr>
[Switch] interface vlan-interface 1
```

<1-4094> は引数の範囲で、<cr>はコマンドを示します。完了させるには、Enter キーを押してコマンドを実行することができます。

- コマンドの後ろに?をつけて入力すると、この文字列で始まるすべてのキーワードが表示されます。

```
<Switch> f?
  fdisk    Partition a storage medium
  fixdisk   Check and repair a storage medium
  format    Format a storage medium
  free      Release a line
  ftp       Open an FTP connection
<Switch> display ftp?
  ftp          FTP module
  ftp-server   FTP server information
  ftp-user     FTP user information
```

1.3 コマンドのundo

コマンドにキーワード undo をつけると、**undo** コマンドを形成できます。

ほとんどの設定コマンドに、undo を付加できます。以下のことができます。

- システムをデフォルトの状態に戻します。
- 機能を無効にします。
- 設定を取り消すときに使用します。

たとえば Information Center を有効にするために、**info-center enable** コマンドを使用した場合、**undo info-center enable** コマンドで Information Center を無効にします。

1.4 コマンドの実行

コマンドを入力することで以下のことができます。

- キーあるいはショートカットキーを使用してコマンドラインを編集できます。
- 省略したキーワードあるいはエイリアスを使用することができます。

1.4.1 コマンドラインの編集

コマンドラインを編集するために、表 1-1に示すキーや表 1-4に示すホットキーを使用することができます。終了するには **Enter** を押してコマンドを実行します。

コマンドラインの最大の長さは、512 文字です。パラメータ（キーワード、引数）、スペース、特殊文字を含みます。

表 1-1 コマンドラインの編集キー

キー	機能
コマンドキー	編集バッファが一杯でなければ、カーソルの位置に文字を挿入し、カーソルを右に移動します。コマンドの最大の長さは、511文字です。コマンドの最大の長さに達した場合、システムは次の行に自動的に移ります。次の行に移るには、**Enter** を押します。
Backspace	カーソルの左側の文字を削除し、1文字分カーソルを戻します。
左矢印キー (←)	カーソルが左に1文字分移動します。
右矢印キー (→)	カーソルが右に1文字分移動します。
上矢印キー (↑)	前に入力した履歴コマンドを表示します。
下矢印キー (↓)	次に入力した履歴コマンドを表示します。
Tab	キーワードの一部でTABキーを押した場合、システムは自動的にキーワードを補完します。 • ただ1つマッチングしたら、システムは不完全なキーワードを完全なキーワードに置き換えて、それを次の行に表示します。 • マッチするものが複数ある場合、キーワードを選択するためTABキーを複数回押してください。 • マッチするものが全くない場合は、システムは不完全なキーワードを補完せず、再度それを次の行に表示します。

コマンドラインの最大長は 512 文字を超過することができません。512 文字にはスペース、特殊文字が含まれます。

装置は以下の特殊文字をサポートします。

- **#**－システムによって隣接セクションと区別するためにコンフィグレーションファイルの中で使用します。
- **version**－ソフトウェアバージョンを示すため、コンフィグレーションファイルの中で使用します。たとえば Version 7.1.x です。

これらのコマンドは以下の理由があるため特殊文字となります。

- CLI でユーザが使用することはできません。
- すべての view で特殊文字を入力する、あるいはすべての値を入力することができます。たとえば、# abc あるいは version abc を入力することができます。しかし設定は適用されません。
- 装置はこれらの特殊文字に関するオンラインヘルプはありません。

1.4.2 引数の文字列あるいはテキストタイプ値の入力

テキストタイプの引数はクエスチョンマーク（?）を除く印刷可能な文字列を使用することができます。

文字列タイプの引数は以下の文字列を除く印刷可能な文字列を使用することができます。

- クエスチョンマーク（?）
- クオーテーションマーク（”）
- バックスラッシュ（\）
- スペース

特定の引数が必要となる場合があります。特定の引数については、関連するコマンドマニュアルを参照してください。

印刷可能な文字列は、文字あるいは ASCII コード（範囲は 32～126 です）を入力することができます。

1.4.3 インタフェースタイプの入力

以下のフォーマットでインタフェースタイプを入力することができます。

- インタフェースタイプのフルスペル
- インタフェースを識別する固有な短縮形
- インタフェースの頭文字

コマンドラインではすべてのインタフェースのタイプは大文字、小文字を区別しません。表 1-2にインタフェースタイプのフルスペルと短縮形を示します。

たとえば、GigabitEthernet 1/0/1 の view に移行するため、**interface** コマンドを入力する場合、コマンドラインで以下のフォーマットを入力することができます。

- interface gigabitethernet 1/0/1
- interface gig 1/0/1
- interface ge 1/0/1

インタフェースのタイプとインタフェースの間のスペースは必要ありません。

表 1-2 インタフェースのタイプのフルスペルと短縮形

フルスペル	短縮形
Bridge-Aggregation	BAGG

フルスペル	短縮形
GigabitEthernet	GE
InLoopBack	InLoop
LoopBack	Loop
M-GigabitEthernet	MGE
NULL	NULL
Ten-GigabitEthernet	XGE
Vlan-interface	Vlan-int

1.4.4 コマンドの補完

コマンドは、キーワードの一部を入力することでコマンドを実行できます。ただし、入力するコマンドを識別するのに十分な文字列を入力した場合のみ有効です。たとえば **system-view** で **s** から始まるコマンドは、**system-view** と **startup saved-configuration** があります。**system-view** を指定する場合、最低でも **sy** を入力する必要があります。**startup saved-configuration** を指定する場合、最低でも **st s** を入力する必要があります。

Tab キーを押すことで、完全なコマンドを表示,入力することができます

1.4.5 コマンドエイリアスの設定と使用方法

キーワードで始まるコマンドや **undo**＋キーワードで始まるコマンドを実行するとき、以下のエイリアスを使用することができます。

- **undo** コマンドを除くコマンドの先頭キーワード
- **undo** コマンドの 2 番目のキーワードのエイリアス

たとえば、**display** のエイリアスとして **show** を設定する場合、**display clock** コマンドを実行するのに、**show clock** コマンドを入力することができます。

たとえば、**display ip routing-table** コマンドの **alias shiprt** を設定する場合、**display ip routing-table** コマンドを実行するため、**shiprt** を入力することができます。**display ip** コマンドの **alias ship** を設定する場合、**display ip** で始まるすべてのコマンドを実行するため、**ship** を入力することができます。

- **display ip routing-table** コマンドを実行するため、**ship routing-table** を入力します。
- **display ip interface** コマンドを実行するため、**ship interface** を入力します。

I. ガイドライン

コマンドエイリアスで定義したコマンドを実行したのち、装置はエイリアスの代わりにキーワードを保存します。カレントコンフィグレーションはオリジナルコマンドが表示されます。

エイリアスによって説明できる文字列は 9 つのパラメータまで設定することができます。各パラメータはドル記号”$”と 1～9 までのシーケンス番号で開始します。

たとえば、**display ip $1 | include $2** を行うために **alias shinc** コマンドを設定することができます。**display hotkey | include CTRL_C** コマンドを実行するため、**shinc hotkey CTRL_C** を入力することができます。

パラメータがあるコマンドのエイリアスを使用する場合、各パラメータの値を指定する必要があります。パラメータの指定を設定するのに失敗した場合、コマンドは不完全で、エイリアスで表示されるコマンドの文字列を表示します。

表 1-3にシステム定義のコマンドエイリアスを示します。システム定義のコマンドエイリアスは削除することができません。

表 1-3 システム定義のコマンドエイリアス

エイリアス	コマンド
access-list	acl
end	return
erase	delete
exit	quit
hostname	sysname
logging	info-center
no	undo
show	display
write	save

II. 設定手順

以下にコマンドエイリアスの設定を以下に示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． コマンドエイリアスを設定する	**alias** *alias command*	デフォルト：設定なし システム定義のコマンドエイリアスは表 1-3を参照してください。
3． （オプション設定項目）コマンドエイリアスで定義されたコマンドを表示する	**display alias** [**alias**]	すべてのviewで実行可能です。

1.4.6 ホットキーを使用した設定と使用方法

CLI を補助するため、表 1-4にホットキーを定義します。またデフォルトで指定済みのホットキーを示します。ホットキーを押すことでコマンドを入力することと同じことを行うことができます。これらのホットキーは装置が定義しています。

端末のソフトウェアから装置と相互に運用する場合、これらのキーは他の操作を実行するために定義されている可能性があります。その場合は、端末のソフトウェアの定義が優先されます。

表 1-4 システムで予約済みのホットキー

ホットキー	昨日
Ctrl+A	カーソルを現在の行の先頭に動かします。
Ctrl+B	カーソルを 1 文字分左に動かします。
Ctrl+C	コマンドの実行を停止させます。
Ctrl+D	現在カーソルがある位置の文字を削除します。
Ctrl+E	カーソルを現在の行の末尾に動かします。
Ctrl+F	カーソルを1文字分右に動かします。
Ctrl+H	カーソルの左側の文字を削除します。
Ctrl+K	外部接続を終了します。
Ctrl+N	履歴バッファの次のコマンドを表示します。
Ctrl+P	履歴バッファの前のコマンドを表示します。
Ctrl+R	現在の行のコマンドを再表示します。
Ctrl+V	クリップボードの中身を貼り付けます。
Ctrl+W	カーソルの左側に続く文字列の文字をすべて削除します。
Ctrl+X	カーソルの左側の文字をすべて削除します。
Ctrl+Y	カーソルの右側の文字をすべて削除します。
Ctrl+Z	終了し、user viewに戻ります。
Ctrl+]	内部接続またはリダイレクト接続を終了します。
Esc+B	カーソルを左側に続く文字列の先頭の文字に移動します。
Esc+D	現在カーソルがある位置の文字列の文字および右側の文字をすべて削除します。
Esc+F	カーソルを右側に続く次の文字列の先頭に移動します。
Esc+N	カーソルを1行下に移動します。Enterキーを入力する前にホットキーを使用することができます。
Esc+P	カーソルを1行上に移動します。Enterキーを入力する前にホットキーを使用することができます。
Esc+<	クリップボードの先頭にカーソルを移動します。
Esc+<	クリップボードの最後にカーソルを移動します。

以下の手順でホットキーを設定します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. コマンドをホットキーに割り当てる	**hotkey** { **ctrl_g** | **ctrl_l** | **ctrl_o** | **ctrl_t** | **ctrl_u** } *command*	デフォルト： ● **Ctrl+G**は**display current-configuration**コマンドを表示します。 ● **Ctrl+L**は**display ip routing-table**コマンドを表示します。 ● **Ctrl+O**は **undo debugging all**コマンドを表示します。 ● **Ctrl+T**コマンドと**Ctrl+U**コマンドは未割り当てです。

操作	コマンド	補足
3. （オプション設定項目）ホットキーを表示する	**display hotkey**	すべてのviewで実行可能です。

1.4.7 情報の同期出力

情報の同期出力とは、システム出力によりユーザの入力が中断された場合、システム出力が完了した後に、システムがコマンドラインプロンプトやそれまで入力していたものを表示する機能を指し、ユーザは操作を中断したところから継続させることができます。

以下の手順で情報の同期出力を設定します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. 情報の同期出力を有効にする	**info-center synchronous**	デフォルト：無効 詳細はコマンドマニュアルのセクション11 *システム管理" Information Center"* を参照してください。

1.5 コマンドラインのエラーメッセージ

Enter キーを押した後、コマンドラインは、コマンドの最初から順番に構文をチェックします。

- 構文エラーがある場合、エラーメッセージが表示されます。
- 構文エラーがない場合、コマンドを実行します。

表 1-5 コマンドラインのエラーメッセージ

エラーメッセージ	原因
% Unrecognized command found at '^' position.	マークしたポジションにあるキーワードが無効です。
% Incomplete command found at '^' position.	1つ以上のキーワードあるいは引数が不完全です。
% Ambiguous command found at '^' position.	入力した文字列があいまいです。
% Too many parameters.	入力した文字列が多すぎます。
% Wrong parameter found at '^' position.	マークしたポジションにあるパラメータが正しくありません。

1.6 履歴コマンドの保存

システムは、使用したコマンドを自動的に保存できます。保存したコマンドを必要に応じて呼び出し、繰り返し使用できます。

システムは、ログインユーザによって実行されたコマンドを自動的に、以下の 2 つの履歴バッファに保存します。

- user line 用のコマンド履歴バッファ

- すべての user line 用のコマンド履歴バッファ

表 1-6に 2 つのコマンド履歴バッファの違いを示します。

表 1-6 コマンド履歴バッファの比較

アイテム	user line のコマンド履歴バッファ	すべての user line のコマンド履歴バッファ
バッファに保存されるコマンドの種類	user lineにログイン中のユーザによって実行されたコマンド	すべてのログインユーザによって実行されたコマンド
ユーザがログアウトしたときに履歴がクリアされるか？	Yes	No
履歴を表示するコマンド	**display history-command**コマンド	**display history-command all**コマンド
履歴を実行するために呼び出す方法	バッファのコマンドを誘導します。Enterキーを押します。	履歴を呼び出すことはできません。
バッファサイズの設定方法	user line view で **history-command max-size** *size-value* コマンドを使用します。 デフォルト：10コマンド	バッファサイズをデフォルトから変更することはできません。 デフォルト：1024コマンド
バッファを無効にする方法	バッファサイズの設定を0にします。	バッファを無効にすることはできません。

履歴コマンドを使用したときのルールを示します。

- 正しいフォーマットで入力されたコマンドを履歴します。たとえば、不完全なコマンドが入力された場合、バッファされたコマンドも不完全となります。
- コマンドを入力するのにエイリアスを使用した場合、コマンドをバッファする前に表示されているコマンドあるいは *command* パラメータにエイリアスを変換します。
- 同一フォーマットのコマンドを連続して複数入力した場合、履歴コマンドには 1 回のみ履歴します。異なるフォーマットのコマンドを連続して複数入力された場合、各コマンドが履歴されます。たとえば **display cu** コマンドと **display current-configuration** コマンドの 2 つのエントリが連続して入力された場合、**display cu** コマンドが繰り返されたと認識し、コマンドのみが履歴されます。
- バッファが一杯の状態では、新しいコマンドを保存するため、最も古いコマンドの履歴が削除されます。

1.7 CLI表示の管理

この項では、CLI 表示を早急に認識できることを補助する管理機能を説明します。

1.7.1 出力のスクリーンの休止

表示する情報が 1 つのスクリーンを上回る場合、以下の表で示される方法のうちの 1 つを用いて情報出力を休止することができます。休止した箇所で----more----と表示します。詳

細な情報を表示させるために出力管理キーに記載されているキーを使用したり、表示を停止することができます。

通常、24 行が 1 つのスクリーンに表示されます。スクリーン画面に表示される行数を変更するため、**screen-length** *screen-length* コマンドを使用できます。詳細は、コマンドマニュアルのセクション 1 *はじめに*”*ログイン*”を参照してください。

現在のセッションで出力のスクリーンの休止を無効にすることができます。すべての出力は一度に表示され、最後にスクリーンが表示されるまで連続してスクリーンが更新されます。

I. 出力管理キー

キー	機能
Space	次画面ページの情報を示し続けます。
Enter	次のラインの情報を示し続けます。
Ctrl+C	表示とコマンド実行を中止します。
<PageUp>	前のページを表示します。
<PageDown>	次のページを表示します。

II. 複数のスクリーン出力機能の無効化

複数のスクリーン出力機能を無効にするには、user view で以下のコマンドを実行してください。

操作	コマンド	備考
現在のセッションで複数のスクリーン出力機能を無効にする	**screen-length disable**	デフォルト：**screen-length** *screen-length* コマンドの設定に依存します。 このコマンドは現在のセッションのみ適用されます。

1.7.2 表示コマンドの各出力ラインの番号表示

display コマンドで**| by-linenum** オプションを使用して、各出力ラインに番号を表示させることができます。

各出力ライン番号は 5 文字とコロン（：）あるいはハイフン（－）で表示されます。

| by-linenum オプションと**| begin** *regular-expression* オプションが指定される場合、正規表現にマッチしないすべての行でハイフンが表示されます。

display コマンドから各出力ラインに番号を表示させる方法を以下に示します。

操作	コマンド
番号付けされた**display**コマンドを表示する	**display** *command* **| by-linenum**

例：

VLAN 999 の情報を各出力ラインに番号付けして出力します。

```
<Switch> display vlan 999 | by-linenum
    1:   VLAN ID: 999
    2:   VLAN type: Static
    3:   Route interface: Not configured
    4:   Description: VLAN 0999
    5:   Name: VLAN 0999
    6:   Tagged ports:   None
    7:   Untagged ports: None
    8:
```

1.7.3 出力のフィルタリング

display コマンドに、**|** { **begin** | **exclude** | **include** } *regular-expression* オプションを使用して出力をフィルタリングすることができます。

- **begin**– 指定した正規表現から後の情報を表示します。
- **exclude**– 指定した正規表現を含まない情報を表示します。
- **include**– 指定した正規表現を含む情報だけを表示します。
- *regular-expression*– 1～256 文字の文字列で、大文字と小文字を区別します。正規表現は表 1-7に示す特殊文字をサポートします。

複雑な正規表現を使用すると表示に多くの時間が必要となります。コマンドを中止する場合、**Ctrl+C** を押します。

表 1-7 サポートする正規表現の特殊文字

文字	意味	例
^	キャレット。この後の文字列が行の先頭にのみ現れる場合にマッチします。	正規表現“^user”は、”user”で始まる文字列にマッチします。”Auser”はマッチします。
$	ドル記号。この前の文字列が行の最後にのみ現れる場合にマッチします。	正規表現"user$”は、”user”で終わる文字列にマッチします。“userA”はマッチします。
. (period)	ピリオド。空白を含む任意の一文字を示します。	“.s”は“as”と“bs”どちらにもマッチします。
*	アスタリスク。直前の文字の 0回以上の繰り返しにマッチします。	”zo*”は“z”や“zoo”にマッチします。(zo)*は”zo”と”zozo”にマッチします。
+	プラス。直前の文字の1回以上の繰り返しにマッチします。	”zo+”は"zo"や”zoo”にマッチするが、"z" にはマッチしません。
|	パイプ。左または右の文字列にマッチします。	”def|int”は、”def”または”int”を含んでいる文字列とマッチします。
( )	括弧。文字列を指定します。"+”や“*”と一緒に使われます。	”(123A)”は文字列“123A”を意味し、“408(12)+”は”40812”” 408121212”にマッチします。”408”にはマッチしません。
\N	Nで表した回数の文字列の繰り返しを示します。文字列とは\の前の( )内の文字列です。 \の前の文字列が一文字の場合は、Nは1のみが指定できます。\の前の文字列がn個の場合、Nは1からnの指定ができます。	“(string)\1”は、stringstringを含む文字列にマッチします。“(string1)(string2)\2”はstring1string2string2を含む文字列にマッチします。 “(string1)(string2)\1\2”はstring1string2string1string2を含む文字列にマッチします。

文字	意味	例
[ ]	ブラケットです。ブラケット内の1文字にマッチします。	“[16A]”は1、6、A、のいずれか1文字にマッチします。“1-36A”は1、2、3、6、Aのうちの1文字にマッチします。(-はハイフン)。“]”にマッチするためには“[”のすぐ後に“]”を入力します。たとえば“[]abc]”です。
[^]	[ ]内の文字列以外を指定します。	“[^16A]“は1、6、A以外で少なくとも1文字を含む文字列にマッチします（例”abc“）。1、6、Aを含む文字列(例”m16“)はマッチするが、1、6、Aのみの文字列（例1、16、16A）はマッチしません。
{n}	正の整数のn回の文字列にマッチします。	“o{2}”は“food”にマッチするが、“Bob”にマッチしません。
{n,}	正の整数のn回以上の文字列にマッチします。	“o{2,}”は“foooood”にマッチするが、“Bob”にマッチしません。
{n,m}	正の整数のnからm回以上の文字列にマッチします。mはnm以上の整数です。	“o{1,3}”は“fod”、“food”、“fooood“にマッチするが、“fd”にマッチしません。
\<	文字列の最初からマッチします。\<の次の文字列のパターンを含みますが、英数字、アンダーバーは含まれません。	”\<do”は”domain”、”doa”にマッチします。
\>	文字列の最後からがstringにマッチします。\>の次の文字列のパターンを含みますが、英数字、アンダーバーは含まれません。	”do\>”は”undo”や"cdo"にマッチします。
\b	[^A- Za-z0-9_]に等しい文字列にマッチします。 英数字、アンダーラインは含みます。	“\ba”は“-a”にマッチするが、“2a”、“ba”にマッチしません。
\B	[A- Za-z0-9_]に等しい文字列にマッチします。 英数字、アンダーラインは含みません。	“\Bt”は“install”にマッチするが、“big top”にマッチしません。
\w	\Bと同一です。	“v\w”は“"vlan”、“service”にマッチします。
\W	\bと同一です。	“\Wa”は“-a”にマッチするが、"2a"、"ba"にマッチしません。
\	エスケープ文字です。この表に記載された特殊文字が\に続くと、その文字を取り除くことを意味します。	”\\”は、”\”を含む文字列にマッチします。”\^”は、”^”を含んでいる文字列にマッチ、”\\b”は”\b”を含んでいる文字列とマッチします。

例：

 # display current-configuration コマンドで**| begin line** を使用し、**line** を含む最後の行の後の情報を表示します。

```
<Switch> display current-configuration | begin line
line class aux
 user-role network-admin
#
line class vty
 user-role network-operator
#
```

```
line aux 0
 user-role network-admin
#
line vty 0 63
 authentication-mode none
 user-role network-admin
 user-role network-operator
#
...
```

 # display ip brief コマンドで**| exclude DOWN** を使用し、UP 状態インタフェースを表示します。

```
<Switch> display interface brief | exclude DOWN
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface            Link Protocol Primary IP      Description
InLoop0              UP   UP(s)    --
NULL0                UP   UP(s)    --
Vlan1                UP   UP       192.168.1.83

Brief information on interfaces in bridge mode:
Link: ADM - administratively down; Stby - standby
Speed: (a) - auto
Duplex: (a)/A - auto; H - half; F - full
Type: A - access; T - trunk; H - hybrid
Interface            Link Speed    Duplex Type PVID Description
GE1/0/1              UP   1000M(a) F(a)   A    1
```

 # display current-configuration コマンドで**| include snmp** を使用し、**snmp** だけを含むエントリを表示します。

```
<Switch> display current-configuration | include snmp
snmp-agent
 snmp-agent community write private
 snmp-agent community read public
 snmp-agent sys-info version all
 snmp-agent target-host trap address udp-domain 192.168.1.26 params securityname
public
```

1.7.4 display コマンドのファイルへの保存

display コマンドは装置の設定と動作情報を示します。出力は時間、ユーザ設定、動作によって異なります。今後の復旧やトラブルシューティング用に設定をファイルに保存することができます。

display コマンドから出力を保存する方法を、以下の手順の 1 つを使用します。

- ファイルを分離して出力を保存します。1 つの **display** コマンド用に 1 つのファイルを使用する場合に使用します。
- ファイルの最後に出力を追記して保存します。複数の **display** コマンド用に 1 つのファイルを使用する場合に使用します。

display コマンドからファイルからに保存するため、以下のコマンドのどちらか 1 つを使用します。

操作	コマンド
コマンドからファイルを分離して出力を保存する	**display** *command* **>** *filename*

操作	コマンド
ファイルの最後に出力を追記する	**display** *command* **>>** *filename*

例：

VLAN 1 の設定をファイル名 vlan.txt のファイルに分離して保存します。

```
<Switch> display vlan 1 > vlan.txt
```

VLAN 1 の設定がファイル名 vlan.txt のファイルに保存されているかどうか確認します。

```
<Switch> more vlan.txt
VLAN ID: 1
 VLAN type: Static
 Route interface: Not configured
 Description: VLAN 0001
 Name: VLAN 0001
 Tagged ports:   None
 Untagged ports: None
```

ファイル名 vlan.txt の最後に VLAN 999 の設定を追記します。

```
<Switch> display vlan 999 >> vlan.txt
```

VLAN 999 の設定がファイル名 vlan.txt のファイルに追記保存されているかどうか確認します。

```
<Switch> more vlan.txt
VLAN ID: 1
 VLAN type: Static
 Route interface: Not configured
 Description: VLAN 0001
 Name: VLAN 0001
 Tagged ports:   None
 Untagged ports: None
VLAN ID: 999
 VLAN type: Static
 Route interface: Configured
 IP address: 192.168.2.1
 Subnet mask: 255.255.255.0
 Description: For LAN Access
 Name: VLAN 0999
 Tagged ports:   None
 Untagged ports: None
```

1.7.5 display コマンドからの出力の有効的な表示、管理

display コマンドからファイルへの出力とフィルタリングを組み合わせることができます。

- **display** コマンドから各出力ラインを番号付けします。
- **display** コマンドからの出力をフィルタします。
- **display** コマンドからの出力をファイルへ保存します。

以下に **display** コマンドからの出力の有効的な表示、管理を組み合わせる方法を示します。これはすべての view で実行可能です。

操作	コマンド
displayコマンドからの出力の有効的な表示、管理を組み合わせる	**display** *command* [**|** [**by-linenum**] { **begin** | **exclude** | **include** } *regular-expression*] [**>** *filename* | **>>** *filename*]

例：

各ラインに番号付けして、分離したファイル test.txt に、稼働中の設定を保存します。

```
<Switch> display current-configuration | by-linenum > test.txt
```

ファイル test.txt に、稼働中の設定の中で snmp を含む行を追記します。

```
<Switch> display current-configuration | include snmp >> test.txt
```

user-group で始まる最初の行から行番号をつけて稼働中の設定を表示します。

```
<Switch> display current-configuration | by-linenum begin user-group
  114:  user-group system
  115-  #
  116-  return
```

//（：）は user-group が含まれる行を示します。（ー）は user-group が含まれない行を示します。

1.8 稼働中の設定の保存

すべての view で、**save** コマンドを使用して、実行されたコマンドを設定ファイルに保存することができます。設定ファイルに保存されたコマンドは、再起動して復活させることができます。**save** コマンドは、指定された情報を表示する **display** コマンドや指定された情報をクリアする **reset** コマンドのような 1 回限りのコマンドには適用されません。1 回限りのコマンドは保存されません。

詳細はコマンドマニュアルのセクション 1 *はじめに ”コンフィグレーションファイル管理”* を参照してください。

目次

このセクションのページは **1-x-x** です。

2 章 RBAC 2-1
2.1 概要 2-1
2.1.1 許可の割り当て 2-1
2.1.2 ユーザロールの割り当て 2-3
2.2 設定作業リスト 2-4
2.3 ユーザロールの作成 2-4
2.4 ユーザロールのルールの設定 2-5
2.4.1 設定の制限とガイドライン 2-5
2.4.2 設定手順 2-5
2.5 機能グループの設定 2-6
2.6 リソースアクセスポリシーの変更 2-6
2.6.1 ユーザロールのインタフェースポリシーの設定 2-7
2.6.2 ユーザロールの VLAN ポリシーの設定 2-7
2.7 ユーザロールの割り当て 2-7
2.7.1 デフォルトユーザロール機能の有効化 2-8
2.7.2 リモート AAA 認証ユーザへのユーザロールの割り当て 2-8
2.7.3 ローカル AAA 認証ユーザへのユーザロールの割り当て 2-8
2.7.4 ユーザラインで非 AAA 認証ユーザへのユーザロールの割り当て 2-9
2.8 一時的なユーザロールの許可設定 2-10
2.8.1 設定ガイドライン 2-10
2.8.2 ユーザロールの認証の設定 2-11
2.8.3 一時的なユーザロールの許可の取得 2-12
2.9 RBAC 設定の表示と維持 2-12
2.10 RBAC の設定例 2-12
2.10.1 ローカル AAA 認証ユーザの RBAC の設定例 2-12
2.10.2 RADIUS 認証ユーザの RBAC の設定例 2-15
2.10.3 RBAC の一時的なユーザロールの許可の設定例 2-18
2.11 RBAC のトラブルシューティング 2-21
2.11.1 ローカルユーザで許可していないコマンドにアクセスできる 2-21
2.11.2 RADIUS ユーザによるログインがいつも失敗する 2-22

2章 RBAC

2.1 概要

RBAC（Role based access control）は、ユーザロールの設定に従って、ユーザのアクセスとシステムリソースを制御します。RBAC では、ユーザのアクセス制限のために、ユーザロール（role）を使用します。システムリソースにはインタフェース、VLAN を含みます。

複数のユーザにアクセス許可を与える場合、同一のユーザロールを異なるユーザに適用してコマンドやリソースへのアクセス許可を与えることも可能です。ユーザと異なりユーザロールは持続するため、ユーザの許可を分割することで、許可管理が容易になります。また、ユーザの責任分担の変更、追加、削除を行う場合、運用中のユーザロール設定の変更や、新規ユーザロールの作成、割り当てをするだけで管理可能です。

2.1.1 許可の割り当て

以下の方法により、ユーザロールに許可を割り当てることができます。

- アクセス可能か不可能か決定するためのルールを定義します。（ユーザロールのルールを参照してください。）
- リソースがユーザロールにアクセス可能かどうかを決定するためのリソースアクセスポリシーを定義します。（リモートアクセスポリシーを参照してください）

インタフェースあるいは VLAN などのシステムリソースに関連したコマンドを使用する場合、ユーザロールで、必要なコマンドとリソースの両方にアクセスできるように設定する必要があります。

たとえば、ユーザロールは、**vlan** コマンドにアクセスし、VLAN 10 のみアクセスできます。ユーザロールが割り当てられたとき、VLAN 10 を作成するため vlan コマンドを使用し、VLAN 10 の view に移行することができます。しかしほかの VLAN を作成することはできません。ユーザロールが VLAN 10 にアクセスできるが **vlan** コマンドにアクセスできない場合、VLAN 10 の view に移行するためにコマンドを使用することができません。

ユーザがすべてのユーザロールでログインし、view で**<?>**を入力した場合、view でヘルプ情報がシステム定義のコマンドのエイリアスで表示されます。しかし、ユーザはコマンドエイリアスにアクセスにアクセスする許可がありません。ユーザがコマンドエイリアスにアクセスできるかどうかは、コマンドエイリアスに対応するコマンドに対するユーザの許可の状態に依存します。コマンドエイリアスに関する情報は、オペレーションマニュアルのセクション 1 *はじめに*“*CLI*”を参照してください。

すべてのユーザロールで装置にログインするユーザがアクセスできるコマンドは **system-view** コマンド、 **quit** コマンド、**exit** コマンドです。

I. ユーザロールのルール

ユーザロールのルールは、コマンドを許可あるいは禁止します。以下に示すように、異なるアクセス制御のルールを詳細に定義することができます。

- **Command rule**– 正規表現に一致するコマンドあるいはコマンドセットのアクセスを管理します。
- **Feature rule**– コマンドタイプにより、コマンドへのアクセスを管理します。
- **Feature group rule**– コマンドタイプにより、コマンドのグループへのアクセスを管理します。

コマンドは以下のタイプによって制御します。

- **Read**– 設定の表示と保守コマンドです。たとえば、**display** コマンド、**dir** コマンドがあります。
- **Write**– システムの機能を設定するコマンドです。たとえば **info-center enable** コマンド、**debugging** コマンドがあります。
- **Execute**– 指定した機能を実行するコマンドです。たとえば **ping** コマンド、**ftp** コマンドがあります。

ユーザロールは、ユーザロールのルールで許可された指定コマンドセットにアクセスできます。ユーザロールは定義済みのユーザロール（*sys-n* で識別されます）とユーザ定義のユーザロールがあります。ユーザロールのルールの優先順位はユーザロールのルールを参照してください。

II. リソースアクセスポリシー

リソースアクセスポリシーは、以下のタイプのように、システムリソースへのユーザロールのアクセスを管理します。

- **Interface policy**– インタフェースへのアクセスを管理します。
- **VLAN policy**– VLAN へのアクセスを管理します。

リソースアクセスポリシーでは **display** コマンドでのインタフェース、VLAN の情報表示についてのアクセス管理は行いません。ユーザロールルールに **display** コマンドのオプションを指定することで、アクセス制御をすることができます。

III. 定義済みユーザロール

システムには定義済みのユーザロールがあります。すべてのユーザロールはすべてのシステムリソース（インタフェース、VLAN）にアクセスできますが、これらのコマンドはアクセス許可とは異なります。表 2-1を参照してください。

すべての定義済みのユーザロールで、**network-admin** と **Level-15** は以下のことを行うことができます。

- RBAC 機能にアクセスすることができます。
- user line view の user-role、authentication-mode、protocol inbound、set authentication password 等の設定変更ができます。
- ローカルユーザとローカルユーザグループの作成、変更、削除を行うことができます。ローカルユーザとローカルユーザグループを設定する権限を持つほかのユーザロールは、自身のパスワードを変更することのみ行うことができます。
- Level-0～Level-14 のユーザは、**display history-command all** コマンドを除いて自身の許可を変更することができます。

表 2-1 定義済みユーザロールと許可

ユーザロール名	許可
network-admin	システムのすべての機能とリソースにアクセス可能です。**display security-logfile summary**コマンド、**info-center security-logfile directory**コマンド、 **security-logfile save**コマンドを除きます。
network-operator	• すべての機能の**display**コマンドとリソースにアクセス可能です。ユーザロールでアクセス可能なコマンドを表示する場合、**display role**コマンドを使用します。 • 自身のパスワードを変更するため、ローカルユーザへのローカル認証が有効です。

level-*n* (*n* = 0 〜 15)	• **level-0**– **ping**、**tracert**、**telnet** 、**ssh2**、**super**コマンドを含む診断コマンドにアクセスできます。**level-0**のアクセス権は設定可能です。
	• **level-1**– **level-0**のコマンドに加えて**display history-command all**コマンドを除く**display**コマンドとリソースが使用可能です。**level-0**のアクセス権は設定可能です。
	• **level-2**〜**level-8**、**level-10** 〜**level-14**– デフォルトでアクセス権はありません。アクセス権は設定可能です。
	• **level-9**– 以下の機能を除いたすべての機能とリソースにアクセス可能です。もしユーザロールが**level-9**のローカルユーザアカウントのユーザにログインした場合、自身のアカウントのパスワードを変更することができます。**level-9**のアクセス権は設定可能です。
	  • RBAC-非デバッグコマンド
	  • ローカルユーザ
	  • ファイル管理
	  • 装置管理
	  • **display history-command all**コマンド
	• **level-15**– network-adminと同じアクセス権があります。

2.1.2 ユーザロールの割り当て

ユーザに、少なくとも 1 つのユーザロールを割り当てることによって、アクセス権を割り当てます。ユーザは割り当てられたユーザロールで許可設定されたコマンドとリソースを使用することができます。たとえば、以下に示すユーザロールを設定することで、すべてのインタフェースで **qos apply policy** コマンドを使用することができます。

- ユーザロール A は **qos apply policy** コマンドの禁止と GigabitEthernet 1/0/1 インタフェースのみアクセス許可を行います。
- ユーザロール B は **qos apply policy** コマンドの許可とすべてのインタフェースのアクセス許可を設定します。

ユーザロールの割り当ては認証方法に依存して以下の方法があります。

- **AAA 許可**– scheme 認証が使用されている場合、AAA モジュールはユーザロールの割り当てを操作できます。
  - □ ユーザがローカル認証にパスした場合、装置はローカルユーザアカウントで指定されたユーザロールを割り当てます。

- ユーザがリモート認証にパスした場合、ユーザにサーバで指定したユーザロールを割り当てます。AAA サーバは RADIUS サーバを使用できます。

- **Non-AAA 許可**– ユーザが認証を使用していない、あるいはパスワード認証の場合、装置はユーザラインで指定されたユーザロールを割り当てます。この方法は公開鍵あるいはパスワードー公開鍵認証を使用する SSH クライアントにも適用されます。SSH クライアントに割り当てられたユーザロールは、ローカル管理に関係するユーザアカウントに指定されます。

AAA、SSH の詳細は、オペレーションマニュアルのセクション 9 *セキュリティ*”*AAA*”、”*SSH*”を参照してください。ユーザラインの詳細は、オペレーションマニュアルのセクション 1 *はじめに*”*ログイン*”、”*CLI によるログイン*”を参照してください。

2.2 設定作業リスト

作業リスト
（必須設定項目）ユーザロールの作成
（必須設定項目）ユーザロールのルールの設定
（オプション設定項目）機能グループの設定
（オプション設定項目）リソースアクセスポリシーの設定 ● ユーザロールインタフェースポリシーの設定 ● ユーザロールVLANポリシーの設定
（オプション設定項目）ユーザロールの割り当て
（オプション設定項目）一時的なユーザロールの許可設定

2.3 ユーザロールの作成

詳細なアクセス管理を行うために、あらかじめ定義されたユーザロールに加えて、64 個までカスタムユーザロールを作成することができます。

以下にユーザロールを作成する手順を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. ユーザロールを作成し、user role view に移行する	**role name** *role-name*	デフォルト：定義済みのユーザロール ● network-admin ● network-operator ● level-n（nは0～15です） level-0～14のユーザロールの許可と説明のみ設定することができます。
3. （オプション設定項目）ユーザロールの説明を設定する	**description** *text*	デフォルト：設定なし

2.4 ユーザロールのルールの設定

指定されたコマンドにユーザロールのアクセスを許可あるいは禁止するため、コマンド、機能、機能グループを設定します。

2.4.1 設定の制限とガイドライン

RBAC ユーザロールのルールを設定するとき、以下の制限とガイドラインに従ってください。

- ユーザロールは以下のコマンドを実行できます。
  - **display history-command all** コマンド
  - **display role、 reboot、startup saved-configuration** キーワードで始まるすべてのコマンド
  - system view で SNMP コミュニティ、ユーザ、グループを作成するコマンド（**snmp-agent community、snmp-agent usm-user、snmp-agent group** コマンド）
  - user line view、user line class view で **user-role、undo user-role、authentication-mode、undo authentication-mode、set authentication password、undo set authentication password** キーワードで始まるすべてのコマンド
  - schedule view あるいは CLI で定義した policy view で **user-role、undo user-role** キーワードで始まるすべてのコマンド
  - イベント MIB 機能のすべてのコマンド
- 1 つのユーザロールには 256 個までのルールを設定することができます。ただし、システム全体で 1024 個を超えるルールを作成することはできません。
- ユーザロールの変更、追加、削除は、変更完了後にユーザロールでログインしたユーザのみ適用されます。
- 同じタイプの 2 つのユーザ定義のルールが混在した場合、高い ID のルールが適用されます。たとえば、以下のコマンドが設定されたルールがある場合、ユーザロールは、**tracert** コマンドを使用しますが、**ping** コマンドを使用しません。
  - **rule 1 permit command ping**
  - **rule 2 permit command tracert**
  - **rule 3 deny command ping**
- level-0～14 のユーザロールにおいて、定義済みのユーザロールとユーザ定義のユーザが混在する場合、ユーザ定義のユーザロールが適用されます。

2.4.2 設定手順

以下にユーザロールのルールの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. user role view に移行する	**role name** *role-name*	―

操作	コマンド	補足
3． ルールを設定する	• コマンドルールの設定： **rule** *number* { **deny** | **permit** } **command** *command-string* • 機能ルールの設定： **rule** *number* { **deny** | **permit** } { **execute** | **read** | **write** }* **feature** [*feature-name*] • 機能グループの設定： **rule** *number* { **deny** | **permit** } { **execute** | **read** | **write** }* **feature-group** *feature-group-name*	デフォルト：なし ユーザロールを複数のルールを作成する場合、繰り返し設定します。最大256まで設定することができます。 ⚠ **重要：** 機能ルールを設定したとき、システムで有効な機能のみ指定することができます。省略した機能名ではなく、大文字小文字を区別して、表示された機能と同じ機能名を正確に設定してください。

2.5 機能グループの設定

機能グループは、機能のセットにコマンドのアクセス権をまとめて割り当てます。あらかじめ定義された機能グループに加えて、64 個の機能グループを作成することができ、複数の機能グループに機能を割り当てることができます。

以下に機能グループの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． 機能グループを作成し、feature group view に移行する	**role feature-group name** *feature-group-name*	デフォルト： • **L2**― すべてのレイヤ2コマンドを含みます。 • **L3**― すべてのレイヤ3コマンドを含みます。 この2つのグループはユーザで設定できません。
3． 機能グループに機能を追加する	**feature** *feature-name*	デフォルト：設定なし 複数の機能を作成する場合、繰り返し設定します。 ⚠ **重要：** システムで有効な機能のみ指定することができます。省略した機能名ではなく、大文字小文字を区別して、表示された機能と同じ機能名を正確に設定してください。

2.6 リソースアクセスポリシーの変更

各ユーザロールは 1 つのインタフェースポリシー、VLAN ポリシーを持ちます。デフォルトでポリシーはすべてのインタフェース、VLAN にアクセスするユーザロールを許可します。ユーザが定義したユーザロールのポリシー、インタフェース、VLAN へのアクセス制

限を行うあらかじめ定義された Level-*n* のユーザロールを変更することができます。変更されたポリシーは、変更後にユーザロールでログインしたユーザのみ適用されます。

2.6.1 ユーザロールのインタフェースポリシーの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. user role view に移行する	**role name** *role-name*	―
3. ユーザロールの interface policy view へ移行する	**interface policy deny**	デフォルト : すべてのインタフェースへのユーザロールのアクセスは有効です。**permit interface**コマンドが設定されていない場合、すべてのインタフェースへのアクセスを禁止します。
4. （オプション設定項目）ユーザロールにアクセス可能なインタフェースのリストを指定する	**permit interface** *interface-list*	デフォルト：設定なし アクセス可能なインタフェースを追加する場合、この操作を繰り返し行ってください。

2.6.2 ユーザロールの VLAN ポリシーの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. user role view に移行する	**role name** *role-name*	―
3. ユーザロールの VLAN policy view へ移行する	**vlan policy deny**	デフォルト：すべてのVLANへのユーザロールのアクセスは有効です。**permit vlan**コマンドが設定されていない場合、すべてのVLANへのアクセスを禁止します。
4. （オプション設定項目）ユーザロールにアクセス可能な VLAN を指定する	**permit vlan** *vlan-id-list*	デフォルト：設定なし アクセス可能なVLANを追加する場合、この操作を繰り返し行ってください。

2.7 ユーザロールの割り当て

システムにユーザロールを管理するため、少なくとも 1 つのユーザロールを割り当てる必要があります。装置または、サーバによって少なくとも 1 つのユーザロールが割り当てられていることを確認してください。ユーザロールはリモート AAA 認証ユーザ、ローカル AAA 認証ユーザ、AAA 認証を行わないユーザで割り当てる手順が異なります。AAA 認証の詳細は、オペレーションマニュアルのセクション 9 *セキュリティ”AAA”* を参照してください。

2.7.1 デフォルトユーザロール機能の有効化

認証サーバ（ローカルあるいはリモート）がユーザロールをユーザに許可していない場合、AAA で認証されているユーザにデフォルトユーザロールを割り当てます。

ユーザロールが割り当てられていないユーザはデフォルトユーザロールでシステムにアクセスできます。

以下に AAA 認証ユーザにデフォルトユーザロール機能を有効にする設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. デフォルトユーザロール機能の有効にする	**role default-role enable** [*role-name*]	デフォルト：無効 ローカルユーザ用に許可されていない場合、デフォルトユーザロール機能を有効にする必要があります。

2.7.2 リモート AAA 認証ユーザへのユーザロールの割り当て

リモート AAA 認証ユーザリモート認証サーバでユーザロールを設定します。RADIUS ユーザにユーザロールを設定する方法については、RADIUS サーバのマニュアルを参照してください。

🕮 **メモ：**

- 特権レベルによるアクセス管理に互換性を持たせるために、装置は自動的に、AAA サーバによって割り当てられた特権レベルにもとづくユーザレベル（0～15）を、RBAC ユーザロール（Level-0～Level-15）に変換します。
- AAA サーバが割り当てたユーザレベルによりユーザロールをユーザに割り当てる場合、ユーザレベルとユーザロールの両方にアクセス可能なコマンドとリソースの組み合わせを使用することができます。

2.7.3 ローカル AAA 認証ユーザへのユーザロールの割り当て

ローカルユーザアカウントのローカル AAA 認証ユーザにユーザロールを設定します。各ローカルユーザはデフォルトユーザロールを持っています。もしデフォルトユーザロールが適当でない場合、削除する必要があります。

以下にローカルユーザにユーザロールを割り当てる設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. ローカルユーザを作成し、local user view に移行する	**local-user** *user-name* [**class** { **manage** | **network** }]	―

操作	コマンド	補足
3. ユーザロールがあるユーザを許可する	**authorization-attribute user-role** *role-name*	デフォルト：ユーザロール network-adminあるいはlevel-15のユーザが作成したローカルユーザのユーザロールは network-operatorが割り当てられます。 ユーザに最大64のユーザロールを割り当てる場合、この操作を繰り返し行ってください。

2.7.4 ユーザラインで非 AAA 認証ユーザへのユーザロールの割り当て

ユーザラインで以下の 2 タイプのログインユーザにユーザロールを指定します。

- パスワード認証あるいは認証をしていないユーザにユーザロールを指定します。
- 公開鍵あるいはパスワード公開鍵認証を使用する SSH クライアントユーザロールを指定します。SSH クライアントに割り当てられるユーザロールは関連するローカル装置管理ユーザアカウントで指定されます。

ユーザラインの詳細は、オペレーションマニュアルのセクション 1 *はじめに*”*ログイン*”、”*CLI によるログイン*”を参照してください。SSH の詳細は、オペレーションマニュアルのセクション 9 *セキュリティ*”*SSH*”を参照してください。

以下にユーザラインで非 AAA ユーザにユーザロールを割り当てる設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. user line view あるいは user line class view に移行する.	● user line viewに移行する：**line** { *first-num1* [*last-num1*]	{ **aux**	**vty** } *first-num2* [*last-num2*] } ● user line class viewに移行する：**line class** { **aux**	**vty** }	user line viewとuser line class viewの優先順位と設定方法については、オペレーションマニュアルのセクション1 *はじめに*”*CLIによるログイン*”を参照してください。
3. ユーザラインでユーザロールを指定する	**user-role** *role-name*	デフォルト：AUXユーザラインでnetwork-adminが指定されます。ほかのユーザラインでnetwork-operatorが指定されます。 ユーザに最大64のユーザロールを割り当てることができます。複数のユーザロールを割り当てる場合、この操作を繰り返し行ってください。

2.8 一時的なユーザロールの許可設定

一時的なユーザロールを許可することで、ログインしていないユーザが装置に再接続することなく、ユーザロールを取得することができます。この機能は設定を行うために一時的にユーザロールを使用する場合に有効です。

一時的なユーザロールの許可の設定は現在のログインにのみ適用されます。この機能は、すでにログインしているユーザアカウントのユーザロールの設定を変更しません。次回、ユーザアカウントでログインする場合、元のユーザロールの設定が適用されます。

2.8.1 設定ガイドライン

一時的なユーザロールの許可を設定する場合、以下のガイドラインに従ってください。

- ユーザが装置に再接続をしないで別のユーザロールを取得するため、ユーザロール認証を設定する必要があります。表 2-2に有効な認証モードと設定要件を記載します。
- RADIUS 認証が使用されている場合、以下のルールを適用します。
  - □ 装置はユーザロールの認証を要求するためのユーザ名を使用しません。装置は **$enab*n*$**のフォーマットを使用します。*n* はユーザロールレベルです。ドメイン名はユーザ名に含まれません。パスワードが正しいとき、ユーザロールの認証にパスすることができます。
  - □ level-*n* のユーザロールを取得するため、RADIUS サーバで**$enab*n*$**のフォーマットで level-*n* のユーザのユーザアカウントを作成する必要があります。*n* はターゲットのユーザロールのレベルです。たとえば、level-3 のユーザロールの許可を取得する場合、ユーザ名を入力します。装置はサーバからユーザロール認証を要求するため、ユーザ名**$enab3$**を使用します。
  - □ 非 level-n のユーザロールを取得するため、以下の処理を行う必要があります。
    - □ サーバでユーザアカウント**$enab0$**を作成します。
    - □ **allowed-roles="***role***"**の形式のアカウントの cisco-av-pair 属性を設定します。変数のロールはターゲットのユーザロールを示します。
- 装置は以下の順番でユーザロール認証の認証ドメインを選択します。

a) 入力されたユーザ名が含まれるISPドメイン

b) デフォルトISPドメイン

- ユーザロールを許可した後、**quit** コマンドを実行した場合、現在のユーザラインをログアウトします。

表 2-2 ユーザロールの認証モード

キーワード	認証モード	記述
local	ローカルパスワード認証のみ（local-only）	装置は認証用にローカルに設定されたパスワードを使用します。 ローカルパスワード認証が設定されない場合、AUX ユーザは文字列を入力するか、何も入力しないで Enterキーを押すことでユーザロール許可を取得することができます。

キーワード	認証モード	記述
scheme	RADIUSによるリモートAAA認証（remote-only）	装置はリモート認証を行うためRADIUSサーバにユーザ名とパスワードを送信します。 このモードを使用するため、以下の設定を実行する必要があります。 ● 要求されたRADIUS scheme、ユーザのschemeを使用するISP domainを設定します。詳細はオペレーションマニュアルのセクション9 *セキュリティ”AAA”*を参照してください。 ● RADIUSサーバにユーザアカウントとパスワードを追加します。
local scheme	最初にローカルパスワード認証を行い、次にリモートAAA認証を行う（local-then-remote）	最初にローカルパスワード認証が実行されます。もしローカルパスワードが設定されていない場合、以下となります。 ● 装置はVTYユーザ用にリモートAAA認証を実行します。 ● AUXユーザは文字列を入力するか、何も入力しないでEnterキーを押すことで一時的なユーザロールを取得することができます。
scheme local	最初にリモートAAA認証を行い、次にローカルパスワード認証を行う（remote-then-local）	最初にAAA認証が実行されます。ローカルパスワード認証は以下のいずれかの状況で実行されます。 ● リモートRADIUSサーバからの応答がありません。 ● 装置でのAAAの設定が無効です。

2.8.2 ユーザロールの認証の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. 認証モードを設定する	**super authentication-mode** { **local** | **scheme** }*	デフォルト: ローカル認証のみ適用します。
3. （オプション設定項目）一時的なユーザロール許可のデフォルトターゲットのユーザロールを指定する	**super default role** *role-name*	デフォルト：**network-admin**
4. ユーザロールのローカル認証パスワードを設定する	**super password** [**role** *role-name*] [{ **hash** | **simple** } *string*]	デフォルト：設定なし ローカルパスワード認証のために、この操作を使用します。 もし**role** *role-name*を指定しない場合、コマンドはデフォルトターゲットのユーザロールのパスワードを設定します。

2.8.3 一時的なユーザロールの許可の取得

ログインを行うユーザアカウントにユーザロールがない AUX や VTY ユーザは、ユーザロールを使用する前に認証をパスする必要があります。

user view で以下の設定を行います。

操作	コマンド	補足
ユーザロールを使用した一時的な許可を取得する	**super** [*role-name*]	[*role-name*]を指定しない場合一時的なユーザロールの許可のデフォルトターゲットユーザロールを取得します。3回連続してパスワードの認証に失敗すると、ユーザロールの取得に失敗します。現在のユーザロールが**super**コマンドを実行できることを確認してください。

2.9 RBAC設定の表示と維持

すべての view で **display** コマンドを実行することができます。

操作	コマンド
ユーザロール情報を表示する	**display role** [**name** *role-name*]
ユーザロール機能の情報を表示する	**display role feature** [**name** *feature-name* | **verbose**]
ユーザロール機能グループ情報を表示する	**display role feature-group** [**name** *feature-group-name*] [**verbose**]

2.10 RBACの設定例

2.10.1 ローカル AAA 認証ユーザの RBAC の設定例

I. ネットワーク要件

図 2-1に示すように、装置は Telnet ユーザ用にローカル AAA 認証を実行します。Telnet ユーザはユーザ名 **user1@bbb** を持ち、ユーザロール **role1** を割り当てます。

role1 に以下の許可を設定します。

- すべての機能の **read** コマンドを実行します。
- VLAN10～VLAN20 を除いた VLAN を設定します。

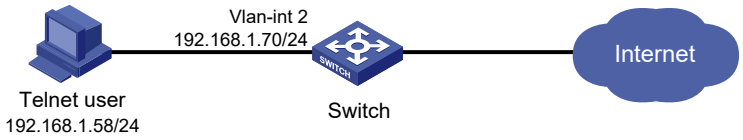


図 2-1 ネットワーク図

II. 設定手順

Telnet ユーザに接続する VLAN インタフェース 2 に IP アドレスを割り当てます。

```
<Switch> system-view
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ip address 192.168.1.70 255.255.255.0
[Switch-Vlan-interface2] quit
```

Telnet サーバを有効にします。

```
[Switch] telnet server enable
```

Telnet ユーザのユーザラインで scheme 認証を有効にします。

```
[Switch] line vty 0 63
[Switch-line-vty0-63] authentication-mode scheme
[Switch-line-vty0-63] quit
```

ISP ドメイン **bbb** 用にローカル認証、許可を有効にします。

```
[Switch] domain bbb
[Switch-isp-bbb] authentication login local
[Switch-isp-bbb] authorization login local
[Switch-isp-bbb] quit
```

ユーザロール **role1** を作成します。

```
[Switch] role name role1
```

すべての機能の read コマンドにアクセスするようにユーザロールを許可するルール 1 を設定します。

```
[Switch-role-role1] rule 1 permit read feature
```

#VLAN を作成し、VLAN view でコマンドにアクセスするユーザロールを許可するルール 2 を設定します。

```
[Switch-role-role1] rule 2 permit command system-view ; vlan *
```

#VLAN 10～VLAN 20 のみ設定するユーザロールを許可するために VLAN ポリシーを変更します。

```
[Switch-role-role1] vlan policy deny
```

```
[Switch-role-role1-vlanpolicy] permit vlan 10 to 20
[Switch-role-role1-vlanpolicy] quit
[Switch-role-role1] quit
```

装置管理ローカルユーザ **user1** を作成し、local user view に移行します。

```
[Switch] local-user user1 class manage
```

ユーザ用にプレーンテキストのパスワード **aabbcc** を設定します。

```
[Switch-luser-manage-user1] password simple aabbcc
```

サービスタイプを Telnet に設定します。

```
[Switch-luser-manage-user1] service-type telnet
```

ユーザにユーザロール **role1** を割り当てます。

```
[Switch-luser-manage-user1] authorization-attribute user-role role1
```

ユーザはユーザロール **role1** の許可のみとするため、ユーザからデフォルトユーザロール network-operator を削除します。

```
[Switch-luser-manage-user1] undo authorization-attribute user-role network-operator
[Switch-luser-manage-user1] quit
```

III. 設定の確認

装置に Telnet を行い、Switch にアクセスするため、ユーザ名とパスワードを入力します。（詳細は省略します）

VLAN 10～VLAN 20 を作成できることを確認します。この例では VLAN10 を使用します。

```
<Switch> system-view
[Switch] vlan 10
[Switch-vlan10] quit
```

VLAN 10～VLAN 20 以外の VLAN を作成できないことを確認します。この例では VLAN30 を使用します。

```
[Switch] vlan 30
Permission denied.
```

すべての機能の read コマンドが使用できることを確認します。この例では **display clock** コマンドを使用します。

```
[Switch] display clock
09:31:56 UTC Sat 01/01/2011
[Switch] quit
```

機能の書き込みあるいは実行コマンドが使用できないことを確認します。

```
<Switch> debugging role all
Permission denied.
```

```
<Switch> ping 192.168.1.58
Permission denied.
```

2.10.2 RADIUS 認証ユーザの RBAC の設定例

I. ネットワーク要件

図 2-2に示すように、装置は Free RADIUS サーバを使用し、Telnet ユーザを含むログインユーザに AAA サービスを提供します。Telnet ユーザはユーザ名 **hello@bbb** を持ち、ユーザロール **role2** が割り当てられます。

ユーザロール **role2** に以下の許可を設定します。

- ISP view ですべてのコマンドを実行します。
- **arp**、**radius** 機能の read、write コマンドを実行します。
- **acl** 機能の read コマンドへのアクセスを禁止します。
- VLAN 1～VLAN 20、インタフェース GigabitEthernet 1/0/1～GigabitEthernet 1/0/4 を設定します。

装置と FreeRADIUS サーバは共有鍵 **expert**、認証ポート 1812 を使用します。装置はサーバにドメイン名のユーザ名を送信します。

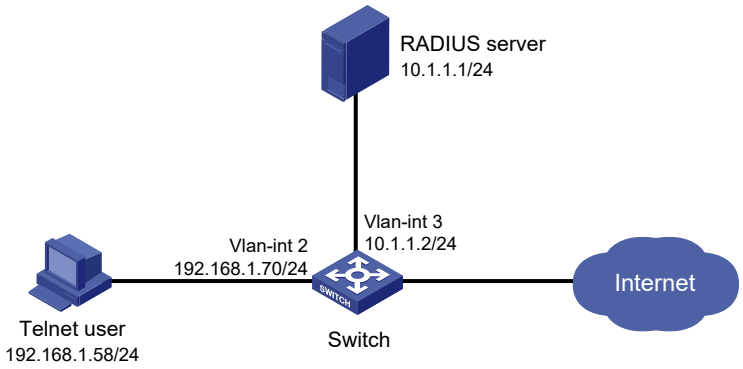


図 2-2 ネットワーク図

II. 設定手順

Switch と RADIUS サーバで設定が一致していることを確認します。

1)　Switch を設定します。

Telnet ユーザと同じサブネットから IP アドレスを VLAN インタフェース 2 に割り当てます。

```
<Switch> system-view
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ip address 192.168.1.70 255.255.255.0
[Switch-Vlan-interface2] quit
```

RADIUS サーバと同じサブネットから IP アドレスを VLAN インタフェース 3 に割り当てます。

```
[Switch] interface vlan-interface 3
[Switch-Vlan-interface3] ip address 10.1.1.2 255.255.255.0
[Switch-Vlan-interface3] quit
```

Telnet サーバを有効にします。

```
[Switch] telnet server enable
```

Telnet ユーザ用に、ユーザラインの scheme 認証を有効にします。

```
[Switch] line vty 0 63
[Switch-line-vty0-63] authentication-mode scheme
[Switch-line-vty0-63] quit
```

RADIUS scheme **rad** を作成し、RADIUS scheme view に移行します。

```
[Switch] radius scheme rad
```

scheme で、プライマリサーバアドレス 10.1.1.1、サービスポート 1812 を指定します。

```
[Switch-radius-rad] primary authentication 10.1.1.1 1812
```

サーバに認証するサーバ用に scheme で専用の共有鍵を設定します。

```
[Switch-radius-rad] key authentication simple expert
[Switch-radius-rad] quit
```

ISP ドメイン **bbb** 用の認証、許可 scheme として scheme **rad** を指定します。

⚠ **重要：**

RADIUS ユーザ認証の情報は許可（authorization）属性を認証（authentication）の応答に入れて送信します。そのため、authorization の radius-scheme と authentication の radius-scheme には同じ scheme を使用してください。

```
[Switch] domain bbb
[Switch-isp-bbb] authentication login radius-scheme rad
[Switch-isp-bbb] authorization login radius-scheme rad
[Switch-isp-bbb] quit
```

機能グループ **fgroup1** を作成します。

```
[Switch] role feature-group name fgroup1
```

機能グループに機能 **arp**、**radius** を追加します。

```
[Switch-featuregrp-fgroup1] feature arp
```

```
[Switch-featuregrp-fgroup1] feature radius
[Switch-featuregrp-fgroup1] quit
```

ユーザロール **role2** を作成します。

```
[Switch] role name role2
```

ISP view ですべてのコマンドを使用するユーザロールを許可するルール 1 を設定します。

```
[Switch-role-role2] rule 1 permit command system-view ; domain *
```

fgroup1 ですべての機能の read、write コマンドを使用するユーザロールを許可するルール 2 を設定します。

```
[Switch-role-role2] rule 2 permit read write feature-group fgroup1
```

acl 機能の read コマンドのアクセスを禁止するルール 3 を設定します。

```
[Switch-role-role2] rule 3 deny read feature acl
```

VLAN を作成し、VLAN view ですべてのコマンドを使用するユーザロールを許可するルール 4 を設定します。

```
[Switch-role-role2] rule 4 permit command system-view ; vlan *
```

interface view に移行し、interface view ですべてのコマンドを使用するユーザロールを許可するルール 5 を設定します。

```
[Switch-role-role2] rule 5 permit command system-view ; interface *
```

VLAN 1～VLAN 20 を除く VLAN の設定を無効にするユーザロール VLAN ポリシーを設定します。

```
[Switch-role-role2] vlan policy deny
[Switch-role-role2-vlanpolicy] permit vlan 1 to 20
[Switch-role-role2-vlanpolicy] quit
```

GigabitEthernet 1/0/1～GigabitEthernet 1/0/4 を除くインタフェースの設定を無効にするユーザロールインタフェースポリシーを設定します。

```
[Switch-role-role2] interface policy deny
[Switch-role-role2-ifpolicy] permit interface gigabitethernet 1/0/1 to gigabitethernet 1/0/4
[Switch-role-role2-ifpolicy] quit
[Switch-role-role2] quit
```

2)　RADIUS サーバを設定します。

Free RADIUS サーバのディレクトリファイルにどちらかのユーザロールの属性を追加します。

```
Cisco-AVPair = "shell:roles=\"role2\""
Cisco-AVPair = "shell:roles*\"role2\""
```

装置と通信する Free RADIUS サーバの必要な設定を行います。（詳細は省略します）

III. 設定の確認

装置に Telnet し、装置にアクセスするため、ユーザ名、パスワードを入力します。（詳細は省略します）

ISP view で有効なすべてのコマンドが使用できることを確認します。

```
<Switch> system-view
[Switch] domain abc
[Switch-isp-abc] authentication login radius-scheme abc
[Switch-isp-abc] quit
```

機能 **radius**、**arp** のすべての read、write コマンドを使用できることを確認します。この例では **radius** を使用します。

```
[Switch] radius scheme rad
[Switch-radius-rad] primary authentication 2.2.2.2
[Switch-radius-rad] display radius scheme rad
...
（display 表示結果は省略します。）
```

VLAN 1～VLAN 20 を除いて VLAN を設定できないことを確認します。この例では VLAN 10 と VLAN 30 を使用します。

```
[Switch] vlan 10
[Switch-vlan10] quit
[Switch] vlan 30
Permission denied.
```

GigabitEthernet 1/0/1～GigabitEthernet 1/0/4 を除いて、インタフェースを設定できないことを確認します。この例では GigabitEthernet 1/0/5 を使用します。

```
[Switch] vlan 10
[Switch-vlan10] port gigabitethernet 1/0/5
Permission denied.
```

2.10.3 RBAC の一時的なユーザロールの許可の設定例

I. ネットワーク要件

図 2-3に示すように、装置はログインユーザ用にローカル認証を実行します。Telnet ユーザはユーザ名 **test@bbb** を持ち、ユーザロール **level-0** が割りあてられます。

一時的なユーザロールの許可を行うため remote-then-local の認証モードを設定します。装置はユーザロール network-admin の認証を許可するため、RADIUS サーバを使用します。AAA の設定が無効あるいは RADIUS サーバが応答していない場合、装置はローカル認証を実行します。

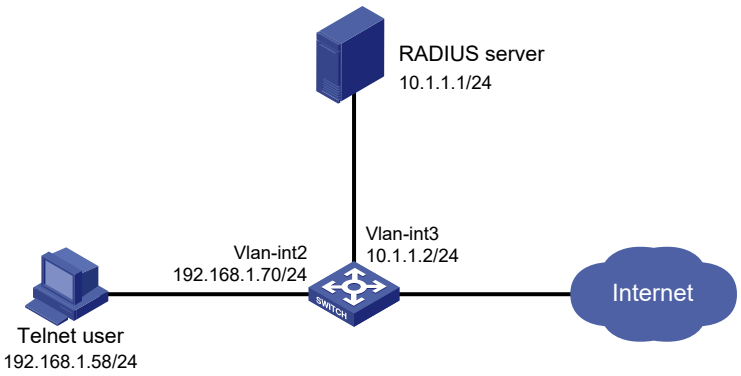


図 2-3 ネットワーク図

II. 設定手順

1)　Switch を設定します。

Telnet ユーザに接続された VLAN インタフェース 2 に IP アドレスを割り当てます。

```
<Switch> system-view
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ip address 192.168.1.70 255.255.255.0
[Switch-Vlan-interface2] quit
```

RADIUS サーバに接続された VLAN インタフェース 3 に IP アドレスを割り当てます。

```
[Switch] interface vlan-interface 3
[Switch-Vlan-interface3] ip address 10.1.1.2 255.255.255.0
[Switch-Vlan-interface3] quit
```

Telnet サーバを有効にします。

```
[Switch] telnet server enable
```

Telnet ユーザ用に、ユーザラインの scheme 認証を有効にします。

```
[Switch] line vty 0 63
[Switch-line-vty0-63] authentication-mode scheme
[Switch-line-vty0-63] quit
```

一時的なユーザロールの許可のため、remote-then-local 認証を有効にします。

```
[Switch] super authentication-mode scheme local
```

RADIUS scheme **radius** を作成し、RADIUS scheme view に移行します。

```
[Switch] radius scheme radius
```

プライマリ認証サーバのアドレスを 10.1.1.1 に指定し、Switch とサーバ間の通信をセキュアにするため、scheme の専用の共有鍵を設定します。

```
[Switch-radius-radius] primary authentication 10.1.1.1 key simple expert
```

RADIUS サーバに送信したユーザ名から ISP ドメイン名を除外します。

```
[Switch-radius-radius] user-name-format without-domain
[Switch-radius-radius] quit
```

ISP ドメイン **bbb** を作成し、ISP domain view に移行します。

```
[Switch] domain bbb
```

ログインユーザでローカル認証を使用する ISP ドメイン **bbb** を設定します。

```
[Switch-isp-bbb] authentication login local
```

ログインユーザでローカル許可を使用する ISP ドメイン **bbb** を設定します。

```
[Switch-isp-bbb] authorization login local
```

ユーザロール認証のため、RADIUS scheme **radius** を ISP ドメインに適用します。

```
[Switch-isp-bbb] authentication super radius-scheme radius
[Switch-isp-bbb] quit
```

装置管理ユーザ **test** を作成し、local user view に移行します。

```
[Switch] local-user test class manage
```

ユーザのサービスタイプを Telnet に設定します。

```
[Switch-luser-manage-test] service-type telnet
```

ユーザのパスワードを **aabbcc** に設定します。

```
[Switch-luser-manage-test] password simple aabbcc
```

level-0 をユーザに割り当てます。

```
[Switch-luser-manage-test] authorization-attribute user-role level-0
```

デフォルトユーザロール network-operator を削除します。

```
[Switch-luser-manage-test] undo authorization-attribute user-role network-operator
[Switch-luser-manage-test] quit
```

ユーザロール network-admin のローカル認証パスワードを abcdef654321 に設定します。

```
[Switch] super password role network-admin simple abcdef654321
[Switch] quit
```

2) RADIUS サーバを設定します。

（詳細は省略します）

III. 設定の確認

1) Switch に Telnet 接続を行い、ユーザ名 test@bbb、パスワード aabbcc を入力します。
診断コマンドにアクセスできることを確認します。

```
<Switch> telnet 192.168.1.70
Trying 192.168.1.70 ...
Press CTRL+K to abort
Connected to 192.168.1.59 ...

login: test@bbb
Password:
<Switch>?
User view commands:
  ping          Ping function
  quit          Exit from current command view
  ssh2          Establish a secure shell client connection
  super         Switch to a user role
  system-view   Enter the System View
  telnet        Establish a telnet connection
  tracert       Tracert function
<Switch>
```

2)　ユーザロール network-admin を取得できることを確認します。

ユーザロール network-admin を取得するため、super password コマンドを使用します。システムはユーザ名とパスワードが表示されたとき、ユーザ名 test@bbb、パスワード 123456 を入力します。

```
<Switch> super network-admin
Username: test@bbb
Password:
```

以下の出力はユーザロール network-admin を取得したことを示します。

```
User privilege role is network-admin, and only those commands that authorized to
the role can be used.
```

#RADIUS サーバが応答しない場合、表示画面でローカル認証のパスワード abcdef654321 を入力します。

```
Invalid configuration or no response from the authentication server.
Change authentication mode to local.
Password:
User privilege role is network-admin, and only those commands that authorized to
the role can be used.
```

出力はユーザロール network-admin を取得したことを示します。

2.11 RBACのトラブルシューティング

この章では、一般的な RBAC 問題と解決方法について記載します。

2.11.1 ローカルユーザで許可していないコマンドにアクセスできる

I. 症状

ローカルユーザで割り当てられたユーザロールで許可していないコマンドが使用できます。

II. 分析

ローカルユーザには意図しないユーザロールが割り当てられている場合があります。たとえば、ローカルユーザを作成すると自動的にデフォルトのユーザロールも割り当てられています。

III. 解決策

1) **display local-user** コマンドを使用し、必要ないユーザロールがあるローカルユーザアカウントを確認し、それを削除します。
2) 問題が解決しない場合、NEC に問い合わせてください。

2.11.2 RADIUS ユーザによるログインがいつも失敗する

I. 症状

以下の状況において RADIUS ユーザによって、ネットワークアクセス装置にログインできません。

- 本装置と RADIUS サーバ間の通信は正常です。
- すべての AAA 設定は正常です。

II. 分析

RBAC は少なくとも 1 つのユーザロールを持つログインユーザが必要です。もし RADIUS サーバがユーザロールを使用するログインユーザを許可していない場合、ユーザは装置にログインすることはできません。

III. 解決策

以下の方法で問題を解決します。

1) 以下のいずれかの方法を使用します。
- ユーザロールが RADIUS サーバに割り当てられていないとき、RADIUS ユーザがデフォルトユーザロールでログインできるようにするため、**role default-role enable** コマンドを設定します。
- ユーザロール許可属性を RADIUS サーバに追加してください。

2) 問題が解決しない場合、NEC に問い合わせてください。

目次

このセクションのページは **1-x-x** です。

3 章 ログイン..... 3-1

3章 ログイン

初回の装置へのログインは、コンソールポートを使用した CLI ログインのみ行うことができます。2回目以降はコンソールログインパラメータの変更やコンソール、Telnet、SSH、Web、SNMP のログイン方法に変更することができます。

⚠ **注意：**
Telnetと SSH の接続ユーザ数はそれぞれ 8ユーザまで、合計 16ユーザまでサポートしています。それ以上のユーザを接続した場合、装置のメモリ消費が大きくなり動作に影響が出る場合がありますので、上記のユーザ数を超えないようにしてください。また、メモリの消費が大きくなると、アラームメッセージが表示されます。メッセージが表示された場合は、接続ユーザの切断を行ってください。

表 3-1 ログイン方法の概要

ログイン方法		デフォルト設定、必要最低限の設定
CLIのログイン	コンソールポートからローカルにログイン	デフォルト設定では、コンソールポートでのログインのみ可能です。初期パスワード”**qx_admin**”のパスワード認証で、ユーザロールはnetwork-adminです。 ログイン後は、装置のセキュリティ確保のため、パスワードの変更あるいはスキームモードによるID/パスワード認証に変更してください。
	Telnet接続によるログイン	デフォルトではTelnet接続によるログインは無効です。 Telnet接続によるログインを行うため、以下の設定が必要です。 ● Telnetサーバ機能を有効にします。 ● レイヤ3インタフェースにIPアドレスを設定し、インタフェースとTelnetクライアント間で通信可能なことを確認します。 ● VTYログインユーザ用に認証モードを設定します。デフォルトではパスワード認証が使用されますが、パスワードは設定されていません。 ● VTYログインユーザにユーザロールを割り当てます。(デフォルトはnetwork-operator)
	SSH接続によるログイン	デフォルトではSSH接続によるログインは無効です。SSH接続によるログインを行うため、以下の設定が必要です。 ● SSHサーバ機能を有効にし、SSH属性を設定します。 ● レイヤ3インタフェースにIPアドレスを設定し、インタフェースとSSHクライアント間で通信可能なことを確認します。 ● VTYログインユーザ用に認証モードを設定します。デフォルトではパスワード認証が使用されます。 ● VTYログインユーザにユーザロールを割り当てます。(デフォルトはnetwork-operator)

ログイン方法	デフォルト設定、必要最低限の設定
Webインタフェースからのアクセス	デフォルトでWebインタフェースからのログインは無効です。Webインタフェースによるログインを行うため、以下の設定が必要です。 ● レイヤ3インタフェースにIPアドレスを設定します。Webインタフェースと Webユーザホスト間で通信可能なことを確認します。 ● Webログインのローカルユーザアカウントを設定し、アカウントにユーザロールを割り当てます。デフォルトは network-operatorです。 ● ユーザにHTTPあるいはHTTPSサービスを割り当てます。デフォルトは設定されていません。
SNMPからのアクセス	デフォルトではSNMPによるログインは無効です。 SNMPによるログインを行うため、以下の設定が必要です。 ● レイヤ3インタフェースにIPアドレスを設定し、インタフェースとNMS間で通信可能なことを確認します。 ● SNMPの基本パラメータを設定します。

目次

このセクションのページは **1-x-x** です。

4 章 コンソールポートによる最初のログイン..... 4-1

4章　コンソールポートによる最初のログイン

初回の装置へのログインは、コンソールポートを使用した CLI ログインのみ行うことができます。

コンソールポートから装置にログインするには、コンソール端末（例 PC）と端末エミュレーションプログラム（例 Windows の HyperTerminal）などのユーザ端末の関連設定をコンソールポートと同じにしなければなりません。端末エミュレーションプログラムの使用方法については、プログラムのユーザガイドあるいはオンラインヘルプを参照してください。

コンソールポートでログインする場合は以下の手順に従ってください。

1) PC のシリアルポートに D-sub9 ピンメスコネクタを接続します。
2) コンソールケーブルの RJ-45 コネクタを装置のコンソールポートに接続します。

⚠ **重要：**

- 接続するポートを確認して間違ったコネクタに接続しないようにしてください。
- PC のシリアルポートはホットスワップ機能にサポートしていません。装置が電源 ON である場合、PC の電源を OFF にしてください。装置に接続する前に PC にコンソールケーブルを最初に接続してください。ケーブルを取り外すときは、最初に装置から取り外してください。

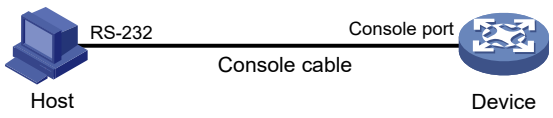


図 4-1 コンソールポートとの接続

3) PC が電源 OFF である場合、PC の電源を ON にしてください。
4) PC で端末エミュレーションソフトウェア（Windows のハイパーターミナルなど）を起動し、装置に接続する端末の設定を行います。通常、端末のコンソールポートのパラメータは以下となっています。

- 通信速度　　— 9600 bps
- フローコントロール — なし
- パリティ　　— なし
- ストップビット　— 1
- データビット　　— 8

5) 装置の電源を入れます。“Press ENTER to get started.”と画面に表示されたのち、<Enter>キーを押下します。

デフォルトの user view のプロンプト<Switch>が表示されます。装置の設定や管理を行うため、コマンドを入力することができます。ヘルプ画面を表示する場合、クエスチョンマーク（?）を入力します。

```
Press Ctrl+B to access EXTENDED BOOT MENU...0
Loading the main image files...
Loading file
略
Press ENTER to get started.
<Switch>%Jan  8 02:16:05:456 2013 Switch SHELL/5/SHELL_LOGIN: TTY logged in from
aux0.
```

目次

このセクションのページは **1-x-x** です。

5章 CLIによるログイン 5-1
5.1 CLI概要 5-1
5.1.1 ユーザライン 5-1
5.1.2 ログイン認証モード 5-2
5.1.3 ユーザロール 5-2
5.2 コンソールポートからのローカルログイン 5-3
5.2.1 None認証の設定 5-3
5.2.2 Password認証の設定 5-4
5.2.3 Scheme認証の設定 5-5
5.2.4 AUXユーザラインの共通設定 5-6
5.3 Telnetからのログイン 5-7
5.3.1 装置のTelnetログインの設定 5-8
5.3.2 装置からTelnetサーバへのTelnet接続 5-14
5.4 SSHからのログイン 5-15
5.4.1 SSHログインの設定 5-15
5.4.2 装置からSSHサーバへのSSH接続 5-17
5.5 CLIログインの表示と維持 5-18

5章 CLI によるログイン

初回の装置へのログインは、コンソールポートを使用した CLI ログインのみ行うことができます。装置の管理を容易にするため、コンソールポートや Telnet、SSH、Web、SNMP でログインすることができます。

CLI への不正アクセスを防止し、ユーザロールを管理するため、以下のことを行うことができます。

- ログイン認証の設定
- ユーザロールの割り当て
- コマンド許可の設定
- 無許可ログインのフィルタリングを行う ACL

この章では設定について方法記載し、ログイン認証、ユーザロール、共通ユーザライン設定を含む CLI ログイン方法について記載します。詳細は、オペレーションマニュアルのセクション 1 *はじめに”ログインユーザの制御”*を参照してください。

5.1 CLI概要

5.1.1 ユーザライン

装置は CLI セッションを管理し、ユーザのふるまいをモニタリングするため、ユーザライン（ユーザインタフェースと呼ばれます）を使用します。ユーザラインでのログイン認証、ユーザロールを含むアクセス管理の設定を行うことができます。ユーザがログインした後、ユーザラインに割り当てられた設定に従う必要があります。

ユーザは、表 5-1のようにログイン方法に依存した異なるユーザラインに割り当てられます。

表 5-1 CLI ログイン方法とユーザライン

ユーザライン	ログイン方法
AUXユーザライン	コンソールポート
Virtual type terminal （VTY）ユーザライン	TelnetあるいはSSH

I. ユーザラインの識別化

各ユーザラインは、識別化のため絶対値と相対値を持っています。

絶対値は、すべてのユーザライン間でユーザラインを一意に認識します。ユーザラインは、AUX と VTY ユーザラインで 0 から 1 ずつ増加するユーザライン番号で番号付けられます。**display line** コマンドでパラメータを指定しない場合、サポートされるユーザラインと絶対値を表示することができます。

相対値は同一タイプのすべてのユーザライン間でユーザラインを識別します。番号フォーマットは *interface type* + *number* です。すべてのユーザラインのタイプは 0 から 1 ずつ増加します。たとえば VTY ユーザラインの最初は VTY0 です。

II. ユーザラインの割り当て

装置は、ログイン方法に依存して、CLI ログインユーザにユーザラインを自動的に割り当てます。各ユーザラインは 1 度に 1 つのユーザにのみユーザラインを割り当てることができます。ユーザラインが有効でない場合、CLI ログインは拒否されます。

CLI ログインで、装置は、ログインタイプ用に、有効で空いているユーザラインから最も低い値を用います。たとえば 4 つの VTY インタフェース（0～3）が設定されている場合、VTY インタフェースの VTY0 と VTY3 は空いています。ユーザが装置に Telnet を行うとき、ユーザに VTY0 が割り当てられ、認証を行い、ユーザを管理するために VTY0 の設定を使用します。

5.1.2 ログイン認証モード

装置の CLI への不正アクセスを防ぐため、ログイン認証を設定することができます。

装置は以下のログイン認証モードをサポートしています。

- **None** – 認証なし。このモードはセキュリティの保護がありません。
- **Password** – パスワード認証が必要です。
- **Scheme** – ローカルあるいはリモートログイン認証を行うため、AAA モジュールを使用します。ログイン時にユーザ名、パスワードを使用する必要があります。

異なるログイン認証モードは、表 5-2のようにユーザラインで異なる設定が必要です。

表 5-2 異なるログイン認証で必要な設定

認証モード	操作
None	認証モードを**none**に設定します。
Password	1. 認証モードを **password** に設定します。 2. パスワードを設定します。
Scheme	1. 認証モードを **scheme** に設定します。 2. ISP domain view でログイン認証方法を設定します。詳細は、オペレーションマニュアルのセクション 9 *セキュリティ*”*AAA*”を参照してください。

5.1.3 ユーザロール

ログインするときユーザはユーザロールが割り当てられます。ユーザロールはユーザが実行できるコマンドを指定します。ユーザロールの詳細は、オペレーションマニュアルのセクション 1 *はじめに*”*RBAC*”を参照してください。

装置はログイン認証モードとログイン方法をもとにしたユーザロールを割り当てます。

- もし None あるいは Password 認証が使用される場合、装置はユーザラインで作成されたユーザロールの設定に従ってユーザロールを割り当てます。

- もし Scheme 認証が使用される場合、以下のようにユーザロールを割り当てます。
  - 公開鍵あるいはパスワード公開鍵を使用する SSH ログインユーザの認証において、装置はユーザラインで設定されたユーザロールに従ってユーザロールを割り当てます。
  - 他のユーザにおいて、AAA モジュールで設定されたユーザロールに従ってユーザロールを割り当てます。リモート AAA 認証ユーザにおいて、もし AAA サーバがユーザにユーザロールを割り当てず、ユーザロール機能が無効である場合、ユーザはログインすることができません。

5.2 コンソールポートからのローカルログイン

図 5-1のように装置にログインし、管理するため、コンソールポートで端末を接続することができます。ログイン手順については、オペレーションマニュアルのセクション 1 *はじめに*”*コンソールポートによる最初のログイン*”を参照してください。

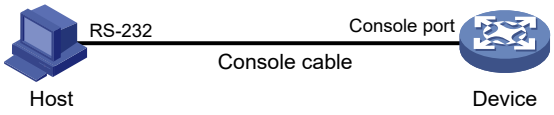


図 5-1 コンソールポートによるログイン

デフォルトでコンソールポートは使用可能で、Password 認証が設定されています。装置のセキュリティの対応を行うため、パスワードの変更あるいは認証スキームモードを設定します。そして初回に装置へログインした後、すぐに必要とされるようにユーザロールを割り当てます。

コンソールログインを設定するため、以下の作業が完了している必要があります。

操作	備考
（必須設定項目）コンソールログイン用のログイン認証の設定: • None認証の設定 • Password認証の設定 • Scheme認証の設定	いずれか一つの認証モードが必要です。
（オプション設定項目）AUXユーザラインの共通設定	—

コンソールログインの設定は、ログイン中のユーザには適用しません。設定が行われた後、次にログインするユーザのみ適用されます。

5.2.1 None 認証の設定

操作	コマンド	備考
1. system view に移行する	**system-view**	—

操作	コマンド	備考
2． AUX line view あるいは class view に移行する	● AUX line viewに移行する： **line aux** *first-number* [*last-number*] ● AUX line class viewに移行する： **line class aux**	どちらか一方を使用します。 User line viewでの設定はユーザラインのみ適用されます。 User line class viewでの設定はclassのすべてのユーザに適用されます。 どちらかの設定がデフォルトから変更された場合、他のviewのデフォルト設定よりも優先されます。 User line viewの設定がデフォルトから変更された場合、user line class viewでデフォルトから変更された設定よりも優先されます。 user line viewでの設定はオンラインユーザにすぐさま適用されます。 User line class viewでの設定は、設定が完了したのち、ログインしたユーザに適用されます。
3． None 認証モードを有効にする	**authentication-mode** *none*	デフォルト： **password**(AUX line class view) **none**(AUX line view)
4． ユーザロールを割り当てる	**user-role** *role-name*	デフォルト：**network-admin**

コンソールポートを使用して、次回ログインを行う場合、ユーザ名あるいはパスワードを必要としません。

5.2.2 Password 認証の設定

操作	コマンド	備考
1． system view に移行する	**system-view**	―
2． AUX line view あるいは class view に移行する	● AUX line viewに移行する： **line aux** *first-number* [*last-number*] ● AUX line class viewに移行する： **line class aux**	どちらか一方を使用します。 User line viewでの設定はユーザラインのみ適用されます。 User line class viewでの設定はclassのすべてのユーザに適用されます。 どちらかの設定がデフォルトから変更された場合、他のviewのデフォルト設定よりも優先されます。 User line viewの設定がデフォルトから変更された場合、user line class viewでデフォルトから変更された設定よりも優先されます。 user line viewでの設定はオンラインユーザにすぐさま適用されます。 User line class viewでの設定は、設定が完了したのち、ログインしたユーザに適用されます。
3． Password 認証モードを有効にする	**authentication-mode password**	デフォルト： **password**(AUX line class view) **none**(AUX line view)

操作	コマンド	備考
4． password を設定する	**set authentication password** { **hash** | **simple** } *password*	デフォルト： **qx_admin**(AUX line class view) 設定なし(AUX line view)
5． ユーザロールを割り当てる	**user-role** *role-name*	デフォルト：**network-admin**

コンソールポートを使用して、次回ログインを行う場合、設定したログインパスワードが必要です。

メモ：

AUX line class view のデフォルトのパスワード **qx_admin** は、工場出荷時の初期パスワードです。セキュリティが損なわれないようパスワードを変更してください。

5.2.3 Scheme 認証の設定

操作	コマンド	備考
1． system view に移行する	**system-view**	―
2． AUX line view あるいは class view に移行する	● AUX line viewに移行する： **line aux** *first-number* [*last-number*] ● AUX line class viewに移行する： **line class aux**	どちらか一方を使用します。 User line viewでの設定はユーザラインのみ適用されます。 User line class viewでの設定はclassのすべてのユーザに適用されます。 どちらかの設定がデフォルトから変更された場合、他のviewのデフォルト設定よりも優先されます。 User line viewの設定がデフォルトから変更された場合、user line class viewでデフォルトから変更された設定よりも優先されます。 user line viewでの設定はオンラインユーザにすぐさま適用されます。 User line class viewでの設定は、設定が完了したのち、ログインしたユーザに適用されます。
3． Scheme 認証を有効にする	**authentication-mode** *scheme*	デフォルト： **password**(AUX line class view) **none**(AUX line view)

Scheme 認証を使用するため、以下の設定が完了している必要があります。

- ISP domain view でコンソールログイン方法を設定します。
- リモート認証を使用し、スキームを設定します。
- ローカル認証を使用し、ローカルユーザと関連する設定を行います。

詳細はオペレーションマニュアルのセクション 9 *セキュリティ”AAA”* を参照してください。

コンソールポートを使用して、次回ログインを行う場合、設定したユーザ名、パスワードが必要です。

5.2.4 AUX ユーザラインの共通設定

AUX ユーザライン用のいくつかの共通の設定は、設定された後すぐに適用され、現在のセッションを中断してしまうことがあります。同一のログイン作業を再度行うことを防ぐため、AUX ユーザラインを変更する前に、コンソールログインとは別のログイン方法を使用します。

設定が完了した後、コンソールポートを経由してログインするため、装置で設定したコンソールポートに合うようにコンソールターミナルの設定を変更します。

以下に AUX ユーザラインの共通設定を示します。

操作	コマンド	備考
1． system view に移行する	**system-view**	―
2． AUX line view あるいは class view に移行する	● AUX line viewに移行する： **line aux** *first-number* [*last-number*] ● AUX line class viewに移行する： **line class aux**	どちらか一方を使用します。 User line viewでの設定はユーザラインのみ適用されます。 User line class viewでの設定はclassのすべてのユーザに適用されます。 どちらかの設定がデフォルトから変更された場合、他のviewのデフォルト設定よりも優先されます。 User line viewの設定がデフォルトから変更された場合、user line class viewでデフォルトから変更された設定よりも優先されます。 user line viewでの設定はオンラインユーザにすぐさま適用されます。 User line class viewでの設定は、設定が完了したのち、ログインしたユーザに適用されます。
3． ボーレートを設定する	**speed** *speed-value*	デフォルト：9600 bps このコマンドはAUX line class viewで設定できません。
4． パリティチェックモードを指定する	**parity** { **even** | **mark** | **none** | **odd** | **space** }	デフォルト：**none**（パリティチェックなし） このコマンドはAUX line class viewで設定できません。
5． ストップビットを設定する	**stopbits** { **1** | **1.5** | **2** }	デフォルト：**1** ストップビットは文字の最後を示します。ストップビットが多いと転送が遅くなります。 このコマンドはAUX line class viewで設定できません。

操作	コマンド	備考
6. データビットを設定する	**databits** { **5** | **6** | **7** | **8** }	デフォルト：**8** 文字コードタイプに依存します。たとえば7に設定されると標準ASCII文字が送信され、8に設定すると拡張ASCII文字が送信されます。 このコマンドはAUX line class viewで設定できません。
7. エスケープキーを設定する	**escape-key** { *key-string* | **default** }	デフォルト：CTRL+C
8. 端末タイプを設定する	**terminal type** { **ansi** | **vt100** }	デフォルト：ANSI 装置はANSIとvt100の2つの端末タイプをサポートします。端末で適した表示を保証するため、両方のタイプを設定し、装置と端末の両方のタイプをvt100に設定することを推奨します。 そうでなければコマンドラインが80文字超えてしまい、カーソル位置がエラーとなったり、異常な端末表示となる場合があります。
9. 画面に表示できる最大行数を設定する	**screen-length** *screen-length*	デフォルト：最大24行 出力の最大行を0とすると画面の表示は停止しません。
10. コマンド履歴バッファのサイズを設定する	**history-command max-size** *value*	デフォルト：10
11. ユーザラインのタイムアウトの時間を設定する	**idle-timeout** *minutes* [*seconds*]	デフォルト：10分 タイムアウト時間内に、ユーザラインで何も実行されないと自動的にユーザラインの接続が終了します。タイムアウト機能を無効にする場合、0に設定します。
12. ユーザが現在のuser lineにログインしたとき、自動で実行されるコマンドを設定する	**auto-execute command** *command*	デフォルト：無効 ユーザが現在のuser lineにログインしたとき、装置は自動で指定されたコマンドを実行します。コマンドが実行されたのち、ユーザの接続を切断します。 このコマンドはAUX line viewあるいはAUX line class viewでサポートしていません。
13. 端末サービスを有効にする	**shell**	デフォルト：有効 AUX line viewあるいはAUX line class viewでコマンドは**undo shell**サポートしていません。

5.3 Telnetからのログイン

装置のリモート管理を行うため、Telnet サーバを使用することができます。また他の装置を管理するため、装置を Telnet クライアントとして使用することができます。

デフォルトでは Telnet からのログインは無効です。Telnet を使用する場合、以下の作業を行ってください。

- Telnet 以外の他のログイン方法を用いて、装置にログインしてください。
- Telnet サーバ機能を有効にしてください。
- 装置の Telnet ログイン認証を設定してください。

5.3.1 装置の Telnet ログインの設定

操作	備考
（必須設定項目）Telnetサーバの有効化	ー
（必須設定項目）Telnetからのログイン認証の設定 ● None認証の設定 ● Password認証の設定 ● Scheme認証の設定	いずれか一つの認証モードが必要です。
（オプション設定項目）現在のTelnetユーザの最大数の設定	ー
（オプション設定項目）出力telnetパケットのDSCP値の設定	ー
（オプション設定項目）VTYユーザラインの共通設定	ー

I. Telnet サーバの有効化

操作	コマンド	備考
1． system view に移行する	**system-view**	ー
2． Telnet サーバを有効化する	**telnet server enable**	デフォルト：無効

II. None 認証の設定

操作	コマンド	備考
1． system view に移行する	**system-view**	ー

操作	コマンド	備考
2． VTY line view または VTY line class view に移行する	● VTY line viewに移行する：**line vty** *first-number* [*last-number*] ● VTY line class viewに移行する：**line class vty**	どちらか一方を使用します。 User line viewでの設定はユーザラインのみ適用されます。 User line class viewでの設定はclassのすべてのユーザに適用されます。 どちらかの設定がデフォルトから変更された場合、他のviewのデフォルト設定よりも優先されます。 User line viewの設定がデフォルトから変更された場合、user line class viewでデフォルトから変更された設定よりも優先されます。 user line viewでの設定はオンラインユーザにすぐさま適用されます。 User line class viewでの設定は、設定が完了したのち、ログインしたユーザに適用されます
3． None認証モードを有効にする	**authentication-mode none**	デフォルト：**password** VTY line viewでは**protocol inbound**コマンドに関連します。 ● どちらかの設定がデフォルトから変更された場合、VTY line viewの設定が適用されます。 ● VTY line viewで両方の設定がデフォルトのままである場合、VTY line class viewの設定が適用されます。
4． （オプション設定項目）ユーザロールの割り当てる	**user-role** *role-name*	デフォルト：**network-operator**

次回 Telnet で装置にログインを行う場合、ユーザ名あるいはパスワードを必要としません。もしログインユーザ数が装置の最大である場合は、ログインに失敗し、"All user lines are used, Please try later!"のメッセージが表示されます。

III. Password 認証の設定

操作	コマンド	備考
1． system view に移行する	**system-view**	—

操作	コマンド	備考
2． VTY line view または VTY line class view に移行する	● VTY line viewに移行する：**line vty** *first-number* [*last-number*] ● VTY line class viewに移行する：**line class vty**	どちらか一方を使用します。 User line viewでの設定はユーザラインのみ適用されます。 User line class viewでの設定はclassのすべてのユーザに適用されます。 どちらかの設定がデフォルトから変更された場合、他のviewのデフォルト設定よりも優先されます。 User line viewの設定がデフォルトから変更された場合、user line class viewでデフォルトから変更された設定よりも優先されます。 user line viewでの設定はオンラインユーザにすぐさま適用されます。 User line class viewでの設定は、ログイン中のユーザには適用しません。設定が完了したのち、ログインしたユーザに適用されます。
3． Password 認証モードを有効にする	**authentication-mode password**	デフォルト：**password** VTY line viewでは**protocol inbound** コマンドに関連します。 ● どちらかの設定がデフォルトから変更された場合、VTY line viewの設定が適用されます。 ● VTY line viewで両方の設定がデフォルトのままである場合、VTY line class viewの設定が適用されます。
4． password の設定	**set authentication password** { **hash** | **simple** } *password*	デフォルト：設定なし
5． （オプション設定項目）ユーザロールを割り当てる	**user-role** *role-name*	デフォルト：**network-operator**

次回 Telnet で装置にログインを行う場合、パスワードが必要となります。もしログインユーザ数が装置の最大である場合は、ログインに失敗し、" All user lines are used, please try later!"のメッセージが表示されます。

```
Password:
<Switch>
```

IV. Scheme 認証の設定

操作	コマンド	備考
1． system view に移行する	**system-view**	ー
2． VTY line view または VTY line class view に移行する	● VTY line viewに移行する：**line vty** *first-number* [*last-number*] ● VTY line class viewに移行する：**line class vty**	どちらか一方を使用します。 User line viewでの設定はユーザラインのみ適用されます。 User line class viewでの設定はclassのすべてのユーザに適用されます。 どちらかの設定がデフォルトから変更された場合、他のviewのデフォルト設定よりも優先されます。 User line viewの設定がデフォルトから変更された場合、user line class viewでデフォルトから変更された設定よりも優先されます。 user line viewでの設定はオンラインユーザにすぐさま適用されます。 User line class viewでの設定は、ログイン中のユーザには適用しません。設定が完了したのち、ログインしたユーザに適用されます。
3． Scheme 認証を有効にする	**authentication-mode scheme**	デフォルト：**password** VTY line viewでは**protocol inbound** コマンドに関連します。 ● どちらかの設定がデフォルトから変更された場合、VTY line viewの設定が適用されます。 ● VTY line viewで両方の設定がデフォルトのままである場合、VTY line class viewの設定が適用されます。

Scheme 認証を行うため、以下の作業を完了してください。

- ISP domain view でログイン認証を設定してください。
- リモート認証を行うため、使用する scheme の設定を行ってください。
- ローカル認証を行うため、ローカルユーザと関連する属性の設定を行ってください。

詳細はオペレーションマニュアルのセクション 9 *セキュリティ*”*AAA*”を参照してください。

次回 Telnet で装置にログインを行う場合、ユーザ名、パスワードが必要となります。もしログインユーザ数が装置の最大である場合は、ログインに失敗し、"All lines are used, please try later!"のメッセージが表示されます。

```
Login: admin
Password:
<Switch>
```

V. Telnet ユーザの最大数の設定

操作	コマンド	備考
1． system view に移行する	**system-view**	―
2． Telnet ユーザの最大数を設定する	**aaa session-limit telnet** *max-sessions*	デフォルト：32 オンライン中のTelnetユーザには影響しません。現在のオンライン中のTelnetユーザ数が、新しく設定した最大数以上である場合、オンラインユーザがログアウトするまで新規にログインすることができません。このコマンドの詳細は、コマンドマニュアルのセクション9 *セキュリティ”AAA”*を参照してください。

VI. 出力 telnet パケットの DSCP 値の設定

DSCP 値は IP あるいは IPv6 パケットの ToS/トラフィッククラスフィールドに入れられ、パケットを転送する優先順位を示します。

以下に出力 telnet パケットの DSCP 値の設定を示します。

操作	コマンド	備考
1． system view に移行する	**system-view**	―
2． 出力 telnet パケットの DSCP 値を設定する	● IPv4で動作するtelnetサーバを設定する： **telnet server dscp** *dscp-value* ● IPv6で動作するtelnetサーバを設定する： **telnet server ipv6 dscp** *dscp-value*	デフォルト：48

VII. VTY ユーザラインの共通設定

VTY ユーザラインにおいて、ユーザログインを行ったときに自動的に実行されるコマンドを指定することができます。指定したコマンドを実行し、操作を行った後、システムは自動的に Telnet セッションを切断します。この機能を設定する前に設定を保存し、異なるユーザラインによって CLI アクセスができることを確認してください。

一般的に、装置がTelnetユーザをX.X.X.Xのアドレスのホストにリダイレクトさせるため、**auto-execute command telnet** *X.X.X.X* コマンドを設定します。ユーザが X.X.X.X の Telnet 接続を切断したとき、現在の装置の接続が切断します。

以下に VTY ユーザラインの共通設定を示します。

操作	コマンド	備考
1． system view に移行する	**system-view**	―
2． VTY line view または VTY line class view に移行する	● VTY line viewに移行する：**line vty** *first-number* [*last-number*] ● VTY line class viewに移行する：**line class vty**	どちらか一方を使用します。 User line viewでの設定はユーザラインのみ適用されます。 User line class viewでの設定はclassのすべてのユーザに適用されます。 どちらかの設定がデフォルトから変更された場合、他のviewのデフォルト設定よりも優先されます。 User line viewの設定がデフォルトから変更された場合、user line class viewでデフォルトから変更された設定よりも優先されます。 user line viewでの設定はオンラインユーザにすぐさま適用されます。 User line class viewでの設定は、ログイン中のユーザには適用されません。次にログインするユーザのみ適用されます。
3． 端末サービスを有効にする	**shell**	デフォルト：有効
4． 指定したユーザラインでサポートするプロトコルを設定する	**protocol inbound** { **all** | **ssh** | **telnet** }	デフォルト：all 次回のログイン時に適用されます。 VTY line viewでは、**authentication-mode**コマンドに関連します。 ● VTY line viewの設定がデフォルトから変更された場合、VTY line viewの他の設定が適用されます。 ● VTY line viewで両方の設定がデフォルトである場合、VTY line class viewの設定が適用されます。
5． エスケープキーを設定する	**escape-key** { *key-string* | **default** }	デフォルト：CTRL+C
6． 端末タイプを設定する	**terminal type** { **ansi** | **vt100** }	デフォルト：ANSI
7． 画面に表示できる最大数を設定する	**screen-length** *screen-length*	デフォルト：24行 出力の最大行を0とすると画面の表示は停止しません。
8． コマンド履歴のバッファサイズを設定する	**history-command max-size** *value*	デフォルト：10 コマンド履歴のバッファは最大10のコマンドを保存します。

操作	コマンド	備考
9. ユーザラインのタイムアウト時間を設定する	**idle-timeout minutes** [***seconds***]	デフォルト：10分 タイムアウト時間内に、ユーザラインで何も実行されないと自動的にユーザラインの接続が終了します。 タイムアウト機能を無効にする場合、0に設定します。
10. ユーザラインにログイン後、自動で実行されるコマンドを指定する	**auto-execute command** *command*	デフォルト：ユーザがユーザラインにログインした際に自動的に実行されるコマンドはなし ⚠ **重要：** user lineにこのコマンドを実行すると、user lineによるCLIアクセスができなくなる可能性があります。このコマンドを設定する前に、異なるuser lineあるいはAUX user lineによってCLIにアクセスできることを確認してください。

5.3.2 装置から Telnet サーバへの Telnet 接続

装置は Telnet クライアントとして Telnet サーバにログインすることができます。もし Telnet サーバが異なるサブネットにある場合、2 つの装置と Telnet サーバ間で通信できることを確認してください。



図 5-2 装置から Telnet サーバへの Telnet 接続

以下に装置から Telnet サーバへのログインの設定を示します。

操作	コマンド	備考
1. system view に移行する	**system-view**	—
2. （オプション設定項目） Telnet パケットの送信元 IPv4 アドレス/インタフェースを指定する	**telnet client source** { **interface** *interface-type interface-number* | **ip** *ip-address* }	デフォルト：送信元IPv4アドレス/インタフェースは設定なし、送信元アドレスとして出力インタフェースのプライマリIPv4アドレスが使われます。
3. user view へ戻る	**quit**	—

操作	コマンド	備考
4. Telnet サーバへのログインする	• IPv4 Telnet サーバへのログイン： **telnet** *remote-host* [*service-port*] [**source** { **interface** *interface-type interface-number* | **ip** *ip-address* }] [**dscp** *dscp-value*] • IPv6 Telnet サーバへのログイン： **telnet ipv6** *remote-host* [**-i** *interface-type interface-number*] [*port-number*] [**dscp** *dscp-value*]	—

5.4 SSHからのログイン

SSH は、より強固なセキュリティを持ったログイン方法のアプローチです。強力な暗号化と認証機能によって IP スプーフィング攻撃、パスワード傍受なども防止することができます。詳細はオペレーションマニュアルのセクション 9 *セキュリティ”SSH*”を参照してください。

装置のリモート管理を行うため、SSH クライアントを使用することができます。また SSH サーバの他の装置を管理するため、装置を SSH クライアントとして使用することができます。

デフォルトでは SSH からのログインは無効です。SSH を使用する場合、SSH 以外の他のログイン方法を用いて、初回に SSH ログインの設定を行う必要があります。

5.4.1 SSH ログインの設定

この章では SSH クライアント認証が password である場合の手順を示します。SSH、公開鍵認証の設定の詳細については、オペレーションマニュアルのセクション 9 *セキュリティ”SSH*”、“*公開鍵*”を参照してください。

以下に装置から SSH ログインの設定を示します。

操作	コマンド	備考
1. system view に移行する	**system-view**	—
2. ローカル鍵ペアを生成する	**public-key local create** { **dsa** | **rsa** } [**name** *key-name*]	デフォルト：なし
3. SSH サーバを有効にする	**ssh server enable**	デフォルト：無効

操作	コマンド	備考
4．（オプション設定項目）SSH ユーザを生成し、認証モードを指定する	**ssh user** *username* **service-type stelnet authentication-type** { *password* | { **any** | **password-publickey** | **publickey** } **assign publickey** *keyname* } **ssh user** *username* **service-type stelnet authentication-type** { **password** | { **any** | **password-publickey** | **publickey** } **assign publickey** *keyname* }	デフォルト：設定なし
5．VTY line view または VTY line class view に移行する	● VTY line viewに移行する：**line vty** *first-number* [*last-number*] ● VTY line class viewに移行する：**line class vty**	どちらか一方を使用します。 User line viewでの設定はユーザラインのみ適用されます。 User line class viewでの設定はclassのすべてのユーザに適用されます。 どちらかの設定がデフォルトから変更された場合、他のviewのデフォルト設定よりも優先されます。 User line viewの設定がデフォルトから変更された場合、user line class viewでデフォルトから変更された設定よりも優先されます。 user line viewでの設定はオンラインユーザにすぐさま適用されます。 User line class viewでの設定は、ログイン中のユーザには適用しません。設定が完了したのち、ログインしたユーザに適用されます。
6．scheme 認証を有効にする	**authentication-mode scheme**	デフォルト：**password** VTY line viewでは**protocol inbound** コマンドに関連します。 ● どちらかの設定がデフォルトから変更された場合、VTY line viewの設定が適用されます。 ● VTY line viewで両方の設定がデフォルトのままである場合、VTY line class viewの設定が適用されます。

操作	コマンド	備考
7.　（オプション設定項目）使用するプロトコルを指定する	**protocol inbound** { **all** | **ssh** | **telnet** }	デフォルト：**all** ログイン中のユーザには適用しません。次回のログイン時に適用されます。 VTY line viewでは、**authentication-mode**コマンドに関連します。 ● VTY line viewの設定がデフォルトから変更された場合、VTY line viewの他の設定が適用されます。 ● VTY line viewで両方の設定がデフォルトである場合、VTY line class viewの設定が適用されます。
8.　system view から戻る	**quit**	—
9.　（オプション設定項目）VTY ユーザラインの共通設定	オペレーションマニュアルのセクション1 *はじめに*”*CLIによるロギング*”の”*Telnetからのログイン*”を参照してください。	—
10.　（オプション設定項目） 現在の SSH ユーザの最大数を設定する	**aaa session-limit ssh** *max-sessions*	デフォルト：32 オンライン中のSSHユーザには影響しません。現在のオンライン中のSSHユーザ数が、新しく設定した最大数以上である場合、オンラインユーザがログアウトするまで新規にログインすることができません。このコマンドの詳細は、コマンドマニュアルのセクション9 *セキュリティ*”*AAA*”を参照してください。

5.4.2 装置から SSH サーバへの SSH 接続

装置は SSH クライアントとして SSH サーバにログインすることができます。もし SSH サーバが異なるサブネットにある場合、2 つの装置と SSH サーバ間で通信できることを確認してください。



図 5-3 装置から SSH サーバへの SSH 接続

以下に user view で装置から SSH サーバへのログインの設定を示します。

操作	コマンド
IPv4 SSH サーバへのログイン	**ssh2** *server*

操作	コマンド
IPv6 SSH サーバへのログイン	**ssh2 ipv6** *server*

SSH サーバを動作させるためには、SSH クライアントの設定を行う必要があります。SSH クライアントの設定の詳細については、オペレーションマニュアルのセクション 9 *セキュリティ*”*SSH*”を参照してください。

5.5 CLIログインの表示と維持

display コマンドはすべての view で実行でき、他のコマンドは user view で実行できます。

操作	コマンド	備考
オンラインユーザ情報を表示する	**display users** [**all**]	―
ユーザラインを表示する	**display line** [*num1* | { **aux** | **vty** } *num2*] [**summary**]	―
送信元IPv4アドレス/インタフェースを表示する	**display telnet client**	―
特定のユーザラインを解放する	**free line** { *num1* | { **aux** | **vty** } *num2* }	複数のユーザが同時に設定することができます。必要に応じて、このコマンドを使用して、ある接続を開放します。このコマンドで自分が使用している接続を開放することはできません。 user viewで使用可能です。
現在のユーザラインをロックする	**lock**	デフォルト：ロックされていません。
ユーザラインにメッセージを送信する	**send** { **all** | *num1* | { **aux** | **vty** } *num2* }	user viewで使用可能です。

目次

このセクションのページは **1-x-x** です。

6 章 Web コンソールによるログイン 6-1
6.1 HTTP ログインの設定 6-1
6.2 HTTPS ログインの設定 6-2
6.3 Web ログインの表示と維持 6-4
6.4 Web ログインの設定例 6-4
6.4.1 HTTP ログインの設定例 6-4

6章 Web コンソールによるログイン

装置は HTTP（1.0、1.1）と HTTPS を使用して Web コンソール機能（Web サーバ機能）をサポートしています。端末の Web ブラウザを使用して、装置の Web コンソールにアクセスしてログインし、装置を管理できます。

HTTPS はクライアントとサーバ間で交換するデータの完全性とセキュリティを保証するため SSL を使用しています。HTTP よりも安全です。正当なクライアントのみが Web インタフェースにアクセスできるように証明書ベースのアクセス管理ポリシーを定義することができます。

Web コンソール機能はデフォルトでは使用できません。Web コンソールによるログインをしたい場合、最初にコンソールポートにてログインし、アクセルできるように設定する必要があります。

6.1 HTTPログインの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. HTTP サービスを有効にする	**ip http enable**	デフォルト：無効
3. （オプション設定項目）HTTP サービスのポート番号を設定する	**ip http port** *port-number*	デフォルト：80
4. （オプション設定項目）Web ユーザの接続のタイムアウトタイマを設定する	**web idle-timeout** *idle-time*	デフォルト：10分
5. （オプション設定項目）オンライン HTTP ユーザの最大数を設定する	**aaa session-limit http** *max-sessions*	デフォルト：32 オンライン中のHTTPユーザには影響しません。現在のオンライン中のHTTPユーザ数が、新しく設定した最大数以上である場合、オンラインHTTPユーザがログアウトするまで新規にログインすることができません。詳細はコマンドマニュアルのセクション9 *セキュリティ”AAA”* を参照してください。
6. ローカルユーザを追加し、local user view に移行する	**local-user** *user-name* [**class manage**]	デフォルト：設定なし

操作	コマンド	補足
7. ローカルユーザのパスワードを設定する	**password** { **cipher** | **simple** } *string*	デフォルト: ローカルユーザのパスワードは設定されていません。 プレーンテキストで設定されたパスワードを含めたすべてのパスワードは、暗号化されて保存されます。 セキュリティのためローカルユーザのパスワードを設定してください。
8. ローカルユーザのユーザロールを設定する	**authorization-attribute user-role** *user-role*	デフォルト：network-operator
9. ローカルユーザのサービスタイプを指定する	**service-type http**	デフォルト：設定なし

6.2 HTTPSログインの設定

装置は HTTPS ログインモードをサポートします。

- **Simplified モード**—装置は自己署名の証明書（装置自身によって作成し署名された証明書）、およびデフォルトの SSL の設定を使用します。装置は装置で HTTPS サービスを有効にしたのち Simplified モードで動作します。
- **Secure モード**—装置は CA、およびセキュリティを保証するためユーザ定義のセキュリティ保護の設定によって署名された証明書を使用します。Secure モードで動作させるため以下の処理を行う必要があります。
  - □ 装置で HTTPS サービスを有効にします。
  - □ サービスの SSL サーバポリシーを指定します。
  - □ PKI ドメインのパラメータを設定します。

Simplified モードは設定が容易ですが Secure モードに比べてセキュリティが高くありません。

SSL、PKIの詳細は *QX シリーズWeb 認証オペレーションマニュアル(V7)*の“*SSL*”、“*PKI*”を参照してください。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー

操作	コマンド	補足
2. HTTPS サービスを有効にする	**ip https enable**	デフォルト：無効 HTTPSサービスを有効にすると、SSLハンドシェイクネゴシエーションが開始します。 ● 装置でローカル認証がある場合、SSLハンドシェイクは成功し、HTTPSサービスが開始します。 ● 装置でローカル証明書がない場合、証明書アプリケーション処理が開始します。証明書アプリケーション処理は時間がかかるため、SSLハンドシェイクのネゴシエーションが失敗し、HTTPSサービスが開始しない可能性があります。この問題に対応するためHTTPSサービスが有効になるまで再度コマンドを実行してください。
3. （オプション設定項目）HTTPS サービスのポート番号を設定する	**ip https port** *port-number*	デフォルト：443
4. （オプション設定項目）Web 接続のタイムアウトタイマを設定する	**web idle-timeout** *idle-time*	デフォルト：10分
5. （オプション設定項目）オンライン HTTP ユーザの最大数を設定する	**aaa session-limit https** *max-sessions*	デフォルト：32 オンライン中のHTTPSユーザには影響しません。現在のオンライン中のHTTPSユーザ数が、新しく設定した最大数以上である場合、オンラインHTTPSユーザがログアウトするまで新規にログインすることができません。詳細はコマンドマニュアルのセクション9 *セキュリティ”AAA”* を参照してください。
6. ローカルユーザを追加し、local user view に移行する	**local-user user-name** [**class manage**]	デフォルト：設定なし
7. ローカルユーザのパスワードを設定する	**password** { **cipher** | **simple** } *string*	デフォルト：ローカルユーザのパスワードは設定されていません。 プレーンテキストで設定されたパスワードを含めたすべてのパスワードは、暗号化されて保存されます。 セキュリティのためローカルユーザのパスワードを設定してください。

操作	コマンド	補足
8. ローカルユーザのユーザロールを設定する	**authorization-attribute user-role** *user-role*	デフォルト：network-operator
9. ローカルユーザのサービスタイプを指定する	**service-type https**	デフォルト：設定なし

6.3 Webログインの表示と維持

すべての view で実行可能です。

操作	コマンド
オンラインWebユーザを表示する	**display web users**
HTTPサービスの設定と状態を表示する	**display ip http**
HTTPSサービスの設定と状態を表示する	**display ip https**
オンラインWebユーザをログオフする	**free web users** { **all** | **user-id** *user-id* | **user-name** *user-name* }

6.4 Webログインの設定例

6.4.1 HTTP ログインの設定例

I. ネットワーク要件

図 6-1に示すように IP ネットワークで通信可能な PC と Device を接続します。HTTP を使用して PC にログインします。



図 6-1 ネットワーク図

II. 設定手順

ローカルユーザ admin を作成します。パスワードを admin、サービスタイプを HTTP、ユーザロールを network-admin に設定します。

```
[Device] local-user admin
[Device-luser-manage-admin] service-type http
[Device-luser-manage-admin] authorization-attribute user-role network-admin
```

```
[Device-luser-manage-admin]  password simple admin
[Device-luser-manage-admin]  quit
```

HTTP を有効にします。

```
[Device] ip http enable
```

III. 設定の確認

1)　PC で IE ブラウザを起動し、アドレスバーに Device の IP アドレスを入力します。
2)　ログインページでユーザ名、パスワードを入力します。“Login”をクリックします。

認証に成功したのち、ホームページが表示されます。Device を設定することができます。

目次

このセクションのページは **1-x-x** です。

7 章 SNMP によるログイン 7-1

7章 SNMP によるログイン

NMS で SNMP を実行することで、装置の MIB の GET、SET を行い、装置の管理/設定を行うことができます。

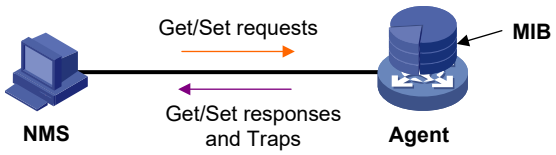


図 7-1 SNMP アクセス

装置は SNMPv1、SNMPv2c、SNMPv3 をサポートし、さまざまなネットワーク管理製品で動作します。NMS は同じ SNMP のバージョンを使用する必要があります。

SNMP に関する詳細は、オペレーションマニュアルのセクション 11 *システム管理*” *SNMP* ” を参照してください。

デフォルトで SNMP によるログインはできません。他の方法で装置にログインして、SNMP によるアクセスを可能にする為の設定を行う必要があります。

目次

このセクションのページは **1-x-x** です。

8 章 RESTful 8-1
8.1 RESTful アクセスについて 8-1
8.2 HTTP 経由の RESTful アクセス設定 8-1
8.3 HTTPS を介した RESTful アクセスの設定 8-1

8章 RESTful

8.1 RESTfulアクセスについて

この装置は Representational State Transfer (RESTful API)、アプリケーションプログラミングインタフェースを提供します。この API に基づいて、Python、Ruby、Java などのプログラミング言語を使用して、次の操作を実行するプログラムを記述できます。

- 認証を通過するための、RESTful リクエストを装置に送信します。
- RESTful API 操作を使用して、装置を設定および管理します。 RESTful API の操作には、Get、Put、Post、および Delete があります。

装置は、RESTful パケットを転送するための HTTP または HTTPS の使用をサポートします。

8.2 HTTP経由のRESTfulアクセス設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. HTTP を経由した RESTful アクセスを有効にする	**restful http enable**	デフォルト：無効
3. ローカルユーザを作成し、ローカル user view に移行する	**local-user** *user-name* [**class manage**]	—
4. ローカルユーザのパスワードを設定する	**password** [{ **hash** | **simple** } *password*]	—
5. (オプション設定項目) ローカルのユーザにユーザロールを割り当てる	**authorization-attribute user-role** *user-role*	デフォルト：ユーザロールは、RESTfulアクセス用のネットワークオペレータユーザです。
6. ローカルユーザの HTTP サービスを指定する	**service-type http**	デフォルト: ローカルユーザにサービスタイプは指定されていません。

8.3 HTTPSを介したRESTfulアクセスの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. HTTPS を経由した RESTful アクセスを有効にする	**restful https enable**	デフォルト：無効

3. ローカルユーザを作成し、ローカル user view に移行する	**local-user** *user-name* [**class manage**]	–
4. ローカルユーザのパスワードを設定する	**password** [{ **hash** | **simple** } *password*]	–
5. (オプション設定項目) ローカルのユーザにユーザロールを割り当てる	**authorization-attribute user-role** *user-role*	デフォルト : ユーザロールは、RESTfulアクセス用のネットワークオペレータユーザです。
6. ローカルユーザの HTTPS サービスを指定する	**service-type https**	デフォルト : ローカルユーザにサービスタイプは指定されていません。

目次

このセクションのページは **1-x-x** です。

9 章 ログインユーザの制御 9-1
9.1 Telnet/SSH ログインの制御 9-1
9.1.1 設定手順 9-1
9.1.2 設定例 9-2
9.2 Web ログインの制御 9-2
9.2.1 送信元 IP アドレスベースの Web ログインの制御 9-3
9.2.2 オンライン Web ユーザのログオフ 9-3
9.2.3 設定例 9-3
9.3 SNMP ログインの制御 9-4
9.3.1 設定手順 9-4
9.3.2 設定例 9-6

9章 ログインユーザの制御

不正なアクセスを防ぐため ACL（Access Control List）を使用し、ユーザのふるまいを監視および制御を行うため、コマンドの許可、アカウンティングの設定を行います。ACL の詳細は、オペレーションマニュアルのセクション 8 *ACL and QoS*”*ACL*”を参照してください。

9.1 Telnet/SSHログインの制御

Telnet、SSH ログインをフィルタするため、異なる条件で ACL を使用します。

- **標準 ACL（2000～2999）**－送信元 IP アドレスを使用します。
- によって Telnet、SSH ログインをフィルタします。
- **拡張 ACL（3000～3999）**－送信元 IP アドレス、宛先 IP アドレスを使用します。
- **L2 ACL（4000～4999）**－送信元 MAC アドレスを使用します。

適用する ACL が存在しないあるいは、ルールがない場合、ユーザはログイン制限が適用されません。ACL がある場合、ACL によって許可されたユーザのみが Telnet あるいは SSH によって装置にアクセスすることができます。

9.1.1 設定手順

以下に Telnet ログインを制御する設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	－
2． Telnet ログインをフィルタする ACL を適用する	• **telnet server acl** [**mac**] *acl-number* • **telnet server ipv6 acl** [**ipv6** | **mac**] *acl-number*	デフォルト：設定なし

以下に SSH ログインを制御する設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	－
2． SSH ログインをフィルタする ACL を適用する	• **ssh server acl** [**mac**] *acl-number* • **ssh server ipv6 acl** [**ipv6** | **mac**] *acl-number*	デフォルト：ACLはなし 詳細はコマンドマニュアルのセクション9 *セキュリティ*”*SSH*”を参照してください。

メモ：

本設定によるフィルタリングでは暗黙の deny が適用されます。

9.1.2 設定例

I. ネットワーク要件

図 9-1に装置が Host A と Host B からの Telnet パケットのみを許可するように設定します。

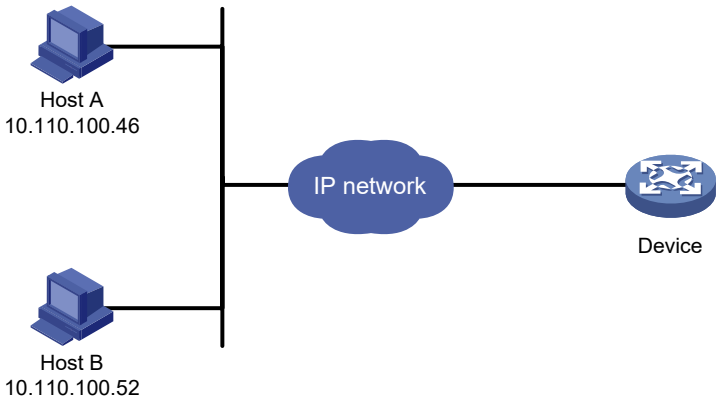


図 9-1 ネットワーク図

II. 設定手順

Host A、Host B からのパケットを許可する ACL を設定します。

```
<Switch> system-view
[Switch] acl basic 2000 match-order  config
[Switch-acl-ipv4-basic-2000]  rule 1 permit source 10.110.100.52  0
[Switch-acl-ipv4-basic-2000]  rule 2 permit source 10.110.100.46  0
[Switch-acl-ipv4-basic-2000]  quit
```

Telnet ログインをフィルタするため ACL を適用します。

```
[Switch] telnet server  acl 2000
```

9.2 Webログインの制御

HTTP、HTTPS ログインをフィルタするため、送信元 IP アドレスによって標準 ACL（2000～2999）を使用します。

適用する ACL が存在しないあるいは、ルールがない場合、ユーザはログイン制限が適用されません。ACL がある場合、ACL によって許可されたユーザのみが HTTP、HTTPS によって装置にアクセスすることができます。

ログインしている疑わしい Web ユーザをログオフすることもできます。

9.2.1 送信元 IP アドレスベースの Web ログインの制御

Web ログイン要求にはユーザ名、パスワードが含まれます。セキュリティのため、装置は常に Web ログイン要求を転送するため HTTPS を使用します。以下の ACL で許可されたユーザのみが HTTP を通して装置にアクセスできます。

- HTTPS サービスに適用する ACL
- HTTP サービスに適用する ACL

以下に送信元 IP アドレスベースの Web ログインを制御する設定を示します。

以下に Web ログインを制御する設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Web ログインをフィルタする ACL を適用する	• **ip http acl** *acl-number* • **ip https acl** *acl-number*	デフォルト：設定なし

9.2.2 オンライン Web ユーザのログオフ

以下にオンライン Web ユーザをログオフする設定を示します。

操作	コマンド	補足
オンラインWebユーザをログオフする	**free web users** { **all** | **user-id** *user-id* | **user-name** *user-name* }	―

9.2.3 設定例

I. ネットワーク要件

図 9-2に示すように Device は HTTP サーバです。Device は Host B のみに HTTP サービスを提供するように設定します。

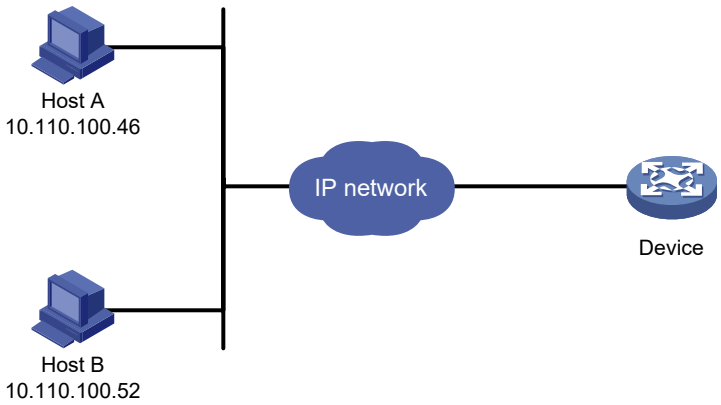


図 9-2 ネットワーク図

II. 設定手順

#ACL を作成します。Host B からのパケットを許可するルール 1 を設定します。

```
<Switch> system-view
[Switch] acl basic 2030 match-order  config
[Switch-acl-ipv4-basic-2030]  rule 1 permit source 10.110.100.52  0
```

Host B の Web ユーザが Device にアクセスできるように HTTP サービスを ACL に関連づけます。

```
[Switch] ip http acl 2030
```

9.3 SNMPログインの制御

送信元 IP アドレスによって SNMP アクセスを制御する標準 ACL（2000～2999）を使用します。要求された MIB view にアクセスするため、NMS は ACL によって許可された送信元 IP アドレスを使用する必要があります。

9.3.1 設定手順

以下に SNMPv1/v2c アクセスを制御する設定を示します。

操作	コマンド	補足
1.　system view に移行する	**system-view**	—

操作	コマンド	補足
2. SNMP v1/v2 コミュニティ、グループ、ユーザに ACL を適用する	● SNMPコミュニティを作成し、ACLを適用する： **snmp-agent community** { **read** | **write** } [**simple** | **cipher**] *community-name* [**mib-view** *view-name*] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } | **acl ipv6** { *ipv6-acl-number* | **name** *ipv6-acl-name* }]* ● SNMPv1/v2cグループを作成し、グループにユーザを追加し、その後ACLを適用する： **snmp-agent group** { **v1** | **v2c** } *group-name* [**read-view** *view-name*] [**write-view** *view-name*] [**notify-view** *view-name*] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } | **acl ipv6** { *ipv6-acl-number* | **name** *ipv6-acl-name* }]* ● SNMPv1/v2cユーザ： **snmp-agent usm-user** { **v1** | **v2c** } *user-name group-name* [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } | **acl ipv6** { *ipv6-acl-number* | **name** *ipv6-acl-name* }]*	SNMPに関する詳細はオペレーションマニュアルのセクション11 *システム管理" SNMP"* を参照してください。

以下に SNMPv3 アクセスを制御する設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. SNMPv3 グループに ACL を適用する	**snmp-agent group v3** *group-name* [**authentication** | **privacy**] [**read-view** *read-view*] [**write-view** *view-name*] [**notify-view** *view-name*] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } | **acl ipv6** { *ipv6-acl-number* | **name** *ipv6-acl-name* }]*	―
3. SNMPv3 ユーザに ACL を適用する	**snmp-agent usm-user v3** *user-name group-name* [{ **cipher** | **simple** } **authentication-mode** { **md5** | **sha** } *auth-password* [**privacy-mode** { **3des** | **aes128** | **des56** } *priv-password*]] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } | **acl ipv6** { *ipv6-acl-number* | **name** *ipv6-acl-name* }]*	SNMPに関する詳細はオペレーションマニュアルのセクション11 *システム管理" SNMP"* を参照してください。

🕮 メモ：

本設定によるフィルタリングでは暗黙の deny が適用されます。

9.3.2 設定例

I. ネットワーク要件

図 9-3のように Device が Host A と Host B からの SNMP のアクセスを許可するように設定します。

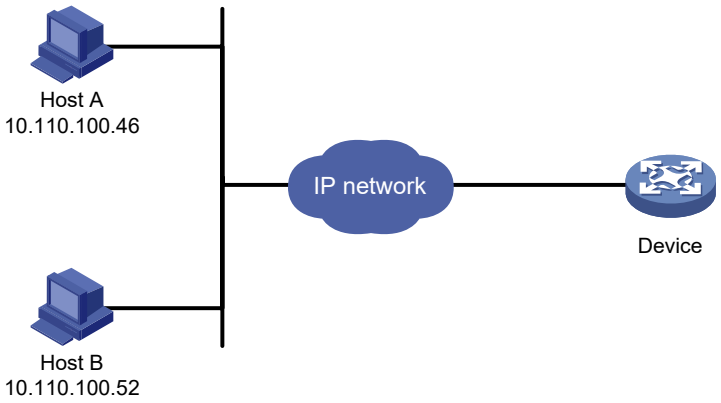


図 9-3 ネットワーク図

II. 設定手順

Host A、Host B からのパケットを許可する ACL を設定します。

```
<Switch> system-view
[Switch] acl basic 2000 match-order  config
[Switch-acl-ipv4-basic-2000]  rule 1 permit source 10.110.100.52  0
[Switch-acl-ipv4-basic-2000]  rule 2 permit source 10.110.100.46  0
[Switch-acl-ipv4-basic-2000]  quit
```

SNMP コミュニティと SNMP グループに関する ACL を適用します。

```
[Switch] snmp-agent  community read aaa acl 2000
[Switch] snmp-agent  group v2c  groupa  acl 2000
[Switch] snmp-agent  usm-user v2c usera groupa  acl 2000
```

目次

このセクションのページは **1-x-x** です。

10 章 FTP.....10-1
10.1 FTP サーバの使用 10-1
10.1.1 認証および許可の設定 10-2
10.1.2 FTP サーバのアクセス制御 10-3
10.1.3 FTP 接続の手動解放 10-3
10.1.4 FTP サーバの表示と維持.....10-3
10.1.5 FTP サーバ設定例.....10-4
10.2 FTP クライアントの使用 10-5
10.2.1 FTP 接続の確立.....10-5
10.2.2 FTP サーバのディレクトリの管理 10-6
10.2.3 FTP サーバの動作.....10-7
10.2.4 別のユーザアカウントへの変更.....10-8
10.2.5 FTP 接続の維持とトラブルシューティング.....10-8
10.2.6 FTP 接続の終了.....10-8
10.2.7 表示コマンドとヘルプ情報.....10-8
10.2.8 FTP クライアントの表示と維持.....10-9
10.2.9 FTP クライアント設定例.....10-9

10章 FTP

FTP （File Transfer Protocol） は、IP ネットワークのサーバとクライアント間でファイルを共有するためのアプリケーションレイヤプロトコルです。FTP を利用することで、ファイルのアップロードやダウンロードが可能です。

FTP はクライアント/サーバモデルで動作します。装置は FTP サーバあるいは FTP クライアントとして動作することができます。



図 10-1 FTPアプリケーションのシナリオ

FTP は、2 つのモードでファイルを送信します。

- **Binary mode**– プログラムファイルの送信に使用します。たとえば、拡張子“**.bin**”、“**.btm**”のファイルです。
- **ASCII mode**– テキストファイルの送信に使用します。たとえば、拡張子“**.txt**”、“**.bat**”、“**.cfg**”のファイルです。

装置が FTP クライアントとして動作する場合、転送モードを設定することができます。デフォルトで binary モードを使用します。

装置が FTP サーバとして動作する場合、転送モードは FTP クライアントによって決定します。

FTP 動作モードは、以下のモードがあります。

- **Active mode（PORT）** – アクティブモードです。FTP サーバはデータ接続リクエストを初期化します。FTP クライアントがプライベートネットワークにあるなどのファイアウォール（Firewall）の内側にある場合、このモードでは使用できません。
- **Passive mode（PASV）** – パッシブモードです。FTP クライアントはデータ接続リクエストを初期化します。サーバ側が、クライアントからランダムポート（1024 以上）で接続することを許可していない場合、使用できません。

FTP 動作モードは、FTP クライアントのプログラムによって変わります。

10.1 FTPサーバの使用

装置を FTP サーバとして使用する場合、装置で FTP サーバを有効にし、認証と許可の設定を行ってください。ほかのコマンドはオプションです。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. FTP を有効にする	**ftp server enable**	デフォルト：無効

操作	コマンド	補足
3.　（オプション設定項目）FTP サーバのアクセス管理を行うため ACL を使用する	**ftp server acl** { *ipv4-acl-number* | **ipv6** *ipv6-acl-number* }	デフォルト：設定なし
4.　（オプション設定項目）idle-timeout タイマを設定する	**ftp timeout** *minutes*	デフォルト：30分 アイドルタイムアウト時間内にFTPサーバとFTPクライアント間で情報のやり取りがなければ、FTP接続は終了します。
5.　（オプション設定項目）送信 FTP パケットの DSCP 値を設定する	● IPv4で動作するFTPサーバ： **ftp server dscp** *dscp-value* ● IPv6で動作するFTPサーバ： **ftp server ipv6 dscp** *dscp-value*	デフォルト：0
6.　（オプション設定項目）現在のログインユーザの最大数を設定する	**aaa session-limit ftp** *max-sessions*	デフォルト：32 この変更はオンラインユーザに影響しません。FTPユーザの現在の数が新しい設定の値以上ならば、オンラインユーザがログアウトするまで、どの追加のFTPユーザもログインすることができません。詳細は、コマンドマニュアルのセクション9 *セキュリティ”AAA”* を参照してください。

10.1.1 認証および許可の設定

FTP サーバは、FTP クライアントを認証し、認証されたクライアントがアクセスできる用に許可されたディレクトリを設定する必要があります。

以下の認証モードが有効です。

- **ローカル認証**– 装置はローカルユーザ名データベースのクライアントのユーザ名とパスワードを確認し、もし一致している場合、認証が成功します。
- **リモート認証**– 装置は認証を行うため、クライアントのユーザ名とパスワードをリモート認証サーバに送信します。ユーザの名は、装置ではなくリモート認証サーバに設定されています。

以下の許可モードが有効です。

- **ローカル許可**– 装置は、ローカルに設定された許可の属性に従い、FTP クライアントのディレクトリを割り当てます。
- **リモート許可**– リモート許可サーバは装置で許可されるディレクトリを FTP クライアントに割り当てます。

認証と許可の詳細は、コマンドマニュアルのセクション 9 *セキュリティ”AAA”* を参照してください。

10.1.2 FTP サーバのアクセス制御

I. FTP サーバのアクセス制御について

ACL は許可されていないアクセスを防ぐために使用します。適用されている ACL が存在しない、あるいはルールがないバイ、ログインの制限は適用されません。ACL が存在し、ルールがある場合、ACL によって許可されている FTP クライアントのみが装置にアクセス可能です。

II. 制限とガイドライン

この設定は FTP 接続を確立する場合のみ適用されます。既存の FTP 接続には適用されません。FTP サーバのアクセス制御を複数行った場合、最後に行った設定が適用されます。

III. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. (オプション設定項目) FTP サーバのアクセス管理を行うため ACL を使用する	**ftp server acl** { *advanced-acl-number* | *basic-acl-number* | **ipv6** { *advanced-acl-number* | *basic-acl-number* } }	デフォルト：設定なし
3. FTP ログイン制御 ACL によって拒否された FTP ログイン試行のログを有効にする	**ftp server acl-deny-log enable**	デフォルト：無効

10.1.3 FTP 接続の手動解放

操作	コマンド
FTP接続を手動で開放する	• 指定したユーザ名を使用して確立したFTP接続を開放する： **free ftp user** *username* • 指定したIPアドレスを使用して確立したFTP接続を開放する： **free ftp user-ip** [**ipv6**] *client-address* [**port** *port-num*]

10.1.4 FTP サーバの表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
FTPサーバの設定とステータス情報を表示する	**display ftp-server**
オンラインFTPユーザの詳細情報を表示する	**display ftp-user**

10.1.5 FTP サーバ設定例

I. ネットワーク要件

- 装置は FTP サーバとして設定します。
- FTP サーバにユーザ名 **abc**、パスワード **123456** のローカルユーザアカウントを作成します。
- ユーザアカウントは、FTP クライアントから FTP サーバにログインするために使用します。
- FTP クライアントから FTP サーバにファイル **temp.bin** をアップグレードします。
- FTP サーバから FTP クライアントにバックアップ用として設定ファイル **config.cfg** をダウンロードします。

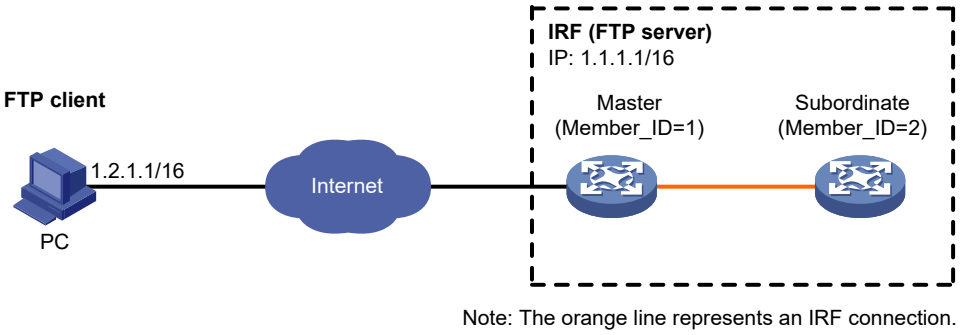


図 10-2 ネットワーク図

II. 設定手順

1) 図 10-2に示すように IP アドレスを設定し、IRF スタックユニットと PC で互いに通信できることを確認します。（詳細は省略します。）
2) FTP サーバを設定します。

IRF スタックメンバ装置の記憶領域を確認します。もし空き容量が不十分である場合、不要なファイルを削除するため、**delete /unreserved** *file-url* コマンドを使用します。（詳細は省略します）

ローカルユーザアカウント **abc**、パスワード **123456** のローカルユーザを作成します。

```
<Switch> system-view
[Switch] local-user abc class manage
[Switch-luser-abc] password simple 123456
```

#ユーザにユーザロール network-admin を割り当てます。マスタ装置のフラッシュメモリのルートディレクトリに作業ディレクトリを設定します。（メンバ装置のフラッシュメモリのルートディレクトリに作業ディレクトリを設定する場合、スロット番号を含め、**authorization-attribute** コマンドの flash:/を slot2#flash:/.に置き換えてください。）

```
[Switch-luser-abc] authorization-attribute user-role network-admin work-directory flash:/
```

サービスタイプ FTP をユーザに割り当てます。

```
[Switch-luser-abc] service-type ftp
[Switch-luser-abc] quit
```

FTP ユーザを有効にします。

```
[Switch] ftp server enable
[Switch] quit
```

3)　FTP クライアントから FTP を実行します。

ローカルユーザアカウント **abc**、パスワード **123456** で FTP サーバ 1.1.1.1 にログインします。

```
c:\> ftp 1.1.1.1
Connected to 1.1.1.1.
220 FTP service ready.
User(1.1.1.1:(none)):abc
331 Password required for abc.
Password:
230 User logged in.
```

FTP 転送モードを ASCII モードに設定し、FTP サーバから PC にバックアップ用の設定ファイル **config.cfg** をダウンロードします。

```
ftp> ascii
200 TYPE is now ASCII
ftp> get config.cfg back-config.cfg
```

FTP 転送モードを binary モードに設定し、PC からマスタのフラッシュのルートディレクトリにファイル **temp.bin** をアップロードします。

```
ftp> binary
200 TYPE is now 8-bit binary
ftp> put temp.bin
```

FTP からログアウトします。

```
ftp> bye
```

10.2 FTPクライアントの使用

10.2.1 FTP 接続の確立

FTP サーバにアクセスするため、FTP クライアントから FTP サーバに接続を確立する必要があります。

以下に IPv4 FTP 接続を確立する設定を示します。

操作	コマンド	補足
1.　system view に移行する	**system-view**	―
2.　（オプション設定項目）送信 FTP パケットの送信元 IP アドレスを設定する	**ftp client source** { **interface** *interface-type interface-number* | **ip** *source-ip-address* }	デフォルト：送信元IPアドレスは、出力インタフェースのプライマリIPアドレスが使用されます。
3.　user view へ戻る	**quit**	―

操作	コマンド	補足
4. FTP サーバにログインする	• （アプローチ1）user viewから直接FTPサーバにログインする：**ftp** [*ftp-server* [*service-port*] [**dscp** *dscp-value* | **source** { **interface** *interface-type interface-number* | **ip** *source-ip-address* }]]* • （アプローチ2） FTP client viewからFTPサーバにログインする： • **ftp** • **open** *server-address* [*service-port*]	**ftp**コマンドで指定された送信元IPアドレスは、**ftp client source**コマンドで指定されたアドレスより優先されます。

以下に IPv6 FTP 接続を確立する設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. （オプション設定項目）送信 FTP パケットの送信元 IPv6 アドレスを設定する	**ftp client ipv6 source** { **interface** *interface-type interface-number* | **ipv6** *source-ipv6-address* }	デフォルト：設定なし 送信元IPv6アドレスは、自動的にRFC3484に従って選択されます。
3. user view へ戻る	**quit**	―
4. FTP サーバにログインする	• （アプローチ1）user viewから直接FTPサーバにログインする：**ftp ipv6** [*ftp-server* [*service-port*]] [**dscp** *dscp-value* | **source** { **ipv6** *source-ipv6-address* | **interface** *interface-type interface-number* }]* [**-i** *interface-type interface-number*]] • （アプローチ2） FTP client viewからFTPサーバにログインする： • **ftp ipv6** • **open** *server-address* [*service-port*]	**ftp ipv6**コマンドで指定された送信元IPアドレスは、**ftp client ipv6 source**コマンドで指定されたアドレスより優先されます。

10.2.2 FTP サーバのディレクトリの管理

操作	コマンド
FTPサーバのディレクトリあるいはファイル情報を表示する	• FTPサーバのディレクトリあるいはファイルの詳細情報を表示する： **dir** [*remotefile* [*localfile*]] • FTPサーバのディレクトリ名あるいはファイル名を表示する： **ls** [*remotefile* [*localfile*]]
FTPサーバの作業ディレクトリを変更する	**cd** { *directory* | **..** | */* }

操作	コマンド
現在のディレクトリを終了して、上位レベルのディレクトリに移行する	**cdup**
FTPサーバの現在のディレクトリを表示する	**pwd**
FTPサーバにディレクトリを作成する	**mkdir** *directory*
リモートFTPサーバで指定した作業ディレクトリを削除する	**rmdir** *directory*

10.2.3 FTP サーバの動作

FTP サーバにログインした後、以下の手順で、許可されたディレクトリからファイルのアップロードあるいはダウンロードすることができます。

1) FTP サーバのディレクトリとファイルの場所を表示するため **dir** コマンドあるいは **ls** コマンドを使用します。
2) 記憶領域の不要なファイルを削除します。
3) FTP 転送モードを設定します。FTP 転送モードは、テキストデータを転送する ASCII モードと、イメージデータを転送する binary モードの 2 つがあります。
4) **lcd** コマンドを使用して、FTP クライアントの作業ディレクトリを変更します。このディレクトリの下にファイルをダウンロードしたり、ダウンロードしたファイルを保存したりすることができます。
5) ファイルのアップロードあるいはダウンロードを行います。

以下に FTP client view で FTP サーバのファイルの動作を示します。

操作	コマンド	補足
FTPサーバのディレクトリあるいはファイル情報を表示する	• FTPサーバのディレクトリあるいはファイルの詳細情報を表示する： **dir** [*remotefile* [*localfile*]] • FTPサーバのディレクトリ名あるいはファイル名の情報を表示する： **ls** [*remotefile* [*localfile*]]	—
FTPサーバの指定したファイルを完全に削除する	**delete** *remotefile*	—
FTP転送モードを設定する	• ASCIIに設定する： **ascii** • バイナリに設定する： **binary**	デフォルト：binary
データ転送モードをpassiveに設定する	**passive**	デフォルト：passive
FTPクライアントの現在の作業ディレクトリを表示あるいは変更する	**lcd** [*directory* | **/**]	—
FTPサーバにファイルをアップロードする	**put** *localfile* [*remotefile*]	—
FTPサーバからファイルをダウンロードする	**get** *remotefile* [*localfile*]	—

操作	コマンド	補足
ローカルファイルをアップロードする	**newer** *remotefile*	―

10.2.4 別のユーザアカウントへの変更

FTP サーバにログインした後、FTP 接続を再確立しないで、ユーザ名を変更することができます。新しいユーザ名とパスワードを正しく入力してください。間違ったユーザ名とパスワードを入力すると接続は切断されます。

別のユーザアカウントに変更するため、user view で以下のコマンドを行います。

操作	コマンド
FTPサーバにログインした後別のユーザアカウントに変更する。	**user** *username* [*password*]

10.2.5 FTP 接続の維持とトラブルシューティング

操作	コマンド	補足
FTPサーバがサポートしているFTP関連コマンドを表示する	**rhelp**	―
FTPサーバがサポートしているFTP関連コマンドのヘルプ情報を表示する	**rhelp** [*protocol-command*]	―
FTP動作の詳細情報の表示を有効あるいは無効にする	**verbose**	デフォルト：有効
FTPクライアントのデバッグを有効あるいは無効にする	**debug**	デフォルト：無効

10.2.6 FTP 接続の終了

操作	コマンド
FTP client viewを終了せずにFTPサーバとの接続を切断する	• **disconnect** • **close**
FTPサーバとの接続を切断し、user viewに戻る	• **bye** • **quit**

10.2.7 表示コマンドとヘルプ情報

以下にサーバにログインした後、ヘルプ情報を表示するコマンドを示します。

操作	コマンド
ヘルプ情報を表示する	• **help** [*command-name*] • **?** [*command-name*]

10.2.8 FTP クライアントの表示と維持

すべての view で **display** コマンドを実行します。

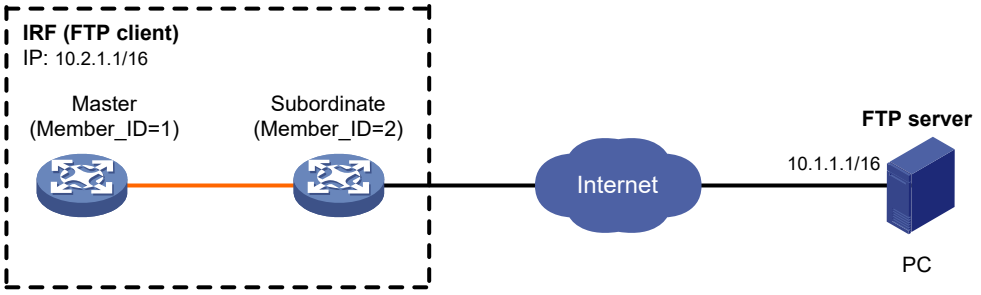
操作	コマンド
FTPクライアントで送信元IPアドレス情報を表示する	**display ftp client source**

10.2.9 FTP クライアント設定例

I. ネットワーク要件

図 10-3に示すように PC は FTP サーバとして動作します。ユーザ名 **abc**、パスワード **123456** のユーザアカウントは PC 上で作成されています。

- FTP クライアントとして IRF スタックユニットが FTP サーバにログインします。
- FTP サーバから FTP クライアントに **temp.bin** ファイルをダウンロードします。
- バックアップ用として FTP クライアントから FTP サーバに設定ファイル **config.cfg** をアップロードします。



Note: The orange line represents an IRF connection.

図 10-3 ネットワーク図

II. 設定手順

#図 10-3に示すように IP アドレスを設定し、IRF スタックユニットと PC で互いに通信できることを確認します。（詳細は省略します。）

IRF スタックのメンバ装置の記憶媒体の空き容量が十分あることを確認します。もし空き容量が十分でない場合、**delete /unreserved** *file-url* コマンドを使用し、不必要なファイルを削除してください。（詳細は省略します。）

ユーザ名 **abc**、パスワード **123456** を使用して、FTP サーバ 10.1.1.1 にログインします。

```
<Switch> ftp 10.1.1.1
Press CTRL+C to abort.
Connected to 10.1.1.1 (10.1.1.1).
220 WFTPD 2.0 service (by Texas Imperial Software) ready for new user
User (10.1.1.1:(none)): abc
331 Give me your password, please
Password:
230 Logged in successfully
Remote system type is MSDOS.
ftp>
```

ファイル転送モードを設定します。

```
ftp> binary
200 TYPE is now 8-bit binary
```

PC から IRF スタックのマスタ装置のフラッシュのルートディレクトリにファイル **temp.bin** をダウンロードします。

```
ftp> get temp.bin
local: temp.bin remote: temp.bin
150 Connecting to port 47457
226 File successfully transferred
23951480 bytes received in 95.399 seconds (251.0 kbyte/s)
```

PC から IRF スタックメンバ ID 2 装置のフラッシュのルートディレクトリにファイル **temp.bin** をダウンロードします。

```
ftp> get temp.bin slot2#flash:/temp.bin
```

FTP 転送モードを ASCII モードに設定し、IRF スタックユニットから PC にバックアップ用に設定ファイル **config.cfg** をアップロードします。

```
ftp> ascii
200 TYPE is now ASCII
ftp> put config.cfg back-config.cfg
local: config.cfg remote: back-config.cfg
150 Connecting to port 47461
226 File successfully transferred
3494 bytes sent in 5.646 seconds (618.00 kbyte/s)
ftp> bye
221-Goodbye. You uploaded 2 and downloaded 2 kbytes.
221 Logout.
<Switch>
```

目次

このセクションのページは **1-x-x** です。

11 章 TFTP.....11-1
11.1 IPv4 TFTP クライアントの設定.....11-1
11.2 IPv6 TFTP クライアントの設定.....11-2

11章 TFTP

TFTP （Trivial File Transfer Protocol）は、FTP を簡略化したプロトコルです。TCP ベースの FTP と比較して TFTP は認証がないあるいはクライアントとサーバ間で複雑なやり取りを必要としないため、より簡単に使用することができます。TFTP は信頼性のあるネットワークで使用する場合に適しています。

装置は TFTP クライアント機能のみをサポートします。装置から TFTP サーバにファイルのアップロードあるいは TFTP サーバから装置にファイルのダウンロードを行うことができます。目的のディレクトリに、同一の名前のファイルがある状態でファイルをダウンロードした場合、既に存在しているファイルは削除され、ダウンロードされたファイルに上書きされます。ネットワークの切断などの理由によってファイルのダウンロードに失敗した場合、もとのファイルを復旧することはできません。そのため同一の名前がないことを確認した後、ファイルの転送を行います。



図 11-1 TFTP アプリケーションシナリオ

11.1 IPv4 TFTPクライアントの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. （オプション設定項目）TFTP サーバにアクセスするクライアントを管理するため ACL を使用する	**tftp-server acl** *acl-number*	デフォルト：設定なし
3. TFTP クライアントの送信元 IP アドレスを設定する	**tftp client source** { **interface** *interface-type interface-number* | **ip** *source-ip-address* }	デフォルト：送信元IPアドレスは、出力インタフェースのプライマリIPアドレスが使用されます。
4. user view へ戻る	**quit**	―
5. IPv4ネットワークでファイルをダウンロードあるいはアップロードする	**tftp** *tftp-server* { **get** | **put** | **sget** } *source-filename* [*destination-filename*] [**dscp** *dscp-value* | **source** { **interface** *interface-type interface-number* | **ip** *source-ip-address* }]*	このコマンドで指定された送信元IPアドレスは、**tftp client source**コマンドで指定されたアドレスより優先されます。 このコマンドはuser viewで使用します。

11.2 IPv6 TFTPクライアントの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. （オプション設定項目）TFTP サーバにアクセスするクライアントを管理するため ACL を使用する	**tftp-server ipv6 acl** *ipv6-acl-number*	デフォルト：設定なし
3. TFTP クライアントの送信元 IPv6 アドレスを設定する	**tftp client ipv6 source** { **interface** *interface-type interface-number* | **ipv6** *source-ipv6-address* }	デフォルト：送信元IPv6アドレスは、RFC3484に従って自動的に選択されます。
4. user view へ戻る	**quit**	ー
5. IPv6 ネットワークでファイルをダウンロードあるいはアップロードする	**tftp ipv6** *tftp-server* [**-i** *interface-type interface-number*] { **get** | **put** | **sget** } *source-filename* [*destination-filename*] [**dscp** *dscp-value* | **source** { **interface** *interface-type interface-number* | **ipv6** *source-ipv6-address* }] *	このコマンドで指定された送信元IPアドレスは、**tftp client ipv6 source**コマンドで指定されたアドレスより優先されます。 このコマンドはuser viewで使用します。

目次

このセクションのページは **1-x-x** です。

12 章 ファイルシステム管理.....12-1
12.1 概要.....12-1
12.1.1 ファイルシステム.....12-1
12.1.2 ディレクトリ.....12-2
12.1.3 ファイル.....12-3
12.1.4 ディレクトリ、ファイル名の指定.....12-3
12.2 ファイルシステムの管理の制限とガイドライン.....12-4
12.3 ファイルシステムの管理.....12-5
12.3.1 記憶媒体のフォーマット.....12-5
12.3.2 記憶媒体の回復.....12-5
12.4 ディレクトリの管理.....12-5
12.4.1 ディレクトリ情報の表示.....12-5
12.4.2 カレント作業ディレクトリの表示.....12-6
12.4.3 カレント作業ディレクトリの変更.....12-6
12.4.4 ディレクトリの作成.....12-6
12.4.5 ディレクトリ名の変更.....12-6
12.4.6 ディレクトリのアーカイブ（圧縮）/解凍.....12-6
12.4.7 ディレクトリの削除.....12-7
12.4.8 ディレクトリの動作モードの設定.....12-7
12.5 ファイルの管理.....12-7
12.5.1 ファイル情報の表示.....12-7
12.5.2 テキストファイルの内容表示.....12-8
12.5.3 ファイル名の変更.....12-8
12.5.4 ファイルのコピー.....12-8
12.5.5 ファイルの移動.....12-8
12.5.6 ファイルの圧縮/解凍.....12-8
12.5.7 ファイルのアーカイブ（圧縮）/解凍.....12-8
12.5.8 ファイルの削除/回復.....12-9
12.5.9 ごみ箱のファイルを削除する.....12-9
12.5.10 ファイルの動作モードの設定.....12-9

12章 ファイルシステム管理

12.1 概要

12.1.1 ファイルシステム

この章では、記録媒体、ディレクトリ、ファイルを含む装置のファイルシステムを管理する方法を示します。

⚠ **重要：**

- 記録媒体、ファイル、ディレクトリを管理する前に、設定が装置に与える影響を確認してから行ってください。
- ピリオド（.）の名前で始まるファイルあるいはディレクトリは、隠しファイルあるいは隠しディレクトリです。ファイルあるいはディレクトリの先頭にピリオド（.）を使用しないでください。
- いくつかの隠しファイルと隠しディレクトリが存在します。ファイルシステムの管理を行う際は、隠しファイルや隠しディレクトリを修正しないでください。

⚠ **注意：**

- 表示される空き容量は実際のファイルサイズで計算されています。保存に必要なサイズはファイルの種類によって実際のファイルサイズと異なる場合がありますので、ファイルの保存は十分な空き容量があることを確認してから行ってください。
- ファイルのダウンロードやコピーを行う場合は、十分な空き容量を確保してから行ってください。空き容量が不足している場合には、エラーとなり異常なファイルが残る場合があります。保存に失敗した場合は、不要なファイルを削除してください。

I. 記憶媒体の命名ルール

装置は 1つのフラッシュメモリをサポートします。フラッシュメモリの名前は flash です。

⚠ **重要：**

- 記憶媒体の名前とスロットの文字列（IRF スタック時）は、小文字で記憶媒体名を入力してください。
- フォルダ名とファイル名は大文字小文字を区別しません。

II. ファイルの位置情報

マスタ装置でファイルシステムを識別する場合、ファイルシステムの位置を指定する必要はありません。IRF スタックのメンバ装置でファイルシステムを識別する場合、**slot*n*#**を指定する必要があります。n は IRF スタックのメンバ ID を示します。たとえば、slot2#はメンバ装置 2 にあるファイルシステムを示します。

III. デフォルトファイルシステム

装置にログインしたのち、デフォルトではデフォルトファイルシステムで動作します。デフォルトファイルのファイルあるいはディレクトリを指定する場合、ファイルシステム名を指定する必要はありません。たとえば、デフォルトファイルシステムのルートディレクトリにカレントコンフィグレーションを保存する場合、すべての位置情報を指定する必要がありません。

デフォルトファイルシステムを変更する場合、BootWare あるいは Boot ROM メニューを使用します。詳細は*インスタレーションマニュアル*を参照してください。

12.1.2 ディレクトリ

ファイルシステムのディレクトリはツリー形状に構成されます。

I. ルートディレクトリ

ルートディレクトリはスラッシュ（/）で示します。たとえば、flash:/はフラッシュメモリのルートディレクトリを示します。

II. 作業ディレクトリ

作業ディレクトリはカレントディレクトリと呼ばれます。

デフォルトの作業ディレクトリはマスタ装置のフラッシュメモリのルートディレクトリです。

III. ディレクトリ命名ルール

ディレクトリの名前を指定する場合、以下のルールに従ってください。

- ディレクトリ名は、英字、数字、以下の文字を除く特殊文字を指定することができます。

  アスタリスク（*）、垂直バー（|）、スラッシュ（/）、バックスラッシュ（\）、クエスチョンマーク（?）、左アングルブラケット（<）、右アングルブラケット（>）、ダブルクォーテーションマーク（"）、コロン（:）
- ドット（.）で始まるディレクトリは隠しディレクトリです。システムがディレクトリを隠さないようにするため、ドット（.）で始まるディレクトリ名を指定しないでください。

IV. 共通使用ディレクトリ

装置はデフォルトのディレクトリがあります。システムは動作中に自動でディレクトリを作成します。以下のディレクトリがあります。

- **diagfile**—診断情報ファイルを記録します。
- **logfile**—ログファイルを記録します。
- **seclog**—セキュリティログファイルを記録します。
- **versionInfo**—ソフトウェアのバージョン情報ファイルを記録します。

12.1.3 ファイル

I. ファイル命名ルール

ファイルの名前を指定する場合、以下のルールに従ってください。

- ファイル名は、英字、数字、以下の文字を除く特殊文字を指定することができます。

  アスタリスク（*）、垂直バー（|）、スラッシュ（/）、バックスラッシュ（\）、クエスチョンマーク（?）、左アングルブラケット（<）、右アングルブラケット（>）、ダブルクォーテーションマーク（"）、コロン（:）
- ドット（.）で始まるファイルは隠しファイルです。システムがファイルを隠さないようにするため、ドット（.）で始まるファイル名を指定しないでください。

II. 共通使用ファイル

装置はデフォルトのファイルがあります。システムは動作中に自動でファイルを作成します。以下のファイルがあります。

- **.ipe file**—圧縮されたソフトウェアイメージの一括ファイル
- **.bin file**—ソフトウェアイメージファイル
- **.cfg file**—コンフィグレーションファイル
- **.mdb file**—バイナリ形式のコンフィグレーションファイル
- **.log file**—ログファイル

12.1.4 ディレクトリ、ファイル名の指定

I. ディレクトリの指定

ディレクトリを指定する場合、絶対パスあるいは相対パスを使用することができます。たとえば、作業ディレクトリは **flash:/**です。図 12-1の test2 ディレクトリを指定する場合、以下の方法を使用することができます。

- flash:/test/test1/test2 （絶対パス）
- flash:/test/test1/test2/ （絶対パス）
- test/test1/test2 （相対パス）
- test/test1/test2/ （相対パス）



図 12-1 ディレクトリ階層の例

II. ファイルの指定

ファイルを指定する場合、以下の方法に従います。

- *filesystem*/*directory1*/*directory2*/…/*directoryn*/*filename* のフォーマットでファイルの絶対パスとファイル名を入力します。ここで *directoryn* はファイルが存在するディレクトリです。
- ファイルの相対パスとファイル名を入力します。

たとえば、作業ディレクトリは **flash:/**です。ファイル samplefile.cfg は、図 12-1の test2 ディレクトリにあります。ファイル samplefile.cfg を指定する場合、以下の方法を使用することができます。

- flash:/test/test1/test2/samplefile.cfg
- test/test1/test2/samplefile.cfg

12.2 ファイルシステムの管理の制限とガイドライン

注意：
ファイル操作中に IRF スタックの Master/Member 装置の切り替えなどは行わないでください。ファイルシステムが破損する恐れがあります。

ファイルシステムの障害を避けるため、ファイルシステムの操作中に以下のことを行わないでください。

- 記憶媒体の挿入あるいは取り外し
- IRF スタックの Master/Member 装置の切り替え

記憶媒体のフォルダやファイルにアクセスしている間に記憶媒体を取り外した場合、装置は再インストールするときに記憶媒体を認識しない可能性があります。このような記憶媒体を再インストールする場合、以下の作業の 1 つを行ってください。

- 記憶媒体のフォルダにアクセスしているとき、カレントディレクトリを変更してください。
- 記憶媒体のファイルにアクセスしているとき、ファイルを閉じてください。
- 別の管理者が記憶媒体にアクセスしていた場合、記憶媒体上をアンマウントしてください。

記録媒体、ファイル、ディレクトリを管理する前に、設定が装置に与える影響を確認してから行ってください。

12.3 ファイルシステムの管理

12.3.1 記憶媒体のフォーマット

注意：
記憶媒体がフォーマットされた後、すべてのファイルとディレクトリは削除され、回復できません。

記憶媒体をフォーマットするとき、他のユーザがアクセスしていないことを確認してください。

user view で以下の操作を実行します。

操作	コマンド
記憶媒体をフォーマットする	**format** *medium-name*

12.3.2 記憶媒体の回復

記憶媒体のスペースが、何らかの異常な操作のためアクセスできない場合、記憶媒体のスペースを回復するために **fixdisk** コマンドを使用できます。

記憶媒体を復旧する前に、他のユーザが記憶媒体へアクセスしていないことを確認してください。そうでないと回復作業は失敗します。

user view で以下の操作を実行します。

操作	コマンド
記憶媒体を回復する	**fixdisk** *filesystem*

12.4 ディレクトリの管理

12.4.1 ディレクトリ情報の表示

user view で以下の操作を実行します。

操作	コマンド
ディレクトリの情報を表示する	**dir** [**/all**] [*file* | *directory* | **/all-filesystems**]

12.4.2 カレント作業ディレクトリの表示

user view で以下の操作を実行します。

操作	コマンド
カレント作業ディレクトリを表示する	**pwd**

12.4.3 カレント作業ディレクトリの変更

user view で以下の操作を実行します。

操作	コマンド
カレント作業ディレクトリを変更する	**cd** { *directory* | **..** | **/** }

12.4.4 ディレクトリの作成

user view で以下の操作を実行します。

操作	コマンド
ディレクトリを作成する	**mkdir** *directory*

12.4.5 ディレクトリ名の変更

user view で以下の操作を実行します。

操作	コマンド
ディレクトリ名を変更する	**rename** *source-directory dest-directory*

12.4.6 ディレクトリのアーカイブ（圧縮）/解凍

ディレクトリをアーカイブ（圧縮）/解凍する場合、ディレクトリの中にあるファイルもアーカイブ（圧縮）/解凍されます。アーカイブ（圧縮）されたディレクトリを表示する場合、ディレクトリの中にあるファイルも解凍されます。

user view で実行可能です。

操作	コマンド
ディレクトリをアーカイブする	**tar create** [**gz**] *archive-file dest-file* [**verbose**] **source** *source-directory* &<1-5>
ディレクトリを解凍する	**tar extract archive-file** *file* [**verbose**] [**screen** | **to** *directory*]
アーカイブされたディレクトリのリストを表示する	**tar list archive-file** *file*

12.4.7 ディレクトリの削除

ディレクトリを削除する場合、ディレクトリ内のすべてのファイルとサブディレクトリを削除する必要があります。ファイルを削除する場合、**delete** コマンドを使用します。サブディレクトリを削除する場合、 **rmdir** コマンド使用します。

ディレクトリを完全に削除すると、ごみ箱のディレクトリ内のすべてのファイルは自動的に完全に削除されます。

user view で以下の操作を実行します。

操作	コマンド
ディレクトリを削除する	**rmdir** *directory*

12.4.8 ディレクトリの動作モードの設定

ファイルシステムには、次のディレクトリの動作モードがあります。

- **alert**：ファイルの破損やデータの損失など、望ましくない結果をもたらす恐れのある操作についてシステムが警告を出します。
- **quiet**：どのような操作に対しても、システムは警告を出しません。

操作ミスによる望ましくない結果を避けるため、**alert** モードがよく使用されます。

以下にディレクトリの動作モードの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. ディレクトリの操作のプロンプトモードを設定する	**file prompt** { **alert** | **quiet** }	デフォルト：**alert** コマンドはファイルの動作モードも設定します。

12.5 ファイルの管理

コピー、ダウンロード、**save** コマンドを使用して、ファイルを作成することができます。ファイルのダウンロードの詳細は、オペレーションマニュアルのセクション 1 *はじめに*”*FTP*”、”*TFTP*”を参照してください。**save** コマンドについては、コマンドマニュアルのセクション 1 *はじめに*”*コンフィグレーションファイル管理*”を参照してください。

12.5.1 ファイル情報の表示

user view で以下の操作を実行します。

操作	コマンド
ファイルの情報を表示する	**dir** [**/all**] [*file* | *directory* | **/all-filesystems**]

12.5.2 テキストファイルの内容表示

user view で以下の操作を実行します。

操作	コマンド
テキストファイルの内容を表示する	**more** *file-url*

12.5.3 ファイル名の変更

user view で以下の操作を実行します。

操作	コマンド
ファイル名を変更する	**rename** *source-file dest-file*

12.5.4 ファイルのコピー

user view で以下の操作を実行します。

操作	コマンド
ファイルをコピーする	**copy** *source-file dest-file*

12.5.5 ファイルの移動

user view で以下の操作を実行します。

操作	コマンド
ファイルを移動する	**move** *source-file* { *dest-file* | *dest-directory* }

12.5.6 ファイルの圧縮/解凍

user view で以下の操作を実行します。

操作	コマンド
ファイルを圧縮する	**gzip** *file*
ファイルを解凍する	**gunzip** *file*

12.5.7 ファイルのアーカイブ（圧縮）/解凍

user view で実行可能です。

操作	コマンド
ファイルをアーカイブする	**tar create** [**gz**] *archive-file dest-file* [**verbose**] **source** *source-file*&<1-5>

操作	コマンド
ファイルを解凍する	**tar extract archive-file** *file* [**verbose**] [**screen** | **to** *directory*]
アーカイブされたファイルのリストを表示する	**tar list archive-file** *file*

12.5.8 ファイルの削除/回復

ファイルを完全に削除あるいは、再利用できるようにごみ箱に移動することができます。ごみ箱に移動したファイルは回復できますが、完全に削除したファイルは回復できません。

ごみ箱のファイルは、記憶媒体のスペースを使用します。ごみ箱のファイルを削除するには、**reset recycle-bin** コマンドを実行します。

user view で以下の操作を実行します。

操作	コマンド
ファイルをごみ箱に移す	**delete** *file*
ファイルをごみ箱から元に戻す	**undelete** *file*
ファイルを完全に削除する	**delete /unreserved** *file*

重要：
ごみ箱のファイルを削除するために **delete** コマンドを使用しないでください。**reset recycle-bin** コマンドを使用してください。

12.5.9 ごみ箱のファイルを削除する

記憶媒体は**.trash** というごみ箱を使用します。ごみ箱のファイルを表示するには以下の方法を使用します。

- 記憶媒体に移動し、**dir /all .trash** コマンドを実行します。
- ごみ箱のフォルダに移動するため、**cd .trash** コマンドを実行し、**dir** コマンドを実行します。

user view でごみ箱のファイルを削除するには以下の操作を実行します。

操作	コマンド
カレントディレクトリ下で、ごみ箱でファイルを削除する	**reset recycle-bin** [**/force**]

12.5.10 ファイルの動作モードの設定

ファイルシステムには、次のファイルの動作モードがあります。

- **alert**：ファイルの破損やデータの損失など、望ましくない結果をもたらす恐れのある操作についてシステムが警告を出します。
- **quiet**：どのような操作に対しても、システムは警告を出しません。

操作ミスによる望ましくない結果を避けるため、**alert** モードがよく使用されます。

以下にファイルの動作モードの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． ファイルの操作のプロンプトモードを設定する	**file prompt** { **alert** | **quiet** }	デフォルト：**alert** コマンドはディレクトリの動作モードも設定します。

目次

このセクションのページは **1-x-x** です。

13 章 コンフィグレーションファイル管理.....13-1
13.1 概要.....13-1
13.1.1 コンフィグレーションタイプ.....13-1
13.1.2 次回の起動に使用するスタートアップコンフィグレーションファイルの冗長..13-2
13.1.3 コンフィグレーションファイルのフォーマット形式.....13-2
13.1.4 スタートアップコンフィグレーションファイルの選択.....13-2
13.1.5 コンフィグレーションファイルの内容とフォーマット.....13-3
13.2 2 つのコンフィグレーション設定の差分表示.....13-3
13.3 カレントコンフィグレーションの保存.....13-4
13.3.1 制限とガイドライン.....13-4
13.3.2 カレントコンフィグレーションの保存方法.....13-5
13.4 次回の起動に使用するスタートアップコンフィグレーションファイルの設定.....13-6
13.5 TFTP サーバへスタートアップコンフィグレーションファイルのバックアップ.....13-7
13.6 TFTP サーバからスタートアップコンフィグレーションファイルの復元.....13-7
13.7 次回の起動で使用するスタートアップコンフィグレーションファイルの削除.....13-8
13.8 コンフィグレーションファイルの表示と維持.....13-9

13章 コンフィグレーションファイル管理

13.1 概要

コンフィグレーションファイルは、CLI あるいは Boot メニューから管理することができます。この章では CLI からコンフィグレーションファイルを管理する方法を記載します。

コンフィグレーションファイルには、装置のソフトウェア機能を設定するためのコマンドのセットが保存されます。設定はコンフィグレーションファイルに保存できるため、設定は再起動後にも適用されます。将来使用するために、コンフィグレーションファイルをホストにバックアップすることもできます。

13.1.1 コンフィグレーションタイプ

装置起動時に読み込まれた設定はスタートアップコンフィグレーションと呼ばれ、装置で動作している設定はカレントコンフィグレーションと呼ばれます。

以下にコンフィグレーションファイルの種類を示します。

I. デフォルトコンフィグレーション

初回起動時のコンフィグレーション設定で、装置固有のコンフィグレーション設定です。ファイルは”.ipe”の拡張子のパッケージファイルでリリースされ、変更できません。コンフィグレーションファイルあるいはスタートアップコンフィグレーションファイルが存在しない場合、デフォルトコンフィグレーションで起動します。

デフォルトコンフィグレーションの設定を表示するには、**display default-configuration** コマンドを使用します。

II. スタートアップコンフィグレーション

ブートメニューあるいは CLI で指定されるコンフィグレーションファイルです。このファイルは次回の起動で使用するスタートアップコンフィグレーションファイルと呼ばれます。スタートアップコンフィグレーションで起動されたのち、カレントコンフィグレーションファイルと呼ばれます。システムの信頼性のため、メインとバックアップの 2 つの次回の起動で使用するスタートアップコンフィグレーションファイルを指定することができます。（詳細はオペレーションマニュアルのセクション 1 *はじめに*”*コンフィグレーションファイル管理*”の”*次回の起動で使用するメインコンフィグレーションファイル*”を参照してください。）

- カレントコンフィグレーションと次回の起動で使用するスタートアップコンフィグレーションの設定を表示するには、**display startup** コマンドを使用します。詳細な設定を表示する場合、**more** コマンドを使用します。

- 次回の起動で使用するコンフィグレーションファイルの内容を表示するには、**display saved-configuration** コマンドを使用します。次回の起動で使用するコンフィグレーションファイルが保存されていない場合は表示されません。

III. カレントコンフィグレーション

装置が動作している現在のコンフィグレーションです。カレントコンフィグレーションはスタートアップコンフィグレーションと新しく設定したコンフィグレーションとなります。カレントコンフィグレーションは装置の一時的な記憶媒体に記録され、保存をしていない場合は、装置の電源 OFF/ON あるいは **reboot** コマンドを実行するときに削除されます。設定を削除しないようにするには、コンフィグレーションファイルにカレントコンフィグレーションを保存します。

カレントコンフィグレーションは **display current-configuration** コマンドを使用して表示することができます。表示されるパラメータはデフォルトコンフィグファイルのパラメータを含みません。

13.1.2 次回の起動に使用するスタートアップコンフィグレーションファイルの冗長

1つの次回の起動に使用するコンフィグレーションファイルとバックアップのコンフィグレーションファイルを指定することができます。

起動時、装置は以下の順番でスタートアップコンフィグレーションファイルの読み込みを行います。

1) メインの次回の起動に使用するコンフィグレーションファイルで起動します。
2) 指定したメインスタートアップファイルがない、あるいは有効でない場合、バックアップの次回の起動に使用するコンフィグレーションファイルで起動します。
3) 指定したバックアップコンフィグレーションファイルがない、あるいは有効でない場合、装置はデフォルトのコンフィグレーションファイルで起動します。

13.1.3 コンフィグレーションファイルのフォーマット形式

コンフィグレーションファイルは、以下のフォーマット形式となります。

拡張子は、“.cfg”を使用する必要があります。“.cfg”ファイルはテキストファイルです。**more** コマンドで内容を表示することができます。“.cfg”で設定を保存したとき、装置は自動的に、同一ファイル名で拡張子が“.mdb”というバイナリデータを保存します。装置は”.mdb“の方が”.cfg“よりも速く読み込みます。

13.1.4 スタートアップコンフィグレーションファイルの選択

起動時、装置は以下の順番でコンフィグレーションファイルを識別します。

1) 装置は有効な“.cfg”の次回の起動で使用するコンフィグレーションファイルを検索します。

2) ファイルが見つかった場合は、“.cfg”と名前と内容が同じ“.mdb”ファイルを検索します。
3) “.mdb”ファイルが見つかった場合は、その“.mdb”ファイルを起動で使用するコンフィグレーションファイルとします。見つからなかった場合は、“.cfg”ファイルを起動で使用するコンフィグレーションファイルとします。

本章で記載するコンフィグレーションファイルは、特に指定がない限り“.cfg”のコンフィグレーションファイルを示します。

13.1.5 コンフィグレーションファイルの内容とフォーマット

重要：
装置を起動するため、コンフィグレーションファイルは、装置で使用する規則とフォーマット形式に従う必要があります。起動時、コンフィグレーションファイルの読み込み失敗を防ぐため、装置で自動に作成されたコンフィグレーションファイルあるいは **save** コマンドを使用してください。もしコンフィグレーションファイルを編集する場合、装置で使われる規則とフォーマットにあわせてください。

コンフィグレーションファイルは以下の規則に従います。

- すべてのコマンドは省略されていない正しい形式のフォーマットで保存されます。
- コマンドは view 毎にセクションに分かれて区別されています。通常は system view、interface view、protocol view、line view などの順番です。
- セクションは、1 行または複数行のブランク行またはコメント行（#）で区切られます。
- 最後に **return** が付きます。

コンフィグレーションファイルを抜粋した例を以下に示します。

```
#
local-user root class manage
 password                                                                hash
$h$6$Twd73mLrN8O2vvD5$Cz1vgdpR4KoTiRQNE9pg33gU14Br2p1VguczLSVyJLO2huV5Syx/LfD
If8ROLtVErJ/C31oq2rFtmNuyZf4STw==
 service-type ssh telnet terminal
 authorization-attribute user-role network-admin
 authorization-attribute user-role network-operator
#
interface Vlan-interface1
 ip address 192.168.1.84 255.255.255.0
#
```

13.2 2つのコンフィグレーション設定の差分表示

2 つのコンフィグレーションファイルで設定の差分を表示することができます。

比較を行うため次回の起動で使用するコンフィグレーションファイルを指定した場合、システムは以下の順番で次回の起動で使用するコンフィグレーションファイルを検索します。

1) 次回の起動で使用するメインコンフィグレーションファイルを検索します

2) 次回の起動で使用するメインコンフィグレーションファイルが有効でない、あるいは不正である場合、次回の起動で使用するバックアップコンフィグレーションファイルを検索します。

メインコンフィグレーションファイルとバックアップコンフィグレーションファイルの両方が有効でない、あるいは不正である場合、次回の起動で使用するコンフィグレーションファイルが存在しませんと表示します。

2 つのコンフィグレーションファイルの設定の差分を表示する方法を以下に示します。

すべての view で **display** コマンドを実行します。

操作	コマンド
指定された2つのコンフィグレーションファイルの差分を表示する	**display diff configfile** *file-name-s* **configfile** *file-name-d*
指定されたコンフィグレーションファイルとカレントコンフィグレーションファイルの差分を表示する	● 方法1： **display diff configfile** *file-name-s* **current-configuration** ● 方法2： **display diff current-configuration configfile** *file-name-d*
指定されたコンフィグレーションファイルと次回の起動で使用するコンフィグレーションファイルの差分を表示する	● 方法1： **display diff configfile** *file-name-s* **startup-configuration** ● 方法2： **display diff startup-configuration configfile** *file-name-d*
次回の起動で使用するコンフィグレーションファイルとカレントコンフィグレーションファイルの差分を表示する	● 方法1： **display diff current-configuration startup-configuration** ● 方法2： **display current-configuration diff** ● 方法3： **display diff startup-configuration current-configuration**

13.3 カレントコンフィグレーションの保存

13.3.1 制限とガイドライン

複数の装置で構成される IRF スタックユニットでは、カレントコンフィグレーションを保存する前に IRF スタックトポロジが正しいかどうか確認するため **display irf** コマンドを使用します。IRF スタックユニットの分裂によりメンバ装置が離脱した後でも、メンバ装置には、カレントコンフィグレーションファイルと次回の起動に使用するコンフィグレーションファイルが保持されています。しかし IRF スタックユニットが回復する前にカレントコンフィグレーションファイルを保存するため、次回の起動で使用するコンフィグレーションファイルからメンバ装置の設定を削除します。

IRF スタックユニットの分裂の後、カレントコンフィグレーションを次回の起動に使用するスタートアップコンフィグレーションファイルに保存していた場合、以下に次回の起動に使用するスタートアップコンフィグレーションファイルを回復する方法を示します。

1) IRF スタックユニットが分裂した問題を回復します。
2) 装置が IRF スタックユニットに再加入した後、メンバ装置を再起動します。
3) メンバ装置の設定が IRF スタックユニットのカレントコンフィグレーションに残されているか確認するため、**display current-configuration** コマンドを実行します。

- □ メンバ装置の設定が残っている場合、IRF スタックユニットのカレントコンフィグレーションを次回の起動に使用するコンフィグレーションファイルに保存します。
- □ メンバ装置の設定が残っていない場合、IRF スタックユニットのメンバ装置を再度設定する必要があります。そしてカレントコンフィグレーションを次回の起動に使用するコンフィグレーションファイルに保存します。

重要：
正常なコンフィグレーションファイルを回復させるため、IRF スタックユニットからメンバ装置を取り外したのち、IRF スタックユニットが再起動していないことを確認してください。

13.3.2 カレントコンフィグレーションの保存方法

カレントコンフィグレーションをコンフィグレーションファイルに保存するとき、次回に起動するコンフィグレーションファイルとして指定することができます。

次回に起動するコンフィグレーションファイルとしてファイルを指定する場合、以下に示すどちらかの方法で、カレントコンフィグレーションの保存を行ってください。

- **高速保存モード**– **safely** キーワードを使わないで **save** コマンドを使用します。より速くファイルを保存しますが、装置が再起動、または処理中に電源が切れた場合、カレントコンフィグレーションファイルを失う可能性があります。装置を再起動した後、新しいスタートアップコンフィグレーションファイルを指定してください。（オペレーションマニュアルのセクション 1 *はじめに*”*コンフィグレーションファイル管理*”の”*次回の起動で使用するスタートアップコンフィグレーションファイルの指定*”を参照してください）
- **セーフモード**– **safely** キーワードを使い **save** コマンドを使用します。高速ではありませんが、装置が再起動、または処理中に電源切れた場合でも、装置でコンフィグレーションファイルを保持することができます。

高速保存モードは、電力供給が安定している環境に適しています。セーフモードは、安定した電力供給が利用できない、あるいは、リモートメンテナンスが複雑になる環境に適しています。

すべての view でカレントコンフィグレーションを保存する方法を以下に示します。

操作	コマンド	補足
指定したファイルに現在の設定を保存します、しかし、コンフィグレーションファイルは次回起動時にファイルとしてセットされません。	**save** *file-url* [**all** | **slot** *slot-number*]	—

操作	コマンド	補足
現在の設定をコンフィグレーションファイルに保存し、次回の起動に使用するスタートアップコンフィグレーションファイルに指定する	**save** [**safely**] [**backup** | **main**] [**force**]	このコマンドは記憶媒体のルートディレクトリのファイルに設定を保存します。 IRFスタックユニットのすべての装置に設定を保存します。 信頼性のあるファイルの保存を行うため、**safety**パラメータを使用することを推奨します。 **force**パラメータを指定した場合、設定は次回の起動に使用されるコンフィグレーションファイルに保存されます。 **force**パラメータを指定しない場合、次回の起動に使用するスタートアップコンフィグレーションファイルを新規作成します。

13.4 次回の起動に使用するスタートアップコンフィグレーションファイルの設定

⚠ **注意：**

IRF スタックユニットにおいて **undo startup saved-configuration** コマンドを使用した場合、IRF スタックユニットの再起動後あるいは IRF スタックメンバの再起動後に IRF スタックの分裂を引き起こす原因となりますので注意してください。

カレントコンフィグを保存するとき、**save** [**safely**] [**backup** | **main**] [**force**]コマンドを使用して、次回の起動で使用するメイン、バックアップ、あるいはその両方のスタートアップコンフィグレーションファイルとして、“.cfg”コンフィグレーションファイルを指定することができます。

また **startup saved-configuration** *cfgfile* [**backup** | **main**]コマンドを使用して次回の起動で使用するメインあるいはバックアップのスタートアップコンフィグレーションファイルを指定することができます。指定したスタートアップコンフィグレーションファイルが有効で、各メンバ装置のデフォルトの記憶領域のルートディレクトリに保存されることを確認してください。

次回の起動に使用するメインあるいはバックアップのスタートアップコンフィグレーションファイルを同一に設定することができますが、高可用性のため、スタートアップコンフィグレーションファイルを分けてください。

undo startup saved-configuration コマンドは次回の起動に使用するメインあるいはバックアップのスタートアップコンフィグレーションファイルを削除する代わりに NULL に変更します。

以下に、user view で、次回の起動に使用するスタートアップコンフィグレーションファイルを指定する設定を示します。

操作	コマンド	補足
次回の起動に使用するスタートアップコンフィグレーションファイルを指定する	**startup saved-configuration** *cfgfile* [**backup** | **main**]	デフォルト：設定なし **backup**あるいは**main**のいずれのキーワードも指定されない場合、次回の起動に使用するメインのスタートアップコンフィグレーションファイルとして保存されます。 設定を確認するには、すべてのviewで**display startup** コマンドと**display saved-configuration**を使用します。

13.5 TFTPサーバへスタートアップコンフィグレーションファイルのバックアップ

バックアップを行う前に、以下の要件が完了していることを確認してください。

- 装置と TFTP サーバ間が通信可能であることを確認してください。
- TFTP サービスが有効にされていることを確認してください。
- 読み書き許可があることを確認してください。

以下に、次回の起動に使用するメインのスタートアップコンフィグレーションファイルを TFTP サーバにバックアップする設定を示します。

操作	コマンド	補足
1.　（オプション設定項目）user view で指定されたスタートアップコンフィグレーションファイルを確認する	**display startup**	スタートアップコンフィグレーションファイルが指定されていない場合、バックアップは失敗します。
2.　user view で TFTP サーバにスタートアップコンフィグレーションファイルをバックアップする	**backup startup-configuration to** *ipv4-server* [*dest-filename*]	—

13.6 TFTPサーバからスタートアップコンフィグレーションファイルの復元

TFTP サーバから装置の次回の起動に使用するメインのスタートアップコンフィグレーションファイルを復元する場合、装置は以下の作業を行います。

- 各メンバ装置のデフォルトの記憶媒体のルートディレクトリに、TFTP サーバからコンフィグレーションファイルをダウンロードします。
- 次回の起動で使用するメインのスタートアップコンフィグレーションファイルを指定します。

次回の起動に使用するメインのスタートアップコンフィグレーションファイルを復元する前に、以下の要件が完了していることを確認してください。

- サーバが到達可能であることを確認してください。
- TFTP サービスが有効にされていることを確認してください。
- 読み書き許可があることを確認してください。

以下に TFTP サーバからスタートアップアップコンフィグレーションファイルを復元する操作を示します。

操作	コマンド	補足
1. user view で TFTP サーバからスタートアップコンフィグレーションファイルを復元する	**restore startup-configuration from** *ipv4-server src-filename*	—
2. （オプション設定項目）メインの次回の起動で使用するように指定されたコンフィグレーションファイルが設定されていることを確認する	**display startup** **display saved-configuration**	—

13.7 次回の起動で使用するスタートアップコンフィグレーションファイルの削除

注意：

この作業を行うと、次回の起動で使用するスタートアップコンフィグレーションファイルを、IRF スタックユニットのすべての装置から完全に削除します。削除を行う前に必要に応じてバックアップを行ってください。

次のいずれかの理由である場合、次回の起動時のスタートアップコンフィグレーションファイルを削除する必要があります。

- システムソフトをアップグレードさせた後、既存のコンフィグレーションファイルが、新しいシステムソフトウェアに合わない場合。
- コンフィグレーションファイルが破損している、あるいは不完全である場合。

メインとバックアップの次回の起動で使用するコンフィグレーションファイルを削除した場合、次回の起動時にデフォルトコンフィグレーションで起動します。

メインとバックアップの両方の次回の起動で使用するスタートアップコンフィグレーションファイルを削除するため、**reset saved-configuration backup** コマンドと **reset saved-configuration main** コマンドを実行する必要があります。このコマンドを行う前は、ファイルを削除する代わりに、属性を削除します。

たとえば **reset saved-configuration backup** コマンドが行われると、バックアップの次回の起動で使用するスタートアップコンフィグレーションファイルの属性が NULL になり、ファイルがメインファイルとして使用されます。ファイルを削除する場合、**reset saved-configuration main** コマンドを行う必要があります。

以下に user view で次回の起動時のスタートアップコンフィグレーションファイルを削除する操作を示します。

操作	コマンド	補足
次回の起動時のスタートアップコンフィグレーションファイルを削除する	**reset saved-configuration** [**backup** | **main**]	**backup**あるいは**main**の両方が指定されない場合、mainのスタートアップコンフィグレーションファイルが削除されます。

13.8 コンフィグレーションファイルの表示と維持

すべての view で **display** コマンドを実行します。

操作	コマンド
カレントコンフィグレーションを表示する	**display current-configuration** [[**configuration** [*module-name*] | **interface** [*interface-type* [*interface-number*]]]]
カレントコンフィグレーションファイルと次回の起動に使用するコンフィグレーションファイルの差分を表示する	**display current-configuration diff**
デフォルトコンフィグレーションを表示する	**display default-configuration**
2つのコンフィグレーションファイルの設定の差分を表示する	• **display diff configfile** *file-name-s* { **configfile** *file-name-d* | **current-configuration** | **startup-configuration** } • **display diff current-configuration** { **configfile** *file-name-d* | **startup-configuration** } • **display diff startup-configuration** { **configfile** *file-name-d* | **current-configuration** }
記憶媒体に保存されたコンフィグレーションファイルを表示する	**display saved-configuration**
今回および次回の起動に使用するコンフィグレーションファイルを表示する	**display startup**
現在のviewで有効な設定を表示する	**display this**
次回の起動時に使用するコンフィグレーションファイルを削除する	**reset saved-configuration** [**backup** | **main**]

目次

このセクションのページは **1-x-x** です。

14 章 ソフトウェアのアップグレード 14-1
14.1 概要.....14-1
14.1.1 ソフトウェアタイプ.....14-1
14.1.2 ソフトウェアファイル名の規則.....14-1
14.1.3 Comware イメージの冗長性と読み込み手順.....14-2
14.1.4 システム起動プロセス.....14-2
14.2 アップグレード方法.....14-3
14.3 アップグレードの制限とガイドライン.....14-4
14.4 アップグレードの準備.....14-4
14.5 アップグレード設定作業リスト.....14-5
14.6 Boot ROM の Boot ROM イメージへの読み込み.....14-5
14.7 スタートアップソフトウェアイメージの指定とアップグレードの完了.....14-5
14.8 ソフトウェア設定の表示と維持.....14-6
14.9 CLI によるソフトウェアアップグレード例.....14-7
14.9.1 再起動によるソフトウェアアップグレード例.....14-7

14章 ソフトウェアのアップグレード

14.1 概要

ソフトウェアアップグレードは、新しい機能の追加や不具合を修正するために行います。

アップグレードを行う前に、新しいソフトウェアのリリースメモを確認して、装置とソフトウェアの互換性およびアップグレードが与える影響を確認してください。

14.1.1 ソフトウェアタイプ

以下にソフトウェアタイプを示します。

- **BootWare イメージ**－Boot ROM イメージとも呼ばれます。”.bin”ファイルは基本セグメントと拡張セグメントが含まれます。基本セグメントはシステムを起動する最小のコードです。拡張セグメントはハードウェア初期化を有効にし、システム管理メニューを提供します。装置が正常に起動しないときに、これらのメニューを使用してソフトウェアとスタートアップコンフィグレーションファイルあるいは管理ファイルを読み込むことができます。
- **Comware イメージ**– 以下に示すサブカテゴリのソフトウェアがあります。
  - **Boot イメージ**– Linux オペレーションのシステムカーネルを含む拡張子が“.bin”のファイルです。 プロセス管理、メモリ管理、ファイルシステム管理のプロセスを持っています。
  - **System ソフトウェアイメージ**– 装置が動作するのに必要最小限の機能を含む、拡張子が“.bin”のファイルです。装置管理、インタフェース管理、設定管理、ルーティング管理の機能を持っています。

読み込まれるソフトウェアイメージはカレントソフトウェアイメージと呼ばれます。次回起動時に指定したファイルで起動するソフトウェアイメージはスタートアップソフトウェアイメージと呼ばれます。

Boot ROM イメージ、Boot イメージ、System ソフトウェアイメージは、装置が起動するために必要です。イメージは拡張子“.ipe”の 1 つのパッケージファイル（Comware イメージ）にまとめられてリリースされます。Comware イメージをスタートアップソフトウェアイメージとして選択するとき、システムは自動的にファイルを解凍し、拡張子“.bin“のブートとシステムイメージをロードします。

14.1.2 ソフトウェアファイル名の規則

本章では、ブートイメージの名前に **boot.bin**、システムイメージの名前に **system.bin** を使用します。

14.1.3 Comware イメージの冗長性と読み込み手順

Comware イメージは、メインとバックアップの 2 セットを指定することができます。

スタートアップソフトウェアイメージの Boot イメージとシステムイメージは同一のバージョンにする必要があります。

システムは常にメインソフトウェアで起動を試みます。もしメインソフトウェアが存在しないあるいは無効である場合、システムはバックアップソフトウェアで起動を試みます。図 14-1に Comware イメージの読み込み手順の全体を示します。

メインソフトウェアとバックアップ Boot イメージが存在しないあるいは無効である場合、コンソールポートに接続し、Boot メニューから Boot イメージを読み込ませるため、電源の OFF/ON を行ってください。Boot イメージのダウンロードと読み込みの詳細はソフトウェアのリリースメモを参照してください。

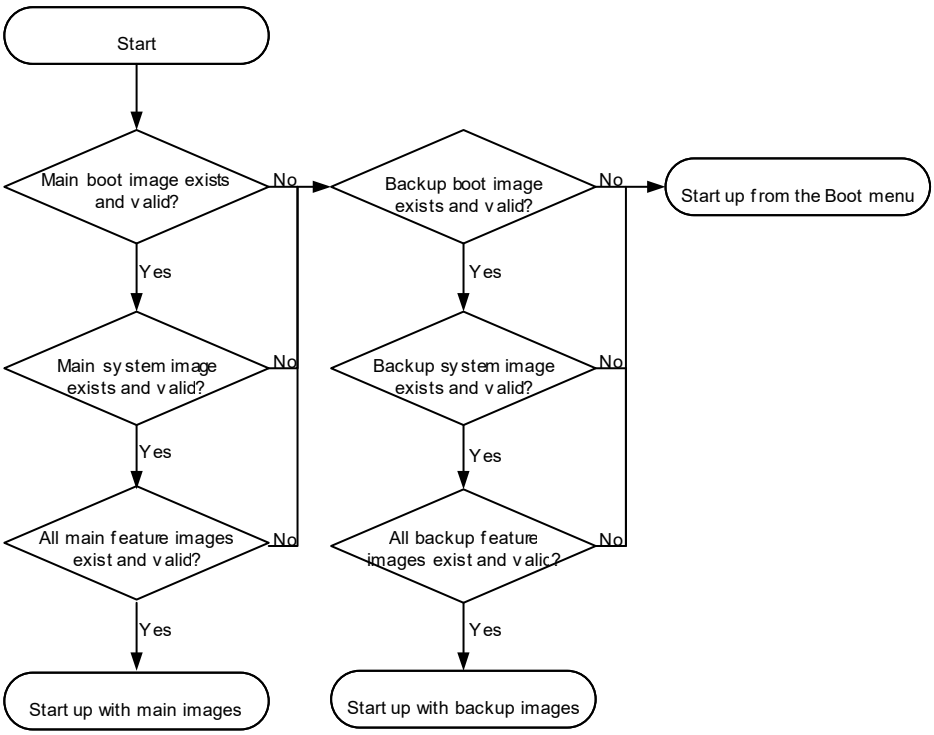


図 14-1 Comware イメージの読み込み手順の全体

14.1.4 システム起動プロセス

装置を起動したのち、ハードウェアを初期化するため Boot ROM イメージ（BootWare イメージ）が起動します。その後、システム全体を動作させるためスタートアップシステムイメージが起動します。

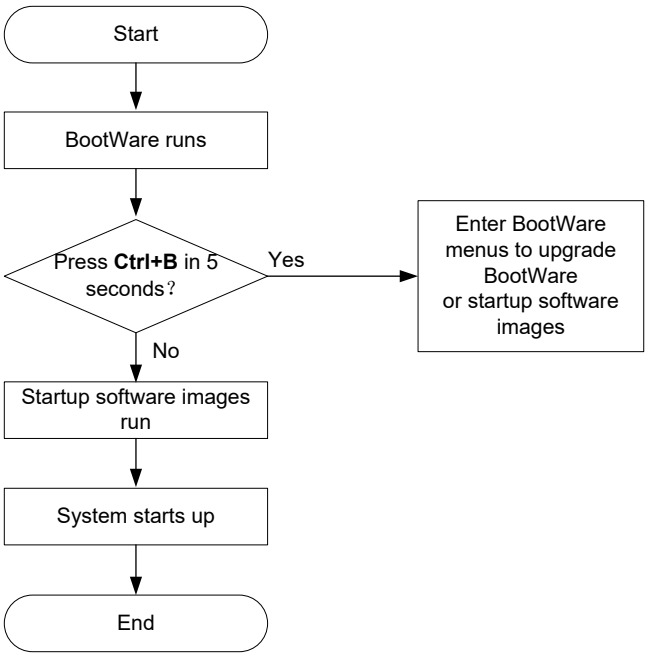


図 14-2 システム起動プロセス

14.2 アップグレード方法

アップグレード方法	ソフトウェアタイプ	補足
CLIからのアップグレード	● Boot ROMイメージ（BootWareイメージ） ● Comwareイメージ	アップグレードを完了するため、再起動が必要となります。ネットワークサービスの中断が発生します。
再起動を伴うソフトウェアのアップグレード	● Comwareイメージ	アップグレードを行うため、装置全体の再起動を行ってください。サービスの中断が発生します。

アップグレード方法	ソフトウェアタイプ	補足
Boot メニューからのアップグレード	• Boot ROMイメージ（BootWareイメージ） • Comwareイメージ	装置が正常に起動しないときに使用します。 最初にコンソールポートに接続し、装置の電源をONにします。その後BootWareメニューにアクセスするため<CTRL+B>を押下します。 BootWareメニューからのアップグレードの詳細は*インストレーションマニュアル*を参照してください。 ⚠ **重要：** IRFスタックのアップデートは、Bootメニューではなく CLIから行ってください。メンバ装置を1台ずつアップデートする必要があるため、Bootメニューではサービスの停止時間が増加します。

この章では CLI からのアップグレードのみ記載します。

14.3 アップグレードの制限とガイドライン

装置はフラッシュメモリからソフトウェアを起動することができます。

14.4 アップグレードの準備

1) 現在の Boot ROM バージョンとスタートアップソフトウェアバージョンを確認するため、**display version** コマンドを使用します。
2) アップグレードソフトウェアバージョンがネットワークに与える影響を確認するため、ソフトウェアアップグレードの以下のことを確認します。
   - □ ソフトウェアとハードウェアの互換性
   - □ ソフトウェアのアップグレードのバージョンとサイズ
   - □ 現在の Boot ROM イメージとアップグレードソフトウェアとの互換性
3) ソフトウェアのアップグレードに十分な記憶媒体を持っているかどうか確認するため、**dir** コマンドを使用します。記憶媒体に十分な空き容量がない場合、不要なファイルを **delete /unreserved** コマンドで完全に削除します。詳細は、オペレーションマニュアルのセクション 1 *はじめに*"*ファイルシステム管理*"を参照してください。
4) FTP あるいは TFTP を使用して、装置の記憶媒体のルートディレクトリにアップグレードソフトウェアファイルをダウンロードします。FTP、TFTP の設定や操作方法についての詳細は、オペレーションマニュアルのセクション 1 *はじめに*"*FTP*"、"*TFTP*"を参照してください。

14.5 アップグレード設定作業リスト

作業リスト	補足
（オプション設定項目）Boot ROMのBoot ROMイメージへの読み込み	ソフトウェアアップグレードを行う際、Boot ROMイメージのアップグレードが必要な場合、Comwareイメージをアップグレードする前に、このコマンドを使用してBoot ROMに新しいBoot ROMイメージをアップグレードします。このコマンドは、予期しない電気的な故障によってアップグレードの失敗が発生するリスクを減少させ、アップグレードを行う時間を削減することができます。 この作業を省略した場合、スタートアップソフトウェアイメージをアップグレードする際に装置は自動的にBootWareをアップグレードします。 Boot ROMイメージは装置を再起動したのち適用します。
（必須設定項目）スタートアップソフトウェアイメージの指定とアップグレードの完了	–

14.6 Boot ROMのBoot ROMイメージへの読み込み

操作	コマンド	補足
Boot ROMイメージを、Boot ROMの通常エリアに読み込む	**bootrom update file** *file* **slot** *slot-number-list*	fileパラメータにフラッシュのBoot ROMイメージが含まれるファイルを指定します。 アップグレードを完了させるために、装置を再起動してください。

14.7 スタートアップソフトウェアイメージの指定とアップグレードの完了

user view で以下の操作を実行します。

操作	コマンド	補足
1. IRF スタックマスタ装置のメインあるいはバックアップスタートアップファイルとしてアップグレードファイルを指定する	• アプローチ1 : **boot-loader file** *ipe-filename* { **all** | **slot** *slot-number* } { **backup** | **main** } • アプローチ2 : **boot-loader file boot** *filename* **system** *filename* { **all** | **slot** *slot-number* } { **backup** | **main** }	アップグレードするファイルはIRFスタックメンバ装置の記憶媒体のルートディレクトリに保存する必要があります。 ファイル名が正しいことを確認してください。 アプローチ1が使用される場合、ファイル名は *storage-medium*:/*base-filename*.**ipe** を使用します。 例 flash:/startup.**ipe** アプローチ2が使用される場合、ファイル名は *storage-medium*:/*base-filename*.**bin** を使用します。 例 flash:/startup-boot.**bin**
2. IRF スタックメンバ装置のメインスタートアップファイルとしてアップグレードファイルを指定する	• アプローチ1 : **boot-loader file** *ipe-filename* { **all** | **slot** *slot-number* } { **backup** | **main** } • アプローチ2 : **boot-loader file boot** *filename* **system** *filename* { **all** | **slot** *slot-number* } { **backup** | **main** }	1台の装置の構成の場合は、この手順をスキップしてください。
3. カレントコンフィグレーションを保存する	**save**	再起動によって設定が削除されないように行います。
4. 装置の再起動	**reboot**	スタートアップ後、各装置はダウンロードされたBoot ROMイメージをRAMに読み込ませ、ファイルのスタートアップソフトウェアを読み込みます。
5. （オプション設定項目）ソフトウェアの設定を確認する	**display boot-loader** [**slot** *slot-number*]	カレントソフトウェアがスタートアップソフトウェアと同一であるか確認します。

14.8 ソフトウェア設定の表示と維持

すべての view で **display** コマンドを実行します。

操作	コマンド
カレントソフトウェアとスタートアップソフトウェアを表示する	**display boot-loader** [**slot** *slot-number*]

14.9 CLIによるソフトウェアアップグレード例

14.9.1 再起動によるソフトウェアアップグレード例

I. ネットワーク要件

IRF スタックユニットの装置にファイル **startup-a2105.ipe** を使用してソフトウェアをアップグレードします。

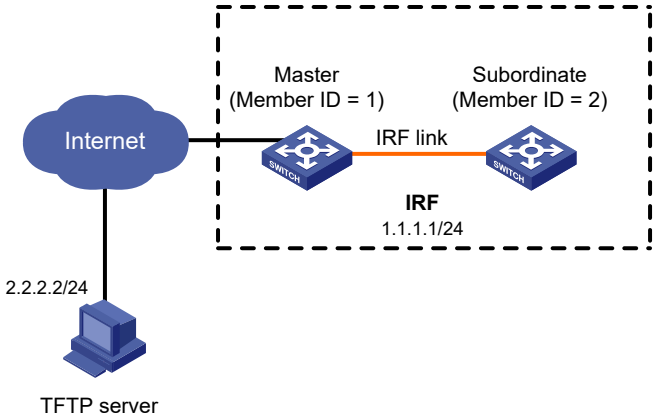


図 14-3 ネットワーク図

II. 設定手順

IP アドレスを設定し、装置と TFTP サーバが通信可能であることを確認します。（詳細は省略します。）

カレントソフトウェアの情報を表示します。

```
<Switch> display version
```

カレントソフトウェアイメージをバックアップします。

```
<Switch> copy boot.bin  boot_backup.bin

<Switch> copy system.bin system_backup.bin
```

IRF スタックメンバ装置のバックアップ BootROM ソフトウェアイメージ boot_backup.bin、バックアップシステムソフトウェアイメージ system_backup.bin を指定します。

```
<Switch> boot-loader file boot flash:/boot_backup.bin system flash:/system_backup.bin slot 1 backup

<Switch> boot-loader file boot flash:/boot_backup.bin system flash:/system_backup.bin slot 2 backup
```

TFTP を使用して TFTP サーバから IRF スタックマスタ装置の記憶媒体のルートディレクトリにソフトウェアファイル **startup-a2105.ipe** をダウンロードします。

```
<Switch> tftp 2.2.2.2 get startup-a2105.ipe
```

すべての IRF スタックメンバ装置のメインスタートアップソフトウェアとして **startup-a2105.ipe** を指定します。

```
<Switch> boot-loader file flash:/startup-a2105.ipe slot 1 main
<Switch> boot-loader file flash:/startup-a2105.ipe slot 2 main
```

スタートアップソフトウェアの設定を確認します。

```
<Switch> display boot-loader
```

装置の再起動を行い、アップグレードを完了させます。

```
<Switch> reboot
```

装置が正しいソフトウェアで動作しているか確認します。

```
<Switch> display version
```

目次

このセクションのページは**1-x-x**です。

15章 装置管理 15-1
15.1 装置名の設定 15-1
15.2 システムクロックの設定 15-1
15.2.1 システムクロックソースの設定 15-1
15.3 著作権情報表示の有効化 15-3
15.4 バナーの設定 15-3
15.4.1 バナーの種類 15-3
15.4.2 バナー入力モード 15-4
15.4.3 設定手順 15-5
15.5 装置の特定 15-5
15.5.1 装置の特定について 15-5
15.5.2 Power LEDの点滅開始 15-5
15.5.3 Power LEDの点滅停止 15-5
15.6 装置の再起動 15-6
15.6.1 CLIによる装置の即時再起動 15-7
15.6.2 装置のスケジュール再起動 15-7
15.7 スケジュール自動実行の設定 15-7
15.7.1 設定ガイドライン 15-7
15.7.2 設定手順 15-8
15.7.3 スケジュール自動実行設定例 15-9
15.8 パスワードリカバリ機能の無効化 15-12
15.9 検出間隔の設定 15-13
15.10 CPU使用率のモニタリングの設定 15-13
15.11 メモリ使用しきい値の設定 15-14
15.12 装置の温度アラームのしきい値の設定 15-16
15.13 トランシーバの情報表示 15-19
15.13.1 トランシーバの情報表示 15-19
15.14 スケジュール自動実行の設定 15-19
15.14.1 スケジュール自動実行について 15-19
15.14.2 制限とガイドライン 15-19
15.14.3 設定手順 15-20
15.15 装置管理の情報表示と維持 15-21

15章 装置管理

この章では装置の基本的なパラメータの設定、装置の管理について記載します。

この章の設定操作は、順番に関係なく実行できます。

15.1 装置名の設定

装置名あるいは、“ホスト名”はネットワークで装置を特定するのに使用されます。システムとしては、装置名は CLI のプロンプトに対応します。装置名が **NEC** の場合、プロンプトは<NEC>です。

以下に装置名を設定する方法を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． 装置名を設定する	**sysname** *sysname*	デフォルト：装置名

15.2 システムクロックの設定

15.2.1 システムクロックソースの設定

正しいシステムクロックの設定はネットワーク管理と通信に不可欠です。ネットワークで装置を動作させる前に、装置のシステム時間を設定してください。

装置はシステムクロックをローカルに設定するか、NTP クロックソースを使用して UTP 時間を設定することができます。

以下の方法で設定できます。

- **None**－ローカルシステムクロックです。CLI を用いて手動でシステムクロックを設定します。装置はシステム時間を維持するため、装置内部の水晶発振器によって生成されたクロック周波数を使用します。装置の再起動を行うとローカルシステム時間はデフォルトに戻るため、再度コマンドを設定してください。
- **NTP**－NTP クロックソースです。装置が NTP のシステムクロックを使用したとき、手動でシステムクロックを変更できません。NTP についての詳細は、オペレーションマニュアルのセクション 11 *システム管理*”*NTP*”を参照してください。

QX-S5100G シリーズは、電源 OFF/ON による再起動あるいは **reboot** コマンドを実行した場合、デフォルトの時刻にリセットされます。手動でシステムクロックを設定している場合は、再度システムクロックを設定してください。

NTP クロックソースから UTC 時間を計算したほうが、ローカルで設定した時間よりも制度が高くなります。

以下にローカルでシステムクロックソースを設定する方法を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． システムクロックのソースを指定する	**clock protocol none**	デフォルト：**ntp** コマンドを複数回実行した場合、最後に指定した設定が適用されます。
3． user view に戻る	**quit**	ー
4． 装置の現在の日時を設定する	**clock datetime** *time date*	デフォルト：UTC時間で2013年1月1日の00:00:00
5． system view に移行する	**system-view**	ー
6． タイムゾーンを設定する	**clock timezone** *zone-name* { **add** | **minus** } *zone-offset*	デフォルト：UTC タイムゾーンを設定したのち、装置はシステム時間を再計算します。システムクロックを確認する場合**display clock**コマンドを使用します。ネットワークのすべての装置で同一のタイムゾーンを使用していることを確認してください。
7． サマータイムを設定する	**clock summer-time** *name start-time start-date end-time end-date add-time*	デフォルト：無効 サマータイムを設定したのち、装置はシステム時間を再計算します。システムクロックを確認する場合**display clock**コマンドを使用します。ネットワークのすべての装置で同一のサマータイムを使用していることを確認してください。

以下に NTP でシステムクロックソースを設定する方法を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． システムクロックのソースを指定する	**clock protocol ntp**	デフォルト：ntp コマンドを複数回実行した場合、最後に指定した設定が適用されます。
3． タイムゾーンを設定する	**clock timezone** *zone-name* { **add** | **minus** } *zone-offset*	デフォルト：UTC タイムゾーンを設定したのち、装置はシステム時間を再計算します。システムクロックを確認する場合**display clock**コマンドを使用します。ネットワークのすべての装置で同一のタイムゾーンを使用していることを確認してください。

操作	コマンド	補足
4． サマータイムを設定する	**clock summer-time** *name start-time start-date end-time end-date add-time*	デフォルト：無効 サマータイムを設定したのち、装置はシステム時間を再計算します。システムクロックを確認する場合**display clock**コマンドを使用します。ネットワークのすべての装置で同一のサマータイムを使用していることを確認してください。

15.3 著作権情報表示の有効化

著作権情報の表示を有効にすると、以下の場合、著作権情報が表示されます。

- Telnet、SSH でログインします。
- コンソールポートから装置にログインした後に user view を終了します。この場合、装置は自動でコンソールセッションを再起動しようとします。

以下に著作権情報表示の有効化の手順を以下に示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． 著作権情報表示を有効にする	**copyright-info enable**	デフォルト：無効

15.4 バナーの設定

バナーはユーザが装置にログインしたときにシステムが表示するプロンプト情報です。

15.4.1 バナーの種類

装置は以下のバナーをサポートしています。

- **Legal** バナー － 認証情報とも呼ばれます。システムは著作権または権限情報を表示し、ユーザがログインする前にバナーを表示して、ユーザがログインするかどうか確認します。”Y”、または Enter キーを入力すると、ユーザはログインプロセスに入ります。”N”を入力すると、ユーザはログインプロセスを終了します。”Y”、”N”は、大文字でも小文字でもかまいません。
- **Message of the Day**（**MOTD**）バナー － 認証前に表示される welcome information です。legal バナーの後、login バナーの前に表示されます。
- **Login** バナー － ログイン認証時の welcome information です。パスワードと scheme 認証が設定されている場合に表示されます。
- **incoming** バナー － Modem ログインユーザが user view に移行する際に表示されます。認証が必要な場合、認証にパスしたのちバナーが表示されます。
- **Shell** バナー － ログインした後に表示します。

システムは **Legal** バナー、**Message of the Day**（**MOTD**）バナー、**Login** バナー、**incoming** バナーあるいは **Shell** バナーの順番で表示します。

15.4.2 バナー入力モード

バナーを設定する場合、1 行入力モードあるいは複数入力モードを使用します。

- 1 行入力モード

コマンドと同様に同一の行に入力します。入力テキストの開始および終了文字は同じにならなければなりませんが、バナー情報には含まれません。このとき、コマンドキーワードを含む入力テキストは 511 文字を超えないようにする必要があります。たとえば、ユーザが shell バナーの user view に移行した際に“Have a nice day.“と表示するように設定します。

```
<Switch> system-view
[Switch] header shell %Have a nice day.%
```

- 複数入力モード

Enter キーを押してすべてのバナー情報を複数行に入力するモードです。バナーには改行を含むことができます。改行は 2 文字分としてカウントされます。

複数行を設定する場合以下のどちらかの方法を使用します。

□ **方法 1**– コマンドキーワードの後ろで直接 **Enter** を押し、設定の最後を"%"にします。Enter および"%"はバナー情報には含まれません。たとえば、ユーザが user view に移行した際に“Have a nice day. Please input the password.“と表示するように設定します。区切り文字を含め 1999 文字まで入力できます。

```
<Switch> system-view
[Switch] header shell
Please input banner content, and quit with the character '%'.
Have a nice day.
Please input the password.%
```

□ **方法 2**– 最初の行のコマンドキーワードの後ろに 1 文字入力し、**Enter** を押します。最初の行に入力した文字で設定を終了します。最初の行の文字および最後の文字はバナー情報には含まれません。たとえば、ユーザが user view に移行した際に“Have a nice day. Please input the password.“と表示するように設定します。区切り文字を含め 1999 文字まで入力できます。

```
<Switch> system-view
[Switch] header shell A
Please input banner content, and quit with the character 'A'.
Have a nice day.
Please input the password.A
```

□ **方法 3** – 最初の行のキーワードの後ろに複数の文字（最初と最後の文字は同じにしない）を入力し、**Enter** を押します。最初の行の最初の文字で設定を終了します。最初の行の最初の文字および最後の文字はバナー情報には含まれません。区切り文字を含め 2002 文字まで入力できます。たとえば、ユーザが user view に移行した際に“Have a nice day. Please input the password. “と表示するように設定します。

```
<Switch> system-view
[Switch] header shell AHave a nice day.
```

```
Please input banner content, and quit with the character 'A'.
Please input the password.
A
```

15.4.3 設定手順

以下の手順に従ってバナーの設定を行います。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. ログイン前の権限情報を設定する	**header legal** *text*	デフォルト：設定なし
3. ログイン前に表示されるバナーを設定する	**header motd** *text*	デフォルト：設定なし
4. ログイン認証時に表示されるバナーを設定する	**header login** *text*	デフォルト：設定なし
5. Modem ログイン認証時に表示されるバナーを設定する	**header incoming** *text*	デフォルト：設定なし
6. ユーザが user view に入るときに表示するバナーを設定する	**header shell** *text*	デフォルト： %Please change the password from the default settings.%

15.5 装置の特定

15.5.1 装置の特定について

本装置は **locator blink** コマンドを使用することで、指定した装置の Power LED を一定時間すばやく赤色と緑色で交互に点滅させます。本機能は装置の位置を特定する際に役立ちます。

15.5.2 Power LED の点滅開始

user view で以下のコマンドを実行します。

操作	コマンド	補足
Power LEDの点滅を開始する	**locator** [**slot** *slot-number*] **blink** *blink-time*	―

15.5.3 Power LED の点滅停止

user view で以下のコマンドを実行します。

操作	コマンド	補足
Power LEDの点滅を停止する	**locator** [**slot** *slot-number*] **blink stop**	—

🕮 **メモ：**

locator blink コマンドは Version7.1.4 を含む以降のソフトウェアからサポートしています。

15.6 装置の再起動

⚠ **注意：**

- ネットワークサービスに割り込んで再起動する可能性があります。
- 設定が消失するのを避けるため、装置を再起動する前に **save** コマンドでカレントコンフィグレーションを保存してください。**save** コマンドの詳細は、コマンドマニュアルのセクション 1 *はじめに*”*コンフィグレーションファイル管理*”を参照してください。
- システム起動時に使用されるコンフィグレーションファイルとスタートアップファイルを確認するには、**display startup** コマンドと **display boot-loader** コマンドを使用してください。スタートアップコンフィグレーションファイルあるいはソフトウェアイメージが異常である場合、装置は正常に起動しません。**display startup** コマンドと **display boot-loader** コマンドの詳細は、コマンドマニュアルのセクション 1 *はじめに*”*ソフトウェア管理*”を参照してください。

以下の方法で装置を再起動できます。

- CLI によるスケジュールリブートを行います。。指定した時間に自動的に再起動させることができます。
- CLI による再起動を即時行うことができます。
- 再起動中、装置は以下の処理を行います。
  - □ 装置内部のすべてのチップをリセットします。
  - □ 圧縮されているイメージを解凍し、イメージを読み込みます。スタートアップソフトウェアを確認するため、BootWare を使用します。
- システムを初期設定します。
- 電源 ON/OFF による再起動を行います。電源を ON/OFF することでハードウェアも再起動させることができます。ただし、稼働中に装置電源を ON/OFF するため、ハードウェアに影響を及ぼす可能性があります。ハードウェアの再起動が必要な場合を除き、装置電源の ON/OFF は推奨できません。

遠隔ホストから CLI により装置を再起動することができます。

データ保護のため、装置がファイルの操作を実行している間、装置の再起動を行わないでください。

15.6.1 CLI による装置の即時再起動

user view で以下のコマンドを実行します。

操作	コマンド	補足
装置を再起動する	**reboot** [**slot** *slot-number*] [**force**]	―

15.6.2 装置のスケジュール再起動

装置はスケジュール再起動を 1 つのコマンドのみサポートします。もし **scheduler reboot at** コマンドあるいは **scheduler reboot delay** コマンドを複数回あるいは、両方のコマンドを設定した場合、最後に設定したコマンドが適用されます。

自動再起動はすべての IRF スタックのメンバ装置に適用されます。IRF スタックの Master とメンバの切り替えが発生する場合、再起動は中止されます。

スケジュール再起動により装置を再起動する場合、user view で以下のコマンドを実行します。

操作	コマンド	補足
再起動時間と日付を指定し、スケジュール再起動機能を有効にする	**scheduler reboot at** *time* [*date*]	デフォルト：設定なし
再起動遅延時間を指定し、スケジュール再起動機能を有効にする	**scheduler reboot delay** *time*	デフォルト：設定なし

15.7 スケジュール自動実行の設定

スケジュール自動実行機能は、管理者を妨げることなく、システムが指定した view で、指定された時間に、指定されたコマンドを自動的に実行します。

スケジュールされるコマンドは 1 回のみ、あるいは定期的に実行されます。1 回のみのスケジュールは設定ファイルに保存されません。装置が再起動したときに失われます。定期的なスケジュールは設定ファイルに保存され、指定時間に定期的に実行されます。

15.7.1 設定ガイドライン

- 再起動するとシステムクロックはデフォルトのシステムクロックがもとに戻ります。スケジュール自動実行機能を行うため、再起動後にシステムクロックを設定あるいは NTP を設定してください。NTP についての詳細は、オペレーションマニュアルのセクション 11 *システム管理”NTP”*を参照してください。
- コマンド（コマンド A）を job に割り当てるため、コマンド A の view に移行するコマンドを job に割り当ててください。
- スケジュール自動実行を行う場合、実行する view と command 引数をチェックしません。command 引数を正確に設定してください。（コマンドの syntax が設定されているか、および正しい view に設定されているかどうかを含みます）

- **telnet** コマンド、**ftp** コマンド、**ssh2** コマンドはスケジュール自動実行することはできません。
- スケジュール自動実行機能はユーザがインタラクティブにコマンドの操作を扱うことができません。もしコマンドが”YES”あるいは”NO”の答えを要求する場合、システムはいつも”Y”あるいは”YES”が入力されます。もし文字列の入力が必要な場合、システムは自動的にデフォルト文字列を入力するか、デフォルト文字列がない場合、空の文字列を入力します。
- 指定した自動実行時間になった後、バックグラウンドに指定されたコマンドを実行します。ログ、トラップ、デバッグなどの情報では表示されません。

15.7.2 設定手順

以下に 1 回のみのスケジュール自動実行を行う設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． job を作成する	**scheduler job** *job-name*	デフォルト：設定なし
3． job にコマンドを割り当てる	**command** *id command*	デフォルト：設定なし 複数のコマンドをjobに割り当てることができ、最も小さいIDから実行されます。
4． system view に戻る	**quit**	―
5． スケジュールを作成する	**scheduler schedule** *schedule-name*	デフォルト：設定なし
6． スケジュールに job を割り当てる	**job** *job-name*	デフォルト：設定なし 複数のjobをスケジュールに割り当てることができ、同時に実行できます。
7． 1 回のみのスケジュールに実行時間テーブルを指定する	● 実行日と時間を指定する： **time at** *time date* ● 実行月日と時間を指定する： **time once at** *time* [**month-date** *month-day* | **week-day** *week-day*&<1-7>] ● 指定された遅延時間後にコマンドを自動実行する： **time once delay** *time*	デフォルト：設定なし いずれか1つのコマンドで設定します。 実行時間が指定された後、**clock datetime**コマンド、**clock summer-time**コマンド、**clock timezone**コマンドは既に設定された実行時間テーブルを変更しません。

以下に定期的なスケジュール自動実行を行う設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． job を作成する	**scheduler job** *job-name*	デフォルト：設定なし
3． job にコマンドを割り当てる	**command** *id command*	デフォルト：設定なし 複数のコマンドをjobに割り当てることができ、最も小さいIDから実行されます。
4． system view に戻る	**quit**	―

操作	コマンド	補足
5． スケジュールを作成する	**scheduler schedule** *schedule-name*	デフォルト：設定なし
6． スケジュールに job を割り当てる	**job** *job-name*	デフォルト：設定なし 複数のjobをスケジュールに割り当てることができ、同時に実行できます。
7． 定期的なスケジュールを指定する	• 指定された時間で定期的にスケジュールを実行する： **time repeating at** *time* [**month-date** [*month-day* | **last**] | **week-day** week-day&<1-7>] • 指定された月日で定期的にスケジュールを実行する： **time repeating** [**at** *time* [*date*]] **interval** *interval-time*	デフォルト：設定なし いずれか1つのコマンドで設定します。 実行時間が指定された後、**clock datetime**コマンド、**clock summer-time**コマンド、**clock timezone**コマンドは既に設定された実行時間テーブルを変更しません。

15.7.3 スケジュール自動実行設定例

I. ネットワーク要件

図 15-1に示すように Device の 2 つのインタフェースがユーザに接続されています。

エネルギーを節約するため、以下のスケジュールを自動で実行します。

- 月曜日から金曜日の AM8:00 に装置の GigabitEthernet 1/0/1 インタフェース、GigabitEthernet 1/0/2 インタフェースを有効にします。
- 月曜日から金曜日の 18:00 にインタフェースを無効にします。

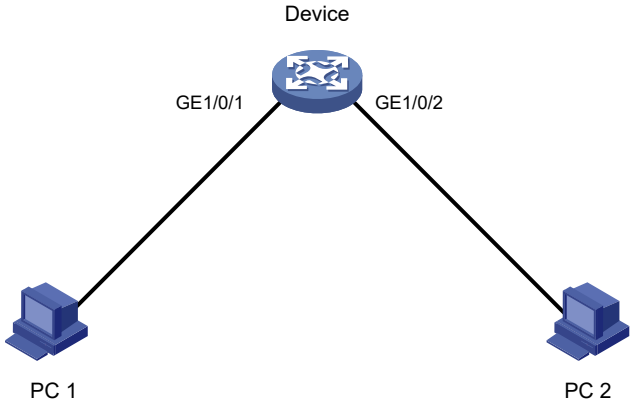


図 15-1 ネットワーク図

II. 設定手順

system view に移行します。

```
<Switch> system-view
```

GigabitEthernet 1/0/1 インタフェースを無効にする job を設定します。

```
[Switch] scheduler job shutdown-GigabitEthernet1/0/1
[Switch-job-shutdown-GigabitEthernet1/0/1] command 1 system-view
[Switch-job-shutdown-GigabitEthernet1/0/1] command 2 interface gigabitethernet 1/0/1
[Switch-job-shutdown-GigabitEthernet1/0/1] command 3 shutdown
[Switch-job-shutdown-GigabitEthernet1/0/1] quit
```

GigabitEthernet 1/0/1 インタフェースを有効にする job を設定します。

```
[Switch] scheduler job start-GigabitEthernet1/0/1
[Switch-job-start-GigabitEthernet1/0/1] command 1 system-view
[Switch-job-start-GigabitEthernet1/0/1] command 2 interface gigabitethernet 1/0/1
[Switch-job-start-GigabitEthernet1/0/1] command 3 undo shutdown
[Switch-job-start-GigabitEthernet1/0/1] quit
```

GigabitEthernet 1/0/2 インタフェースを無効にする job を設定します。

```
[Switch] scheduler job shutdown-GigabitEthernet1/0/2
[Switch-job-shutdown-GigabitEthernet1/0/2] command 1 system-view
[Switch-job-shutdown-GigabitEthernet1/0/2] command 2 interface gigabitethernet 1/0/2
[Switch-job-shutdown-GigabitEthernet1/0/2] command 3 shutdown
[Switch-job-shutdown-GigabitEthernet1/0/2] quit
```

GigabitEthernet 1/0/2 インタフェースを有効にする job を設定します。

```
[Switch] scheduler job start-GigabitEthernet1/0/2
[Switch-job-start-GigabitEthernet1/0/2] command 1 system-view
[Switch-job-start-GigabitEthernet1/0/2] command 2 interface gigabitethernet 1/0/2
[Switch-job-start-GigabitEthernet1/0/2] command 3 undo shutdown
[Switch-job-start-GigabitEthernet1/0/2] quit
```

月曜日から金曜日の AM8:00 にインタフェースを定期的に有効にするスケジュールを設定します。

```
[Switch] scheduler schedule START-pc1/pc2
[Switch-schedule-START-pc1/pc2] job start-GigabitEthernet1/0/1
[Switch-schedule-START-pc1/pc2] job start-GigabitEthernet1/0/2
[Switch-schedule-START-pc1/pc2] time repeating at 8:00 week-day mon tue wed thu fri
[Switch-schedule-START-pc1/pc2] quit
```

月曜日から金曜日の 18:00 にインタフェースを定期的に無効にするスケジュールを設定します。

```
[Switch] scheduler schedule STOP-pc1/pc2
[Switch-schedule-STOP-pc1/pc2] job shutdown-GigabitEthernet1/0/1
[Switch-schedule-STOP-pc1/pc2] job shutdown-GigabitEthernet1/0/2
[Switch-schedule-STOP-pc1/pc2] time repeating at 18:00 week-day mon tue wed thu fri
[Switch-schedule-STOP-pc1/pc2] quit
```

III. 設定の確認

すべての job の設定を表示します。

```
[Switch] display scheduler job
Job name: shutdown-GigabitEthernet1/0/1
 system-view
 interface gigabitethernet 1/0/1
 shutdown

Job name: shutdown-GigabitEthernet1/0/2
 system-view
 interface gigabitethernet 1/0/2
 shutdown

Job name: start-GigabitEthernet1/0/1
 system-view
 interface gigabitethernet 1/0/1
 undo shutdown

Job name: start-GigabitEthernet1/0/2
 system-view
 interface gigabitethernet 1/0/2
 undo shutdown
```

スケジュール情報を表示します。

```
[Switch] display scheduler schedule
Schedule name        : START-pc1/pc2
Schedule type        : Run on every Mon Tue Wed Thu Fri at 08:00:00
Start time           : Wed Sep 28 08:00:00 2011
Last execution time  : Wed Sep 28 08:00:00 2011
Last completion time : Wed Sep 28 08:00:03 2011
Execution counts     : 1
-------------------------------------------------------------------------
Job name                                          Last execution status
start-GigabitEthernet1/0/1                                 Successful
start-GigabitEthernet1/0/2                                 Successful

Schedule name        : STOP-pc1/pc2
Schedule type        : Run on every Mon Tue Wed Thu Fri at 18:00:00
Start time           : Wed Sep 28 18:00:00 2011
Last execution time  : Wed Sep 28 18:00:00 2011
Last completion time : Wed Sep 28 18:00:01 2011
Execution counts     : 1
-------------------------------------------------------------------------
Job name                                          Last execution status
shutdown-GigabitEthernet1/0/1                              Successful
shutdown-GigabitEthernet1/0/2                              Successful
```

スケジュールログの情報を表示します。

```
[Switch] display scheduler logfile
Job name        : start-GigabitEthernet1/0/1
Schedule name   : START-pc1/pc2
```

```
Execution time  : Wed Sep 28 08:00:00 2011
Completion time : Wed Sep 28 08:00:02 2011
---------------------------------- Job output ----------------------------------
<Switch>system-view
System View: return to User View with Ctrl+Z.
[Switch]interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1]undo shutdown

Job name        : start-GigabitEthernet1/0/2
Schedule name   : START-pc1/pc2
Execution time  : Wed Sep 28 08:00:00 2011
Completion time : Wed Sep 28 08:00:02 2011
---------------------------------- Job output ----------------------------------
<Switch>system-view
System View: return to User View with Ctrl+Z.
[Switch]interface gigabitethernet 1/0/2.
[Switch-GigabitEthernet1/0/2]undo shutdown

Job name        : shutdown-GigabitEthernet1/0/1
Schedule name   : STOP-pc1/pc2
Execution time  : Wed Sep 28 18:00:00 2011
Completion time : Wed Sep 28 18:00:01 2011
---------------------------------- Job output ----------------------------------
<Switch>system-view
System View: return to User View with Ctrl+Z.
[Switch]interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1]shutdown

Job name        : shutdown-GigabitEthernet1/0/2
Schedule name   : STOP-pc1/pc2
Execution time  : Wed Sep 28 18:00:00 2011
Completion time : Wed Sep 28 18:00:01 2011
---------------------------------- Job output ----------------------------------
<Switch>system-view
System View: return to User View with Ctrl+Z.
[Switch]interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2]shutdown
```

15.8 パスワードリカバリ機能の無効化

パスワードリカバリ機能は Boot ROM メニューからデバイス構成と SDRAM へのアクセスを制御できます。

パスワードリカバリ機能が有効の場合、コンソールからのユーザは認証なしで装置にアクセスでき、新しいパスワードを設定することができます。

パスワードリカバリ機能が無効の場合、コンソールからのユーザは、新しいパスワードを設定する前に、工場出荷コンフィグレーションに戻す必要があります。工場出荷コンフィグレーションに戻すことで、次回に起動で使用するコンフィグレーションファイルを削除します。工場出荷コンフィグレーションはデフォルトコンフィグレーションを読み込んでいない設定になります。

次回起動時に使用するコンフィグレーションファイルにアクセスする不正なユーザからのアクセスを防ぐため、パスワードリカバリ機能を無効にできます。

以下にパスワードリカバリ機能を無効にする設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． パスワードリカバリ機能を無効にする	**undo password-recovery enable**	デフォルト：有効

15.9 検出間隔の設定

特定の環境において、いくつかのプロトコルはポートをシャットダウンします。ポートがシャットダウンした後、装置は検出間隔タイマを開始します。検出間隔が経過した際にポートがまだダウンされている場合、物理的にポートを復旧させます。

以下に検出間隔を設定する方法を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． 検出間隔を設定する	**shutdown-interval** *time*	デフォルト：30秒

15.10 CPU使用率のモニタリングの設定

CPU 使用率を検出するため、装置は以下の処理を行います。

- サンプリング間隔は 1 分間隔です。CPU 使用率のしきい値とサンプリング間隔を比較します。サンプリング間隔が CPU 使用率のしきい値に到達した場合、装置は trap を送信します。
- CPU 使用率の記録が有効である場合、設定した間隔で CPU 使用率を検出し、保存します。**display cpu-usage history** コマンドを使用して、CPU 使用率の履歴統計を座標系で表示できます。

装置は、次の CPU 使用率しきい値をサポートします。

- **Minor しきい値**: CPU 使用率が Minor しきい値以上に増加したが、Severe しきい値未満である場合、CPU 使用率は Minor アラーム状態になります。CPU 使用率が Severe しきい値を超えるか、Minor アラームが削除されるまで、装置は Minor アラームを定期的に送信します。
- **Severe しきい値**: CPU 使用率が Severe しきい値を超えると、CPU 使用率は Severe アラーム状態になります。装置は、Severe アラームが削除されるまで、Severe アラームを定期的に送信します。
- **リカバリしきい値**: CPU 使用率がリカバリしきい値を下回ると、CPU 使用率はリカバリ状態になります。装置がリカバリ通知を送信します。

CPU 使用率のアラームと通知は、NETCONF イベント、SNMP トラップとインフォーム、およびログメッセージとしてカプセル化するために、NETCONF、SNMP、および information center に送信できます。詳細については、オペレーションマニュアルのセクション 11 *システム管理*"*NETCONF*"、"*SNMP*"、"*Information Center*"を参照してください。

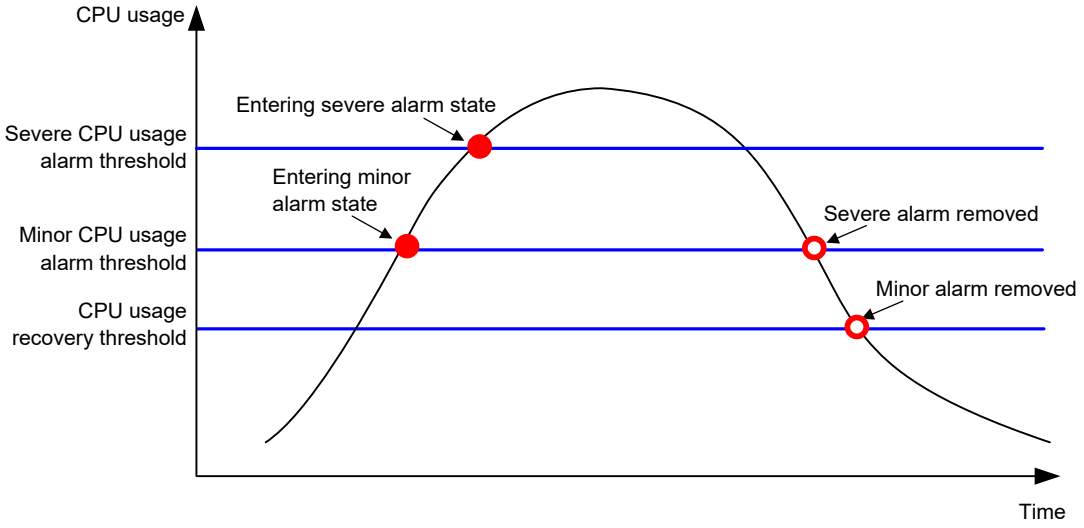


図 15-2 CPU alarm および alarm-removed 通知

以下に CPU 使用率のモニタリングの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. CPU 使用率アラームしきい値を設定する	**monitor cpu-usage threshold** *severe-threshold* **minor-threshold** *minor-threshold* **recovery-threshold** *recovery-threshold*[**slot** *slot-number* [**cpu** *cpu-number*]]	デフォルト： • Severe CPU使用率アラームしきい値—99% • Minor CPU使用率アラームしきい値—98% • CPU使用率リカバリしきい値—50%
3. CPU 使用率アラームの再送間隔を設定する	**monitor resend cpu-usage** { **minor-interval** *minor-interval* | **severe-interval** *severe-interval* } * [**slot** *slot-number* [**cpu** *cpu-number*]]	デフォルト：Minorアラームの再送間隔は300秒、Severeアラームの再送間隔は60秒です。
4. **display cpu-usage history** コマンドの情報取得間隔を設定する	**monitor cpu-usage interval** *interval* [**slot** *slot-number* [**cpu** *cpu-number*]]	デフォルト：1分
5. CPU 使用率の追跡を有効にする	**monitor cpu-usage enable** [**slot** *slot-number* [**cpu** *cpu-number*]]	デフォルト：有効

🕮 **メモ：**

monitor cpu-usage interval コマンドは **monitor cpu-usage threshold** コマンドの CPU 使用率を取得する間隔ではありません。**display cpu-usage history** コマンドの情報を取得する間隔です。

15.11 メモリ使用しきい値の設定

メモリ使用率をモニタするため、装置は以下の処理を行います。

- サンプリング間隔は 1 分です。メモリ容量がしきい値に達したとき、装置はトラップを作成し、送信します。
- 適切な動作とメモリ使用率を改善するため、装置はリアルタイムにおける空きメモリ容量をモニタリングします。空きメモリ容量がしきい値に達したとき、送致は alarm 通知あるいは alarm-removed 通知を生成し、関連するサービスモジュールあるいはプロセスに送信します。

表 15-1と図 15-3に示すように装置は以下のレベルのしきい値をサポートしています。

表 15-1 Memory alarm 通知と memory alarm-removed 通知

通知	トリガー状況	補足
Minor alarm通知	空きメモリ容量が最初にminor alarmしきい値以下に達した	minor alarm通知を作成、送信した後、装置は最初にminor alarmがキャンセルされるまで追加でminor alarm通知を作成、送信しません。
Severe alarm通知	空きメモリ容量が最初にsevere alarmしきい値以下に達した	severe alarm通知を作成、送信した後、装置は最初にsevere alarmがキャンセルされるまで追加でsevere alarm通知を作成、送信しません。
Critical alarm通知	空きメモリ容量が最初にcritical alarmしきい値以下に達した	critical alarm通知を作成、送信した後、装置は最初にcritical alarmがキャンセルされるまで追加でcritical alarm通知を作成、送信しません。
Critical alarm-removed 通知	空きメモリ容量が最初にsevere alarmしきい値以上に達した	ー
Severe alarm-removed 通知	空きメモリ容量が最初にminor alarmしきい値以上に達した	ー
Minor alarm-removed 通知	空きメモリ容量が最初にnormal alarmしきい値以上に達した	ー

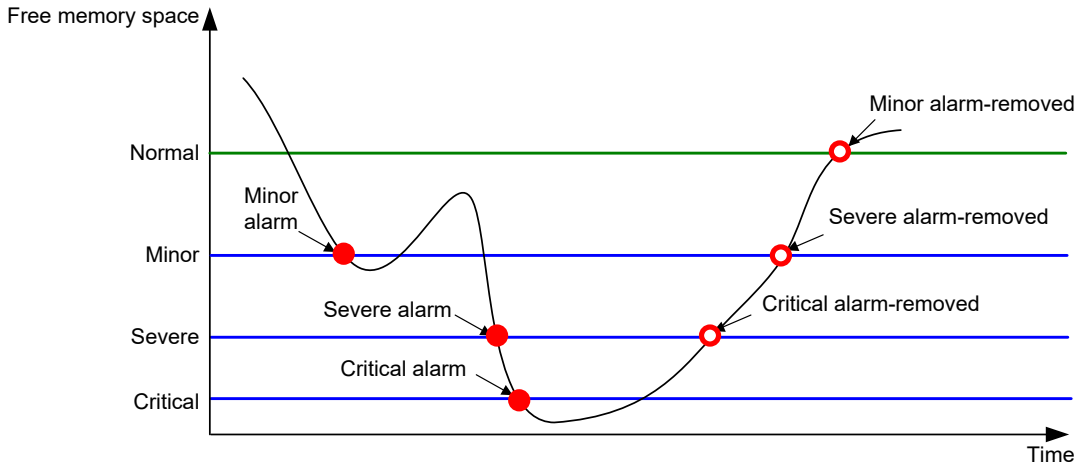


図 15-3 メモリ alarm 通知と alarm-removed 通知

以下にメモリ使用率のしきい値の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． メモリ使用率しきい値を設定する	**memory-threshold** [**slot** *slot-number* [**cpu** *cpu-number*]] **minor** *minor-value* **severe** *severe-value* **critical** *critical-value* **normal** *normal-value*	デフォルト： • **Minor alarmしきい値**– 60MB • **Severe alarmしきい値**– 56MB • **Critical alarmしきい値**– 52MB • **Normal stateしきい値**– 64MB
3． メモリ不足アラームの再送間隔を設定する	**monitor resend memory-threshold** { **critical-interval** *critical-interval* | **minor-interval** *minor-interval* | **severe-interval** *severe-interval* } * [**slot** *slot-number* [**cpu** *cpu-number*]]	デフォルト： • **Minor alarm再送信間隔**– 12時間 • **Severe alarm再送信間隔**– 3時間 • **Critical alarm再送信間隔** – 1時間

15.12 装置の温度アラームのしきい値の設定

装置は以下のしきい値をもとに温度をモニタします。

- 下限温度しきい値
- 高温ワーニング温度しきい値
- 高温アラーム温度しきい値

温度が下限温度しきい値を下回ったとき以下の動作を行います。または高温ワーニング温度しきい値、高温アラーム温度しきい値に到達したとき、以下の動作を行います。

- ログメッセージを送信します。
- トラップを送信します。
- 装置の前面にある LED で通知します。

以下に温度アラームしきい値を設定する方法を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． 温度アラームしきい値を設定する	**temperature-limit slot** *slot-number* **hotspot** *sensor-number lowlimit warninglimit* [*alarmlimit*]	デフォルト：表 15-2を参照してください。 ワーニング温度しきい値とアラーム温度しきい値は下限温度しきい値よりも高い温度に設定してください。アラーム温度しきい値はワーニング温度しきい値よりも高い温度に設定してください。

表 15-2 温度アラームのしきい値のデフォルトと推奨値

装置	センサ	下限温度	ワーニング温度の推奨	ワーニング温度のデフォルト	アラーム温度の推奨	アラーム温度のデフォルト
QX-S5124GT-4X	Hotspot 1	0	79	84	84	98
	Hotspot 2	0	94	100	99	110
	Hotspot 3	0	97	100	102	110
	Hotspot 4	0	93	100	98	110
QX-S5148GT-4X	Hotspot 1	0	87	84	92	98
	Hotspot 2	0	94	84	99	98
	Hotspot 3	0	102	100	107	110
	Hotspot 4	0	100	100	105	110
	Hotspot 5	0	108	100	113	110
	Hotspot 6	0	113	100	118	110
	Hotspot 7	0	111	100	116	110
	Hotspot 8	0	105	100	110	110
QX-S5124GP-4X	Hotspot 1	0	76	88	81	102

装置	センサ	下限温度	ワーニング温度の推奨	ワーニング温度のデフォルト	アラーム温度の推奨	アラーム温度のデフォルト
	Hotspot 2	0	77	100	82	115
	Hotspot 3	0	79	100	84	115
	Hotspot 4	0	79	100	84	115
	Hotspot 5	0	76	100	81	115
	Hotspot 6	0	78	100	83	115
	Hotspot 7	0	80	100	85	115
QX-S5124GT-4X-PW	Hotspot 1	0	71	84	76	98
	Hotspot 2	0	92	100	97	110
	Hotspot 3	0	93	100	98	110
	Hotspot 4	0	83	100	88	110
	Hotspot 5	0	81	100	86	110
	Hotspot 6	0	71	110	76	130
QX-S5148GT-4X-PW	Hotspot 1	0	88	84	93	98
	Hotspot 2	0	92	84	97	98
	Hotspot 3	0	101	100	106	110
	Hotspot 4	0	102	100	107	110
	Hotspot 5	0	107	100	112	110
	Hotspot 6	0	114	100	119	110
	Hotspot 7	0	113	100	118	110
	Hotspot 8	0	106	100	111	110
	Hotspot 9	0	88	100	93	130

🕮 **メモ：**
設定温度をデフォルトのしきい値から推奨温度のしきい値に変更することを推奨します。

15.13 トランシーバの情報表示

15.13.1 トランシーバの情報表示

搭載しているトランシーバ（SFP、SFP+など）のタイプ、コネクタの形状、送信するレーザーの中心波長、転送距離の情報を表示させることができます。

搭載しているトランシーバの情報表示を行うには、以下の手順に従ってください。

操作	コマンド	補足
トランシーバの情報を表示する	**display transceiver interface** [*interface-type interface-number*]	–

15.14 スケジュール自動実行の設定

15.14.1 スケジュール自動実行について

スケジュール自動実行機能は、管理者を妨げることなく、システムが指定した view で、指定された時間に、指定されたコマンドを自動的に実行します。

スケジュールされるコマンドは 1 回のみ、あるいは定期的に実行されます。1 回のみのスケジュールは設定ファイルに保存されません。装置が再起動したときに失われます。定期的なスケジュールは設定ファイルに保存され、指定時間に定期的に実行されます。

15.14.2 制限とガイドライン

- システムクロックは再起動により常に一旦初期値に戻ります。スケジュール自動実行を期待通りに動作させる為に、再起動後に必ずシステムクロックの再設定を行うか、NTP によりシステムクロックが設定されるように設定を行ってください。NTP についての詳細については、オペレーションマニュアルのセクション 11 *システム管理"NTP"*を参照してください。
- スケジュール自動実行を行う場合、実行する view と command 引数をチェックしません。command 引数を正確に設定してください。（コマンドの syntax が設定されているか、および正しい view に設定されているかどうかを含みます）
- **telnet** コマンド、**ftp** コマンド、**ssh2** コマンドはスケジュール自動実行することはできません。
- スケジュール自動実行機能はユーザがインタラクティブにコマンドの操作を扱うことができません。もしコマンドが YES あるいは NO の答えを要求する場合、システムはいつも Y あるいは YES が入力されます。もし文字列の入力が必要な場合、シス

テムは自動的にデフォルト文字列を入力するか、デフォルト文字列がない場合、空の文字列を入力します。

- 指定した自動実行時間になった後、バックグラウンドに指定されたコマンドを実行します。ログ、トラップ、デバッグなどの情報では表示されません。

15.14.3 設定手順

以下に 1 回のみのスケジュール自動実行を行う設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． job を作成する	**scheduler job** *job-name*	デフォルト：設定なし
3． job にコマンドを割り当てる	**command** *id command*	デフォルト：設定なし 複数のコマンドをjobに割り当てることができ、最も小さいIDから実行されます。
4． system view に戻る	**quit**	ー
5． スケジュールを作成する	**scheduler schedule** *schedule-name*	デフォルト：設定なし
6． スケジュールに job を割り当てる	**job** *job-name*	デフォルト：設定なし 複数のjobをスケジュールに割り当てることができ、同時に実行できます。
7． スケジュールにユーザロールを割り当てる	**user-role** *role-name*	デフォルト : ユーザロールを作成したユーザロールを持ちます。 スケジュールの1つ以上のユーザロールが許可される場合、スケジュールのコマンドは実行できます。
8． 1 回のみのスケジュールに実行時間テーブルを指定する	● 実行日と時間を指定する: **time at** *time date* ● 実行月日と時間を指定する: **time once at** *time* [**month-date** *month-day* | **week-day** *week-day*&<1-7>] ● 指定された遅延時間後にコマンドを自動実行する: **time once delay** *time*	デフォルト：設定なし いずれか1つのコマンドで設定します。 実行時間が指定された後、**clock datetime**コマンド、**clock summer-time**コマンド、**clock timezone**コマンドは既に設定された実行時間テーブルを変更しません。

以下に定期的なスケジュール自動実行を行う設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． job を作成する	**scheduler job** *job-name*	デフォルト：設定なし
3． job にコマンドを割り当てる	**command** *id command*	デフォルト：設定なし 複数のコマンドをjobに割り当てることができ、最も小さいIDから実行されます。

操作	コマンド	補足
4． system view に戻る	**quit**	ー
5． スケジュールを作成する	**scheduler schedule** *schedule-name*	デフォルト：設定なし
6． スケジュールにユーザロールを割り当てる	**user-role** *role-name*	デフォルト：スケジュールを作成したユーザのユーザロールを持ちます。 スケジュールの1つ以上のユーザロールが許可される場合、スケジュールのコマンドは実行できます。
7． スケジュールに job を割り当てる	**job** *job-name*	デフォルト：設定なし 複数のjobをスケジュールに割り当てることができ、同時に実行できます。
8． 定期的なスケジュールを指定する	● 指定された時間で定期的にスケジュールを実行する: **time repeating at** *time* [**month-date** [*month-day* | **last**] | **week-day** week-day&<1-7>] ● 指定された月日で定期的にスケジュールを実行する: **time repeating** [**at** *time* [*date*]] **interval** *interval-time*	デフォルト：設定なし いずれか1つのコマンドで設定します。 実行時間が指定された後、**clock datetime**コマンド、**clock summer-time**コマンド、**clock timezone**コマンドは既に設定された実行時間テーブルを変更しません。

15.15 装置管理の情報表示と維持

すべての view で **display** コマンドを実行し、user view で **reset** コマンドを実行できます。

操作	コマンド
システムクロック、日時、タイムゾーン、サマータイムを表示する	**display clock**
CPU使用率の統計情報を表示する	**display cpu-usage** [**slot** *slot-number* [**cpu** *cpu-number*]]
CPU使用率のモニタリング設定を表示する	**display cpu-usage configuration** [**slot** *slot-number* [**cpu** *cpu-number*]]
CPU使用率のヒストリ統計情報をグラフで表示する	**display cpu-usage history** [**job** *job-id*] [**slot** *slot-number* [**cpu** *cpu-number*]]
ハードウェアについての情報を表示する	**display device** [**slot** *slot-number* | **verbose**]
装置の製造情報を表示する	**display device manuinfo** [**slot** *slot-number*]
電源装置の製造情報を表示する	**display device manuinfo slot** *slot-number* **power** *power-id*
複数のモジュールの動作の統計情報を表示する	**display diagnostic-information** [**hardware** | **infrastructure** | **l2** | **l3** | **service**]
装置の温度情報を表示する	**display environment** [**slot** *slot-number*]
装置のファンの稼動情報を表示する	**display fan** [**slot** *slot-number* [*fan-id*]]
装置のメモリ使用率を表示する	**display memory** [**slot** *slot-number* [**cpu** *cpu-number*]]
装置のメモリ使用率のしきい値を表示する	**display memory-threshold** [**slot** *slot-number* [**cpu** *cpu-number*]]
電源ユニットの状態を表示する	**display power** [**slot** *slot-number* [*power-id*]]

操作	コマンド
スケジュール自動実行機能の設定状態を表示する	**display scheduler job** [*job-name*]
スケジュール自動実行機能のログ情報を表示する	**display scheduler logfile**
スケジュールリブート機能の設定状態を確認する	**display scheduler reboot**
スケジュール自動実行機能の情報を表示する	**display scheduler schedule** [*schedule-name*]
システムバージョンを表示する	**display version**
スケジュール自動実行機能のログ情報を削除する	**reset scheduler logfile**

目次

このセクションのページは **1-x-x** です。

16 章 Python.....16-1
16.1 Python shell への移行.....16-1
16.2 Python スクリプトの実行.....16-1
16.3 Python shell の終了.....16-1
16.4 Python 使用例.....16-1

16章 Python

Python とは汎用プログラミング言語の 1 つで、分かりやすい文法が特徴です。

Python インタプリタは以下の機能をサポートします。

- Python 2.7 コマンド。
- Python 2.7 標準 API。
- Comware 7 拡張 API。詳細は、オペレーションマニュアルのセクション 1 *はじめに "Comware 7 python 拡張 API"*を参照してください。
- Python スクリプト。Python スクリプトを使用して、システム制御が可能です。

16.1 Python shellへの移行

Python コマンドや API を使用するには、Python shell に移行する必要があります。以下に Python shell に移行する方法を示します。

操作	コマンド	補足
user viewからPython shellに移行する	**python**	—

16.2 Pythonスクリプトの実行

以下に user view で python スクリプトを実行する方法を示します。

操作	コマンド	補足
Pythonスクリプトを実行する	**python** *filename*	—

16.3 Python shellの終了

以下に python shell を終了する方法を示します。

操作	コマンド	補足
Python shellを終了する	**exit()**	—

16.4 Python使用例

I. ネットワーク要件

以下を行う Python スクリプトを使用します。

- コンフィグレーションファイル main.cfg と backup.cfg をダウンロードします。

- ダウンロードしたファイルを、次回起動時のメインとバックアップコンフィグレーションファイルに指定します。



図 16-1 ネットワーク図

II. 手順

PC 上でテキストエディタを使用し、以下の python スクリプト test.py を作成します。

```
#!usr/bin/python
import comware

comware.Transfer('tftp', '192.168.1.26', 'main.cfg', 'flash:/main.cfg')
comware.Transfer('tftp', '192.168.1.26', 'backup.cfg', 'flash:/backup.cfg')
comware.CLI('startup   saved-configuration   flash:/main.cfg   main   ;startup
saved-configuration flash:/backup.cfg backup')
```

TFTP を使用し、スクリプトをダウンロードします。

```
<Switch> tftp 192.168.1.26  get test.py
```

スクリプトを実行します。

```
<Switch> python flash:/test.py
<Switch>startup saved-configuration  flash:/main.cfg  main
Please wait...... Done.
<Switch>startup saved-configuration  flash:/backup.cfg  backup
Please wait...... Done.
```

III. 確認

スタートアップコンフィグレーションファイルを表示します。

```
<Switch> display startup
 Current startup saved-configuration file: flash:/startup.cfg
 Next main startup saved-configuration file: flash:/main.cfg
 Next backup startup saved-configuration file: flash:/backup.cfg


#!usr/bin/python
import comware

comware.Transfer('tftp', '192.168.1.26', 'main.cfg', 'flash:/main.cfg')
comware.Transfer('tftp', '192.168.1.26', 'backup.cfg', 'flash:/backup.cfg')
comware.CLI('startup   saved-configuration   flash:/main.cfg   main   ;startup
saved-configuration flash:/backup.cfg backup')
```

目次

このセクションのページは **1-x-x** です。

17 章 Comware 7 python 拡張 API 17-1
17.1 CLI 17-1
17.2 get_error 17-2
17.3 get_output 17-2
17.4 get_self_slot 17-3
17.5 get_slot_info 17-3
17.6 get_slot_range 17-4
17.7 get_standby_slot 17-4
17.8 Transfer 17-5

17章 Comware 7 python 拡張 API

Comware 7 python 拡張 API は Python syntax と互換性があります。

17.1 CLI

CLI を実行し、comware 7 CLI コマンドの実行と CLI オブジェクトを作成します。

I. Syntax

CLI(*command*='', *do_print*=True)

II. Parameters

command: 実行するコマンドを指定します。複数のコマンドを実行するには、スペースとセミコロン(;)を区切り文字として使用します。User view 以外の view でコマンドを実行するは、コマンド実行前にその view へ移行する必要があります。たとえば、**local-user test class manage** コマンドを実行するには、'**system-view ;local-user test class manage**' を実行しておく必要があります。

do_print: コマンド実行時の出力を行うかどうかを指定します。

- **True**—実行結果を表示します。この値がデフォルトです。
- **False**—実行結果を表示しません。

III. Usage guidelines

この API は comware コマンドのみサポートします。Linux、Python や TCL コマンドではサポートしません。

IV. Returns

CLI オブジェクト

V. Examples

ローカルユーザ **test** を作成します。

```
<Switch> python
Python 2.7.3 (default)
[GCC 4.4.1] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> import comware
>>> comware.CLI('system-view ;local-user test class manage')
```

VI. Sample output

```
<Switch> system-view
System View: return to User View with Ctrl+Z.
[Switch] local-user test class manage
New local user added.
<comware.CLI object at 0xb7f680a0>
```

17.2 get_error

get_error を使用して、ダウンロード時のエラー情報を取得します。

I. Syntax

Transfer.get_error()

II. Returns

エラー情報(エラー情報が無ければ、**None** が返ります。)

III. Examples

test.cfg を TFTP サーバ 1.1.1.1 からダウンロードし、エラー情報を取得します。

```
<Switch> python
Python 2.7.3 (default)
[GCC 4.4.1] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> import comware
>>> c = comware.Transfer('tftp', '1.1.1.1', 'test.cfg', 'flash:/test.cfg',
user='', password='')
>>> c.get_error()
```

IV. Sample output

```
"Timeout was reached”
```

17.3 get_output

get_output を使用して、コマンド実行時の出力を得ることができます。

I. Syntax

CLI.get_output()

II. Returns

コマンド実行時の出力が返ります。

III. Examples

ローカルユーザを追加し、コマンド出力を得ます。

```
<Switch> python
Python 2.7.3 (default)
[GCC 4.4.1] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> import comware
>>> c = comware.CLI('system-view ;local-user test class manage', False)
>>> c.get_output()
```

IV. Sample output

```
['<Switch>system-view', 'System View: return to User View with Ctrl+Z.',
'[Switch]local-user test class manage', 'New local user added.']
```

17.4 get_self_slot

get_self_slot を使用して、マスタ装置のメンバ ID を取得します。

I. Syntax

get_self_slot()

II. Returns

リストオブジェクト(フォーマットは[-1,*slot-number*])。*slot-number* がマスタ装置のメンバ ID を示します。

III. Examples

マスタ装置のメンバ ID を取得します。

```
<Switch> python
Python 2.7.3 (default)
[GCC 4.4.1] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> import comware
>>> comware.get_self_slot()
```

IV. Sample output

```
[-1,0]
```

17.5 get_slot_info

get_slot_info を使用して、メンバ装置情報を取得します

I. Syntax

get_slot_info()

II. Returns

辞書オブジェクト(フォーマットは{'Slot': *slot-number*, 'Status': '*status*', 'Chassis': chassis-number, 'Role': '*role*', 'Cpu': *CPU-number* })。*slot-number* は装置のメンバ ID を示します。*status* はメンバ装置のステータスを示します。chassis-number と CPU-number は 0 固定です。*role* はメンバ装置の役割を示します。

III. Examples

メンバ装置情報を取得します。

```
<Switch> python
Python 2.7.3 (default)
[GCC 4.4.1] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> import comware
>>> comware.get_slot_info(1)
```

IV. Sample output

```
{'Slot': 1, 'Status': 'Normal', 'Chassis': 0, 'Role': 'Master', 'Cpu': 0}
```

17.6 get_slot_range

get_slot_range を使用して、使用可能なメンバ ID の範囲を取得します。

I. Syntax

get_slot_range()

II. Returns

辞書オブジェクト（フォーマットは {'MaxSlot': *max-slot-number,* 'MinSlot': *min-slot-number* }）。*max-slot-number* はメンバ ID の最大値を示します。*min-slot-number* はメンバ ID の最小値を示します。

III. Examples

使用可能な IRF メンバ ID の範囲を取得します。

```
<Switch> python
Python 2.7.3 (default)
[GCC 4.4.1] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> import comware
>>> comware. get slot range()
```

IV. Sample output

```
{'MaxSlot': 10, 'MinSlot': 1}
```

17.7 get_standby_slot

get_standby_slot を使用して、スタンバイ装置のメンバ ID を取得します。

I. Syntax

get_standby_slot()

II. Returns

以下のフォーマットでリストオブジェクトが返ります。

- [ ]—IRF スタックにスタンバイ装置がありません。
- [[-1,*slot-number*]]—IRF スタックに一つのスタンバイ装置があります。
- [[-1,*slot-number1*],[-1,*slot-number2*],...]—IRF スタックに複数のスタンバイ装置があります。

slot-number はスタンバイ装置のメンバ ID です。

III. Examples

メンバ装置のメンバ ID を取得します。

```
<Switch> python
Python 2.7.3 (default)
[GCC 4.4.1] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> import comware
>>> comware.get standby slot()
```

IV. Sample output

```
[[-1, 1], [-1, 2]]
```

17.8 Transfer

Transfer を使用して、サーバからファイルをダウンロードします。

I. Syntax

Transfer(*protocol*='', *host*='', *source*='', *dest*='', *vrf*='',*login_timeout*=10, *user*='', *password*='')

II. Parameters

protocol: ダウンロードで使用するプロトコルを指定します。

- **ftp**—FTP を使用します。
- **tftp**—TFTP を使用します。
- **http**—HTTP を使用します。

host: リモートサーバの IP アドレスを指定します。

source: リモートサーバからダウンロードするファイル名を指定します。

dest: ダウンロードしたファイルの名前を指定します。

vrf: 本パラメータは未サポートです。Null('')を指定してください。

login_timeout: タイムアウト値を秒で指定します。デフォルトは 10 秒です。

user: サーバログイン用のユーザ名を指定します。

password: ログインパスワードを指定します。

III. Returns

Transfer object

IV. Examples

test.cfg を TFTP サーバ 192.168.1.26 からダウンロードします。

```
<Switch> python
Python 2.7.3 (default)
[GCC 4.4.1] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> import comware
>>> comware.Transfer('tftp', '192.168.1.26', 'test.cfg', 'flash:/test.cfg',
user='', password='')
```

V. Sample output

```
<comware.Transfer object at 0xb7f700e0>
```

目次

このセクションのページは **1-x-x** です。

18 章 Auto Config 18-1
18.1 一般的なアプリケーションシナリオ 18-1
18.2 Auto Config の動作 18-2
18.2.1 DHCP による IP アドレスと設定パラメータの取得.....18-2
18.2.2 TFTP サーバからのコンフィグレーションファイルの取得.....18-3
18.2.3 コンフィグレーションファイルの適用.....18-5

18章 Auto Config

Auto Config は、スタートアップコンフィグレーションファイルを設定されていない状態で装置が起動する場合、自動でコンフィグレーションファイルを取得し、適用することを可能にします。Auto Config はネットワークの設定を簡略化とネットワーク管理を容易にすることで、メンテナンスの作業負荷を削減することができます。

Auto Config を実装するために、ネットワーク管理者はサーバにコンフィグレーションファイルを保存しておく必要があります。装置は自動でコンフィグレーションファイルを取得し、その設定を適用します。

18.1 一般的なアプリケーションシナリオ

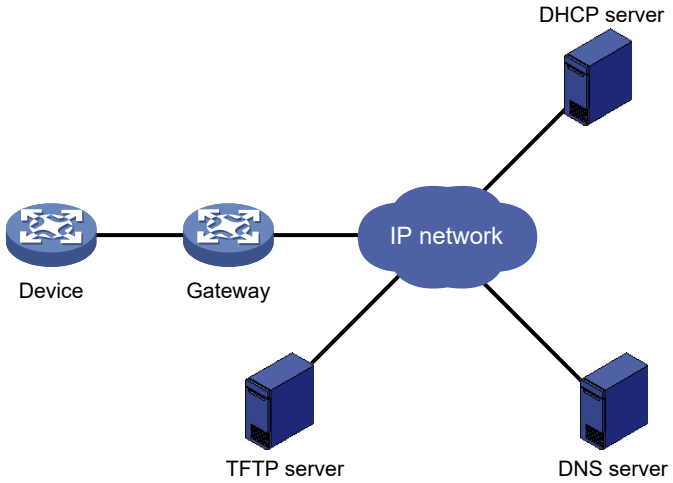


図 18-1 ネットワーク図

図 18-1に示すように、装置は以下のサーバによって Auto Config を実現します。

- **DHCP サーバ** – 装置は IP アドレスと、コンフィグレーションファイル名、TFTP サーバおよび DNS サーバの IP アドレスなどのパラメータを取得します。
- **TFTP サーバ** – Auto Config に必要なファイルを保存しておきます。機器は、ホスト IP アドレスとホスト名のマッピングを含むホスト名ファイル（network.cfg)やコンフィグレーションファイルなど、必要なファイルを TFTP サーバから取得します。
- **DNS サーバ** – IP アドレスとホスト名を決定します。装置が DNS サーバを通して対応するホスト名の IP アドレスを解決した場合、TFTP サーバにホスト名と同じ名前を持つコンフィグレーションファイル（hostname.cfg)を要求します。装置が DHCP レスポンスによって TFTP サーバのドメイン名を取得するならば、DNS サーバを通して TFTP サーバのドメイン名から TFTP サーバの IP アドレスを導き出すことも可能です。

DHCP サーバ、TFTP サーバ、DNS サーバ、機器が同一セグメントのネットワークにない場合、ゲートウェイの上で DHCP リレーエージェントを設定し、各サーバと機器が相互通信できるようにルーティングプロトコルを設定する必要があります。

18.2 Auto Configの動作

Auto Config は以下のように動作します。

1) スタートアップ時、装置はインタフェース Vlan を作成し、IP アドレスと TFTP サーバ名、DNS サーバ IP アドレス、およびコンフィグレーションファイル名などを DHCP サーバに要求するための DHCP クライアントにします。

   装置が、IP アドレスまたはコンフィグレーションファイル名を DHCP サーバから得ることに失敗した場合、1 つの IP アドレスと 1 つのコンフィグレーションファイル名を得るまで、機器は要求を繰り返します。

   処理を中断する場合、<CTRL+C>を押下します。

2) 関連するパラメータを取得したのち、装置は指定した TFTP サーバからコンフィグレーションファイルを取得するため、TFTP 要求を送信します。そして取得したコンフィグレーションファイルを適用します。クライアントがコンフィグレーションを取得できない場合、デフォルトコンフィグレーションで起動します。

Auto Config を実現するために、DHCP サーバ、DNS サーバ、TFTP サーバを設定する必要がありますが、Auto Config を行う装置に設定をする必要はありません。

Auto Config を使用する場合、装置を起動させる前に、Auto Config で必要なインタフェースのみをネットワークに接続してください。

18.2.1 DHCP による IP アドレスと設定パラメータの取得

I. アドレス取得プロセス

装置は起動時に DHCP クライアントのためにインタフェース Vlan を作成します。

DHCP クライアントは、オプション 55 フィールドでコンフィグレーションファイル名、TFTP サーバのドメイン名と IP アドレス、DNS サーバの IP アドレスなどのクライアントが DHCP サーバから得たい情報を指定し、DHCP 要求をブロードキャストで送信します。

DHCP サーバから DHCP 応答を受信したのち、装置は IP アドレスを取得し、DHCP 応答の以下のフィールドを解決します。

- **オプション 67 あるいは file フィールド**－コンフィグレーションファイル名を取得します。装置は最初にオプション 67 を解決します。オプション 67 にコンフィグレーションファイル名が含まれる場合、装置はファイルフィールドを解決しません。オプション 67 にコンフィグレーションファイル名が含まれない場合、装置は file フィールドを解決します。
- **オプション 66**－TFTP サーバのドメイン名を取得します。
- **オプション 150**－TFTP サーバの IP アドレスを取得します。
- **オプション 6**－DNS サーバの IP アドレスを取得します。

DHCP サーバから DHCP 応答を受信しない場合、装置は一時的なコンフィグレーションを削除し、デフォルトコンフィグレーションで起動します。

一時的なコンフィグレーションは、下記の 2 つです。

- Auto Config を実行するために起動時に設定されたコンフィグレーション
- ホスト名ファイルを使用した際に設定された **ip host** コマンド

DHCP の詳細は、オペレーションマニュアルのセクション 4 *IP サービス*“*DHCP の概要*”を参照してください。**ip host** コマンドの詳細は、コマンドマニュアルのセクション 4 *IP サービス*“*DNS*”を参照してください。

II. DHCP サーバのアドレスプールの選択の基本

DHCP サーバは、クライアント用にアドレスプールから IP アドレスや、ほかのネットワークのコンフィグレーションパラメータを選択します。

DHCP は以下のタイプのアドレスプールをサポートします。

- **ダイナミックアドレスプール** – ダイナミックアドレスプールは、DHCP サーバがクライアントに動的に割り当てる IP アドレス範囲とほかのパラメータが含まれます。
- **スタティックアドレスプール** – スタティックアドレスプールには IP アドレスと MAC アドレス（またはクライアント ID)のバインディングが含まれます。DHCP サーバはバインディングされた IP アドレスと関連するコンフィグレーションパラメータを、MAC アドレスまたは ID がバインディングと一致する要求を持ったクライアントに割り当てます。これにより、クライアントは固定の IP アドレスを取得できます。

以下のいずれかの方法からアドレスプールの使用方法を選んでください。

- 複数の装置が同一のコンフィグレーションファイルを使う場合、同一のコンフィグレーションパラメータ（たとえばコンフィグレーションファイル名)と IP アドレスを装置に割り当てるために DHCP サーバ上のダイナミックアドレスプールを設定することができます。この場合に、コンフィグレーションファイルは装置共通のコンフィグレーションのみを含むことができ、各装置の具体的なコンフィグレーションは、ほかの方法で行う必要があります。たとえば、コンフィグレーションファイルは、管理者が装置で各装置に特定のコンフィグレーション（各インタフェースの IP アドレスを設定など)を実行できるようにするために、Telnet を有効にし、装置のローカルユーザを作成することができます。
- 複数の装置が異なるコンフィグレーションファイルを使用する場合、各装置で固定の IP アドレス、特定のコンフィグレーションファイルを取得できるようにするため、スタティックアドレスプールを設定する必要があります。この方法では装置に追加で設定をする必要はありません。

スタティックアドレスプールを設定するため、対応するクライアント ID を取得する必要があります。装置のクライアント ID を取得する場合、装置が DHCP を通して IP アドレスを取得したのち、DHCP サーバのアドレスの割り当て情報を表示する **display dhcp server ip-in-use** コマンドを使用します。

18.2.2 TFTP サーバからのコンフィグレーションファイルの取得

Auto Config 中、装置は TFTP サーバから以下のファイルを取得することができます。

- DHCP 応答のオプション 67 あるいは file フィールドによって指定されたコンフィグレーションファイルを取得することができます。

- IP アドレスとホスト名のマッピングが記載されているホスト名ファイル network.cfg を取得することができます。

たとえば、ホスト名ファイルには以下が含まれます。

```
ip host host1 101.101.101.101
ip host host2 101.101.101.102
ip host client1 101.101.101.103
ip host client2 101.101.101.104
```

⚠ **重要：**

- ip hostの文字列の行の先頭には半角スペースが必要です。
- ホスト名ファイルで定義するホスト名は、該当するホストで使用する予定のコンフィグレーションファイル名と同一にする必要があります。

- ホスト名ファイルで定義されたホスト名とファイル名が一致するコンフィグレーションファイル hostname.cfg を取得することができます。（たとえば、ホスト名が aaa である場合、コンフィグレーションファイル名は aaa.cfg です。）
- デフォルトのコンフィグレーションファイルを取得することができます。デフォルトのコンフィグレーションファイル名は device.cfg です。

I. コンフィグレーションファイルの取得手順

Auto Config は、以下の手順で動作します。

1) レイヤ 2 イーサネットインタフェースのステータスを識別します。1 つ以上のレイヤ 2 イーサネットインタフェースが UP 状態にあるならば、機器はデフォルト VLAN の VLAN インタフェース(vlan1)を使います。
2) すべてのレイヤ 2 イーサネットインタフェースが、Down 状態ならば、機器は 30 秒待った後、ステップ 1 に戻り、リトライします。

II. TFTP 要求の送信モード

装置は以下に示すように TFTP 要求をユニキャストとブロードキャストのどちらで送信するか選択します。

- DHCP 応答に適切な TFTP サーバの IP アドレスが含まれている場合、装置は TFTP サーバに TFTP 要求をユニキャストで送信します。
- DHCP 応答に適切な TFTP サーバの IP アドレスが含まれていない場合、装置は DHCP 応答に含まれる TFTP サーバのドメイン名を解決します。ドメイン名は DNS サーバを使用して IP アドレスにマッピングされます。TFTP サーバのドメイン名の解決が行われた場合、装置は TFTP サーバに TFTP 要求をユニキャストで送信します。TFTP サーバのドメイン名の解決が行われなかった場合、装置は TFTP サーバに TFTP 要求をブロードキャストで送信します。
- DHCP 応答に TFTP サーバの IP アドレス、およびドメイン名が含まれていない、あるいは TFTP サーバが不正である場合、装置は TFTP 要求をブロードキャストで送信します。

TFTP 要求をブロードキャストで送信したのち、コンフィグレーションファイルを取得するため、装置は TFTP 要求に最初に応答した TFTP サーバを選択します。要求したコンフィグレーションファイルが TFTP サーバに存在しない場合、TFTP 要求は失敗します。一

時的なコンフィグレーションの設定を削除し、デフォルトコンフィグレーションで起動します。

装置と TFTP サーバが異なるサブネットにある場合、装置からの TFTP 要求をブロードキャストではなく、ユニキャストパケットに変更します。指定した TFTP サーバにユニキャストパケットを送信するため、ゲートウェイで UDP ヘルパーを設定する必要があります。

装置と TFTP サーバが異なるサブネットにある場合、装置からブロードキャストで送信された TFTP 要求をゲートウェイでユニキャストパケットに変更し、ユニキャストパケットを指定された TFTP サーバに転送するように UDP ヘルパー機能を設定する必要があります。

18.2.3 コンフィグレーションファイルの適用

コンフィグレーションファイルを取得したのち、装置は一時的なコンフィグレーションの設定を削除し、取得したコンフィグレーションファイルを適用します。コンフィグレーションファイルを取得していない場合、30 秒待った後、Auto Config を繰り返します。プロセスを止めるために、Ctrl+C または Ctrl+D キーを押してください。

基本的にコンフィグレーションファイルは適用した後に削除されます。**save** コマンドでコンフィグレーションの設定を保存してください。設定を保存せずに再起動をした場合、再起動後に Auto Config が再度実行されます。**save** コマンドの詳細は、コマンドマニュアルのセクション 1 *はじめに "コンフィグレーションファイル管理"* を参照してください。

🕮 **メモ**：

TFTP サーバに保存するコンフィグレーションファイルの末尾に **save force** コマンドを含めることで自動的に保存まで行うことが可能です。

⚠ **重要**：

auto-config 機能で未設定のコマンドは、デフォルト値となります。

QX-S4800X シリーズ Ethernet スイッチ

オペレーションマニュアル

2. IRF スタック

本マニュアルは以下に示す章で構成されています。

01-IRF スタック

目次

このセクションのページは **2-x-x** です。

1 章 IRF スタック 1-1
1.1. 概要 1-1
1.1.1. IRF ネットワークモデル 1-1
1.1.2. IRF スタックの利点 1-1
1.1.3. 基本コンセプト 1-2
1.1.4. IRF ネットワークトポロジ 1-4
1.1.5. Master の選定 1-5
1.1.6. インタフェースの命名規則 1-6
1.1.7. ファイルシステム命名規則 1-6
1.1.8. 設定の同期メカニズム 1-7
1.1.9. マルチアクティブの検知の処理 1-7
1.1.10. MAD メカニズム 1-10
1.2. 制限とガイドライン 1-14
1.2.1. IRF スタックのハードウェアの互換性 1-14
1.2.2. IRF スタックのソフトウェア 1-14
1.2.3. IRF スタック物理インタフェースの選択 1-14
1.2.4. IRF スタックのトランシーバモジュールとケーブルの選定 1-15
1.2.5. IRF スタックポートの接続 1-15
1.2.6. IRF スタック物理インタフェースの制限とガイドライン 1-16
1.3. IRF スタック設定作業リスト 1-17
1.4. IRF スタックユニットのセットアップの計画 1-17
1.5. IRF スタックユニットの設定 1-18
1.5.1. IRF スタックユニット設定作業リスト 1-18
1.5.2. 各 IRF スタックメンバ装置へのメンバ ID の割り当て 1-18
1.5.3. 各メンバ装置のプライオリティの設定 1-19
1.5.4. IRF スタックポートと物理インタフェースへの関連付け 1-19
1.5.5. IRF スタック物理インタフェースの接続 1-22
1.5.6. IRF スタックユニットのアクセス 1-22
1.6. MAD の設定 1-22
1.6.1. 制限とガイドライン 1-22
1.6.2. LACP MAD の設定 1-23
1.6.3. BFD MAD の設定 1-24
1.6.4. ARP MAD の設定 1-27
1.6.5. MAD によるシャットダウンアクションからのサービスインタフェースの除外の設定 1-30
1.6.6. IRF スタックユニットの回復 1-31
1.7. IRF スタックユニットの IRF スタックの設定の最適化 1-31
1.7.1. メンバ装置の説明の設定 1-31
1.7.2. IRF スタックの bridge MAC アドレスの設定 1-32
1.7.3. ソフトウェア同期用のソフトウェアオートアップグレードの有効化 1-33
1.7.4. IRF スタックリンクダウン検出遅延の設定 1-34
1.7.5. IRF スタック物理インタフェースを持つ拡張インタフェースカードの取り外し 1-35
1.7.6. IRF スタック物理インタフェースを持つ拡張インタフェースカードの交換 1-35
1.8. IRF スタックの表示と維持 1-36

1.9. IRF スタックの設定例 ····· 1-36
1.9.1. LACP MAD を使用する場合の IRF スタックの設定例 ····· 1-36
1.9.2. BFD MAD を使用する場合の IRF スタックの設定例 ····· 1-42
1.9.3. ARP MAD を使用する場合の IRF スタックの設定例 ····· 1-48

1章 IRF スタック

1.1. 概要

IRF(Intelligent Resilient Framework)スタック機能は、同一レイヤの複数の装置を IRF スタック(IRF fabric)ポートで相互接続することにより、仮想的に 1 つの装置とすることができます。データセンタクラスの有効性、柔軟性を提供します。IRF スタック仮想化技術は複数の装置の電力、装置間の動作、管理、連続したメンテナンスを一括して行うことができます。

1.1.1. IRF ネットワークモデル

図 1-1 に 2 つのメンバ装置がある IRF スタックユニットを示します。上位レイヤおよび下位レイヤのユーザには、1 つの装置として見えます。

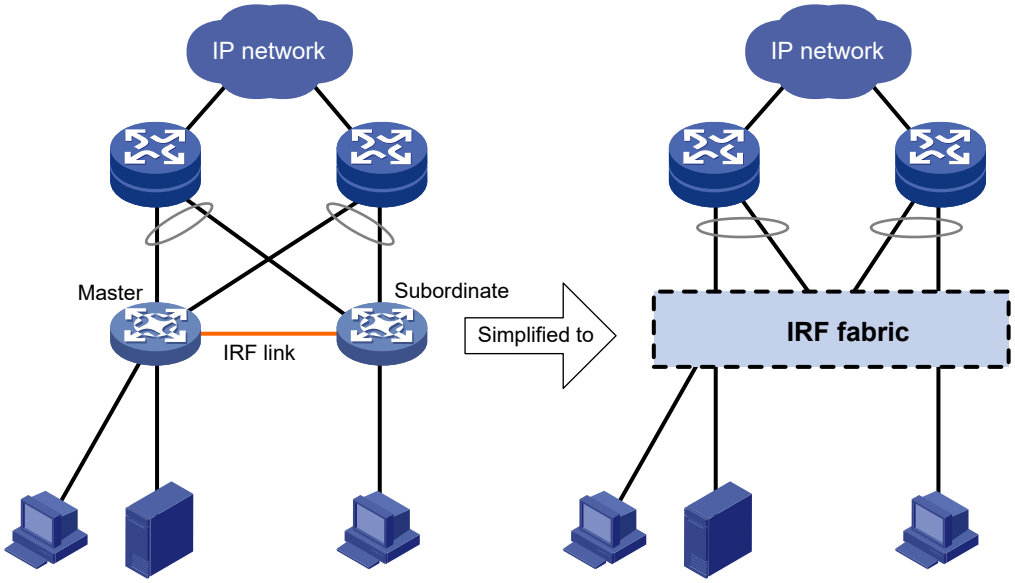


図 1-1 IRF アプリケーションシナリオ

1.1.2. IRF スタックの利点

IRF スタックは以下の利点があります。

- **簡素化されたトポロジと容易な管理**—IRF スタックユニットは 1 つのノードとして、ネットワーク上で 1 つの IP アドレスでアクセス可能です。IRF スタックユニットのすべてのメンバ装置を管理するために、この IP アドレスを使用し、メンバ装置にログインすることができます。加えて IRF スタックメンバ装置でスパニングツリーを動作させる必要がありません。

- **1:N 冗長性**－IRF スタックユニット全体を管理し、制御するため、IRF スタックで 1 つのメンバ装置が Master として動作します。Master をバックアップする間、ほかのすべてのメンバはサービスを処理します。Master が故障したとき、ほかのメンバ装置はサービスを中断することなく、メンバ装置の中から新しい Master を選定します。
- **IRF スタックリンクアグリゲーション**–負荷分散されたリンクアグリゲート IRF スタック接続を作成するため、隣接したメンバ装置間で、IRF スタックポートに複数の物理リンクを割り当てることができます。
- **マルチシャーシリンクアグリゲーション**－IRF スタックユニットと IRF スタックメンバを経由して上流あるいは下流の装置間で物理リンクを集約するために、Ethernet リンクアグリゲーション機能を使用することができます。
- **ネットワークのスケーラビリティと信頼性**－IRF スタックユニットの処理能力はすべてのメンバ装置の全処理能力と同一です。ネットワークのトポロジを変更することなく、メンバ装置を追加することで容易に、ポート、ネットワーク帯域幅、IRF スタックユニットの処理能力を増加することができます。

1.1.3. 基本コンセプト

I. IRF スタックメンバ役割

IRF スタックは、Master と standby（ここでは subordinate と呼ばれます）の 2 つのメンバの役割(ロール)を使用します。

装置は IRF スタックユニットを形成するとき、IRF スタックユニットを管理、制御するため、Master を選定し、ほかの装置は Master をバックアップします。Master 装置が故障したとき、ほかの装置が自動的に新しい Master を選定します。Master の選定についての詳細は、オペレーションマニュアルのセクション 2 *IRF スタック* "*IRF スタック*"の"*Master の選定*"を参照してください。

II. IRF スタックメンバ ID

IRF スタックユニットでは、メンバ装置を識別し、管理するためにメンバ ID を使用します。メンバ ID 情報は、IRF スタックユニットのインタフェースとファイルを識別するため、インタフェースをインタフェース番号とファイルのパスの最初の部分が含まれます。2 つの装置が同じ IRF スタックメンバ ID を持つとき、IRF スタックユニットを形成することはできません。装置の IRF スタックメンバ ID がすでに IRF スタックユニットで使用されている場合、装置は IRF スタックに加入することができません。

III. メンバプライオリティ

メンバプライオリティで IRF スタックの役割を決めます。高いプライオリティを設定したメンバ装置が Master になりやすくなります。

IV. IRF スタックポート

IRF スタックポートは IRF スタックメンバ装置間の接続を行うための論理的なインタフェースです。IRF が有効な各装置は 2 つの IRF スタックポートをサポートします。

IRF スタックポートは IRF スタックポート *n*/1、IRF スタックポート *n*/2 と記載され、*n* は装置のメンバ ID です。本書では、2 つの IRF スタックポートを IRF スタックポート 1、IRF スタックポート 2 と表記します。

IRF スタックポートを使用するため、最小限 1 つの IRF スタック物理ポートを IRF スタックポートに結びつける必要があります。IRF スタックポートに割り当てられた IRF スタック物理ポートは自

動的にアグリゲート IRF スタックリンクを形成します。IRF スタックのすべての IRF スタック物理ポートがダウンした場合、IRF スタックポートはダウンします。

V. IRF スタック物理ポート

IRF スタック物理ポートは IRF スタックメンバ装置に接続し、IRF スタックポートに結びつける必要があります。IRF スタック物理ポートは、IRF スタックメンバ装置間の IRF スタックプロトコルパケットと、IRF スタックメンバ装置を通過するデータパケットを転送します。

VI. IRF スタックの分裂

図 1-2 に示すように、IRF スタックユニットで障害が発生した際、2 つ以上の IRF スタックユニットに分裂します。分裂した IRF スタックは同一 IP アドレスで動作するため、ネットワークのルーティングと転送の問題を引き起こします。マルチアクティブコリジョンを早急に検知するため、最小限 MAD メカニズムを設定してください。(オペレーションマニュアルのセクション 2 *IRF スタック* "*IRF スタック*"の"MAD の設定"を参照してください。)

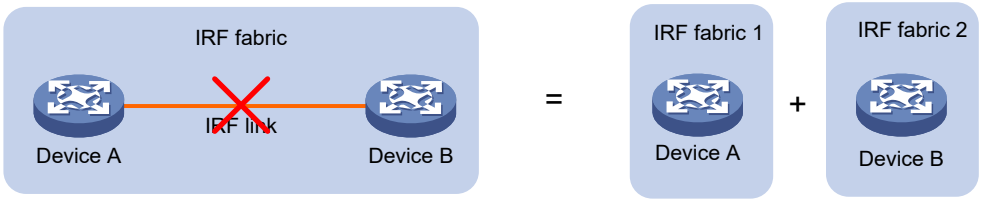


図 1-2 IRF スタックの分裂

VII. IRF スタックの結合

IRF スタックの結合とは、図 1-3 のように分裂した 2 つの IRF スタックユニットを再結合したり、2 つの独立な IRF スタックユニットを接続します。

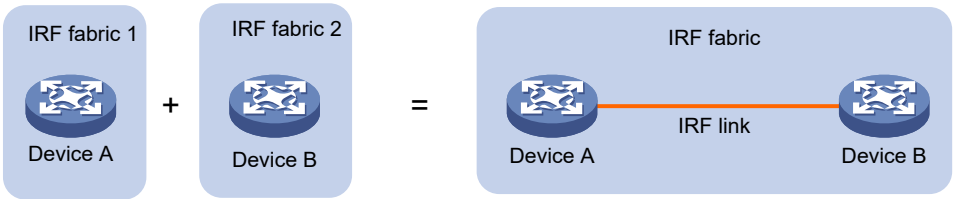


図 1-3 IRF スタックの結合

VIII. MAD

IRF スタックリンクに障害が発生すると、同一 IP アドレスが含まれる同一レイヤ 3 の設定で動作する 2 つの IRF スタックユニットに分裂します。IP アドレスの衝突とネットワークの問題を防ぐため、IRF スタックは複数の IRF スタックユニットを識別し、衝突を処理し、故障から回復する MAD（multi-active detection）メカニズムを使用します。

IX. IRF スタックドメイン ID

IRF スタックユニットは 1 つの IRF スタックドメインを形成します。IRF は IRF スタックユニットを識別するために IRF スタックドメイン ID を使用し、IRF スタックユニットが互いに干渉しないようにします。

図 1-4 に示すように、Device A と Device B は IRF 1 を形成しています。Device C と Device D は IRF 2 を形成しています。各 IRF スタックユニットは LACP MAD のリンクを持っています。メンバ装置が MAD 用の拡張 LACP パケットを受信したとき、パケットがローカル IRF スタックユニットから受信したのかどうかを調べるため、パケットのドメイン ID を確認します。それにより、メンバ装置は正しくパケットを処理することができます。

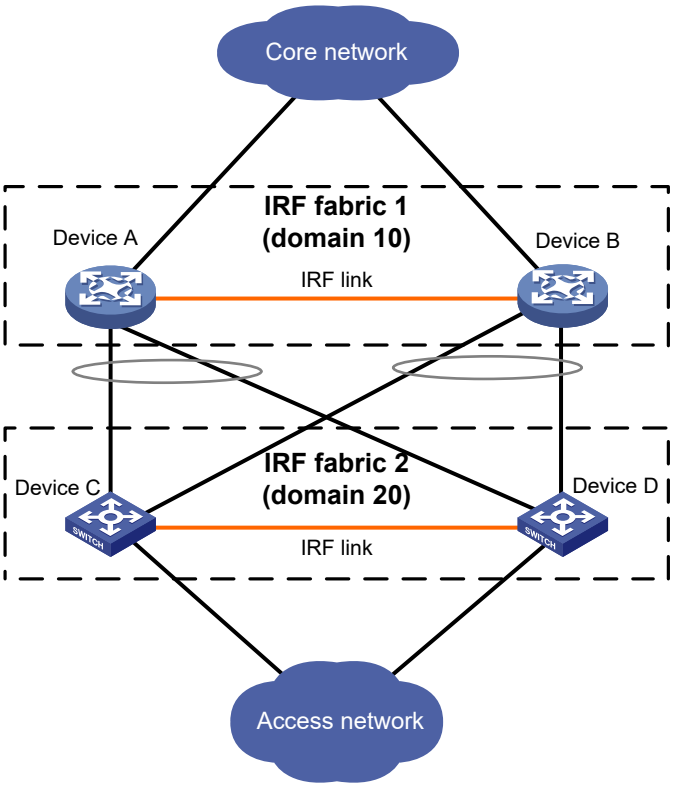


図 1-4 2 つの IRF スタックドメインによるネットワーク

1.1.4. IRF ネットワークトポロジ

IRF スタックは、デイジーチェーン構成、またはリング構成のトポロジを構成することができます。リング構成は信頼性のある構成となります(図 1-5 を参照してください。)。リング構成では 1 つのリンクが故障しても、IRF スタックの分裂を起こさず、IRF スタックサービスに影響を与えないでデイジーチェーン構成になります。

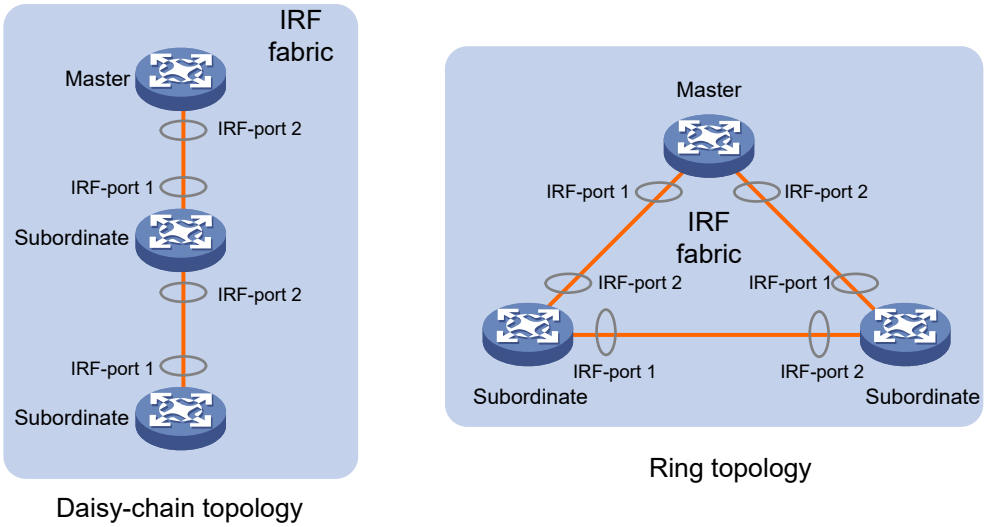


図 1-5 デイジーチェーン構成とリング構成

1.1.5. Master の選定

Master の選定は以下の状況下で IRF スタックユニットのトポロジの変更があるたびに行われます。

- IRF スタックユニットが確立されました。
- Master 装置の故障や取り外しが行われました。
- IRF スタックユニットが分裂しました。
- 独立した IRF スタックユニットが結合しました。

メモ：

Master の選定は分裂した 2 つの IRF スタックユニットを結合するときには行われません。結合した IRF スタックユニットの Master 装置の詳細は、オペレーションマニュアルのセクション 2 *IRF スタック* "*IRF スタック*"の“*故障回復*”を参照してください。

Master の選定は降順で以下のルールを使用します。

1. 新しい IRF スタックメンバのプライオリティが高くても現在の Master が有効となります。

   IRF スタックユニットが形成中で、すべての IRF スタックメンバがそれぞれ Master と認識している場合、このルールは省略されます。

2. より高いプライオリティを持つ IRF スタックメンバが有効となります。すべての IRF スタックメンバが同一のプライオリティである場合、このルールは省略されます。
3. システムの稼動時間がもっとも長いメンバ装置が有効となります。

   スタートアップから 10 分以内である場合、稼働時間は同時とみなされます。これらのメンバ装置は次の tiebreaker が適用されます。

4. もっとも低い CPU MAC アドレスを持つメンバ装置が有効になります。

新しい IRF スタックユニットをセットアップするため、subordinate (Standby)メンバ装置は、Master の選定が行われた後、再起動する必要があります。

IRF スタックユニットの結合を行う間、Master の選択に失敗した IRF スタックユニットのメンバは手動で再起動する必要があります。

1.1.6. インタフェースの命名規則

インタフェース名は *chassis-number/slot-number/port-index* のフォーマットで命名されます。

- *chassis-number*–スイッチの IRF スタックメンバ ID です。デフォルトは 1 です。スイッチが IRF スタックユニットの一部かどうかにかかわらず、常に IRF スタックメンバ ID が適用されます。スイッチが 1 台である場合、スタンドアロン（1 台構成）の IRF スタック構成であると認識します。
- *slot-number*–装置のフロントパネルあるいは背面にある拡張インタフェースカードのスロット番号です。
  - フロントパネルのスロット番号は 0 です。
  - インタフェースが拡張インタフェースカード上にある場合、スロット番号は 1 です。
- *interface-index*–装置のインタフェースのインデックスです。インタフェースのインデックスは装置で有効なポート数に依存します。インタフェースのインデックスを識別する場合、装置のポートインデックスマークを参照してください。

例：

スタンドアロンのスイッチにて Ten-GigabitEthernet 3/0/1 は装置の最初のポートを示します。リンクタイプをトランクに設定します。

```
<Switch> system-view
[Switch] interface Ten-gigabitethernet 3/0/1
[Switch-Ten-GigabitEthernet3/0/1] port link-type trunk
```

1.1.7. ファイルシステム命名規則

スタンドアロンの IRF スタックユニットの装置のファイルシステムにアクセスするには、記憶媒体の名前を用いることができます。

複数の装置から構成される IRF スタックユニットでは、Master のファイルシステムにアクセスするため、記憶媒体の名前を用いることができます。ほかの IRF スタックメンバのファイルシステムに、**slot***member-ID#storage-device-name* のフォーマットを用いて、アクセスすることができます。

記憶媒体の命名規則の詳細は、オペレーションマニュアルのセクション 1 *はじめに"ファイルシステム管理"*を参照してください。

例：

- Master 装置に搭載されているフラッシュのルートディレクトリ直下に **test** フォルダを作成してアクセスするには、以下のステップを実行してください。

```
<Master> mkdir test
Creating directory flash:/test... Done.
<Master> cd test
```

```
<Master> dir
Directory of flash:/test
The directory is empty.

1038336 KB total (690572 KB free)
```

- IRF スタックメンバ 3 に搭載されているフラッシュのルートディレクトリ直下の **test** フォルダにアクセスするには、以下のステップを実行してください。

```
<Master> mkdir slot3#flash:/test
Creating directory slot3#flash:/test... Done.
<Master> cd slot3#flash:/test
<Master> dir
Directory of slot3#flash:/test
The directory is empty.

1038336 KB total (690572 KB free)
```

1.1.8. 設定の同期メカニズム

IRF スタックは厳密なカレントコンフィグレーション同期メカニズムを使用します。IRF スタックユニットで、すべての装置は Master のカレントコンフィグレーションを取得し稼働させます。設定の変更は自動的に Master から残された装置に伝番されます。これらの装置のコンフィグレーションファイルは保持されますが、コンフィグレーションファイルは適用されません。IRF スタックユニットから削除されたのち、自身の次回の起動に使用するコンフィグレーションファイルを使用して起動します。

装置を IRF スタックユニットにメンバとして追加する前に、装置の次回に起動するスタートアップコンフィグレーションファイルをバックアップしてください。

メンバ装置の次回に起動するスタートアップコンフィグレーションファイルは、Master とメンバで次回に起動するスタートアップコンフィグレーションファイルに同一のファイル名を使用する場合、上書きされる可能性があります。バックアップファイルを使用すると、IRF スタックユニットからメンバを削除した後に元の設定を復元できます。

コンフィグレーション管理の詳細は、オペレーションマニュアルのセクション 1 *はじめに* "*コンフィグレーションファイル管理*"を参照してください。

1.1.9. マルチアクティブの検知の処理

マルチアクティブの処理は検知、衝突処理、故障回復があります。

I. 検知処理

IRF スタックは LACP、BFD、ARP を拡張することによって MAD メカニズムを提供します。

MAD メカニズムはドメイン ID とアクティブ ID(Master のメンバ ID)で各 IRF スタックユニットを識別します。もし複数のアクティブ ID をドメイン内で検知すると、MAD は IRF スタックの衝突や分裂が起こったと判断します。

MAD メカニズムの詳細は、オペレーションマニュアルのセクション 2 *IRF スタック* "*IRF スタック*" の"*MAD メカニズム*"を参照してください。

II. 衝突処理

マルチアクティブ衝突を検出すると、MAD はデータトラフィックを Recovery 状態にすることで、データトラフィックを転送するものを除くすべての IRF スタックユニットを無効にします。Recovery 状態に置かれた IRF スタックユニットは、非アクティブ IRF スタックユニットと呼ばれます。トラフィックを転送し続ける IRF スタックユニットは、アクティブ IRF スタックユニットと呼ばれます。

LACP MAD、BFD MAD は、以下の手順でマルチアクティブ衝突を処理します。

1. それぞれの IRF スタックでメンバ数を比較します。
2. メンバ数がもっとも多い IRF スタックユニットを除いた IRF スタックユニットを Recovery 状態にします。
3. メンバ数が同じ場合、LACP MAD は Master のメンバ ID を比較します。
4. もっとも数字の小さい Master のいる IRF スタックユニットを除いた IRF スタックユニットを Recovery 状態にします。
5. Recovery 状態となった IRF スタックユニットで、以下のポートを除いたすべての IRF スタック物理ポートをシャットダウンします。
   - IRF スタック物理インタフェース
   - **mad exclude interface** コマンドで指定されたポート

対照的に ARP MAD は、IRF スタックユニットのメンバ数を比較しません。MAD メカニズムは以下の処理でマルチアクティブ衝突を行います。

1. IRF スタックユニットの Master のメンバ ID を比較します。
2. もっとも数字の小さい Master のいる IRF スタックユニットを除いた IRF スタックユニットを Recovery 状態にします。
3. Recovery 状態となった IRF スタックユニットのネットワークポートに LACP MAD、BFD MAD と同様の設定をします。

III. 故障回復

2 つの分割された IRF スタックユニットを結合するため、故障した IRF スタックリンクを修復し、IRF スタックリンクの故障を取り除きます。

分裂した IRF スタックユニット間で故障した IRF スタックリンクが回復したとき、アクティブでない IRF スタックユニットのすべてのメンバ装置は subordinate(Standby)メンバとしてアクティブの IRF スタックユニットに加入します。そして MAD によってシャットダウンされたネットワークポートは、図 1-6 に示すようにもとの状態に戻ります。

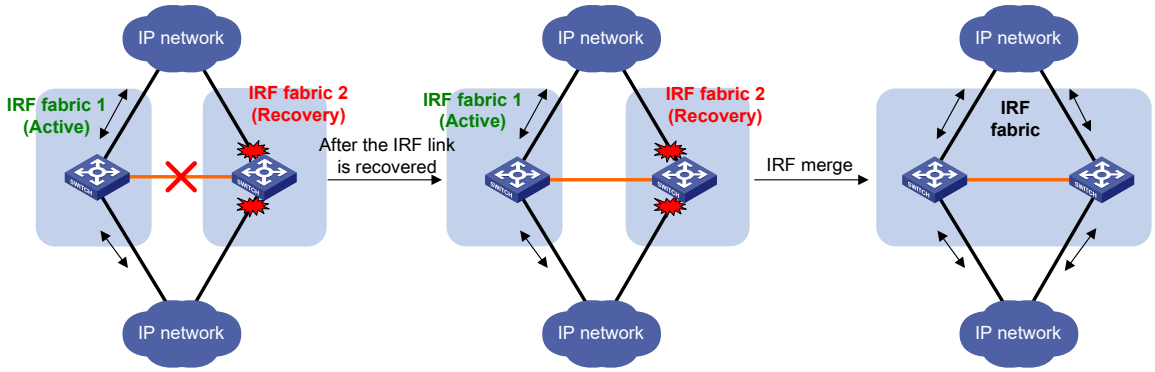


図 1-6 IRF スタックユニットの回復

IRF スタックリンクが回復する前にアクティブ状態の IRF スタックユニットが､故障した場合(図 1-7 を参照してください)、アクティブ状態でない IRF スタックユニットを回復するため、**mad restore** コマンドを実行してください。このコマンドはアクティブ状態でない IRF スタックユニットを Detect 状態に変更し、MAD によってシャットダウンとなったすべてのネットワークポートをアクティブ状態に変更します。IRF スタックリンク障害が回復したのち、IRF スタックが結合されます。

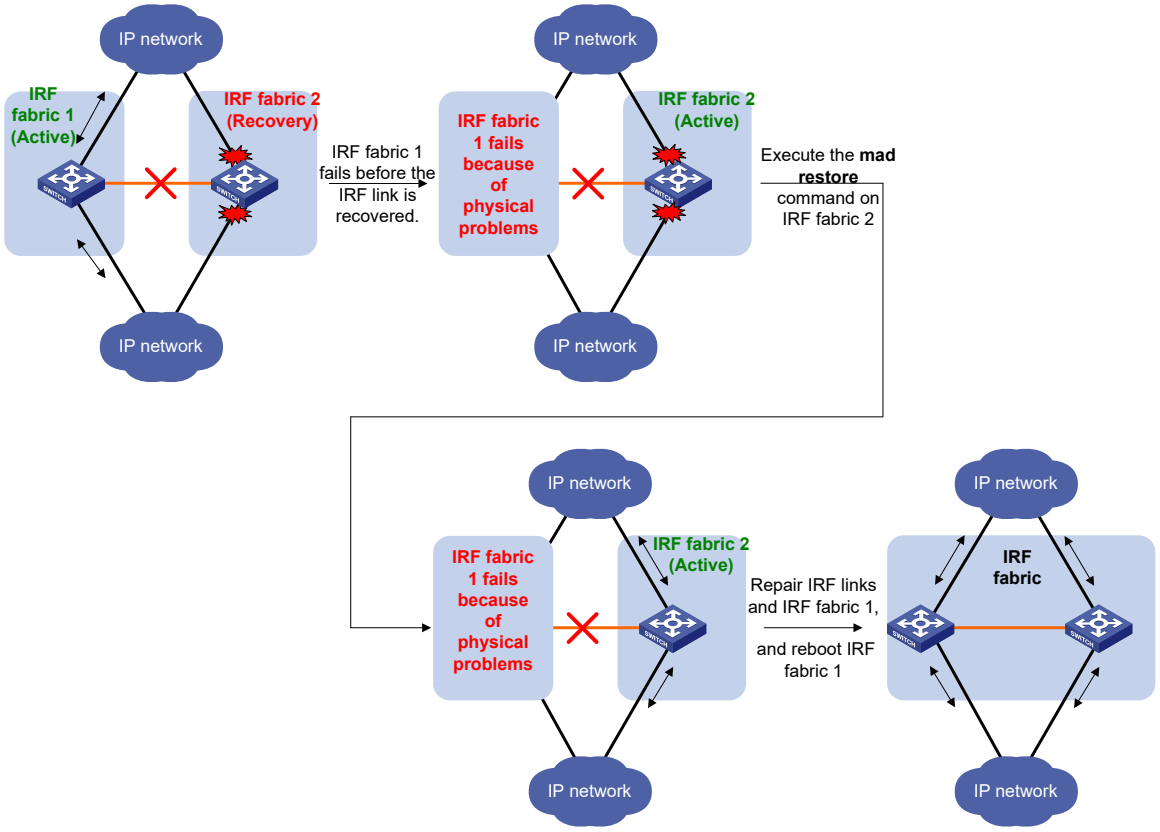


図 1-7 IRF スタックリンクが回復する前にアクティブ状態の IRF スタックユニットが故障した場合

1.1.10. MAD メカニズム

IRF スタックは LACP、BFD、ARP を拡張することで MAD メカニズムを提供します。

表 1-1 に MAD メカニズムとアプリケーションの比較を示します。

表 1-1 MAD 機能の比較

MAD 機能	長所	短所	アプリケーション
LACP MAD	• 検知速度が速いです。 • MAD 専用の IRF スタック物理ポートあるいはレイヤ 3 インタフェースが不必要です。	拡張LACPをサポートする中継装置が必要です。	IRFスタックユニットと上流または下流装置との間でリンクアグリゲーションを使用します。
BFD MAD	• 検知速度が速いです。 • 中継装置を使用する場合、ベンダの制限はありません。	ユーザトラフィックの転送に使用しないMAD専用ポートやレイヤ3インタフェースが必要です。	• さまざまなネットワーク構成に適用されます。 • 中継装置を使用しない場合、お互いのスイッチが近くに設置され少数のメンバで構成される IRF スタックユニットに適します。
ARP MAD	• 中継装置が不要です。 • 中継装置を使用する場合、ベンダの制限はありません。 • MAD 専用の IRF スタック物理ポートが不必要です。	• 検知速度が BFD MAD や LACP MAD より遅いです。 • ARP MAD リンクで共通の Ethernet ポートを使用している場合、スパニングツリー機能の有効化が必要です。	共通のEthernetポートを使用している場合、リンクアグリゲーションを使用せず、スパニングツリーを有効化するIPv4ネットワークに適します。

I. LACP MAD

図 1-8 に示すように、LACP MAD は以下の要件があります。

- 各 IRF スタックメンバは中間装置（対向装置）とリンクしている必要があります。
- すべてのリンクはダイナミックリンクアグリゲーショングループを形成する必要があります。
- 中間装置は拡張 LACP をサポートする必要があります。

IRF スタックメンバ装置は、IRF スタックユニットのドメイン ID とアクティブ ID を含んだ拡張 LACP データユニット(LACPDU)を送信します。中間装置は、1 つの IRF スタックメンバ装置からの拡張 LACP データユニットをほかのすべての IRF スタックメンバ装置に転送します。

- すべての IRF スタックメンバ装置が送信する拡張 LACPDU 内のドメイン ID とアクティブ ID が同じならば、IRF スタックユニットが正常に動作していると判断します。

- ドメイン ID が同じであってもアクティブ ID が異なる場合、IRF スタックが分裂していると判断します。この場合、LACP MAD はセクション 2 *IRF スタック オペレーションマニュアル*の“*IRF スタック*”の“*衝突処理*”に説明した衝突処理を行います。

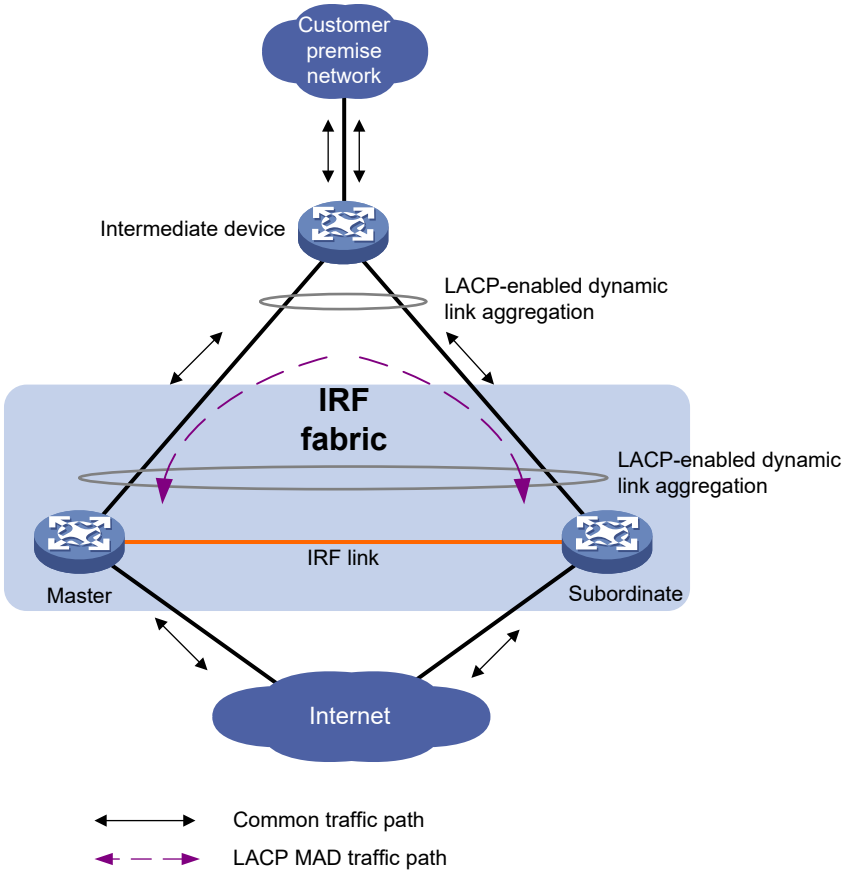


図 1-8 LACP MAD シナリオ

II. BFD MAD

BFD MAD は BFD を使用することでマルチアクティブ衝突を検知します。

BFD MAD は共通あるいはマネジメント Ethernet ポートを使用することができます。

マネジメント Ethernet ポートを使用する場合、中継装置が必要です。以下の要件に従うかどうか確認してください。

- 各 IRF スタックのメンバ装置は中継装置に接続する BFD MAD リンクがあります。
- 各 IRF スタックのメンバ装置はマスタ装置のマネジメント Ethernet ポートの MAD IP アドレスが割り当てられます。

共通 Ethernet ポートを使用する場合、以下の要件に従うかどうか確認してください。

- 各 IRF スタックのメンバ装置が中継装置に接続する BFD MAD リンクがあるか、すべてのメンバ装置が互いに BFD MAD リンクがあります。
- 中継装置がない場合、すべてのメンバ装置は互いに BFD MAD リンクがある必要があります。IRF スタックユニットに 2 つ以上のメンバ装置がある場合、IRF スタックメンバ装置に接続するため、中継装置を使用することを推奨します。IRF スタックメンバをフルメッシュにした場合、ブロードキャストループを発生する可能性があります。

- BFD MAD リンクの各ポートは BFD MAD で使用する VLAN に割り当てられます。各メンバ装置は VLAN インタフェースの MAD IP アドレスが割り当てられます。

BFD MAD リンクあるいは BFD MAD VLAN は専用のリンクが必要です。ほかの目的で BFD MAD リンクあるいは BFD MAD VLAN を使用しないでください。

メモ:

- BFD MAD リンクに接続されているポートに同じ VLAN を割り当ててください。
- IRF スタックユニットのすべてのマネジメント Ethernet ポートで、マスタのマネジメント Ethernet ポートのみがアクセス可能です。

図 1-9 に、中継装置を使用する一般的な BFD MAD シナリオを示しています。中継装置で、BFD MAD リンク上のポートを同じ VLAN に割り当てます。

図 1-10 に、中継装置を使用しない一般的な BFD MAD シナリオを示します。

BFD MAD では、Master は、送信元 IP アドレスとして MAD IP アドレスを使用して、他のメンバ装置との BFD セッションを確立しようと試みます。

- IRF スタックユニットが結合されている場合、Master の MAD IP アドレスのみが有効になります。 Master は他のメンバと BFD セッションを確立できません。 **display bfd session** コマンドを実行すると、BFD セッションの状態は **Down** になります。
- IRF スタックユニットが分裂すると、分裂した IRF スタックユニット内の Master の IP アドレスが有効になります。Master は BFD セッションを確立できます。**display bfd session** コマンドを実行すると、2 つの装置間の BFD セッションの状態は **Up** になります。

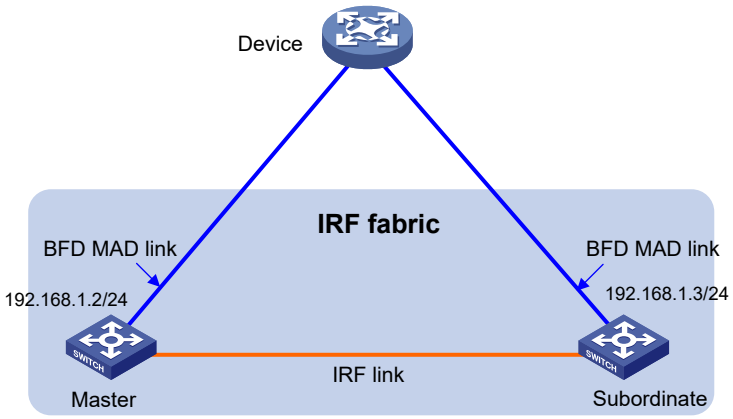


図 1-9 中継装置を使用する一般的な BFD MAD シナリオ

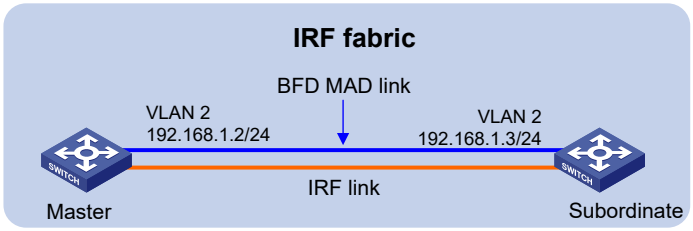


図 1-10 中継装置を使用しない一般的な BFD MAD シナリオ

III. ARP MAD

ARP MAD は、IRF ドメイン ID とアクティブ ID を含んだ拡張 ARP パケットによってマルチアクティブ衝突を検知します。

ARP MAD は共通 Ethernet ポート、マネジメント Ethernet ポートで使用することができます。

マネジメント Ethernet ポートを使用する場合、ARP MAD は中継装置で動作する必要があります。以下の要件に従ってください。

- 各メンバ装置のマネジメント Ethernet ポートを中継装置に接続してください。
- 中継装置で ARP MAD に使用するポートは同一 VLAN にしてください。

共通 Ethernet ポートを使用する場合、中継装置への接続に関わらず、ARP MAD が動作することができます。以下の要件に従ってください。

- 中継装置を使用する場合、図 1-11 に示すように各メンバ装置を中継装置に接続してください。IRF スタックユニットと中継装置間でスパニングツリー機能を動作させてください。この状態ではデータリンクは使用することができます。
- 中継装置を使用しない場合、各 IRF スタックメンバ装置をほかのメンバ装置に接続してください。この状態では IRF スタックリンクは ARP MAD として使用することができません。

各 IRF スタックメンバは、受信した拡張 ARP パケットに含まれるドメイン ID とアクティブ ID を比較します。

- ドメイン ID が異なる場合、異なる IRF スタックメンバユニットからの拡張 ARP パケットと判断し、MAD メカニズムの処理を継続しません。
- ドメイン ID が同じ場合、装置はアクティブ ID を比較します。
  - アクティブ ID が異なる場合、IRF スタックユニットが分裂していると判断します。
  - アクティブ ID が同じ場合、IRF スタックユニットは正常に動作していると判断します。

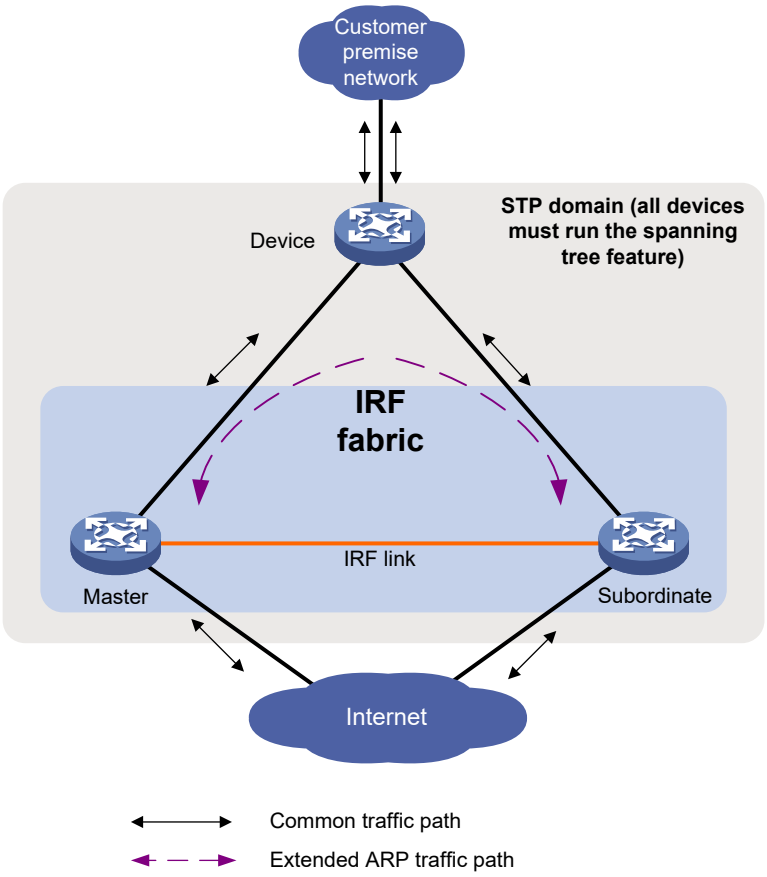


図 1-11 ARP MAD シナリオ

1.2. 制限とガイドライン

1.2.1. IRF スタックのハードウェアの互換性

QX-S4800X シリーズは、同じシリーズの装置でのみ IRF スタック(IRF fabric)ユニットを形成できます。

1.2.2. IRF スタックのソフトウェア

すべての IRF スタックメンバは、同じソフトウェアバージョンを使用してください。すべてのメンバ装置でソフトウェアオートアップグレード機能ができることを確認してください。

1.2.3. IRF スタック物理インタフェースの選択

IRF スタックリンクの拡張インタフェースカードの以下のポートを使用します。

- 10GBase-T Ethernet ポート
- SFP+ポート

- QSFP+ポート

QSFP+10-GE 分割インタフェースは IRF スタック物理インタフェースとして使用することはできません。

1.2.4. IRF スタックのトランシーバモジュールとケーブルの選定

トランシーバモジュールとケーブルを選択するとき、以下の制限とガイドラインに従ってください。

- 短い距離で通信するために 10GE ポートを接続する場合、カテゴリ-6A 以上のツイストペアケーブルを使用してください(カテゴリ-6A、カテゴリ-6E、カテゴリ 7 を含みます)。
- 短い距離で通信するために SFP+ポートを接続する場合、SFP+ 銅線ケーブルを使用してください。
- 長い距離で通信する場合、SFP+ポートを接続する場合、SFP+光ファイバケーブルを使用します。
- QSFP+ポートでは、QSFP+ トランシーバモジュールとファイバを長距離接続に使用し、QSFP+ケーブルを短距離接続に使用します。
- トランシーバモジュールは、IRF スタックリンクの対向ポートと同じタイプを使用してください。

SFP+/QSFP+ポート、SFP+/QSFP+銅線ケーブル、SFP+/QSFP+ トランシーバモジュールの詳細は、*インスタレーションマニュアル*を参照してください。

メモ:

本装置に使用するトランシーバモジュールとケーブルは、NEC 指定の SFP+/QSFP+ トランシーバモジュール、SFP+/QSFP+ケーブルを使用してください。
なお、サポートする SFP+/QSFP+ トランシーバモジュールと SFP+/QSFP+ケーブルは、変更する可能性があります。

1.2.5. IRF スタックポートの接続

2 つの隣接する IRF スタックメンバを接続するとき、以下の制限とガイドラインに従ってください。

- 一方のメンバの IRF スタックポート 1 の IRF スタック物理インタフェースを他方の IRF スタックポート 2 の IRF スタック物理インタフェースに接続してください。
- 一方のメンバ装置の両方の IRF スタックポートの IRF スタック物理インタフェースをほかの装置の両方の IRF スタックポートの IRF スタック物理インタフェースに接続しないでください。

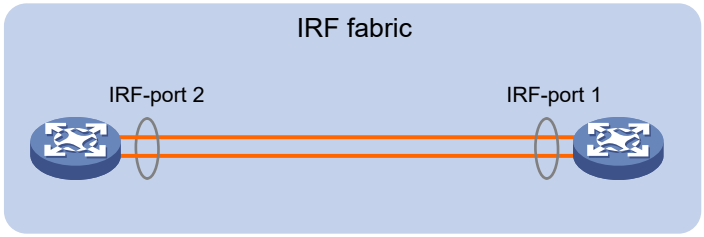


図 1-12 IRF スタック物理インタフェースの接続

1.2.6. IRF スタック物理インタフェースの制限とガイドライン

I. コマンドの制限

IRF スタックポートに関連付けられている物理インタフェースでは以下のコマンドのみ実行することができます。

- 以下のインタフェースコマンド
  - **description**
  - **flow-interval**
  - **shutdown**

  詳細はコマンドマニュアルのセクション 3 *アクセス "Ethernet インタフェース"*を参照してください。
- MAC アドレステーブルの **mac-address static source-check enable** コマンドを実行することができます。詳細はコマンドマニュアルのセクション 3 *アクセス "MAC アドレステーブル"*を参照してください。
- 以下の LLDP コマンド
  - **lldp admin-status**
  - **lldp check-change-interval**
  - **lldp enable**
  - **lldp encapsulation snap**
  - **lldp notification remote-change enable**
  - **lldp tlv-enable**

  詳細はコマンドマニュアルのセクション 3 *アクセス "LLDP "*を参照してください。

IRF スタック物理インタフェースで **mirroring-group reflector-port** コマンドを実行したとき、物理インタフェースと IRF スタックポート間のバインディングが削除されます。インタフェースが IRF スタックポートのメンバインタフェースだけになる場合、IRF スタックの分裂を避けるため、リフレクタポートとして物理インタフェースを設定しないでください。コマンドの詳細は、コマンドマニュアルのセクション 11 *システム管理 "ポートミラーリング"*を参照してください。

II. IRF スタック物理インタフェースのループ除去メカニズムと SNMP のモニタリング

IRF スタックメンバ装置がパケットを転送する前に、送信元と宛先の物理インタフェースと IRF スタックトポロジにもとづいて、フォワーディングパス上にループが存在するかどうかを識別します。

ループが存在する場合、装置はループパスの送信元インタフェース上のパケットを破棄します。このループ除去メカニズムは、IRF スタック物理インタフェース上で大量のブロードキャストパケットを削除します。 SNMP ツールを使用するときにパケット廃棄の SNMP 通知を減らすには、IRF スタック物理インタフェースでパケット転送を監視しないでください。

1.3. IRFスタック設定作業リスト

IRF スタック(IRF fabric)設定作業リスト
1. IRF スタックユニットの設定
2. MAD の設定 IRFスタックユニットで少なくとも1つのMADメカニズムを設定してください。 MADの互換性についての詳細は、オペレーションマニュアルのセクション2 *IRFスタック* “*IRFスタック*”の“*MADメカニズムの互換性*”を参照してください。 • LACP MAD の設定 • BFD MAD の設定 • ARP MAD の設定 • MAD によるシャットダウンアクションからのサービスインタフェースの除外 この機能は、IRFスタックユニットが**Recovery**状態に移行するときに、管理またはその他の特別な目的のためのシャットダウンアクションからサービスインタフェースを除外します。 • IRF スタックの回復
3. （オプション設定項目）IRF スタックユニットの IRF スタックの設定の最適化 • メンバ装置の説明の設定 • IRF スタックの bridge MAC アドレスの設定 • ソフトウェア同期用のソフトウェアオートアップグレードの有効化 この機能は、Masterの現在のソフトウェアイメージを、IRFスタックユニットに結合しようとしている装置と自動的に同期します。 • IRF スタックリンクダウン検出遅延の設定 • IRF スタック物理インタフェースを持つ拡張インタフェースカードの取り外し • IRF スタック物理インタフェースを持つ拡張インタフェースカードの交換

1.4. IRFスタックユニットのセットアップの計画

IRF スタック(IRF fabric)ユニットを構成するとき、以下の点を検討してください。

- ハードウェアの互換性と制限事項
- IRF スタックユニットの大きさ
- Master 装置
- IRF スタック物理インタフェース
- メンバ ID とプライオリティの割り当て計画
- IRF スタックユニットのトポロジとケーブル計画
- IRF スタック物理インタフェース

メモ：

IRF スタック構成装置で L3 ルーティングを使用する場合、GR（グレースフルリスタート）の使用を推奨します。

1.5. IRFスタックユニットの設定

重要:

IRF を構築する際は以下に注意をしてください。

- system view の設定はすべての IRF スタックメンバで同じ設定にすることを推奨します(物理インタフェース設定や slot 設定を除く)。
- max-ecmp-num コマンドはすべての IRF スタックメンバで同じ設定にしてください。異なる場合は IRF スタックを構築できません。

1.5.1. IRF スタックユニット設定作業リスト

IRF スタック(IRF fabric)ユニット設定作業リスト
1. 各メンバ ID、プライオリティ、IRF スタック物理インタフェースの設定 a. 各 IRF スタックメンバ装置へのメンバ ID の割り当て b. （オプション設定項目）各メンバ装置のプライオリティの設定 c. IRF スタックポートと物理インタフェースへの関連付け メンバID、プライオリティ、IRFスタック物理インタフェースがinterface rangeで設定する場合、この作業をスキップしてください。
2. IRF スタック物理インタフェースの接続
3. IRF スタックユニットのアクセス

1.5.2. 各 IRF スタックメンバ装置へのメンバ ID の割り当て

I. 制限とガイドライン

IRF スタックユニットを設定するには、それぞれのメンバ装置に固有なメンバ ID を割り当てる必要があります。

予期せぬ設定の変更やパケットロスを避けるため、IRF スタックユニットの構築後はメンバ ID を変更しないでください。

新しいメンバ ID は、再起動することによって有効になります。装置が再起動したのち、設定が保存されていたかどうかにかかわらず物理的なリソース（物理的なネットワークポートを含む）に関連するすべてのメンバ ID の設定は削除されます。

IRF スタックユニットでは、IRF スタックメンバ ID を変更すると、望ましくない設定変更やデータ損失が発生する可能性があります。これを行う前に、設定をバックアップし、ネットワークへの影響を十分に理解しておく必要があります。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. メンバ装置にメンバ ID を設定する	**irf member** *member-id* **renumber** *new-member-id*	デフォルト：1
3. (オプション設定項目) 設定を保存する	**save**	IRFスタックポートにIRFスタック物理インタフェースを関連づけたり、メンバプライオリティを割り当てた場合は、再起動する前に設定を保存してください。
4. 装置を再起動する	**reboot** [**slot** *slot-number*] [**force**]	—

1.5.3. 各メンバ装置のプライオリティの設定

I. IRF スタックメンバ装置のプライオリティの設定

IRF スタックメンバプライオリティは、IRF スタックの Master に選ばれる可能性を示します。プライオリティがより高いほど、可能性は高くなります。

メンバプライオリティを変更すると、次回に Master を選ぶ際の選定に影響を及ぼしますが、すぐに Master の選定が発生することはありません。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. 装置のプライオリティを指定する	**irf member** *member-id* **priority** *priority*	デフォルト：1

1.5.4. IRF スタックポートと物理インタフェースへの関連付け

I. 制限とガイドライン

セクション 2 *IRF スタック オペレーションマニュアル*の“*IRF スタック*”の“*IRF スタック物理インタフェースの選択*”に記載されているように IRF スタック物理インタフェースとして物理インタフェースを選択します。

物理インタフェースを IRF スタックポートに関連づけた後、**irf-port-configuration active** コマンドを使用して IRF スタックポートの設定をアクティブにする必要があります。 次の状況では、IRF スタックポート設定が自動的にアクティブになります。

- 装置が起動するコンフィグレーションファイルには、IRF スタックポートのバインディングが含まれています。
- IRF スタックユニットが形成された後、IRF スタックポート(UP 状態)に物理インタフェースを追加しています。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. interface view あるいは interface range view に移行する	• interface view に移行する: **interface** *interface-type interface-number* • interface range view に移行する: **interface range** { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-24> **interface range name** *name* [**interface** { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-24>]	IRFスタック物理インタフェースの範囲をシャットダウンするため、interface range viewに移行します。 IRFスタック物理インタフェースをシャットダウンするため、interface viewに移行します。
3. インタフェースまたはインタフェース範囲をシャットダウンする	**shutdown**	デフォルト : すべてのポートはup
4. system view に戻る	**quit**	ー
5. IRF port view に移行する	**irf-port** *member-id/port-number*	ー

操作	コマンド	補足
6. 各 IRF スタック物理インタフェースに IRF スタックポートを関連づける	**port group interface** *interface-type interface-number*	デフォルト : 全ポート関連づけなし リンクの冗長性のため、複数のIRFスタック物理インタフェースをIRFスタックポートに割り当てる場合、このコマンドを繰り返してください。 1つの論理ポートに最大2ポートのIRFスタック物理インタフェースを関連づけることができ、装置として最大4ポートまでを関連づけることができます。
7. system view に戻る	**quit**	ー
8. interface view あるいは interface range view に移行する	• interface view に移行する: **interface** *interface-type interface-number* • interface range view に移行する: **interface range** { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-24> **interface range name** *name* [**interface** { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-24>]	IRFスタック物理インタフェースの範囲をシャットダウンするため、interface range viewに移行します。 IRFスタック物理インタフェースをシャットダウンするため、interface viewに移行します。
9. インタフェースまたはインタフェース範囲をシャットダウンする	**shutdown**	デフォルト : すべてのポートはup
10. system view に戻る	**quit**	ー
11. 設定を保存する	**save**	IRFスタックポートの設定を有効にするとIRFスタックが結合し、再起動します。データの削除を防ぐため、操作を行う前に設定を保存してください。
12. IRF スタックポートの設定を有効にする	**irf-port-configuration active**	ー

1.5.5. IRF スタック物理インタフェースの接続

制限に従う IRF スタックポートの接続は、IRF スタックの物理インタフェースと、トポロジとケーブル接続方式にもとづいています。 装置はマスタ選定を行います。 Master の選定に失敗したメンバ装置は自動的に再起動し、Master 装置で IRF スタックユニットを形成します。

1.5.6. IRF スタックユニットのアクセス

IRF スタックが形成されると、1 つのスイッチとして操作することできます。Master の CLI で、すべての IRF スタックメンバの設定と管理を行うことができます。すべての設定は、IRF スタックメンバに自動的に反映されます。

IRF スタックユニットにアクセスする場合、以下の方法があります。

- **ローカルログイン**–メンバ装置のコンソールポートを用いてログインします
- **リモートログイン**–Telnet や SNMP を用いてメンバ装置のレイヤ 3 インタフェースにログインします。

IRF スタックユニットにログインするとき、どのメンバ装置からログインしても、実際には、IRF スタックの Master にログインします。

詳細はオペレーションマニュアルのセクション 1 *はじめに* "*ログイン*"を参照してください。

1.6. MADの設定

1.6.1. 制限とガイドライン

I. MAD メカニズムの互換性

ベストプラクティスとして、IRF スタック(IRF fabric)ユニットでの MAD メカニズムですくなくとも 1 つを、IRF スタックの分裂を迅速に検出するために設定します。 MAD メカニズムは異なるコリジョン処理プロセスを使用するため、IRF スタックユニットで複数の MAD メカニズムを構成する際には、次の制限とガイドラインに従ってください。

- LACP MAD を ARP MAD と一緒に設定しないでください。
- BFD MAD を ARP MAD と一緒に設定しないでください。

II. IRF スタックドメイン ID の割り当て

2 つの IRF スタックユニット間で LACP MAD、ARP MAD が動作する場合、各 IRF スタックユニットに一意の IRF スタックドメイン ID を割り当ててください。（BFD MAD では必須ではありません。）

IRF スタックユニットは 1 つの IRF スタックドメイン ID のみを持つことができます。

irf domain コマンド、**mad enable** コマンド、 **mad arp enable** コマンドを使用して IRF スタックドメイン ID を変更することができます。これらのコマンドを使用して設定された IRF スタックドメイン ID は、たがいに上書きされます。

III. MAD によるサービスインタフェースのシャットダウンからの除外

IRF スタックユニットが Recovery 状態に遷移するとき、ポートがシャットダウンにならないようにするため、**mad exclude interface** コマンドを使用します。Recovery 状態の IRF スタックユニット

でポートをアップ状態にする場合、**undo shutdown** コマンドの代わりにコマンドを使用します。**mad restore** コマンドは Recovery 状態の IRF スタックユニットをアクティブにします。

1.6.2. LACP MAD の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. IRF スタックユニットにドメイン ID を割り当てる	**irf domain** *domain-id*	デフォルト：0
3. アグリゲートインタフェースを作成し、aggregate interface view に移行する	**interface bridge-aggregation** *interface-number*	中継装置でもこの操作を行ってください。
4. ダイナミックアグリゲーションモードでアグリゲーショングループを設定する	**link-aggregation mode dynamic**	デフォルトでは、アグリゲーショングループはスタティックモードです。 LACP MADはダイナミックアグリゲートインタフェースでのみ有効です。 中継装置でもこの操作を行ってください。
5. LACP MAD を有効にする	**mad enable**	デフォルト：無効
6. system view に戻る	**quit**	―
7. interface view あるいは interface range view に移行する	• interface view に移行する: **interface** *interface-type interface-number* • interface range view に移行する: **interface range** { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-24> **interface range name** *name* [**interface** { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-24>]	アグリゲーショングループにポート範囲を割り当てるためにinterface range viewに移行してください。 アグリゲーショングループに1つずつポートを割り当てるためにinterface viewに移行してください。

操作	コマンド	補足
8. ポートまたはポート範囲を指定のアグリゲーショングループに割り当てる	**port link-aggregation group** *number*	中継装置でもこの操作を行ってください。

1.6.3. BFD MAD の設定

I. 制限とガイドライン

BFD MAD を設定する前に、BFD MAD リンク方式を選択してください。詳細はオペレーションマニュアルのセクション 2 *IRF スタック* “*IRF スタック*”の“*概要*”の“*BFD MAD*”を参照してください。

BFD MAD を設定した後、BFD MAD のリンクを接続してください。

VLAN インタフェースで BFD MAD を設定するとき、以下の制限とガイドラインに従ってください。

カテゴリ	制限とガイドライン

BFD MAD VLAN	• VLAN インタフェース 1 で、BFD MAD を有効にすることはできません。
	• 中継装置を使用する場合、以下の作業を行ってください。
	  ○ IRF スタックユニットと中継装置で BFD MAD の VLAN と VLAN インタフェースを作成してください。
	  ○ IRF スタックユニットと中継装置で BFD MAD の VLAN に BFD MAD のポートを関連付けてください。
	  ○ IRF スタックユニットで BFD MAD VLAN の VLAN インタフェースを作成してください。
	• ネットワークの IRF スタックユニットは異なる BFD MAD の VLAN を使用してください。
	• 正しいトラフィックの転送を行うため、BFD MAD VLAN は BFD MAD リンクのポートのみを使用してください。もし BFD MAD リンクのポートでない場合、BFD MAD VLAN からのポートを取り除いてください。**port trunk permit vlan all** コマンドですべての VLAN にポートが割り当てられている場合、BFD MAD VLAN からポートを除外するため、**undo port trunk permit** コマンドを使用してください。

BFD MAD VLANと機能の互換性	BFD MAD のVLANをほかの用途で使用しないでください。 • BFD MAD で使用される VLAN インタフェースでは **mad bfd enable** コマンドと **mad ip address** コマンドのみ設定できます。もしほかの機能を設定する場合、BFD MAD とインタフェースのほかの機能の両方は正常に動作しない可能性があります。 • BFD MAD の VLAN のポートでは、スパニングツリー機能を無効にしてください。MAD 機能はスパニングツリー機能と同時に使用することはできません。
MAD IP address	• BFD MAD を有効にした VLAN インタフェースで MAD の IP アドレスを設定する場合、**ip address** コマンドの代わりに

カテゴリ	制限とガイドライン
	mad ip address コマンドを使用してください。 • すべての MAD IP アドレスは、同じサブネット上にある必要があります。

マネジメント Ethernet インタフェースで BFD MAD を設定するとき、以下の制限とガイドラインに従ってください。

カテゴリ	制限とガイドライン
BFD MADのマネジメントEthernetポート	各IRFスタックメンバ装置上のマネジメントEthernetポートを、中継装置の共通Ethernetポートに接続します。
BFD MAD VLAN	• 中継装置で BFD MAD 用の VLAN を作成し、BFD MAD で使用するポートを割り当ててください。IRF スタックユニットで BFD MAD が有効なマネジメント Ethernet ポートに VLAN を割り当てる必要はありません。 • ネットワークの IRF スタックユニットは異なる BFD MAD の VLAN を使用してください。 • 中継装置で BFD MAD VLAN に BFD MAD リンクのポートのみが存在することを確認してください。
MAD IP address	• BFD MAD を有効にした VLAN インタフェースで MAD の IP アドレスを設定する場合、**ip address** コマンドの代わりに **mad ip address** コマンドを使用してください。 • BFD MAD が有効な VLAN インタフェースのすべての MAD IP アドレスは、同じサブネット上にある必要があります。

II. VLAN インタフェースでの BFD MAD の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. （オプション設定項目）IRF スタックユニットにドメイン ID を割り当てる	**irf domain** *domain-id*	デフォルト： 0
3. BFD MAD 時に稼動する VLAN を作成する	**vlan** *vlan-id*	デフォルト：VLAN 1のみ存在します。 VLANインタフェース1でBFD MADを有効にしないでください。 中継装置がある場合、このステップを繰り返してください。
4. system view に戻る	**quit**	—

操作	コマンド	補足
5. interface view あるいは interface range view に移行する	• interface view に移行する: **interface** *interface-type interface-number* • interface range view に移行する: **interface range** { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-24> **interface range name** *name* [**interface** { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-24>]	BFD MAD VLANのポート範囲を割り当てるためにinterface range viewに移行してください。 BFD MAD VLANに1つずつポートを割り当てるためにinterface viewに移行してください。
6. BFD MAD VLAN にポートまたはポート範囲を割り当てる	• アクセスポートとして割り当てる: **port access vlan** *vlan-id* • トランクポートとして割り当てる: **port trunk permit vlan** *vlan-id* • ハイブリッドポートとして割り当てる: **port hybrid vlan** *vlan-id* { **tagged** | **untagged** }	ポートタイプによって1つのコマンドを選択してください。 デフォルト : アクセスポート 中継装置がある場合、このステップを繰り返してください。
7. system view に戻る	**quit**	—
8. VLAN interface view に移行する	**interface vlan-interface** *vlan-interface-id*	—
9. BFD MAD を有効にする	**mad bfd enable**	デフォルト：無効
10. メンバ装置の VLAN インタフェースに MAD IP アドレスを割り当てる	**mad ip address** *ip-address* { *mask* | *mask-length* } **member** *member-id*	デフォルト：設定なし VLANインタフェースの各メンバ装置にMAD IPアドレスを割り当てる場合、操作を繰り返してください。

III. マネジメント Ethernet ポートを使用した BFD MAD の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—

操作	コマンド	補足
2. （オプション設定項目）IRF スタックユニットにドメイン ID を割り当てる	**irf domain** *domain-id*	デフォルト： 0
3. system view に戻る	**quit**	―
4. management Ethernet interface view に移行する	**interface m-gigabitethernet** *interface-number*	IRFスタックユニットのすべてのマネジメントEthernetポートのうち、Masterのマネジメントポートのみにアクセスできます。
5. BFD MAD を有効にする	**mad bfd enable**	デフォルト：無効
6. メンバ装置の VLAN インタフェースに MAD IP アドレスを割り当てる	**mad ip address** *ip-address* { *mask* | *mask-length* } **member** *member-id*	デフォルト：設定なし

1.6.4. ARP MAD の設定

I. 制限とガイドライン

中継装置を使用する場合、ARP MAD リンクとして共通のデータリンクを使用することができます。中継装置を使用しない場合、IRF スタックメンバ装置間で専用の ARP MAD リンクを設定してください。

VLAN インタフェースで ARP MAD を設定するとき、以下の制限とガイドラインに従ってください。

Category	制限とガイドライン
ARP MAD VLAN	• VLAN インタフェース 1 で、ARP MAD を有効にすることはできません。 • 中継装置を使用する場合、以下の作業を行ってください。 　○ IRF スタックユニットと中継装置で ARP MAD の VLAN を作成してください。 　○ IRF スタックユニットと中継装置で ARP MAD リンクのポートを ARP MAD の VLAN に割り当ててください。 　○ IRF スタックユニットで ARP MAD の VLAN インタフェースを作成してください。 • ARP MAD の VLAN はほかの目的で使用しないでください。
ARP MADと機能	中継装置を使用する場合、以下の要件を確認してください。 • IRF スタックユニットと中継装置の間でスパニングツリー機能を動作させてください。転送状態の ARP MAD リンクが 1 つのみ存在することを確認してください。詳細はオペレーションマニュアルのセクション 3 *アクセス "STP "*を参照してください。 • IRF スタックユニットから Master が離脱した際に bridge MAC アドレスが即座に変更されるように IRF スタックユニットを設定してください。 • IRF スタックユニットに中継装置がある場合、分裂を間違っ

Category	制限とガイドライン
	て検知しないように ARP MAD を有効にした IRF スタックユニットと異なるドメイン ID を割り当ててください。

マネジメント Ethernet ポートを使用する ARP MAD を設定するとき、以下の制限とガイドラインに従ってください。

カテゴリ	制限とガイドライン
ARP MADのマネジメントEthernetポート	中継装置の共通EthernetポートをIRFスタックユニットのマネジメントEthernetポートに接続してください。
ARP MAD VLAN	中継装置でARP MADのVLANを作成してください。 VLANにARP MADで使用するポートを割り当ててください。 IRFスタックユニットではマネジメントEthernetポートをVLANに割り当てる必要はありません。
ARP MAD and feature configuration	• IRF スタックユニットから Master が離脱した際に bridge MAC アドレスが即座に変更されるように IRF スタックユニットを設定してください。 • IRF スタックユニットに中継装置がある場合、分裂を間違って検知しないように ARP MAD を有効にした IRF スタックユニットと異なるドメイン ID を割り当ててください。

II. VLAN インタフェースでの ARP MAD の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. IRF スタックユニットにドメイン ID を割り当てる	**irf domain** *domain-id*	デフォルト： 0
3. Bridge MAC アドレスのオーナが離脱したときすぐに IRF スタック Bridge MAC アドレスを変更できるように設定する	**undo irf mac-address persistent**	デフォルトでは、Bridge MACアドレスのオーナが離脱した後、6分間はBridge MACアドレスを保持します。
4. ARP MAD 時に稼動する VLAN を作成する	**vlan** *vlan-id*	デフォルト：VLAN 1のみ存在します。 VLANインタフェース1でARP MADを有効にしないでください。 中継装置がある場合、このステップを繰り返してください。
5. system view に戻る	**quit**	—

操作	コマンド	補足
6. interface view あるいは interface range view に移行する	• interface view に移行する: **interface** *interface-type interface-number* • interface range view に移行する: **interface range** { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-24> **interface range name** *name* [**interface** { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-24>]	ARP MAD VLANのポート範囲を割り当てる場合 interface range viewに移行してください。 ARP MAD VLANに1つずつポートを割り当てる場合 interface viewに移行してください。
7. ARP MAD の VLAN にポートを割り当てる	• アクセスポートとして割り当てる: **port access vlan** *vlan-id* • トランクポートとして割り当てる: **port trunk permit vlan** *vlan-id* • ハイブリッドポートとして割り当てる: **port hybrid vlan** *vlan-id* { **tagged** | **untagged** }	ポートタイプによって1つのコマンドを選択してください。 デフォルト : アクセスポート 中継装置がある場合、このステップを繰り返してください。
8. system view に戻る	**quit**	―
9. VLAN interface view に移行する	**interface vlan-interface** *vlan-interface-id*	―
10. インタフェースに IP アドレスを割り当てる	**ip address** *ip-address* { *mask* | *mask-length* }	デフォルト：設定なし
11. ARP MAD を有効にする	**mad arp enable**	デフォルト：無効

III. マネジメント Ethernet ポートでの ARP MAD の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. IRF スタックユニットにドメイン ID を割り当てる	**irf domain** *domain-id*	デフォルト： 0

操作	コマンド	補足
3. Master の離脱時すぐに IRF スタック Bridge MAC アドレスを変更できるように設定する	**undo irf mac-address persistent**	デフォルトでは、Master離脱後、6分間はBridge MACアドレスを保持します。
4. management Ethernet interface view に移行する	**interface m-gigabitethernet** *interface-number*	IRFスタックユニットのすべてのマネジメントEthernetポートは、Master装置のマネジメントEthernetポートのみアクセス可能です。
5. インタフェースに IP アドレスを割り当てる	**ip address** *ip-address* { *mask* | *mask-length* }	デフォルト：設定なし
6. ARP MAD を有効にする	**mad arp enable**	デフォルト：無効

1.6.5. MAD によるシャットダウンアクションからのサービスインタフェースの除外の設定

I. MAD によるシャットダウンアクションからのサービスインタフェースの除外

IRF スタックユニットが Recovery 状態に移行するとき、以下のサービスインタフェースを除いてネットワークのすべてのポートが自動的にシャットダウンします。

- IRF スタック物理インタフェース
- BFD MAD で使用するインタフェース
- アグリゲートインタフェースがシャットダウンから除外されている場合、アグリゲートインタフェースのメンバインタフェース

管理やほかの特別な目的のため、シャットダウン動作からネットワークポートを除外することができます。たとえば以下のようなことができます。

- シャットダウンアクションからポートを除外して、管理装置からポートに telnet することができます。
- シャットダウンアクションから VLAN インタフェースやレイヤ 2 ポートを除外して、VLAN インタフェースにログインすることができます。

II. 制限とガイドライン

レイヤ 2 ポートが複数のメンバ装置に提供されている場合、シャットダウンアクションから VLAN インタフェースとレイヤ 2 ポートを除外しないでください。シャットダウンアクションから VLAN インタフェースとレイヤ 2 ポートを除外した場合、IRF スタックユニットがアクティブ状態でもアクティブでない状態でも、VLAN インタフェースが有効となるため IP アドレス衝突を招く可能性があります。

III. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—

操作	コマンド	補足
2. IRF スタックユニットが Recovery 状態になるときシャットダウンアクションから除外するネットワークポートを設定する	**mad exclude interface** *interface-type interface-number*	デフォルト： Recovery状態のIRFスタックユニットのすべてのネットワークポートがシャットダウン（IRFスタック物理インタフェースとコンソールポートを除きます）

メモ:

Standby 装置で MAD によるシャットダウンアクションが発生した場合、装置の管理機能(Telnet や FTP 等)のセッションが切断されます。

1.6.6. IRF スタックユニットの回復

I. IRF スタックユニットの回復

IRF スタックのリンクが回復する前にアクティブな IRF スタックユニットに障害が発生した場合、非アクティブの IRF スタックユニットでこの処理を行い、トラフィック転送のために IRF スタックユニットを回復します。手動で IRF スタックユニットを回復する場合、非アクティブな IRF スタックユニットの MAD によってシャットダウンされたすべてのサービスインタフェースが UP 状態になります。

II. 設定手順

操作	コマンド
1. system view に移行する	**system-view**
2. アクティブ状態でない IRF スタックユニットを回復する	**mad restore**

1.7. IRFスタックユニットのIRFスタックの設定の最適化

1.7.1. メンバ装置の説明の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—

操作	コマンド	補足
2. メンバ装置の説明を設定する	**irf member** *member-id* **description** *text*	デフォルト：設定なし

1.7.2. IRF スタックの bridge MAC アドレスの設定

注意:

- IRF スタック(IRF fabric)の bridge MAC アドレスを変更すると一時的にトラフィックの通信の中断が発生します。
- IRF スタックで IPv6 リンクローカルアドレスを自動生成で使用している場合は、**irf mac-address persistent always** コマンドを設定し、Bridge MAC アドレスが変更されないようにすることを推奨します。always にしていない場合、マスタ切り替え時に MAC アドレスの変更が発生して IPv6 リンクローカルアドレスが変更されます。

I. IRF スタックの bridge MAC アドレス

デフォルトで IRF スタックユニットを確立させた装置は、Bridge MAC アドレスとして Master 装置の Bridge MAC アドレスを使用します。この Bridge MAC アドレスは、たとえば LACP のように IRF スタックユニットを識別するためにレイヤ 2 プロトコルで使用され、LAN で固有な値でなければなりません。

IRF スタックユニットが結合されると、IRF スタックは IRF スタック Bridge MAC アドレスを無視し、IRF スタックユニット内の各メンバ装置の Bridge MAC アドレスをチェックします。 2 つのメンバ装置が同じ Bridge MAC アドレスを持つ場合、IRF スタックの結合は失敗します。

IRF スタックユニットを結合した後、結合された IRF スタックユニットは IRF スタック bridge MAC アドレスとして Master の選定に選ばれた IRF スタックユニットの Bridge MAC アドレスを使用します。

IRF スタックユニットの IRF スタック Bridge MAC アドレスを設定する場合、以下の方法を使用できます。

- IRF スタック Bridge MAC アドレスの保持を設定します。

  この機能は、IRF スタックユニットの MAC アドレスを IRF スタックとして継続できる時間を指定します。時間が満了すると、IRF スタックユニットは現在の Master の Bridge MAC アドレスを IRF スタック Bridge MAC アドレスとして使用します。

II. 制限とガイドライン

IRF スタック Bridge MAC アドレスを設定するとき、以下の制限とガイドラインに従ってください。

- ARP MAD でスパニングツリー機能を使用している場合、**undo irf mac-address persistent** コマンドを使用して IRF スタック Bridge MAC アドレスの永続使用を無効にする必要があります。IRF スタック Bridge MAC アドレスとして MAC アドレスを指定しないでください。
- IRF スタックユニットで複数の装置のアグリゲートリンクがある場合、**undo irf mac-address persisten** コマンドを使用しないでください。衝突が発生し、トラフィックの中断が発生する可能性があります。

III. IRF スタック Bridge MAC アドレスの保持の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. IRF スタック bridge MAC の保持を設定する	• Master が変更しても、Bridge MAC アドレスを保持する **irf mac-address persistent always** • Master の離脱後、6 分間は Bridge MAC アドレスを保持する **irf mac-address persistent timer** • Master の離脱後、すぐに Bridge MAC アドレスを変更する **undo irf mac-address persistent**	デフォルトでは、Master離脱後、6分間はBridge MACアドレスを保持します。 **irf mac-address persistent timer**コマンドは、装置の再起動、一時的なリンク障害、または意図的リンク切断によって引き起こされる不要なブリッジMACアドレスの変更を回避します

1.7.3. ソフトウェア同期用のソフトウェアオートアップグレードの有効化

I. IRF スタックのソフトウェアオートアップグレード

ソフトウェアオートアップグレード機能は、Master の現在のソフトウェアを IRF スタックユニットに参加しようとする装置と自動的に同期します。

IRF スタックユニットに加わるには、Master のソフトウェアと同じソフトウェアを使用する必要があります。

装置を IRF スタックユニットに追加するとき、ソフトウェアオートアップグレード機能は加入しようとする装置のソフトウェアを IRF スタックの Master のソフトウェアと比較します。ソフトウェアが異なる場合、装置は自動で以下の処理を行います。

1. 装置は自動的に Master からソフトウェアをダウンロードします。
2. 新しいソフトウェアとしてダウンロードしたソフトウェアを設定します。
3. 再起動し、そして再び IRF スタックユニットに加わります。

オートアップグレード機能が無効である場合、IRF スタックユニットに装置を追加する前、装置のソフトウェアを手動でアップグレードしてください。

II. 制限とガイドライン

複数のユーザがいる環境でソフトウェアオートアップグレードを正常に行うため、オートアップグレード中に再起動を行わないようにしてください。ソフトウェアオートアップデートの状態を information center に出力することができます。(詳細はオペレーションマニュアルのセクション 11 *システム管理* "*Information Center*"を参照してください。)

IRF スタックユニットに加えようとする装置に新しいソフトウェアを格納するための十分な空き容量があることを確認してください。

もし十分なメモリ容量がない場合、装置は現在のソフトウェアを自動的に削除します。それでもメモリ容量が不十分な場合は、スイッチは自動更新を完了できません。手動で再起動を行い、BootWare メニューでいくつかのファイルを削除してください。

III. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. ソフトウェアオートアップグレード機能を有効にする	**irf auto-update enable**	デフォルト：有効

1.7.4. IRF スタックリンクダウン検出遅延の設定

I. IRF スタックリンクダウン検出遅延

リンクが短時間で状態変化する間、IRF スタックの分裂、結合が頻繁に発生しないようにするため、IRF スタックポートでリンクダウンのイベント通知を遅延させるように設定します。

IRF スタックリンク状態が up から down に変更したとき、IRF スタックポートはすぐに IRF スタックユニットに通知しません。Link-delay 時間後、IRF スタックリンク状態が down の状態である場合、IRF スタックポートは IRF スタックユニットに通知します。

IRF スタックポートは up 状態のイベントに対しては遅延させません。IRF スタックリンク状態が down から up に変更したとき、すぐに IRF スタックユニットに通知します。

II. 制限とガイドライン

IRF スタックの Link-delay が上位レイヤプロトコル(たとえば、CFD、OSPF)のタイムアウトの設定よりも短いことを確認してください。この上位プロトコルのタイムアウトの時間は、上位レイヤプロトコルでリンクがダウンしたと認識する間隔です。もし Link-delay がプロトコルのタイムアウト時間より長い場合、不必要な再計算が発生する可能性があります。

以下の状況では Link-delay を 0 秒に設定してください。

- IRF スタックユニットが Master/ subordinate(Standby)あるいは IRF スタックリンクの素早い切り替えが必要である場合
- RRPP、BFD あるいは GR が使用されている場合
- IRF スタックの IRF スタック物理インタフェースをシャットダウンする、あるいは IRF スタックメンバ装置を再起動する場合(操作を完了したのち、ネットワークの状況に従って遅延を再設定します。)

III. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. Link-delay を設定する	**irf link-delay** *interval*	デフォルト：500ミリ秒

1.7.5. IRF スタック物理インタフェースを持つ拡張インタフェースカードの取り外し

IRF スタック物理インタフェースを提供する拡張インタフェースカードを取り外すには、以下の手順に従ってください。

1. 次のいずれかのタスクを実行して、一時的なパケット損失を排除します。
   - 拡張インタフェースカードの IRF スタック物理インタフェースからケーブルを取り外します。
   - **shutdown** コマンドを使用して、カード上の IRF スタック物理インタフェースをシャットダウンします。
2. 拡張インタフェースカードを取り外します。

1.7.6. IRF スタック物理インタフェースを持つ拡張インタフェースカードの交換

I. 古い拡張インタフェースカードから別の種類の拡張インタフェースカードへの交換

1. **shutdown** コマンドを使用して、古い拡張インタフェースカードの IRF スタック物理インタフェースをシャットダウンします。
2. 物理インタフェースを含む IRF スタックポートのバインディングを削除します。
3. 古い拡張インタフェースカードを取り外し、交換用拡張インタフェースカードを取り付けます。
4. **display device** コマンドを使用して、交換用拡張インタフェースカードが正しく取り付けられていることを確認します。
5. IRF スタックポートのバインディングを再設定します。オペレーションマニュアルのセクション 2 *IRF スタック*“*IRF スタック*”の“*IRF スタックポートと物理インタフェースへの関連付け*”を参照してください。
6. **irf-port-configuration active** コマンドを使用して IRF スタックポートの設定をアクティブにします。

   バインディングを追加するときに IRF スタックポートが UP 状態になっている場合、このステップをスキップできます。

II. 古い拡張インタフェースカードから同一種類の拡張インタフェースカードへの交換

1. **shutdown** コマンドを使用して、古い拡張インタフェースカードの IRF スタック物理インタフェースをシャットダウンします。
2. 古い拡張インタフェースカードを取り外し、交換用拡張インタフェースカードを取り付けます。
3. **display device** コマンドを使用して、交換用拡張インタフェースカードが正しく取り付けられていることを確認します。
4. インタフェースカードの起動後に **undo shutdown** コマンドを使用して物理インタフェースを起動します。

1.8. IRFスタックの表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
すべてのIRFスタックメンバの情報を表示する	**display irf**
IRFスタックユニットのトポロジ情報を表示する	**display irf topology**
IRFスタックのリンク情報を表示する	**display irf link**
IRFスタックの設定を表示する	**display irf configuration**
MAD設定を表示する	**display mad** [**verbose**]

1.9. IRFスタックの設定例

この章では異なる MAD を使用する場合の IRF スタック(IRF fabric)ユニットの設定例を示します。

1.9.1. LACP MAD を使用する場合の IRF スタックの設定例

I. ネットワーク要件

図 1-13 に示すように、エンタープライズネットワークのアクセスレイヤで 4 台の IRF スタックユニットを設定します。

拡張 LACP をサポートする Device E に複数の装置を接続させるため、IRF スタックに LACP MAD を設定してください。

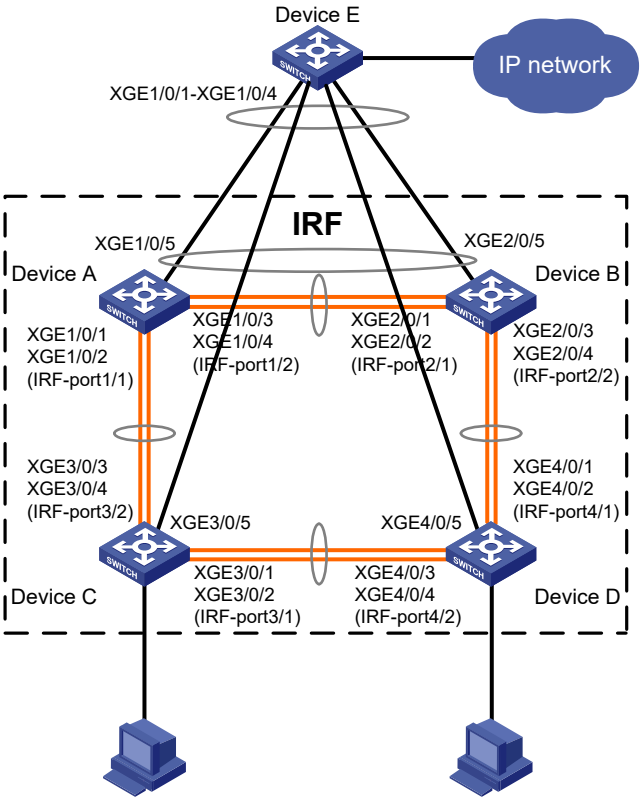


図 1-13 ネットワーク図

II. 設定手順

1. Device A を設定します。

   # interface range コマンドで IRF スタックリンクに使用する IRF スタック物理インタフェースをシャットダウンします。interface range コマンドについては、オペレーションマニュアルのセクション 3 *アクセス*“*Interface range*”を参照してください。

```
<Switch> system-view
[Switch] interface range ten-gigabitethernet 1/0/1 to ten-gigabitethernet 1/0/4
[Switch-if-range] shutdown
[Switch-if-range] quit
```

   # Ten-GigabitEthernet 1/0/1 と Ten-GigabitEthernet 1/0/2 を IRF スタックポート 1/1 に関連づけます。

```
[Switch] irf-port 1/1
[Switch-irf-port1/1] port group interface ten-gigabitethernet 1/0/1
[Switch-irf-port1/1] port group interface ten-gigabitethernet 1/0/2
[Switch-irf-port1/1] quit
```

   # Ten-GigabitEthernet 1/0/3 と Ten-GigabitEthernet 1/0/4 を IRF スタックポート 1/2 に関連づけます。

```
[Switch] irf-port 1/2
[Switch-irf-port1/2] port group interface ten-gigabitethernet 1/0/3
[Switch-irf-port1/2] port group interface ten-gigabitethernet 1/0/4
[Switch-irf-port1/2] quit
```

物理インタフェースを UP にし、設定を保存します。

```
[Switch] interface range ten-gigabitethernet 1/0/1 to ten-gigabitethernet 1/0/4
[Switch-if-range] undo shutdown
[Switch-if-range] quit
[Switch] save
```

IRF スタックポートの設定を有効にします。

```
[Switch] irf-port-configuration active
```

2. Device B を設定します。

Device B のメンバ ID を 2 に変更し、変更を有効にするため、装置を再起動します。

```
<Switch> system-view
[Switch] irf member 1 renumber 2
Renumbering the member ID may result in configuration change or loss. Continue?
[Y/N]:y
[Switch] quit
<Switch> reboot
```

図 1-13 に示すように Device B を Device A に接続し、Device B にログインします。(詳細は省略します。)

IRF スタック物理インタフェースをシャットダウンします。

```
<Switch> system-view
[Switch] interface range ten-gigabitethernet 2/0/1 to ten-gigabitethernet 2/0/4
[Switch-if-range] shutdown
[Switch-if-range] quit
```

Ten-GigabitEthernet 2/0/1 と Ten-GigabitEthernet 2/0/2 を IRF スタックポート 2/1 に関連づけます。

```
[Switch] irf-port 2/1
[Switch-irf-port2/1] port group interface ten-gigabitethernet 2/0/1
[Switch-irf-port2/1] port group interface ten-gigabitethernet 2/0/2
[Switch-irf-port2/1] quit
```

Ten-GigabitEthernet 2/0/3 と Ten-GigabitEthernet 2/0/4 を IRF スタックポート 2/2 に関連づけます。

```
[Switch] irf-port 2/2
[Switch-irf-port2/2] port group interface ten-gigabitethernet 2/0/3
[Switch-irf-port2/2] port group interface ten-gigabitethernet 2/0/4
[Switch-irf-port2/2] quit
```

物理インタフェースを UP にし、設定を保存します。

```
[Switch] interface range ten-gigabitethernet 2/0/1 to ten-gigabitethernet 2/0/4
[Switch-if-range] undo shutdown
[Switch-if-range] quit
[Switch] save
```

IRF スタックポートの設定を有効にします。

```
[Switch] irf-port-configuration active
```

2 台の装置は Master 選定を行い、選定されなかった 1 台は Master とともに IRF スタックを形成するために再起動します。

3. Device C を設定します。

Device C のメンバ ID を 3 に変更し、再起動します。

```
<Switch> system-view
[Switch] irf member 1 renumber 3
Renumbering the member ID may result in configuration change or loss. Continue?
[Y/N]:y
[Switch] quit
<Switch> reboot
```

図 1-13 に示すように Device C を Device A に接続し、Device C にログインします。(詳細は省略します。)

IRF スタック物理インタフェースをシャットダウンします。

```
<Switch> system-view
[Switch] interface range ten-gigabitethernet 3/0/1 to ten-gigabitethernet 3/0/4
[Switch-if-range] shutdown
[Switch-if-range] quit
```

Ten-GigabitEthernet 3/0/1 と Ten-GigabitEthernet 3/0/2 を IRF スタックポート 3/1 に関連づけます。

```
[Switch] irf-port 3/1
[Switch-irf-port3/1] port group interface ten-gigabitethernet 3/0/1
[Switch-irf-port3/1] port group interface ten-gigabitethernet 3/0/2
[Switch-irf-port3/1] quit
```

Ten-GigabitEthernet 3/0/3 と Ten-GigabitEthernet 3/0/4 を IRF スタックポート 3/2 に関連づけます。

```
[Switch] irf-port 3/2
[Switch-irf-port3/2] port group interface ten-gigabitethernet 3/0/3
[Switch-irf-port3/2] port group interface ten-gigabitethernet 3/0/4
[Switch-irf-port3/2] quit
```

物理インタフェースを UP にし、設定を保存します。

```
[Switch] interface range ten-gigabitethernet 3/0/1 to ten-gigabitethernet 3/0/4
[Switch-if-range] undo shutdown
[Switch-if-range] quit
[Switch] save
```

IRF スタックポートの設定を有効にします。

```
[Switch] irf-port-configuration active
```

Device C を IRF スタックユニットに加入させるため再起動します。

4. Device D を設定します。

Device D のメンバ ID を 4 に変更し、再起動します。

```
<Switch> system-view
[Switch] irf member 1 renumber 4
Renumbering the member ID may result in configuration change or loss. Continue?
[Y/N]:y
[Switch] quit
<Switch> reboot
```

図 1-13 に示すように Device D を Device B、Device C に接続し、Device D にログインします。(詳細は省略します。)

IRF スタック物理インタフェースをシャットダウンします。

```
<Switch> system-view
[Switch] interface range ten-gigabitethernet 4/0/1 to ten-gigabitethernet 4/0/4
[Switch-if-range] shutdown
[Switch-if-range] quit
```

Ten-GigabitEthernet 4/0/1 と Ten-GigabitEthernet 4/0/2 を IRF スタックポート 4/1 に関連づけます。

```
[Switch] irf-port 4/1
[Switch-irf-port4/1] port group interface ten-gigabitethernet 4/0/1
[Switch-irf-port4/1] port group interface ten-gigabitethernet 4/0/2
[Switch-irf-port4/1] quit
```

Ten-GigabitEthernet 4/0/3 と Ten-GigabitEthernet 4/0/4 を IRF スタックポート 4/2 に関連づけます。

```
[Switch] irf-port 4/2
[Switch-irf-port4/2] port group interface ten-gigabitethernet 4/0/3
```

```
[Switch-irf-port4/2] port group interface ten-gigabitethernet 4/0/4
[Switch-irf-port4/2] quit
```

物理インタフェースを UP にし、設定を保存します。

```
[Switch] interface range ten-gigabitethernet 4/0/1 to ten-gigabitethernet 4/0/4
[Switch-if-range] undo shutdown
[Switch-if-range] quit
[Switch] save
```

IRF スタックポートの設定を有効にします。

```
[Switch] irf-port-configuration active
```

Device C は IRF スタックユニットに加入させるため再起動します。4 台の IRF スタックユニットが形成されます。

5. IRF スタックユニットの LACP MAD を設定します。

IRF スタックユニットのドメイン ID に 1 を設定します。

```
<Switch> system-view
[Switch] irf domain 1
```

#ダイナミックアグリゲーションインタフェースを作成し、LACP MAD を有効にします。

```
[Switch] interface bridge-aggregation 2
[Switch-Bridge-Aggregation2] link-aggregation mode dynamic
[Switch-Bridge-Aggregation2] mad enable
You need to assign a domain ID (range: 0-4294967295)
[Current domain is: 1]:
The assigned domain ID is: 1
MAD LACP only enable on dynamic aggregation interface.
[Switch-Bridge-Aggregation2] quit
```

Ten-GigabitEthernet 1/0/5、Ten-GigabitEthernet 2/0/5、Ten-GigabitEthernet 3/0/5、Ten-GigabitEthernet 4/0/5 にアグリゲートインタフェースを割り当てます。

```
[Switch] interface range ten-gigabitethernet 1/0/5 ten-gigabitethernet 2/0/5
ten-gigabitethernet 3/0/5 ten-gigabitethernet 4/0/5
[Switch-if-range] port link-aggregation group 2
[Switch-if-range] quit
```

6. 中継装置として Device E を設定します。

注意:

中継装置が IRF スタックユニットの中にある場合、正しい分裂の検出を行うため、IRF スタックユニットとは異なるドメイン ID を IRF スタックユニットに割り当ててください。間違った検出は IRF スタックの分裂を引き起こします。

ダイナミックアグリゲーションインタフェースを作成します。

```
<Switch> system-view
[Switch] interface bridge-aggregation 2
[Switch-Bridge-Aggregation2] link-aggregation mode dynamic
[Switch-Bridge-Aggregation2] quit
```

Ten-GigabitEthernet 1/0/1 ～ Ten-GigabitEthernet 1/0/4 にアグリゲートインタフェースを割り当てます。

```
[Switch] interface range ten-gigabitethernet 1/0/1 to ten-gigabitethernet 1/0/4
[Switch-if-range] port link-aggregation group 2
[Switch-if-range] quit
```

1.9.2. BFD MAD を使用する場合の IRF スタックの設定例

I. ネットワーク要件

図 1-14 に示すように、エンタープライズネットワークのコアレイヤで 4 台の IRF スタックユニットを設定します。

- IRF スタックユニット内で BFD MAD を設定し、各メンバ装置と中継装置との間で BFD MAD リンクが確立するようにしてください。
- BFD MAD とスパニングツリーの 2 つの機能は併用できないので、BFD MAD に使用するポートではスパニングツリー機能を無効にしてください。

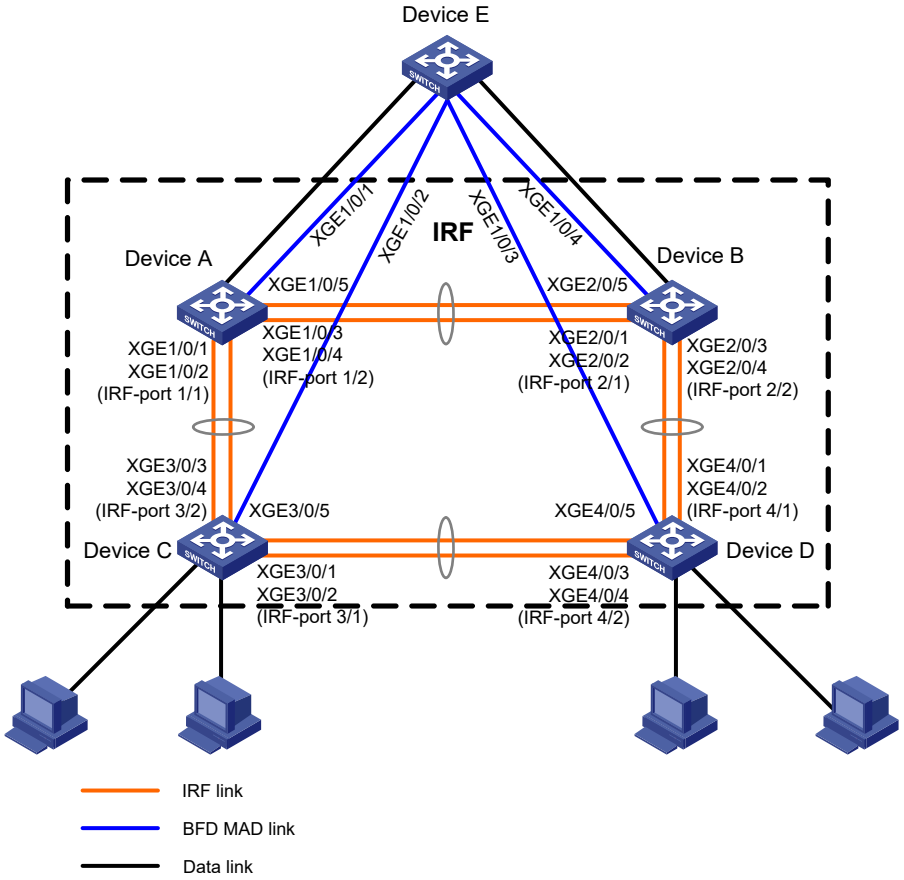


図 1-14 ネットワーク図

II. 設定手順

1. Device A を設定します。

IRF スタックリンクに使用する IRF スタック物理インタフェースをシャットダウンします。

```
<Switch> system-view
[Switch] interface range ten-gigabitethernet 1/0/1 to ten-gigabitethernet 1/0/4
[Switch-if-range] shutdown
[Switch-if-range] quit
```

Ten-GigabitEthernet 1/0/1 と Ten-GigabitEthernet 1/0/2 を IRF スタックポート 1/1 に関連づけます。

```
[Switch] irf-port 1/1
[Switch-irf-port1/1] port group interface ten-gigabitethernet 1/0/1
[Switch-irf-port1/1] port group interface ten-gigabitethernet 1/0/2
[Switch-irf-port1/1] quit
```

Ten-GigabitEthernet 1/0/3 と Ten-GigabitEthernet 1/0/4 を IRF スタックポート 1/2 に関連づけます。

```
[Switch] irf-port 1/2
[Switch-irf-port1/2] port group interface ten-gigabitethernet 1/0/3
[Switch-irf-port1/2] port group interface ten-gigabitethernet 1/0/4
[Switch-irf-port1/2] quit
```

物理インタフェースを UP にし、設定を保存します。

```
[Switch] interface range ten-gigabitethernet 1/0/1 to ten-gigabitethernet 1/0/4
[Switch-if-range] undo shutdown
[Switch-if-range] quit
[Switch] save
```

IRF スタックポートの設定を有効にします。

```
[Switch] irf-port-configuration active
```

2. Device B を設定します。

Device B のメンバ ID を 2 に変更し、再起動します。

```
<Switch> system-view
[Switch] irf member 1 renumber 2
Renumbering the member ID may result in configuration change or loss. Continue?
[Y/N]:y
[Switch] quit
<Switch> reboot
```

図 1-14 に示すように Device B を Device A に接続し、Device B にログインします。(詳細は省略します。)

IRF スタック物理インタフェースをシャットダウンします。

```
<Switch> system-view
[Switch] interface range ten-gigabitethernet 2/0/1 to ten-gigabitethernet 2/0/4
[Switch-if-range] shutdown
[Switch-if-range] quit
```

Ten-GigabitEthernet 2/0/1 と Ten-GigabitEthernet 2/0/2 を IRF スタックポート 2/1 に関連づけます。

```
[Switch] irf-port 2/1
[Switch-irf-port2/1] port group interface ten-gigabitethernet 2/0/1
[Switch-irf-port2/1] port group interface ten-gigabitethernet 2/0/2
[Switch-irf-port2/1] quit
```

Ten-GigabitEthernet 2/0/3 と Ten-GigabitEthernet 2/0/4 を IRF スタックポート 2/2 に関連づけます。

```
[Switch] irf-port 2/2
[Switch-irf-port2/2] port group interface ten-gigabitethernet 2/0/3
[Switch-irf-port2/2] port group interface ten-gigabitethernet 2/0/4
[Switch-irf-port2/2] quit
```

物理インタフェースを UP にし、設定を保存します。

```
[Switch] interface range ten-gigabitethernet 2/0/1 to ten-gigabitethernet 2/0/4
[Switch-if-range] undo shutdown
[Switch-if-range] quit
[Switch] save
```

IRF スタックポートの設定を有効にします。

```
[Switch] irf-port-configuration active
```

2 台の装置は Master 選定を行い、選定されなかった 1 台は Master とともに IRF スタックユニットを形成するために再起動します。

3. Device C を設定します。

Device C のメンバ ID を 3 に変更し、再起動します。

```
<Switch> system-view
[Switch] irf member 1 renumber 3
Renumbering the member ID may result in configuration change or loss. Continue? [Y/N]:y
[Switch] quit
<Switch> reboot
```

図 1-14 に示すように Device C を Device A に接続し、Device C にログインします。(詳細は省略します。)

IRF スタック物理インタフェースをシャットダウンします。

```
<Switch> system-view
[Switch] interface range ten-gigabitethernet 3/0/1 to ten-gigabitethernet 3/0/4
[Switch-if-range] shutdown
[Switch-if-range] quit
```

Ten-GigabitEthernet 3/0/1 と Ten-GigabitEthernet 3/0/2 を IRF スタックポート 3/1 に関連づけます。

```
[Switch] irf-port 3/1
[Switch-irf-port3/1] port group interface ten-gigabitethernet 3/0/1
[Switch-irf-port3/1] port group interface ten-gigabitethernet 3/0/2
[Switch-irf-port3/1] quit
```

Ten-GigabitEthernet 3/0/3 と Ten-GigabitEthernet 3/0/4 を IRF スタックポート 3/2 に関連づけます。

```
[Switch] irf-port 3/2
[Switch-irf-port3/2] port group interface ten-gigabitethernet 3/0/3
[Switch-irf-port3/2] port group interface ten-gigabitethernet 3/0/4
[Switch-irf-port3/2] quit
```

物理インタフェースを UP にし、設定を保存します。

```
[Switch] interface range ten-gigabitethernet 3/0/1 to ten-gigabitethernet 3/0/4
[Switch-if-range] undo shutdown
[Switch-if-range] quit
[Switch] save
```

IRF スタックポートの設定を有効にします。

```
[Switch] irf-port-configuration active
```

Device C を IRF スタックユニットに加入させるため再起動します。

4. Device D を設定します。

Device D のメンバ ID を 4 に変更し、再起動します。

```
<Switch> system-view
[Switch] irf member 1 renumber 4
Renumbering the member ID may result in configuration change or loss. Continue?
[Y/N]:y
[Switch] quit
<Switch> reboot
```

図 1-14 に示すように Device D を Device B、Device C に接続し、Device D にログインします。(詳細は省略します。)

IRF スタック物理インタフェースをシャットダウンします。

```
<Switch> system-view
[Switch] interface range ten-gigabitethernet 4/0/1 to ten-gigabitethernet 4/0/4
[Switch-if-range] shutdown
[Switch-if-range] quit
```

Ten-GigabitEthernet 4/0/1 と Ten-GigabitEthernet 4/0/2 を IRF スタックポート 4/1 に関連づけます。

```
[Switch] irf-port 4/1
[Switch-irf-port4/1] port group interface ten-gigabitethernet 4/0/1
[Switch-irf-port4/1] port group interface ten-gigabitethernet 4/0/2
[Switch-irf-port4/1] quit
```

Ten-GigabitEthernet 4/0/3 と Ten-GigabitEthernet 4/0/4 を IRF スタックポート 4/2 に関連づけます。

```
[Switch] irf-port 4/2
[Switch-irf-port4/2] port group interface ten-gigabitethernet 4/0/3
[Switch-irf-port4/2] port group interface ten-gigabitethernet 4/0/4
[Switch-irf-port4/2] quit
```

物理インタフェースを UP にし、設定を保存します。

```
[Switch] interface range ten-gigabitethernet 4/0/1 to ten-gigabitethernet 4/0/4
[Switch-if-range] undo shutdown
[Switch-if-range] quit
[Switch] save
```

IRF スタックポートの設定を有効にします。

```
[Switch] irf-port-configuration active
```

Device D を IRF スタックユニットに加入させるため再起動します。4 台の IRF スタックユニットが形成されます。

5. IRF スタックユニットの BFD MAD を設定します。

VLAN3 を作成し、Ten-GigabitEthernet 1/0/5、Ten-GigabitEthernet 2/0/5、Ten-GigabitEthernet 3/0/5、Ten-GigabitEthernet 4/0/5 を VLAN3 に割り当てます。

```
[Switch] vlan 3
[Switch-vlan3] port ten-gigabitethernet 1/0/5 ten-gigabitethernet 2/0/5 ten-gigabitethernet 3/0/5 ten-gigabitethernet 4/0/5
[Switch-vlan3] quit
```

VLAN インタフェース 3 を作成し、各メンバ装置の VLAN インタフェースに MAD IP アドレスを設定します。

```
[Switch] interface vlan-interface 3
[Switch-Vlan-interface3] mad bfd enable
[Switch-Vlan-interface3] mad ip address 192.168.2.1 24 member 1
[Switch-Vlan-interface3] mad ip address 192.168.2.2 24 member 2
[Switch-Vlan-interface3] mad ip address 192.168.2.3 24 member 3
[Switch-Vlan-interface3] mad ip address 192.168.2.4 24 member 4
[Switch-Vlan-interface3] quit
```

Ten-GigabitEthernet 1/0/1、Ten-GigabitEthernet 2/0/1、Ten-GigabitEthernet 3/0/1、Ten-GigabitEthernet 4/0/1 のスパニングツリー機能を無効にします。

```
[Switch] interface range ten-gigabitethernet 1/0/5 ten-gigabitethernet 2/0/5 ten-gigabitethernet 3/0/5 ten-gigabitethernet 4/0/5
[Switch-if-range] undo stp enable
[Switch-if-range] quit
```

6. 中継装置として Device E を設定します。

VLAN3 を作成し、BFD MAD パケットを転送するように Ten-GigabitEthernet 1/0/1 ～ Ten-GigabitEthernet 1/0/4 を VLAN 3 に割り当てます。

```
<DeviceE> system-view
[DeviceE] vlan 3
[DeviceE-vlan3] port ten-gigabitethernet 1/0/1 to ten-gigabitethernet 1/0/4
[DeviceE-vlan3] quit
```

1.9.3. ARP MAD を使用する場合の IRF スタックの設定例

I. ネットワーク要件

図 1-15 に示すように、エンタープライズネットワークで 4 台の IRF スタックユニットを設定します。

- IRF スタックユニットで ARP MAD を設定し ARP MAD パケットを転送するように Device E につながるリンクを使用します。
- ループが発生しないように、スパニングツリー機能を Device E と IRF スタックユニットの間で実行します。

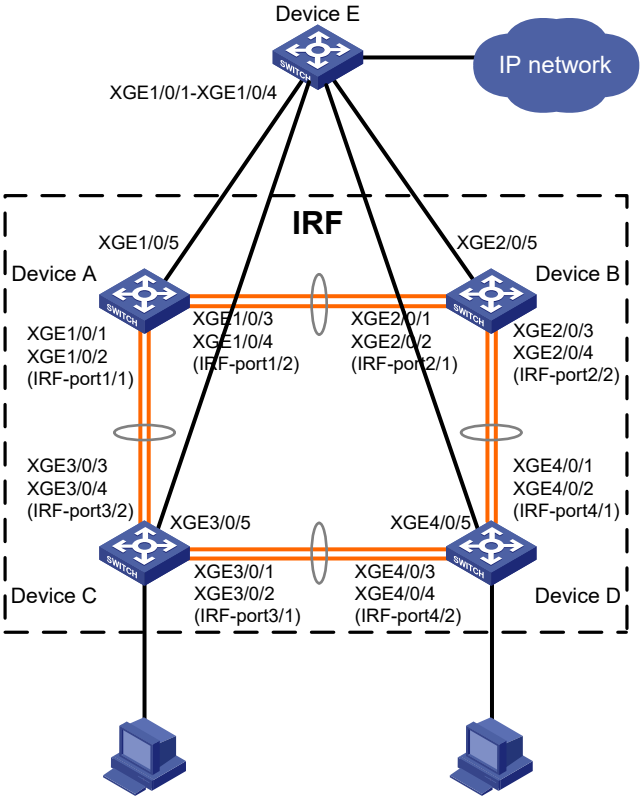


図 1-15 ネットワーク図

II. 設定手順

1. Device A を設定します。

   # IRF スタック接続に使用する IRF スタック物理インタフェースをシャットダウンします。

```
<Switch> system-view
[Switch] interface range ten-gigabitethernet 1/0/1 to ten-gigabitethernet 1/0/4
[Switch-if-range] shutdown
[Switch-if-range] quit
```

Ten-GigabitEthernet 1/0/1 と Ten-GigabitEthernet 1/0/2 を IRF スタックポート 1/1 に関連づけます。

```
[Switch] irf-port 1/1
[Switch-irf-port1/1] port group interface ten-gigabitethernet 1/0/1
[Switch-irf-port1/1] port group interface ten-gigabitethernet 1/0/2
[Switch-irf-port1/1] quit
```

Ten-GigabitEthernet 1/0/3 と Ten-GigabitEthernet 1/0/4 を IRF スタックポート 1/2 に関連づけます。

```
[Switch] irf-port 1/2
[Switch-irf-port1/2] port group interface ten-gigabitethernet 1/0/3
[Switch-irf-port1/2] port group interface ten-gigabitethernet 1/0/4
[Switch-irf-port1/2] quit
```

物理インタフェースを UP にし、設定を保存します。

```
[Switch] interface range ten-gigabitethernet 1/0/1 to ten-gigabitethernet 1/0/4
[Switch-if-range] undo shutdown
[Switch-if-range] quit
[Switch] save
```

IRF スタックポートの設定を有効にします。

```
[Switch] irf-port-configuration active
```

2. Device B を設定します。

Device B のメンバ ID を 2 に変更し、再起動します。

```
<Switch> system-view
[Switch] irf member 1 renumber 2
Renumbering the member ID may result in configuration change or loss. Continue?
[Y/N]:y
[Switch] quit
<Switch> reboot
```

図 1-15 に示すように Device B を Device A に接続し、Device B にログインします。(詳細は省略します。)

IRF スタック物理インタフェースをシャットダウンします。

```
<Switch> system-view
[Switch] interface range ten-gigabitethernet 2/0/1 to ten-gigabitethernet 2/0/4
[Switch-if-range] shutdown
[Switch-if-range] quit
```

Ten-GigabitEthernet 2/0/1 と Ten-GigabitEthernet 2/0/2 を IRF スタックポート 2/1 に関連づけます。

```
[Switch] irf-port 2/1
[Switch-irf-port2/1] port group interface ten-gigabitethernet 2/0/1
[Switch-irf-port2/1] port group interface ten-gigabitethernet 2/0/2
[Switch-irf-port2/1] quit
```

Ten-GigabitEthernet 2/0/3 と Ten-GigabitEthernet 2/0/4 を IRF スタックポート 2/2 に関連づけます。

```
[Switch] irf-port 2/2
[Switch-irf-port2/2] port group interface ten-gigabitethernet 2/0/3
[Switch-irf-port2/2] port group interface ten-gigabitethernet 2/0/4
[Switch-irf-port2/2] quit
```

物理インタフェースを UP にし、設定を保存します。

```
[Switch] interface range ten-gigabitethernet 2/0/1 to ten-gigabitethernet 2/0/4
[Switch-if-range] undo shutdown
[Switch-if-range] quit
[Switch] save
```

IRF スタックポートの設定を有効にします。

```
[Switch] irf-port-configuration active
```

2 台の装置は Master 選定を行い、選定されなかった 1 台は Master とともに IRF スタックユニットを形成するために再起動します。

3. Device C を設定します。

Device C のメンバ ID を 3 に変更し、再起動します。

```
<Switch> system-view
[Switch] irf member 1 renumber 3
Renumbering the member ID may result in configuration change or loss. Continue?
[Y/N]:y
[Switch] quit
<Switch> reboot
```

図 1-15 に示すように Device C を Device A に接続し、Device C にログインします。(詳細は省略します。)

IRF スタック物理インタフェースをシャットダウンします。

```
<Switch> system-view
[Switch] interface range ten-gigabitethernet 3/0/1 to ten-gigabitethernet 3/0/4
[Switch-if-range] shutdown
[Switch-if-range] quit
```

Ten-GigabitEthernet 3/0/1 と Ten-GigabitEthernet 3/0/2 を IRF スタックポート 3/1 に関連づけます。

```
[Switch] irf-port 3/1
[Switch-irf-port3/1] port group interface ten-gigabitethernet 3/0/1
[Switch-irf-port3/1] port group interface ten-gigabitethernet 3/0/2
[Switch-irf-port3/1] quit
```

Ten-GigabitEthernet 3/0/3 と Ten-GigabitEthernet 3/0/4 を IRF スタックポート 3/2 に関連づけます。

```
[Switch] irf-port 3/2
[Switch-irf-port3/2] port group interface ten-gigabitethernet 3/0/3
[Switch-irf-port3/2] port group interface ten-gigabitethernet 3/0/4
[Switch-irf-port3/2] quit
```

物理インタフェースを UP にし、設定を保存します。

```
[Switch] interface range ten-gigabitethernet 3/0/1 to ten-gigabitethernet 3/0/4
[Switch-if-range] undo shutdown
[Switch-if-range] quit
[Switch] save
```

IRF スタックポートの設定を有効にします。

```
[Switch] irf-port-configuration active
```

Device C を IRF スタックユニットに加入させるため再起動します。

4. Device D を設定します。

Device D のメンバ ID を 4 に変更し、再起動します。

```
<Switch> system-view
[Switch] irf member 1 renumber 4
Renumbering the member ID may result in configuration change or loss. Continue?
[Y/N]:y
[Switch] quit
<Switch> reboot
```

図 1-15 に示すように Device D を Device B、Device C に接続し、Device D にログインします。(詳細は省略します。)

IRF スタック物理インタフェースをシャットダウンします。

```
<Switch> system-view
[Switch] interface range ten-gigabitethernet 4/0/1 to ten-gigabitethernet 4/0/4
[Switch-if-range] shutdown
[Switch-if-range] quit
```

Ten-GigabitEthernet 4/0/1 と Ten-GigabitEthernet 4/0/2 を IRF スタックポート 4/1 に関連づけます。

```
[Switch] irf-port 4/1
[Switch-irf-port4/1] port group interface ten-gigabitethernet 4/0/1
[Switch-irf-port4/1] port group interface ten-gigabitethernet 4/0/2
[Switch-irf-port4/1] quit
```

Ten-GigabitEthernet 4/0/3 と Ten-GigabitEthernet 4/0/4 を IRF スタックポート 4/2 に関連づけます。

```
[Switch] irf-port 4/2
[Switch-irf-port4/2] port group interface ten-gigabitethernet 4/0/3
[Switch-irf-port4/2] port group interface ten-gigabitethernet 4/0/4
[Switch-irf-port4/2] quit
```

物理インタフェースを UP にし、設定を保存します。

```
[Switch] interface range ten-gigabitethernet 4/0/1 to ten-gigabitethernet 4/0/4
[Switch-if-range] undo shutdown
[Switch-if-range] quit
[Switch] save
```

IRF スタックポートの設定を有効にします。

```
[Switch] irf-port-configuration active
```

Device D を IRF スタックユニットに加入させるため再起動します。4 台の IRF スタックユニットが形成されます。

5. IRF スタックの ARP MAD を設定します。

グローバルでスパニングツリー機能を有効にします。ARP MAD の VLAN を MST region の MSTI 1 に割り当てます。

```
<Switch> system-view
[Switch] stp global enable
[Switch] stp region-configuration
[Switch-mst-region] region-name arpmad
[Switch-mst-region] instance 1 vlan 3
[Switch-mst-region] active region-configuration
[Switch-mst-region] quit
```

Bridge MAC アドレスオーナが離脱するとすぐに Bridge MAC アドレスを変更するよう IRF スタックユニットを設定します。

```
[Switch] undo irf mac-address persistent
```

IRF スタックユニットのドメイン ID を 1 に設定します。

```
[Switch] irf domain 1
```

VLAN3 を作成し、Ten-GigabitEthernet 1/0/5、Ten-GigabitEthernet 2/0/5、Ten-GigabitEthernet 3/0/5、Ten-GigabitEthernet 4/0/5 を VLAN3 に割り当てます。

```
[Switch] vlan 3
[Switch-vlan3] port Ten-gigabitethernet 1/0/5 Ten-gigabitethernet 2/0/5 Ten-gigabitethernet 3/0/5 Ten-gigabitethernet 4/0/5
[Switch-vlan3] quit
```

VLAN インタフェース 3 を作成し、IP アドレスを割り当てます。インタフェースで ARP MAD を有効にします。

```
[Switch] interface vlan-interface 3
[Switch-Vlan-interface3] ip address 192.168.2.1 24
[Switch-Vlan-interface3] mad arp enable
You need to assign a domain ID (range: 0-4294967295)
[Current domain is: 1]:
The assigned domain ID is: 1
```

6. 中継装置として Device E を設定します。

注意:

中継装置が IRF スタックユニットの中にある場合、正しい分裂の検出を行うため、IRF スタックユニットとは異なるドメイン ID を IRF スタックユニットに割り当ててください。間違った検出は IRF スタックの分裂を引き起こします。

グローバルでスパニングツリー機能を有効にします。ARP MAD の VLAN を MST region の MSTI 1 に割り当てます。

```
<DeviceE> system-view
[DeviceE] stp global enable
[DeviceE] stp region-configuration
[DeviceE-mst-region] region-name arpmad
[DeviceE-mst-region] instance 1 vlan 3
[DeviceE-mst-region] active region-configuration
[DeviceE-mst-region] quit
```

VLAN3 を作成し、ARP MAD のパケットを転送するため Ten-GigabitEthernet 1/0/1 ～ Ten-GigabitEthernet 1/0/4 を VLAN3 に割り当てます。

```
[DeviceE] vlan 3
[DeviceE-vlan3] port Ten-gigabitethernet 1/0/1 to Ten-gigabitethernet 1/0/4
[DeviceE-vlan3] quit
```

QX-S5100G シリーズ Ethernet スイッチ

オペレーションマニュアル

3. アクセス

本マニュアルは以下に示す章で構成されています。

01-Ethernet インタフェース

02-ループバックインタフェースと Null インタフェース

03-Interface range

04-MAC アドレステーブル

05-MAC information

06-リンクアグリゲーション

07-Port Isolation

08-STP

09-ループ検出

10-VLAN

11-Private VLAN

12-Voice VLAN

13-QinQ

14-VLAN マッピング

15-LLDP

16-L2PT

目次

このセクションのページは **3-x-x** です。

1 章 Ethernetインタフェース 1-1
1.1 Ethernet インタフェースの命名ルール 1-1
1.2 Ethernet インタフェースの共通設定 1-1
1.2.1 コンボインタフェースの設定(QX-S5124GP-4X、QX-S5124GT-4X-PW) 1-1
1.2.2 Ethernet インタフェースの基本設定 1-2
1.2.3 ジャンボフレームの設定 1-3
1.2.4 Ethernet インタフェースの抑制の設定 1-4
1.2.5 Ethernet インタフェースのループバックテストの実行 1-4
1.2.6 インタフェースの一般的なフロー制御の設定 1-5
1.2.7 Ethernet インタフェースの節電機能の有効化 1-6
1.2.8 統計情報のポーリング間隔の設定 1-7
1.2.9 ストーム制御機能の設定 1-7
1.2.10 インタフェース での output パケットの廃棄 1-8
1.3 Layer 2 Ethernet インタフェースの設定 1-9
1.3.1 Ethernet インタフェースのオートネゴシエーションの通信速度の設定 1-9
1.3.2 Ethernet インタフェースのストーム抑止の設定 1-10
1.3.3 Ethernet インタフェースの MDI モードの設定 1-11
1.3.4 Ethernet インタフェースのケーブル接続テスト 1-13
1.4 Ethernet インタフェースの表示と維持 1-13

1章 Ethernet インタフェース

装置は Ethernet インタフェース、コンソールインタフェースをサポートしています。サポートするインタフェースタイプと番号は、装置の種類により異なります。インタフェースタイプと番号については、*インスタレーションマニュアル*を参照してください。

この章では Ethernet インタフェースの設定方法について記載します。

1.1 Ethernetインタフェースの命名ルール

Ethernet インタフェースは *interface type A/B/C* のフォーマットで指定されます。文字は以下のインタフェースタイプを表します。

- **A**– IRF スタックメンバ ID。IRF スタックがない場合、A はデフォルトで 1 となります。
- **B**– 装置のスロット番号。固定インタフェースは 0 となります。
- **C**– インタフェース番号。

1.2 Ethernetインタフェースの共通設定

この章は Ethernet インタフェースの共通設定について記載します。

1.2.1 コンボインタフェースの設定(QX-S5124GP-4X、QX-S5124GT-4X-PW)

コンボインタフェースは、論理的なインタフェースです。オプティカルポート（fiber）かメタルポート（copper）を選択します。メタルポートと、オプティカルポートを同時に使用できません。一方を使用する場合、もう一方は自動的に使用不可になります。

オプティカルポートと、メタルポートは別の interface view となります。オプティカルポートあるいはメタルポートのどちらかを有効化し、インタフェースの速度や通信モードのような、ポートの属性を設定します。

I. 設定必要条件

コンボインタフェースを設定する前に以下の処理が完了していることを確認してください。

- **display interface** コマンドを使用して、コンボポートのどのポート（オプティカルポートあるいはメタルポート）が有効かを確認します。
  - □ メタルポートが有効な場合、"Media type is twisted pair, Port hardware type is 1000_BASE_T."と表示されます。
  - □ オプティカルポートが有効な場合、上記の表示はありません。

- コンボインタフェースの設定を表示するため各コンボインタフェースの view で **display this** コマンドを使用してください。
  - □ オプティカルポートが有効な場合、**combo enable fiber** コマンドがあります。
  - □ メタルポートが有効な場合、**combo enable fiber** コマンドがありません。

II. コンボインタフェースのアクティブポートの変更

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Ethernet interface view に移行する	**interface** *interface-type interface-number*	―
3. コンボポートを有効にする	**combo enable** { **copper** | **fiber** | **auto** }	デフォルト：auto

🕮 **メモ：**

- コンボポートは使用するポートのみケーブルまたは SFP モジュールを接続してください。
- SFP トランシーバモジュールのコンボポートと RJ-45 コンボポートが実装された場合、SFP トランシーバモジュールのコンボポートが優先されます。
- SFP トランシーバモジュールが実装され、RJ-45 ケーブルが接続されていない場合、SFP トランシーバモジュールのコンボポートが有効になります。SFP トランシーバモジュールのコンボポートが実装されたのち、RJ-45 コンボポートに RJ-45 ケーブルを接続してもリンクアップしません。
- RJ-45 コンボポートに RJ-45 ケーブルが接続され、SFP トランシーバモジュールのコンボポートが実装されていない場合、RJ-45 コンボポートが有効になります。RJ-45 コンボポートが接続されリンクアップされていたのち、SFP トランシーバモジュールがコンボポートに実装されても、RJ-45 コンボポートがリンクアップのままとなります。

1.2.2 Ethernet インタフェースの基本設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Ethernet interface view に移行する	**interface** *interface-type interface-number*	―
3. 説明を設定する	**description** *text*	デフォルト：*interface-name* **Interface** たとえば“GigabitEthernet 1/0/1 Interface”です。
4. 通信モードを設定する	**duplex** { **auto** | **full** | **half** }	デフォルト：auto 1000BASE-Tを含むSFP/SFP+トランシーバモジュールで動作するポート、1000Mbpsで動作するRJ-45ポートは、halfパラメータが未サポートです。

操作	コマンド	補足
5. 通信速度を設定する	**speed** { **10** | **100** | **1000** | **auto** }	デフォルト：auto インタフェースタイプによってサポート速度は異なります。
6. Ethernetインタフェースを有効にする	**undo shutdown**	デフォルト：up

🕮 **メモ：**

- SFP/SFP+ポートでは speed 10 及び 100 はサポートしておりません。speed 1000 または auto のみサポートしています。

1.2.3 ジャンボフレームの設定

Ethernet で起こる莫大な量のトラフィックにより、フレームが Ethernet フレームの標準サイズよりも大きくなることがあります。このようなフレーム （ジャンボフレームと呼ばれます） が Ethernet ポートを通過できるようにすることで、標準サイズより大きなフレーム （ただし指定したパラメータ範囲内のもの） を転送できます。

- Ethernet インタフェースでジャンボフレームの設定が無効（**undo jumboframe enable** コマンド）にされているとき、ジャンボフレームの処理を行わないで廃棄します。
- Ethernet インタフェースでジャンボフレームの設定が行われているとき、以下の処理を行います。
  - □ 指定したフレーム長でジャンボフレームを処理します。
  - □ 指定したフレーム長を超過したフレームは処理を行わないで廃棄します。

以下にジャンボフレームを設定する手順を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Ethernet interface view に移行する	**interface** *interface-type interface-number*	―
3. ジャンボフレームを設定する	**jumboframe enable** [*value*]	デフォルト：10000バイトのジャンボフレームが可能です。

🕮 **メモ：**

ジャンボフレームの設定は、タグ(1つにつき 4 バイト)を含むパケットサイズで設定して下さい。

1.2.4 Ethernet インタフェースの抑制の設定

I. 物理状態の変更抑制

Ethernet インタフェースは、up あるいは down の物理的なリンク状態のどちらかで動作します。物理的なリンク状態が up あるいは down となる際、物理レイヤは CPU に変更を通知します。CPU は以下の処理を行います。

- パケット転送を処理する上位レイヤモジュール(ルーティングやフォワーディングモジュールのような)にパケット転送の変更を反映します。
- トラップ、ログの作成、対応するアクションをユーザに通知します。

up、down を頻繁に繰り返すことによるシステムのパフォーマンスの低下を防ぐため、物理リンク状態の変更レポートを遅らせます。つまりリンクの変化を抑制する設定を行います。遅延時間が経過した後、システムは CPU に変更を通知します。

II. 制限とガイドライン

RRPP、STP、MSTP、RSTP、PVST、Smart Link が有効な Ethernet インタフェースでは抑制の設定を行うことができません。

リンクアップイベントとリンクダウンイベントに異なる抑制間隔を設定することができます。

複数回の設定を行った場合、最後の設定が適用されます。

インタフェースでリンクアップイベントとリンクダウンイベントに異なる抑制間隔を設定することができます。リンクアップイベントとリンクダウンイベントで **link-delay** コマンドを複数設定した場合、最後に行った設定が適用されます。

III. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Layer 2 Ethernet interface view に移行する	**interface** *interface-type interface-number*	―
3. Ethernet インタフェースの抑制を設定する	**link-delay { down | up } [msec]** *delay-time*	デフォルト : リンクの変化がある場合、すぐに CPU に通知します。

1.2.5 Ethernet インタフェースのループバックテストの実行

注意：
インタフェースでループバックテストを有効にした場合、インタフェースはトラフィックデータを転送しません。

ループバックテストは以下のタイプに分けられます。

- **内部ループバックテスト** – Ethernet インタフェースに関連したスイッチングチップ内にあるすべての機能のテストを実行します。
- **外部ループバックテスト** – Ethernet インタフェースのハードウェアのテストを行います。外部ループバックテストを行うため、インタフェースにループバックプラグを挿入します。外部ループバックテストを行っている間、インタフェースはテストパケットを送信します。そこでプラグで折り返してインタフェースにループします。もしインタフェースがテストパケットを受信しない場合、インタフェースのハードウェアが故障しています。

I. 設定の制限とガイドライン

- インタフェースがシャットダウンされている場合（インタフェースのステータスは **ADM** あるいは **Administratively DOWN** と表示されます）は、内部/外部ループバックテストともに利用できません。
- ループバックテストの間、**speed**、**duplex**、**mdix-mode**、**shutdown** コマンドは適用できません。
- ループバックテスト実行中、Ethernet インタフェースは全二重モードで動作します。テスト終了後はもとの設定で動作します。

II. 設定手順

以下に Ethernet インタフェースのループバックテストの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	–
2. Ethernet interface view に移行する	**interface** *interface-type interface-number*	–
3. ループバックテストを実行する	**loopback** { **external** | **internal** }	デフォルト：実行なし

1.2.6 インタフェースの一般的なフロー制御の設定

リンクのエンド間で一般的なフロー制御を有効にすることで、リンクでのパケット廃棄を防ぐことができます。受信エンドでフロー制御を有効にすると、フロー制御（Pause フレーム）を送信エンドに通知し、トラフィック輻輳が発生した際に一時的にパケットの送信を停止することができます。一般的なフロー制御には、次のタイプがあります。

- **TxRx モードフロー制御**: **flow-control** コマンドを使用して有効にします。インタフェースは送受信の両方のフロー制御を有効にすることができます。
  - 輻輳が発生すると、インタフェースはピアにフロー制御フレームを送信します。
  - インタフェースはピアからフロー制御フレームを受信したとき、パケットの送信を停止します。
- **Rx モードフロー制御**: **flow-control receive enable** コマンドを使用して有効にします。有効の場合、インタフェースはフロー制御フレームを受信できますが、フロー制御フレームを送信できません。
  - 輻輳が発生すると、インタフェースはフロー制御フレームをピアに送信できません。
  - インタフェースは、ピアからフロー制御フレームを受信すると、ピアへのパケットの送信を中断します。

リンクの単方向トラフィック輻輳を処理するには、一方の端で **flow-control receive enable** コマンドを設定し、もう一方の端で **flow-control** コマンドを設定します。リンクの両端でトラフィックの輻輳を処理できるようにするには、両端で **flow-control** コマンドを設定します。

以下に Ethernet インタフェースでフロー制御の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Ethernet interface view に移行する	**interface** *interface-type interface-number*	―
3. フロー制御を設定する	• TxRx モードフロー制御を有効にする **flow-control** • Rx モードフロー制御を有効にする **flow-control receive enable**	デフォルト：無効

1.2.7 Ethernet インタフェースの節電機能の有効化

I. Ethernet インタフェースのオートパワーダウン設定

重要：
オートパワーダウン機能は、SFP/SFP+ポートで未サポートです。

オートパワーダウン機能が有効なインタフェースで一定期間ダウンしているとき、装置は以下のことを行います。

- 装置は自動的にインタフェースへの電力供給を停止します。
- インタフェースはパワーセーブモードになります。

一定期間は装置のチップの仕様に依存します。一定期間の設定はできません。

インタフェースがアップするとき、以下のことを行います。

- 装置は自動的にインタフェースへの電力供給を回復します。
- インタフェースは通常のモードに戻ります。

以下にオートパワーダウンの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Ethernet interface view に移行する	**interface** *interface-type interface-number*	―
3. オートパワーダウンを有効にする	**port auto-power-down**	デフォルト：無効

II. Ethernet インタフェースの EEE 省電力機能の有効化

EEE（Energy Efficient Ethernet）省電力機能を有効にすることで、ポートで一定期間、パケットを受信しない場合、アップリンクポートを低電力状態に遷移します。この期間はチップの仕様に依存し、設定を変更することができません。パケットが到着した後、ポートは通常の状態に遷移します。

以下に EEE 省電力機能を有効にする設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. Ethernet interface view に移行する	**interface** *interface-type interface-number*	—
3. EEE 省電力機能を有効にする	**eee enable**	デフォルト：無効 この機能はRJ-45ポートでのみ有効です。

1.2.8 統計情報のポーリング間隔の設定

以下に Ethernet インタフェースで統計情報のポーリング間隔の設定を行う方法を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. Ethernet interface view に移行する	**interface** *interface-type interface-number*	—
3. 統計情報のポーリング間隔を設定する	**flow-interval** *interval*	デフォルト：300秒

設定したポーリング間隔によって収集された統計情報を表示するには、**display interface** コマンドを使用します。

1.2.9 ストーム制御機能の設定

ストーム抑制により、インタフェースでブロードキャスト、マルチキャスト、不明なユニキャストトラフィックの制御ができます。ブロードキャスト、マルチキャスト、不明なユニキャストトラフィックがしきい値を超過しているとき、装置は、トラフィックがしきい値を下回るまでパケットを廃棄します。

I. 設定の制限とガイドライン

- 同じタイプのトラフィックでは、**storm constrain** コマンドの設定を行わず、**broadcast-suppression** コマンド、**multicast-suppression** コマンド、**unicast-suppression** コマンドのいずれかのコマンドを使用します。そうでないとス

トームの制御は正しく動作しません。**storm-constrain** コマンドについては、オペレーションマニュアルのセクション 3 *アクセス "Ethernet インタフェース"の"Ethernet インタフェースのストーム抑止の設定"*を参照してください。

- 抑制するしきい値を kbps で設定するとき、正確な抑制しきい値は、設定する値と異なります。
  - □ 設定された値が 64 よりも小さい場合、64 の値が適用されます。
  - □ 設定された値が 64 の整数倍より大きく、64 の整数倍でない場合、設定された 64 の整数倍にもっとも近い値が適用されます。

適用される抑制しきい値は、装置のプロンプトを参照してください。

II. 設定手順

以下に Ethernet インタフェースでストーム抑制のしきい値を設定する方法を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Ethernet interface view に移行する	**interface** *interface-type interface-number*	―
3. ブロードキャストパケット転送抑制を設定し、しきい値を設定する	**broadcast-suppression** { *ratio* | **pps** *max-pps* | **kbps** *max-kbps* }	デフォルト: すべてのブロードキャストを通過します。
4. マルチキャストパケット転送抑制を設定し、しきい値を設定する	**multicast-suppression** { *ratio* | **pps** *max-pps* | **kbps** *max-kbps* }	デフォルト: すべてのマルチキャストを通過します。
5. 不明なユニキャストパケット転送抑制を設定し、しきい値を設定する	**unicast-suppression** { *ratio* | **pps** *max-pps* | **kbps** *max-kbps* }	デフォルト: すべての不明なユニキャストを通過します。

注意:
suppression 機能を Ethernetインタフェースもしくはポートグループに複数設定した場合、設定値は以下の優先度で有効化されます。
ブロードキャスト＞不明なユニキャスト＞マルチキャスト
たとえば、**broadcast-suppression** コマンド、**multicast-suppression** コマンド、**unicast-suppression** コマンドをそれぞれ抑制比率 10/20/30 で設定した場合、ブロードキャストの値が反映され、ブロードキャスト、マルチキャスト、不明なユニキャストの合計が 10%まで疎通可能となります。
suppression 機能を **pps** で使用する場合、標準の 10/100/1000BASE-T ポートでは 65 の倍数、SFP/SFP+ポートでは 650 の倍数で制御します。

1.2.10 インタフェースでの output パケットの廃棄

以下にインタフェースでの output パケットの廃棄の設定手順を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―

操作	コマンド	補足
2. Ethernet interface view に移行する	**interface** *interface-type interface-number*	—
3. インタフェースでのアンノンユニキャスト Output パケットの破棄を有効にする	**unknown-unicast block outbound**	デフォルト：無効

1.3 Layer 2 Ethernetインタフェースの設定

1.3.1 Ethernet インタフェースのオートネゴシエーションの通信速度の設定

Ethernet インタフェースでオートネゴシエーションの通信速度の設定を行った場合、デフォルトでは、エンド間でサポートされているもっとも早い通信速度でネゴシエーションされます。もしもっとも早い通信速度にしたくない場合、ネゴシエーション用に通信速度のパラメータを限定することができます。

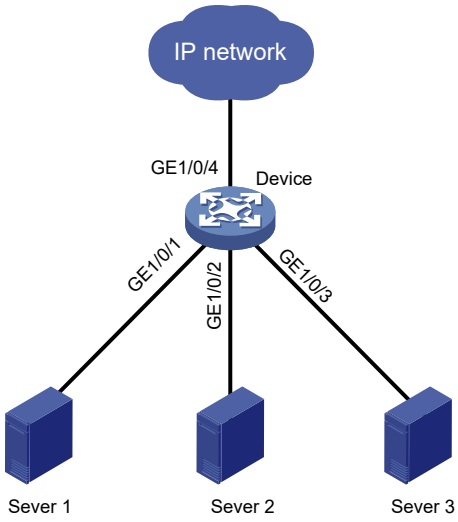


図 1-1 オートネゴシエーションの通信速度の設定

図 1-1に示すようなネットワーク構成があるとします。

- すべてのインタフェースは、最大速度が 1000Mbps の通信速度オートネゴシエーションモードに設定されています。
- GigabitEthernet 1/0/4 はサーバのためインタネットにアクセスを許可します。

もしサーバクラスタの各サーバの転送レートが 1000Mbps である場合、全転送レートは、インタネットにアクセスする GigabitEthernet 1/0/4 インタフェースの容量を超えてしまいます。

GigabitEthernet 1/0/4 の負荷を下げるため、GigabitEthernet 1/0/1、GigabitEthernet 1/0/2、GigabitEthernet 1/0/3 のネゴシエーションの通信速度のパラメータを 100Mbps に設定します。これによって各インタフェースの転送レートが 100Mbps に制限されます。

以下に Ethernet インタフェースのオートネゴシエーションの通信速度の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Ethernet interface view に移行する	**interface** *interface-type interface-number*	―
3. オートネゴシエーションの通信速度を設定する	**speed auto** { **10** | **100** | **1000** }*	デフォルト：設定なし **speed**コマンドと**speed auto**コマンドは一緒に設定することはできません。最初に設定したコマンドが廃棄され、後から設定された設定が有効となります。

1.3.2 Ethernet インタフェースのストーム抑止の設定

I. 概要

ストーム抑止は、ブロードキャスト、マルチキャスト、不明なユニキャストトラフィックを Ethernet インタフェースで受信した各トラフィックと比較します。ストーム抑止は、トラフィックの各タイプにしきい値の下限と上限があります。

インタフェースのトラフィックが上限のしきい値を超えた場合、インタフェースは設定によって以下のどちらかのアクションを行います。

- **トラフィックの特定のタイプをブロックし、他のタイプを転送** – インタフェースが転送されずにブロックされた場合でも、トラフィックはカウントされます。ブロックされたトラフィックがしきい値を下回ったと判断した場合、インタフェースはトラフィックの転送を開始します。
- **インタフェースの自動シャットダウン** – インタフェースが自動でシャットダウンし、すべてのトラフィックの転送を行いません。ブロックされたトラフィックがしきい値を下回ったと判断した場合でも、インタフェースはトラフィックを転送しません。インタフェースをアップにする場合、**undo shutdown** コマンドを行うか、ストーム抑止を無効にする必要があります。

モニタしたトラフィックが以下の状況になったとき、管理用にトラップを送信する設定とログを記録するようにインタフェースに設定することができます。

- トラフィックがしきい値の上限を超過する
- トラフィックがしきい値の下限を下回る

broadcast-suppression コマンド、**multicast-suppression** コマンド、**unicast-suppression** コマンドはハードウェアのチップを使用するため、ソフトウェアでトラフィックを制御する **storm-constrain** コマンドに比べて装置の性能への影響は少なくなります。

ストーム抑止はトラフィックデータを収集するのにポーリングサイクルを使用し、次回のサイクルにデータの解析を行います。インタフェースで、2つのポーリング間隔の設定を行ってください。

II. 設定の制限とガイドライン

トラフィックの同じタイプに **storm constrain** コマンドと、**broadcast-suppression** コマンド、**multicast-suppression** コマンド、**unicast-suppression** コマンドのいずれかの設定を一緒に設定しないでください。一緒に設定した場合、トラフィックの抑止は正しく動作しません。**broadcast-suppression** コマンド、**multicast-suppression** コマンド、**unicast-suppression** コマンドについては、オペレーションマニュアルのセクション 3 *アクセス "Ethernet インタフェース"の"ストーム制御機能の設定"*を参照してください。

III. 設定手順

Ethernet インタフェースにストーム抑止を設定する方法を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. （オプション設定項目）ストーム抑止のポーリング間隔を設定する	**storm-constrain interval** *seconds*	デフォルト：10秒 ネットワークの信頼性のため、デフォルト値以上の値を使用してください。
3. Ethernet interface view に移行する	**interface** *interface-type interface-number*	―
4. （オプション設定項目）ストーム抑止の設定を有効にし、ブロードキャスト、マルチキャスト、不明なユニキャストトラフィックの上限/下限を設定する	**storm-constrain** { **broadcast** | **multicast** | **unicast** } { **pps** | **kbps** | **ratio** } *upperlimit lowerlimit*	デフォルト：無効
5. トラフィックが上限を超過したときのアクションを設定する	**storm-constrain control** { **block** | **shutdown** }	デフォルト：無効
6. （オプション設定項目）ストーム抑止しきい値イベントのログの送信を有効にする	**storm-constrain enable log**	デフォルト: トラフィックが上限を上回るか、上限になった後に下限を下回った場合、インタフェースはログメッセージを送信します。
7. （オプション設定項目）ストーム抑止しきい値イベントのトラップの送信を有効にする	**storm-constrain enable trap**	デフォルト: 上限を超過したときあるいは下回ったときトラップを送信します。

1.3.3 Ethernet インタフェースの MDI モードの設定

重要：

MDI モードの機能は、SFP/SFP+ポートで未サポートです。

メタルの Ethernet インタフェースは、8 ピンのケーブルを使用します。各ピンはそれぞれ固有の役割があります。たとえば、ピン 1 とピン 2 は信号を送信し、ピン 3 とピン 6 は信号を受信します。Ethernet インタフェースに接続するためクロスオーバーケーブルとストレートケーブルの両方を使用することができます。Ethernet インタフェースが自動でケーブルタイプを適用させるため、以下の MDI（Medium Dependent Interface-Crossover）モードのいずれかで動作します。

- MDIX モード－ピン 1、ピン 2 は信号を受信し、ピン 3 とピン 6 は信号を送信します。
- MDI モード－ピン 1、ピン 2 は信号を送信し、ピン 3 とピン 6 は信号を受信します。
- Auto MDIX モード－ピア間でインタフェースのネゴシエーションが行われます。

🕮 **メモ：**

この機能は物理インタフェースのピン 4、ピン 5、ピン 7、ピン 8 に影響しません。

- 10Mbps あるいは 100Mbps で動作するインタフェースのピン 4、ピン 5、ピン 7、ピン 8 は信号の送受信を行いません。
- 1000Mbps で動作するインタフェースのピン 4、ピン 5、ピン 7、ピン 8 は信号の送受信を行います。

ピア間でインタフェースと通信できるように、以下のガイドラインに従ってインタフェースの MDIX モードを設定してください。

- 通常、インタフェースの MDIX モードを Auto MDIX モードに設定してください。装置がケーブルタイプを確定できないとき、インタフェースの MDIX モードを MDI あるいは MDIX モードに設定してください。
- ストレートケーブルを使用する場合、ローカル MDI モードとリモート MDI モードは異なる必要があります。
- クロスオーバーケーブルを使用する場合、以下のいずれかのモードに設定してください。
  - □ ローカル MDI モードとリモート MDI モードは同じにしてください。
  - □ どちらか一端を Auto MDIX モードに設定してください。

以下に Ethernet インタフェースに MDI モードを設定する手順を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. Ethernet interface view に移行する	**interface** *interface-type interface-number*	—
3. Ethernet インタフェースへの MDI モードを設定する	**mdix-mode** { **automdix** | **mdi** | **mdix** }	デフォルト：**automdix**

1.3.4 Ethernet インタフェースのケーブル接続テスト

重要：
このコマンドは SFP/SFP+ポートで未サポートです。
リンクアップしていないポートでは動作しません。

以下に Ethernet インタフェースのケーブル接続テストを行う手順を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. Ethernet interface view に移行する	**interface** *interface-type interface-number*	—
3. Ethernetインタフェースに接続されたケーブルをテストする	**virtual-cable-test**	—

1.4 Ethernetインタフェースの表示と維持

すべての view で **display** コマンドを実行し、user view で **reset** コマンドを実行できます。

操作	コマンド
インタフェースのトラフィック統計情報を表示する	**display counters** { **inbound** | **outbound** } **interface** [*interface-type* [*interface-number*]]
最後のサンプリング間隔からのトラフィックレートの統計情報を表示する	**display counters rate** { **inbound** | **outbound** } **interface** [*interface-type* [*interface-number*]]
指定されたEthernetインタフェースあるいは全インタフェースの動作情報とステータス情報を表示する	**display interface** [*interface-type* [*interface-number*]]
指定されたEthernetインタフェースあるいは全インタフェースの概要情報を表示する	**display interface** [*interface-type* [*interface-number*]] [**brief** [**description** | **down**]]
指定されたEthernetインタフェースあるいは全インタフェースのストーム抑止を表示する	**display storm-constrain** [**broadcast** | **multicast** | **unicast**] [**interface** *interface-type interface-number*]
インタフェースの統計情報を削除する	**reset counters interface** [*interface-type* [*interface-number*]]

目次

このセクションのページは **3-x-x** です。

2 章 ループバックインタフェースと Null インタフェース 2-1
2.1 ループバックインタフェースの設定 2-1
2.2 Null インタフェースの設定 2-1
2.3 ループバックインタフェースと NULL インタフェースの表示と維持 2-2

2章 ループバックインタフェースと Null インタフェース

この章ではループバックインタフェースと Null インタフェースを設定する方法について記載します。

2.1 ループバックインタフェースの設定

ループバックインタフェースは、仮想的なインタフェースです。手動でコマンドによるシャットダウンをしない限り、ループバックインタフェースの物理レイヤ状態とリンクレイヤプロトコルは、常に UP しています。この利点によって以下のように広く使用されます。

- **装置が作成したパケットの送信元 IP アドレスとしてループバックアドレスを設定**
  - ループバックインタフェースアドレスは安定したユニキャストアドレスであるため、装置を識別するのに使用されます。
    - 認証ルールあるいはセキュリティサーバで、装置が作成したパケットの許可/禁止のルールを設定するとき、装置を識別するループバックインタフェースアドレスを送信元 IP アドレスとしたパケットを許可/禁止するようにルールを簡略化することができます。
    - ループバックインタフェースに IP アドレスを割り当て、送信元アドレスに使用した場合、ループバックインタフェースからピアまでのルートが届くことを確認してください。ループバックインタフェースに送信されるすべてのデータパケットは装置自体に送信されていると認識するため、装置はこのパケットを転送しません。
- **ダイナミックルーティングプロトコルのループバックインタフェースの使用** – ダイナミックルーティングプロトコル用にルータ ID を設定する際、ルータ ID として最も高いループバックインタフェースの IP アドレスを使用します。

以下にループバックインタフェースを設定する方法を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. ループバックインタフェースを作成し loopback interface view に移行する	**interface loopback** *interface-number*	—
3. ループバックインタフェースの説明を設定する	**description** *text*	デフォルト：*interface name* **Interface** (例 **LoopBack1 Interface**)
4. ループバックインタフェースを up にする	**undo shutdown**	デフォルト：up

2.2 Nullインタフェースの設定

NULL インタフェースは、論理的インタフェースで、常に UP しています。しかし、データパケットを転送したり、IP アドレスやリンクレイヤプロトコルを設定したりできません。

NULL インタフェースをスタティックルートのネクストホップとして具体的なネットワークセグメントに指定した場合、ネットワークセグメントに送信されたパケットはすべて破棄されます。したがって、ACL を適用する代わりにパケットを NULL インタフェースに送信することで、不要なトラフィックをフィルタすることができます。

以下に NULL インタフェースを設定する方法を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. null interface view に移行する	**interface null 0**	NULL 0インタフェースはデフォルト固定です。 NULLインタフェースは装置に一つだけサポートしています。NULLインタフェースは削除、作成することはできません。
3. NULL インタフェースの説明を設定する	**description** *text*	デフォルト：NULL0 Interface

2.3 ループバックインタフェースとNULLインタフェースの表示と維持

すべての view で **display** コマンドを実行し、user view で **reset** コマンドを実行できます。

操作	コマンド
指定したあるいはすべてのループバックインタフェースの情報を表示する	**display interface loopback** [*interface-number*] [**brief** [**description** | **down**]]
NULLインタフェースを表示する	**display interface null** [**0**] [**brief** [**description** | **down**]]
指定したあるいはすべてのループバックインタフェースの情報を削除する	**reset counters interface loopback** [*interface-number*]
NULLインタフェースを削除する	**reset counters interface null** [**0**]

目次

このセクションのページは **3-x-x** です。

3 章 Interface range 3-1
3.1 設定ガイドライン 3-1
3.2 設定手順 3-2
3.3 表示と維持 3-2

3章 Interface range

interface range コマンドはインタフェースレンジを作成し、interface range view に移行します。同じ機能を 1 つずつインタフェースに設定する代わりに、interface range view に移行して、複数のインタフェースにまとめて設定することができます。たとえば、複数のインタフェースをまとめてシャットダウンする場合、interface range view で **shutdown** コマンドを実行します。

interface range でインタフェースを設定するとき、**interface range** コマンドあるいは **interface range name** コマンドを使用して interface range を設定し、その view に移行する必要があります。

interface range コマンドを使用して設定した場合、interface range で指定した各インタフェースに反映されます。**interface range name** コマンドでは、繰り返し interface range を使用することはできません。繰り返し設定する場合は、**interface range name** コマンドを使用します。

3.1 設定ガイドライン

interface range view で interface range を使用する際は、以下の点に注意してください。

- interface range view では、**interface range** コマンドで最初に指定したインタフェースでサポートされるコマンドのみ有効です。
- **interface** *interface-type interface-number* コマンドで interface view に移行できない場合、interface range で最初に指定したインタフェースでインタフェース設定をしないでください。
- リンクアグリゲーションのアグリゲートインタフェースとメンバポートを同じ interface range に設定しないでください。設定した場合、あるコマンドによってリンクアグリゲーションが失敗することがあります。
- interface range のインタフェースの最大数に制限はありませんが、interface range でのインタフェースが多くなれば、実行時間も長くなります。
- 1000 個以上の interface range name を作成しないでください。
- interface range view でコマンドを実行した後、以下の状態の 1 つになります。
  - □ システムはエラーメッセージを表示し、interface range view にとどまります。これは 1 つ以上のメンバインタフェースで実行が失敗したことを示します。
    - □ インタフェースレンジの最初に指定したインタフェースでコマンドの実行に失敗した場合、他のメンバインタフェースで実行されません。
    - □ 最初に指定したインタフェースではないインタフェースで、コマンドの実行に失敗した場合、残りのメンバインタフェースでコマンドが適用されます。
  - □ システムは interface range view に移行します。以下のことを示します。
    - □ コマンドは system view と interface range view でサポートされます。
    - □ interface range view のメンバインタフェースでコマンドの実行に失敗した場合、システムは system view でコマンドを実行します。
    - □ システムは後続のメンバインタフェースでコマンドを実行しません。

各メンバインタフェースの interface view の設定を確認する場合、**display this** コマンドを使用することができます。また system view の設定が必要でない場合、**undo** コマンドで設定を削除することができます。

3.2 設定手順

Interface range の設定をするには以下の手順に従ってください。

操作	コマンド	補足
1. system view へ移行する	**system-view**	–
2. Interface range view へ移行する	● 名前設定なし： **interface range** { *interface-type interface-number* **to** *interface-type interface-number* }&<1-24> ● 名前設定あり： **interface range name** *name* [**interface** { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-24>]	**interface range name**コマンドを使用すると interface rangeに名前を割り当てることができます。そしてinterface range viewに移行するためにinterface rangeを入力する代わりに名前を指定することができます。
3. （オプション設定項目）最初に指定したインタフェースで有効なコマンドを表示する	Interface range viewで”?”を入力する	–
4. インタフェースに設定を行う	有効なコマンドはインタフェースによって異なる	–
5. （オプション設定項目）設定を確認する	**display this**	–

3.3 表示と維持

すべての view で **display** コマンドを実行します。

操作	コマンド
インタフェースレンジの情報を表示する	**display interface range** [**name** *name*]

目次

このセクションのページは **3-x-x** です。

4 章 MAC アドレステーブル 4-1
4.1 概要 4-1
4.1.1 MAC アドレスエントリの作成方法 4-1
4.1.2 MAC アドレスエントリのタイプ 4-2
4.2 MAC アドレス設定作業リスト 4-2
4.3 MAC アドレスエントリの設定 4-3
4.3.1 設定ガイドライン 4-3
4.3.2 グローバルでのスタティック/ダイナミック MAC アドレスエントリの追加/修正 4-4
4.3.3 インタフェースでのスタティック/ダイナミック MAC アドレスエントリの追加/修正 4-4
4.3.4 ブラックホール MAC アドレスエントリの追加/修正 4-4
4.3.5 マルチポートユニキャスト MAC アドレスエントリの追加/変更 4-5
4.4 MAC アドレス学習の無効化 4-6
4.4.1 グローバルでの MAC アドレス学習の無効化 4-6
4.4.2 インタフェースでの MAC アドレス学習の無効化 4-6
4.4.3 VLAN での MAC アドレス学習の無効化 4-7
4.5 ダイナミック MAC アドレスエントリのエージングタイマの設定 4-7
4.6 インタフェースで学習可能な MAC アドレス数の設定 4-8
4.7 インタフェースで学習可能な MAC アドレスの上限到達後での未知のフレームの転送の設定 4-8
4.8 MAC アドレスローミングの有効化 4-9
4.9 MAC アドレスの移動の通知と抑制機能の有効化 4-10
4.10 MAC アドレスの移動による ARP クイックアップデートの有効化 4-12
4.11 MAC アドレステーブルの SNMP 通知の有効化 4-12
4.12 MAC アドレステーブルのハッシュバケットサイズの設定 4-13
4.12.1 概要 4-13
4.12.2 制限とガイドライン 4-13
4.12.3 設定手順 4-13
4.12.4 MAC アドレスの学習モードの設定 4-14
4.13 MAC アドレステーブルの表示と維持 4-14
4.14 MAC アドレステーブルの設定例 4-15
4.14.1 ネットワーク要件 4-15
4.14.2 設定手順 4-15
4.14.3 設定の確認 4-15

4章 MAC アドレステーブル

4.1 概要

Ethernet 装置は、フレームを転送するために MAC アドレステーブルを使用します。このテーブルは、宛先 MAC アドレス、出力インタフェース、VLAN ID を記載しています。フレームを転送した場合、装置は最初に MAC アドレステーブルにフレームの MAC アドレスと一致するか検索します。

- エントリがある場合、出力インタフェースへパケットを転送します。
- エントリがない場合、装置はフレームが所属する VLAN にフレームをブロードキャストします。

4.1.1 MAC アドレスエントリの作成方法

MAC アドレステーブルのエントリは 2 つのソースから成り立ちます。装置によって自動的に学習されたエントリと、管理者によって手動で追加されたエントリから構成されます。

I. MAC アドレスの学習

通常、MAC アドレステーブルは装置の各インタフェースに入力された送信元 MAC アドレスを学習することによって自動的に MAC アドレステーブルを生成します。

装置は入力パケットの MAC アドレスを学習するため以下の処理を行います。

1) フレームの送信元 MAC アドレス（例：MAC-SOURCE）を確認します。
2) フレームの MAC アドレスに対応するエントリを MAC アドレステーブルから検索します。
   - □ MAC アドレスに対応するエントリがある場合、そのエントリを更新します。
   - □ MAC アドレスに対応するエントリがない場合、MAC-SOURCE と入力ポートのエントリに追加します。

この送信元 MAC アドレスの学習を行った後に MAC-SOURCE 宛のフレームを受信したとき、装置は以下の処理を行います。

1) MAC アドレステーブルから MAC-SOURCE を検索します。
2) エントリのポートからフレームを転送します。

装置は、不明な送信元 MAC アドレスのフレームを受信したとき、MAC アドレステーブルが完全に書き込まれるまで、毎回学習プロセスを行います。

II. MAC アドレスエントリの手動設定

装置が送信元 MAC アドレス学習を介して動的に MAC アドレスを学習するとき、装置は正規ユーザのフレームかハッカーからのフレームかを見分けることができません。これは潜在的にセキュリティに危険をもたらします。ホスト A がポート A に接続されていると

き、MAC アドレスエントリはホスト A の MAC アドレス（たとえば、MAC A）を学習します。不正なユーザがポート B への送信元 MAC アドレスとして MAC A のフレームを送信するとき、装置は以下の処理を行います。

1) 出力インタフェースとしてポート B の新しい MAC アドレスエントリを学習し、MAC A の古いエントリに上書きします。
2) ポート B から MAC A の宛先のフレームを不正ユーザに転送します。

その結果、不正なユーザはホスト A のデータを取得します。ポート A のセキュリティを強化するために、ホスト A をポート A と結合するため、スタティックエントリを手動で設定します。ホスト A のフレームは常にポート A に向けて送信されます。ホスト A の偽造した MAC アドレスを使っている他のホストはホスト A の宛先フレームを取得することができません。

4.1.2 MAC アドレスエントリのタイプ

MAC アドレステーブルには以下のタイプのエントリがあります。

- **スタティックエントリ** – スタティックエントリは、関連したインタフェースから特定の宛先 MAC アドレスによってフレームを転送するため、手動で設定されます。エージアウトしません。スタティックエントリはダイナミックエントリよりも優先されます。
- **ダイナミックエントリ** – 手動で設定されたダイナミックエントリ、または動的に学習したエントリです。エージアウトします。手動で設定されたダイナミックエントリと動的に学習したエントリの優先度は同じです。
- **ブラックホールエントリ** – 手動で設定され、エージアウトしません。ブラックホールエントリは特定の宛先 MAC アドレスでフレームをフィルタするために設定されます。たとえば、セキュリティに問題のある指定したユーザへのすべてのフレームを、ブラックホール MAC アドレスエントリとしてユーザの MAC アドレスを設定することができます。
- **マルチポートユニキャストエントリ** – 特定のユニキャスト宛先 MAC アドレスを持つフレームを複数のポートから送信するために、マルチポートユニキャストエントリが手動で追加され、期限切れになりません。マルチポートユニキャストエントリは、ダイナミックに学習されたエントリよりも高いプライオリティを持ちます。

スタティック、ブラックホール、マルチポートユニキャスト MAC アドレスエントリはダイナミック MAC アドレスに上書きすることができます。逆にダイナミック MAC アドレスは上書きすることができません。

4.2 MACアドレス設定作業リスト

この項で記載される設定項目はすべてオプション設定であり、設定する順番は関係ありません。必要に応じて設定を行ってください。

作業リスト
（オプション設定項目）MACアドレステーブルの設定 • グローバルでのスタティック/ダイナミックMACアドレスエントリの追加/修正 • インタフェースでのスタティック/ダイナミックMACアドレスエントリの追加/修正 • ブラックホールMACアドレスエントリの設定 • マルチポートユニキャストMACアドレスエントリの追加/変更
（オプション設定項目）MACアドレス学習の無効化
（オプション設定項目）ダイナミックMACアドレスエントリのエージングタイマの設定
（オプション設定項目）インタフェースで学習可能なMACアドレス数の設定
（オプション設定項目）インタフェースで学習可能なMACアドレスの上限到達後での未知のフレームの転送の設定
（オプション設定項目）MACアドレスローミングの有効化
（オプション設定項目）MACアドレスの移動の通知と抑制機能の有効化
（オプション設定項目）MACアドレスの移動によるARPクイックアップデートの有効化
（オプション設定項目）MACアドレステーブルのSNMP通知の有効化
（オプション設定項目）MACアドレステーブルのハッシュバケットサイズの設定
（オプション設定項目）MACアドレスの学習モードの設定

4.3 MACアドレスエントリの設定

4.3.1 設定ガイドライン

- 自動学習した MAC アドレスと異なる出力インタフェースで同じ MAC アドレスが存在する場合、ダイナミックエントリは適用されません。
- 設定を保存していない場合、手動で設定されたスタティック、ブラックホール、マルチポートユニキャスト MAC アドレスエントリは、再起動が行われると削除されます。手動で設定されたダイナミック MAC アドレスは設定を保存するあるいはしないに関わらず、削除されます。

送信元 MAC アドレスのフレームが、異なるタイプの MAC アドレスエントリとマッチするフレームは、別に処理されます。

タイプ	説明
スタティックMACアドレスエントリ	フレームの入力インタフェースがエントリのインタフェースと同一かどうかにかかわらず、宛先MACアドレスにフレームを転送します。
マルチポートユニキャストMACアドレスエントリ	• フレームのMACアドレスを学習し、ダイナミックMACアドレスエントリを生成しますが、生成されたダイナミックMACアドレスエントリは有効になりません。 • マルチポートユニキャストMACアドレスエントリにもとづいてフレームを転送します。
ブラックホールMACアドレスエントリ	フレームを廃棄します。
ダイナミックMACアドレスエントリ	• そのエントリと異なるインタフェースから入力したフレームのMACアドレスを学習し、元のエントリに上書きします。 • そのエントリと異なるインタフェースから入力したフレームを転送し、エージングタイマをアップデートします。

4.3.2 グローバルでのスタティック/ダイナミック MAC アドレスエントリの追加/修正

操作	コマンド	補足
1. system view に移行する	**system-view**	–
2. MAC アドレスエントリを追加/変更する	**mac-address** { **dynamic** | **static** } *mac-address* **interface** *interface-type interface-number* **vlan** *vlan-id*	デフォルト : グローバルで設定された MAC アドレスエントリはありません。 VLAN が作成され、VLAN にインタフェースが割り当てられていることを確認してください。

4.3.3 インタフェースでのスタティック/ダイナミック MAC アドレスエントリの追加/修正

操作	コマンド	補足
1. system view に移行する	**system-view**	–
2. interface view に移行する	● interface view に移行する : **interface** *interface-type interface-number* ● aggregate interface view に移行する : **interface bridge-aggregation** *interface-number*	–
3. スタティック、ダイナミック MAC アドレスエントリを追加/変更する	**mac-address** { **dynamic** | **static** } *mac-address* **vlan** *vlan-id*	デフォルト : インタフェースで設定された MAC アドレスエントリはありません。 VLAN が作成され、VLAN にインタフェースが割り当てられていることを確認してください。

4.3.4 ブラックホール MAC アドレスエントリの追加/修正

操作	コマンド	補足
1. system view に移行する	**system-view**	–
2. ブラックホール MAC アドレスエントリを追加/変更する	**mac-address blackhole** *mac-address* **vlan** *vlan-id*	デフォルト : 設定されたブラックホール MAC アドレスエントリはありません。 VLAN が作成されていることを確認してください。

4.3.5 マルチポートユニキャスト MAC アドレスエントリの追加/変更

I. マルチポートユニキャスト MAC アドレスエントリの設定

ユニキャスト宛先 MAC アドレスを複数のポートに割り当てるため、マルチポートユニキャスト MAC アドレスエントリを設定することができます。エントリにマッチする宛先 MAC アドレスのフレームは複数のポートに送信されます。

たとえば、NLB ユニキャストの場合、以下となります。

- クラスタ内のすべてのサーバは自身のアドレスとしてクラスタの MAC アドレスを使用します。
- クラスタ向けのフレームはグループの各サーバに転送されます。

この場合、サーバに接続された装置でマルチポートユニキャスト MAC アドレスを設定することができます。装置はクラスタ内のサーバに接続されたすべてのポートを通してサーバ向けのフレームを転送することができます。

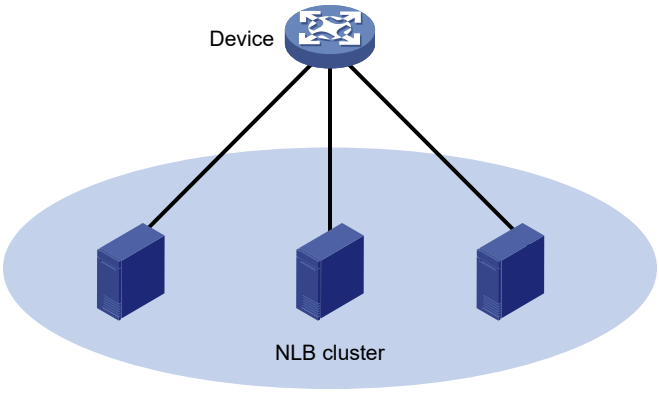


表 4-1 NLB クラスタ

グローバルあるいはインタフェースでマルチポートユニキャスト MAC アドレスエントリを設定することができます。

II. グローバルでのマルチポートユニキャスト MAC アドレスエントリの設定

操作	コマンド	補足
1. system view へ移行する	**system-view**	–
2. マルチポートユニキャスト MAC アドレスエントリを追加あるいは削除する	**mac-address multiport** *mac-address* **interface** *interface-list* **vlan** *vlan-id*	デフォルト：設定なし すでに VLAN が作成済みで、インタフェースに VLAN が割り当てられていることを確認してください。

III. インタフェースでのマルチポートユニキャスト MAC アドレスエントリの設定

操作	コマンド	補足
1. system view へ移行する	**system-view**	–

操作	コマンド	補足
2. interface view へ移行する	● Ethernet interface view へ移行する: **interface** *interface-type interface-number* ● aggregate interface view へ移行する: **interface bridge-aggregation** *interface-number*	–
3. インタフェースにマルチポートユニキャスト MAC アドレスエントリを追加する	**mac-address multiport** *mac-address* **vlan** *vlan-id*	デフォルト：設定なし すでに VLAN が作成済みで、インタフェースに VLAN が割り当てられていることを確認してください。

4.4 MACアドレス学習の無効化

MAC アドレス学習はデフォルトで有効です。装置が攻撃者から攻撃をうけたとき、MAC アドレステーブルが満たされないようにするため、MAC アドレスの学習を無効にします。たとえば、攻撃者からの異なる送信元 MAC アドレスの大量のフレームを学習しないように装置で MAC アドレスの学習を無効にすることができます。

MAC アドレス学習を無効にしたのち、装置は早急に既存のダイナミック MAC アドレスエントリを削除します。

4.4.1 グローバルでの MAC アドレス学習の無効化

操作	コマンド	補足
1. system view に移行する	**system-view**	–
2. グローバルで MAC アドレス学習を無効にする	**undo mac-address mac-learning enable**	デフォルト：有効

4.4.2 インタフェースでの MAC アドレス学習の無効化

グローバルで MAC アドレス学習が有効であるとき、インタフェースごとに MAC アドレス学習を無効にすることができます。

以下にインタフェースでの MAC アドレス学習を無効にする設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	–

操作	コマンド	補足
2. interface view に移行する	● interface viewに移行する：**interface** *interface-type interface-number* ● aggregate interface viewに移行する：**interface** *bridge-aggregation interface-number*	―
3. インタフェースで MAC アドレス学習を無効にする	**undo mac-address mac-learning enable**	デフォルト：有効

4.4.3 VLAN での MAC アドレス学習の無効化

グローバルで MAC アドレス学習が有効であるとき、VLAN ごとに MAC アドレス学習を無効にすることができます。

以下に VLAN での MAC アドレス学習を無効にする設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. グローバルで MACアドレス学習を有効にする	**mac-address mac-learning enable**	デフォルト：有効
3. VLAN view に移行する	**vlan** *vlan-id*	―
4. VLAN で MAC アドレス学習を無効にする	**undo mac-address mac-learning enable**	デフォルト：有効

4.5 ダイナミックMACアドレスエントリのエージングタイマの設定

装置の MAC アドレステーブルには、セキュリティとダイナミックエントリのリソースの浪費を防ぐために、エージングタイマがあります。もしエージングタイマが満了する前にダイナミック MAC アドレスエントリのアップデートが行われないと、装置はエントリを削除します。エージング機能は、MAC アドレステーブルを、最新のネットワークトポロジの変化に対応して即座にアップデートするためのものです。

エージングタイマは適切な時間に設定してください。トポロジの変更が少ない安定したネットワークではエージングタイマを長い時間にする必要があり、トポロジの変更が多いネットワークではエージングタイマを短い時間にする必要があります。

エージング間隔が長いと、有効期限切れのエントリを MAC アドレステーブルに残す可能性があり、最新のネットワークの変化に対応できなくなる可能性があります。また、エージング間隔が短いと、有効なエントリを削除してしまい、装置のパフォーマンスに影響をおよぼす不要なブロードキャストを送信する結果になる可能性があります。

不必要なエージングアウトからダイナミックエントリを防ぐために、エージングタイマの設定を長くするあるいはエージングタイマを無効にすることで安定したネットワークのブロードキャストを削減することができます。ネットワークのパフォーマンスを向上するだけでなく、思いがけない宛先にデータフレームを送信することを減らすことができるため、セキュリティも改善することができます。

以下に MAC アドレス学習のエージングタイマを設定する方法を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. ダイナミック MAC アドレスエントリのエージングタイマを設定する	**mac-address timer** { **aging** *seconds* | **no-aging** }	デフォルト：300秒 **no-aging**パラメータを使用した場合、エージングタイマを無効にします。

4.6 インタフェースで学習可能なMACアドレス数の設定

この機能は MAC アドレステーブルサイズを制限します。MAC アドレステーブルが大きくなって転送処理が低下することを防ぐためにポートまたはポートグループごとに学習可能な MAC アドレス数を制限することができます。

以下にインタフェースで学習可能な MAC アドレス数の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. interface view に移行する	**interface** *interface-type interface-number*	—
3. インタフェースで学習可能な MAC アドレス数を設定する	**mac-address max-mac-count** *count*	デフォルト：設定なし

4.7 インタフェースで学習可能なMACアドレスの上限到達後での未知のフレームの転送の設定

この章では、未知のフレームは、送信元 MAC アドレスが MAC アドレステーブルにないフレームのことを示します。

インタフェースで学習できる MAC アドレスの数が制限に到達したのち、インタフェースで受信された未知のフレームを装置が転送することを有効あるいは無効にすることができます。

以下にインタフェースで受信された未知のフレームの転送の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—

操作	コマンド	補足
2. interface view に移行する	**interface** *interface-type interface-number*	–
3. インタフェースで学習できる MAC アドレスの数が制限に到達したのち、インタフェースで受信された未知のフレームを装置が転送することを有効にする	**mac-address max-mac-count enable-forwarding**	デフォルト：有効

4.8 MACアドレスローミングの有効化

不必要なパケットの送信を防ぎ、転送速度を改善するため、すべてのメンバ装置は同一の MAC アドレステーブルがあることを確認してください。MAC アドレスを同期化したのち、各メンバ装置は学習した MAC アドレスエントリをほかのメンバ装置に通知します。

図 4-1に以下のような構成を示します。

- Device A と Device B は MAC アドレスの同期化が有効にされている IRF スタックです。
- Device A と Device B はそれぞれ AP C と AP D に接続されています。

Client A を AP C に関連づけたとき、Device A は Client A の MAC アドレスを学習し、Device B に通知します。

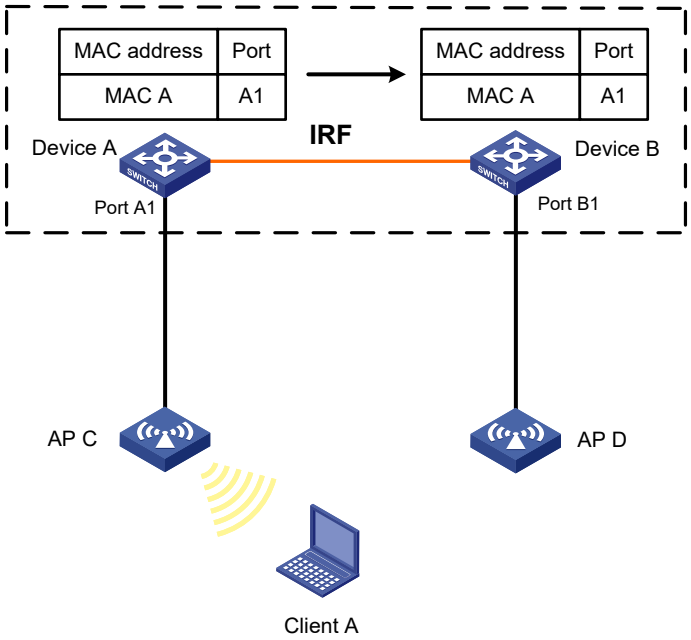


図 4-1 Client A を AP C に関連づけたときの装置の MAC アドレステーブル

Client A が AP D にローミング（移動）したとき、Device B は Client A の MAC アドレスエントリを学習します。図 4-2に示すように、Client A のサービスを継続できるように、Device B は学習した MAC アドレスエントリを Device A に通知します。

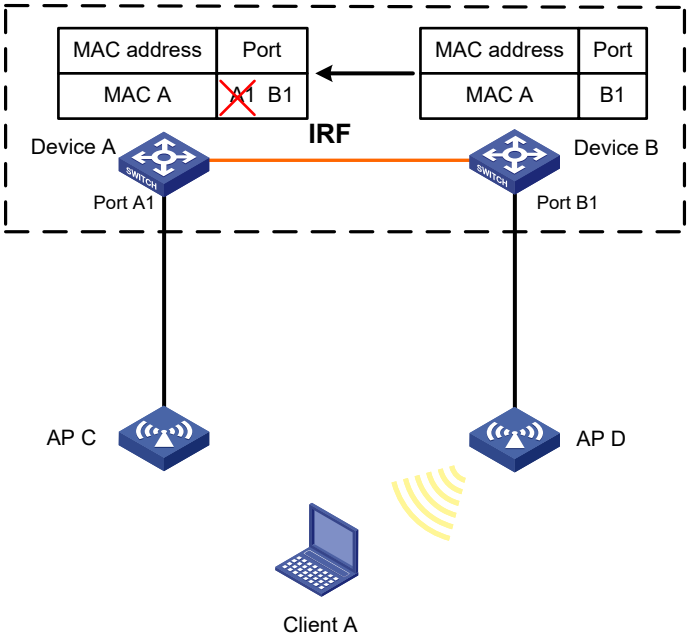


図 4-2 Client A が AP D に関連づけたときの装置の MAC アドレステーブル

以下に MAC アドレスローミングの有効化の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. MAC アドレスローミングを有効にする	**mac-address mac-roaming enable**	デフォルト：無効

4.9 MACアドレスの移動の通知と抑制機能の有効化

以下の状況である場合、インタフェース A で学習された MAC アドレスエントリの出力インタフェースがインタフェース B に変更します。

- インタフェース B が、送信元 MAC アドレスのパケットを受信します。
- インタフェース B がインタフェース A と同じ VLAN に所属しています。

この場合、MAC アドレスがインタフェース A からインタフェース B に移動し、MAC アドレスの移動が発生します。

MAC アドレスの移動の通知機能は、MAC アドレスの移動を検出したとき、MAC アドレスが移動したことのログを出力します。

2 つのインタフェース間で継続して MAC アドレスが移動した場合、レイヤ 2 のループが発生する可能性があります。ループを検出し、位置を特定するために **display**

mac-address mac-move コマンドで MAC アドレスの移動情報を表示することができます。

インタフェースから MAC アドレスの移動が頻繁に移動することをシステムが検出するとき、インタフェースをダウンさせるため、インタフェースで MAC アドレスの移動の抑制を設定することができます。指定した抑制間隔の経過後、インタフェースは自動で UP 状態になります。あるいは手動でインタフェースを UP にすることができます。MAC アドレスの抑制を適用するため、ARP クイックアップデートの機能と一緒に設定する必要があります。ARP クイックアップデートの詳細は次項を参照してください。

以下に MAC アドレスの移動の通知を設定する手順を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. MAC アドレスの移動を通知することを有効にし、MAC アドレスの検出間隔を指定します。	**mac-address notification mac-move** [**interval** *interval-value*]	デフォルト：無効 パラメータを指定しない場合、デフォルトで1分が指定されます。 このコマンドを実行した後、システムはInformation Center にsyslogメッセージのみを送信します。**snmp-agent trap enable mac-address**コマンドが有効である場合、装置のSNMPモジュールにSNMP情報を送信します。
3. （オプション設定項目）検出間隔内に送信元インタフェースから移動する MAC アドレスのしきい値と検出間隔を設定する	**mac-address notification mac-move suppression** { **interval** *interval* | **threshold** *threshold* }	デフォルト : 検出間隔内に送信元インタフェースから移動するMACアドレスのしきい値は3です。MACアドレスの抑制間隔は30秒です。
4. interface view に移行する	● interface view に移行する：**interface** *interface-type interface-number* ● aggregate interface view に移行する：**interface bridge-aggregation** *interface-number*	—
5. MAC アドレスの移動の抑制機能を有効にする	**mac-address notification mac-move suppression**	デフォルト：無効
6. MAC アドレスの移動による ARP クイックアップデートを有効にする	**mac-address mac-move fast-update**	MACアドレスの移動の抑制機能を有効にした場合、必要です。 デフォルト：有効

4.10 MACアドレスの移動によるARPクイックアップデートの有効化

MAC アドレスの移動による ARP クイックアップデート機能は、MAC アドレスの出力インタフェースを変更したのち、ARP エントリをすぐにアップデートすることができます。この機能によってデータ通信を中断することなく行うことができます。

図 4-3に示すように、モバイルユーザ Laptop が AP1 あるいは AP2に接続されているネットワークにアクセスします。ユーザが接続している AP が変更したとき、スイッチは MAC アドレスローミングを検出したのち、ユーザの ARP エントリをすぐにアップデートします。

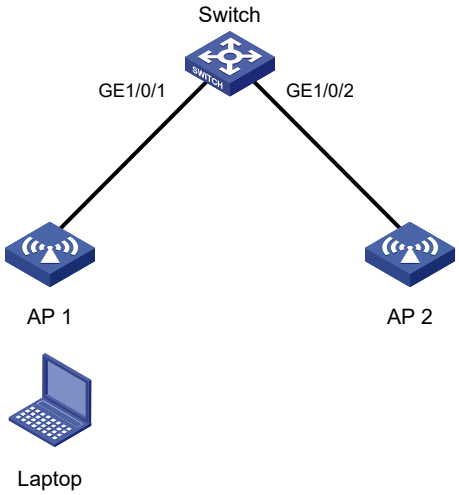


図 4-3 ARP クイックアップデートアプリケーションシナリオ

以下に MAC アドレスの移動による ARP クイックアップデートの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. MAC アドレスの移動による ARP クイックアップデートを有効にする	**mac-address mac-move fast-update**	デフォルト：有効

4.11 MACアドレステーブルのSNMP通知の有効化

MAC アドレステーブルの SNMP 通知を有効にしたのち、装置は NMS に重要なイベントを通知するため、SNMP モジュールに SNMP 通知を送信します。送信する通知の属性を決定するため、SNMP の送信パラメータを SNMP 通知に設定することができます。

MAC アドレステーブルの SNMP 通知を無効にした場合、装置は Information Center モジュールにログメッセージの送信を行います。MAC アドレステーブルモジュールのログメ

ッセージを調査するため、出力ルールと宛先を設定することができます。SNMP 通知と Information Center の詳細は、オペレーションマニュアルのセクション 11 *システム管理*" *SNMP*"、" *Information Center*" を参照してください。

以下に MAC アドレステーブルの SNMP 通知の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. MAC アドレステーブルの SNMP 通知を有効にする	**snmp-agent trap enable mac-address**	デフォルト：無効

4.12 MACアドレステーブルのハッシュバケットサイズの設定

4.12.1 概要

装置はハッシュチェーンを通じて MAC アドレステーブルを保存します。複数の MAC アドレスがハッシュによって同じハッシュキーを取得する場合、MAC アドレスハッシュの競合が発生し、デバイスはこれらの MAC アドレスの一部を学習できません。デバイスは、未知の MAC アドレス宛てにトラフィックをブロードキャストします。この MAC アドレスは、帯域幅とリソースを消費します。

MAC アドレステーブルのハッシュバケットサイズを大きくすると、MAC アドレスハッシュの競合を減らすことができます。ハッシュバケットサイズが大きいほど、より多くのシステムリソースが必要になります。システムリソースに応じて、ハッシュバケットのサイズを適切に設定してください。**display mac-address hash-bucket-size** コマンドを使用すると、現在のハッシュバケットサイズと、次の起動時に有効になるハッシュバケットサイズを表示できます。

4.12.2 制限とガイドライン

設定されたハッシュバケットサイズは、次回の起動時に有効になります。

4.12.3 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. MAC アドレステーブルのハッシュバケットサイズを設定する	**mac-address hash-bucket-size** *size*	デフォルト：4

4.12.4 MAC アドレスの学習モードの設定

装置のデフォルトは、MAC アドレスの学習をソフトウェア処理でおこなっています。そのため、ワイヤーレート で MAC アドレスを学習できません。 MAC アドレスの学習モードを変更するには、以下の手順に従ってください。

表7-1 MAC アドレスの学習モード変更の設定

操作	コマンド	補足
system view に移行する	**system-view**	–
MAC アドレスの学習モードを変更する	**mac-learn-mode** { **hardware** | **software** }	必須設定項目 デフォルト：ソフトウェア

⚠ **注意:**

- MAC アドレスの学習モードを"hardware"モードに設定した場合、すべてのインタフェースで MAC アドレスの学習モードが"hardware モードになります。
- MAC アドレスの学習モードを"hardware"モードに設定しても、802.1X 認証機能、または **mac-address max-mac-count** 設定を行ったポートでは、内部的に"software"モードでの動作となる為、ワイヤーレートでの MAC アドレス学習はできません。

4.13 MACアドレステーブルの表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
MAC アドレステーブル情報を表示する	**display mac-address** [*mac-address* [**vlan** *vlan-id*] | [[**dynamic** | **static**] [**interface** *interface-type interface-number*] | **blackhole** | **multiport**] [**vlan** *vlan-id*] [**count**]]
ダイナミックMAC アドレスエントリのエージングタイマを表示する	**display mac-address aging-time**
グローバルMAC アドレスの学習状態と指定された、あるいはすべてのインタフェースのMAC アドレスの学習状態を表示する	**display mac-address mac-learning** [**interface** *interface-type interface-number*]
MAC アドレスの統計情報を表示する	**display mac-address statistics**
MAC アドレスの移動記録を表示する	**display mac-address mac-move** [**slot** *slot-number*]
MAC アドレステーブルのハッシュバケットサイズを表示する	**display mac-address hash-bucket-size**

4.14 MACアドレステーブルの設定例

4.14.1 ネットワーク要件

図 4-4に示すように、以下の要件を設定します。

- Host A （000f-e235-dc71）は Device のインタフェース GigabitEthernet 1/0/1 に接続され、VLAN1 に属しています。
- ネットワークで一度疑わしいふるまいをした Host B （000f-e235-abcd）は VLAN1 に属しています。

MAC アドレスの設定を以下に示します。

- MAC アドレス spoofing を防ぐため、Device の MAC アドレステーブルの Host A にスタティックエントリを追加します。
- Host B で定義されたすべてのフレームを廃棄するように、Host にブラックホール MAC アドレスエントリを追加します。
- ダイナミック MAC アドレスエントリのエージングタイマを 500 秒に設定します。

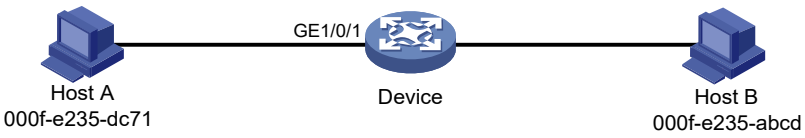


図 4-4 ネットワーク図

4.14.2 設定手順

VLAN1 に属している GigabitEthernet 1/0/1 に MAC アドレス 000f-e235-dc71 のスタティック MAC アドレスエントリを追加します。

```
<Device> system-view
[Device] mac-address static 000f-e235-dc71 interface gigabitethernet 1/0/1 vlan 1
```

#VLAN1に属している MACアドレス 000f-e235-abcdにブラックホール MACアドレスエントリを追加します。

```
[Device] mac-address blackhole 000f-e235-abcd vlan 1
```

ダイナミック MAC アドレスエントリのエージングタイマを 500 秒に設定します。

```
[Device] mac-address timer aging 500
```

4.14.3 設定の確認

GigabitEthernet 1/0/1 のスタティック MAC アドレスエントリを表示します。

```
[Device] display mac-address static interface gigabitethernet 1/0/1
```

```
MAC Address       VLAN ID    State           Port/NickName           Aging
000f-e235-dc71    1          Static          GE1/0/1                 N
```

ブラックホール MAC アドレスエントリを表示します。

```
[Device] display mac-address blackhole
MAC Address       VLAN ID    State           Port/NickName           Aging
000f-e235-abcd    1          Blackhole       N/A                     N
```

ダイナミック MAC アドレスエントリのエージングタイマを表示します。

```
[Device] display mac-address aging-time
MAC address aging time: 500s.
```

目次

このセクションのページは **3-x-x** です。

5 章 MAC information 5-1
5.1 MAC Information の有効化 5-1
5.2 MAC Information モードの設定 5-1
5.3 log あるいは SNMP トラップメッセージの送信間隔の設定 5-2
5.4 MAC Information のキュー長の設定 5-2
5.5 MAC Information 設定例 5-2
5.5.1 ネットワーク要件 5-2
5.5.2 設定の制限とガイドライン 5-3
5.5.3 設定手順 5-3

5章 MAC information

MAC Information 機能は MAC アドレスエントリが学習あるいは削除された場合、Syslog メッセージあるいは SNMP トラップメッセージを作成します。これらのメッセージを解析することによって、監視端末はネットワークにアクセスしているユーザを監視することができます。

MAC Information 機能は、MAC アドレスの変更の Syslog メッセージあるいは SNMP トラップメッセージをキューに格納します。以下の場合、装置はキューの最後の MAC アドレス変更を最新の MAC アドレス変更に上書きします。

- MAC アドレス変更を通知するタイマが満了していない場合
- キューが使い果たされた場合

Syslog メッセージあるいは SNMP トラップメッセージが作成された後、すぐに送信するようにキューの長さを 0 に設定します。

5.1 MAC Informationの有効化

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. グローバルで MAC Information を有効にする	**mac-address information enable**	デフォルト：無効
3. Layer 2 Ethernet interface view に移行する	**interface** *interface-type interface-number*	―
4. インタフェースで MAC Information を有効にする	**mac-address information enable** { **added** | **deleted** }	デフォルト：無効 インタフェースでMAC Informationを有効にする前にグローバルで有効であることを確認してください。

5.2 MAC Informationモードの設定

MAC アドレスの変更を通知するため、MAC Information は以下のモードがあります。

- **Syslog**– 装置は MAC アドレスの変更を通知するため、Syslog メッセージを送信します。このモードでは Syslog メッセージは監視端末の Information Center に送信します。Information Center についての詳細は、オペレーションマニュアルのセクション 11 *システム管理* "*Information Center*"を参照してください。
- **Trap**– 装置は MAC アドレスの変更を通知するため、SNMP トラップメッセージを送信します。このモードでは NMS に SNMP トラップメッセージを送信します。SNMP についての詳細は、オペレーションマニュアルのセクション 11 *システム管理* "*SNMP*"を参照してください。

以下に MAC Information モードを設定する方法を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―

操作	コマンド	補足
2. (オプション設定項目)MAC Information モードを設定する	**mac-address information mode** { **syslog** | **trap** }	デフォルト：**trap**

5.3 logあるいはSNMPトラップメッセージの送信間隔の設定

Syslog メッセージあるいはトラップメッセージを頻繁に送信することを防ぐため、送信間隔の設定を行うことができます。

以下に Syslog メッセージあるいはトラップメッセージの送信間隔を設定する方法を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. Syslog メッセージあるいは SNMP トラップメッセージの送信間隔を設定する	**mac-address information interval** *interval-time*	デフォルト：1秒

5.4 MAC Informationのキュー長の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. MAC Information のキュー長を設定する	**mac-address information queue-length** *value*	デフォルト：50

5.5 MAC Information設定例

5.5.1 ネットワーク要件

図 5-1に示すように、ログホストの Host B に MAC アドレスの変更があった場合 Syslog メッセージを送信するため、Device のインタフェース GigabitEthernet 1/0/1 に MAC Information を有効にします。

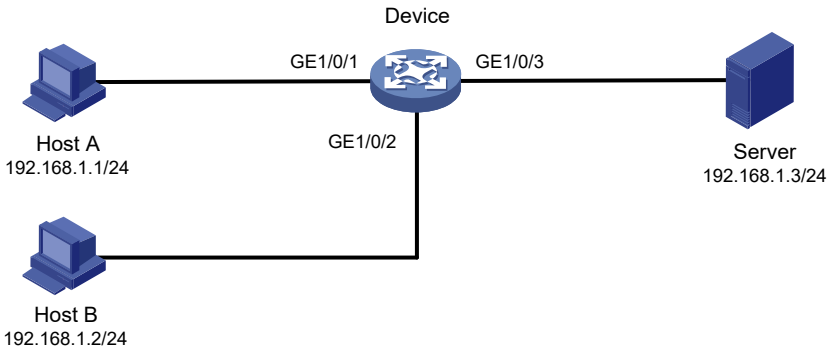


図 5-1 ネットワーク図

5.5.2 設定の制限とガイドライン

ファイル**/etc/syslog.conf** を編集するときのガイドラインを以下に示します。

- コメントは個別の行に記入し、“#”記号で始めてください。
- ファイル名に不要なスペース等をいれないでください。
- ロギングファシリティ名とファイル**/etc/syslog.conf** が指定するログ情報の重要度は、**info-center loghost** コマンドと **info-center source** コマンドで装置に設定したものと一致しなければなりません。一致しないと、ログ情報は正しくログホストに出力されないことがあります。

5.5.3 設定手順

1)　Device で Host B に Syslog メッセージを送信する設定を行います。

information center を有効にします。

```
<Device> system-view
[Device] info-center enable
```

ログホスト 192.168.1.2/24 を指定し、ロギング facility として local4 を指定します。

```
[Device] info-center loghost 192.168.1.2 facility local4
```

ログホストへの出力を無効にします。

```
[Device] info-center source default loghost deny
```

出力ルールを設定する前に、不必要な情報の送信をしないように、出力するログから指定した宛先へのすべてモジュールを無効にします(この例では **loghost**)。

informational レベル以上の severity を持つ MAC アドレスのログをログホストに出力するルールを設定します。

```
[Device] info-center source mac loghost level informational
```

2)　ログホスト Host B を設定します。

以下のように Solaris で動作する設定を行います。同様にほかの UNIX OS の設定を行います。

a)　ルートユーザとしてログホストにログインします。

b)　ディレクトリ**/var/log/**にサブディレクトリ**Device**を作成します。

```
# mkdir /var/log/Device
```

c)　**Device**からのログを保存するため、**Device**ディレクトリに**info.log**を作成します。

```
# touch /var/log/Device/info.log
```

d)　ディレクトリ**/etc/**の**syslog.conf**を編集し、以下の内容を追加します。

メッセージを設定します。

```
local4.info  /var/log/Device/info.log
```

この設定では、**local4** はログを受信するのに使用するログホストのロギング facility の名前です。info は informational レベルです。UNIX システムはファイル **/var/log/Device/info.log** に informational 以上の severity レベルのログ情報を記録します。

e)　**syslogd**のプロセスIDを表示します。**syslogd**のプロセスを削除し、新しい設定を適用するため、**-r**オプションを使用して**syslogd**を再起動します。

```
# ps -ae | grep syslogd
147
# kill -HUP  147
# syslogd -r &
```

Device は、ログホストに MAC アドレスのログを出力し、指定したファイルにログを記録することができます。

3)　Device で MAC Information を有効にします。

グローバルで MAC Information を有効にします。

```
[Device] mac-address information enable
```

MAC Information モードを Syslog に設定します。

```
[Device] mac-address information mode syslog
```

MAC アドレスの情報の変更を記録するため、GigabitEthernet 1/0/1 で MAC Information を有効にします。

- 新しい MAC アドレスを学習します。
- 既存の MAC アドレスを削除します。

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] mac-address information enable added
[Device-GigabitEthernet1/0/1] mac-address information enable deleted
[Device-GigabitEthernet1/0/1] quit
```

MAC Information のキュー長を 100 に設定します。

```
[Device] mac-address information queue-length 100
```

Syslog またはトラップメッセージの送信間隔を 20 秒に設定します。

```
[Device] mac-address information interval 20
```

目次

このセクションのページは **3-x-x** です。

6 章 リンクアグリゲーション 6-1
6.1 概要 6-1
6.1.1 アグリゲーショングループ、メンバポート、アグリゲートインタフェース 6-1
6.1.2 アグリゲーショングループのメンバポートのステート 6-1
6.1.3 オペレーショナルキー 6-2
6.1.4 コンフィグレーションタイプ 6-2
6.1.5 リンクアグリゲーションモード 6-3
6.1.6 スタティックモードのリンクアグリゲーションの動作 6-3
6.1.7 LACP 6-5
6.1.8 ダイナミックリンクアグリゲーションの動作 6-6
6.1.9 アグリゲーショングループの負荷分散 6-9
6.2 リンクアグリゲーション設定作業リスト 6-9
6.3 アグリゲーショングループの設定 6-9
6.3.1 設定の制限とガイドライン 6-9
6.3.2 アグリゲーショングループの設定 6-10
6.4 アグリゲートインタフェースの設定 6-12
6.4.1 アグリゲートインタフェースの説明の設定 6-12
6.4.2 アグリゲーショングループの Selected ポートの最小と最大数の設定 6-12
6.4.3 アグリゲートインタフェースのシャットダウン 6-13
6.5 グローバルでのリンクアグリゲーションのロードシェアリングモードの設定 6-13
6.6 local-first ロードシェアリングモードの有効化 6-14
6.7 リンクアグリゲーションの表示と維持 6-15
6.8 リンクアグリゲーションの設定例 6-15
6.8.1 スタティックアグリゲーション設定例 6-15
6.8.2 ダイナミックアグリゲーション設定例 6-17

6章 リンクアグリゲーション

6.1 概要

リンクアグリゲーションは、複数の Ethernet インタフェースを束ねて、一つの論理インタフェースとして扱う機能です。図 6-1は、3 つの Ethernet インタフェースを束ねて、一つの論理インタフェース（Link aggregation 1）として接続している例です。

これにより、装置間の接続帯域幅を拡大することができます。また、1 つの Ethernet インタフェースが故障した場合に、残った Ethernet インタフェースで通信を継続する冗長性を確保できます。



図 6-1 リンクアグリゲーション図

6.1.1 アグリゲーショングループ、メンバポート、アグリゲートインタフェース

アグリゲーショングループは、集約された Ethernet インタフェースのグループです。アグリゲーショングループには、アグリゲートインタフェースと呼ばれる論理的なインタフェースが作成されます。上位レイヤエンティティにリンクアグリゲーションを使用すると、以下のようになります。

アグリゲートインタフェースのレートは、Selected ステートのそのメンバポートのレートの合計と同一です。また通信モードは Selected ステートのメンバポートと同一です。アグリゲーショングループのメンバポートの状態についての詳細は、オペレーションマニュアルのセクション 3 *アクセス "リンクアグリゲーション"の"アグリゲーショングループのメンバポートのステート"*を参照してください。

6.1.2 アグリゲーショングループのメンバポートのステート

アグリゲーショングループのメンバポートは、以下のステートのどちらかとなります。

- **Selected**：ユーザにトラフィックを送受信できます。
- **Unselected**：ユーザにトラフィックを送受信できません。
- **Individual**：Individual ポートは通常の物理インタフェースとしてトラフィックを転送することができます。以下の状態の場合、ポートは Individual 状態となります。
  - 対応するアグリゲートインタフェースがエッジアグリゲートインタフェースとして設定されました。

□ ポートがピアポートから LACPDU（Link Aggregation Control Protocol Data Units）を受信していません。

6.1.3 オペレーショナルキー

ポートを集約する際に、リンクアグリケーションは、通信速度、通信モードのような設定を含むポート属性にもとづいてオペレーショナルキーをそれぞれのポートに自動的に制御し割り当てます。

リンクアグリゲーショングループ内にある Selected ステートのすべてのメンバポートは、同じオペレーショナルキーを持っています。

6.1.4 コンフィグレーションタイプ

リンクアグリゲーショングループのメンバポートに設定するすべての設定は、グループのポートのアグリゲーションステートに影響を与える可能性があります。影響を与える設定は以下のコンフィグレーションタイプに分類されます。

- **属性コンフィグレーション**– Selected ポートになるためには、メンバポートはアグリゲートインタフェースとして同じ属性の設定を持つ必要があります。表 6-1に属性コンフィグレーションを示します。

  Selected ポートへの同期化に失敗した場合、ポートは Unselected ポートに移行します。ポートが再度 Selected ポートになるために、アグリゲートインタフェースあるいはメンバポートの属性コンフィグレーションを変更します。同期化が失敗しても、アグリゲートインタフェースで変更された属性コンフィグレーションの変更に影響しません。アグリゲートインタフェースが削除された後でも、これらのメンバポートの設定は保持されます。

  属性コンフィグレーションの変更は、リンクアグリゲーションメンバポートのアグリゲーションのステートと動作中のサービスに影響する可能性があります。この影響を確認するため、システムは、メンバポートの属性設定を変更するごとに警告メッセージを表示します。

表 6-1 属性コンフィグレーション

機能	考慮事項
Port isolation	● Isolationグループへのポートの加入状態。 ● ポートが所属しているグループ。 Portisolationについては、オペレーションマニュアルのセクション3 *アクセス* "*Port isolation*"を参照してください。
QinQ	QinQが有効な状態（有効/無効）。 QinQについては、オペレーションマニュアルのセクション3 *アクセス* "*QinQ*"を参照してください。
VLANマッピング	ポートで設定されたVLANマッピング。 QinQについては、オペレーションマニュアルのセクション3 *アクセス* "*QinQ*"を参照してください。

機能	考慮事項
VLAN	以下を含むVLAN属性コンフィグレーション。 ● 許可されたVLAN ID ● PVID ● リンクタイプ（trunk、hybrid、access） ● VLANタグモード VLANについては、オペレーションマニュアルのセクション3 *アクセス "VLAN"*を参照してください。

- **プロトコルコンフィグレーション**– プロトコルコンフィグレーションは、アグリゲートインタフェースの変更があってもメンバポートのアグリゲートステートに影響しません。プロトコルコンフィグレーションの例として、MAC アドレス学習があります。

  アグリゲーションインタフェースのプロトコルコンフィグレーションのみ適用します。メンバポートのプロトコルコンフィグレーションは、ポートがアグリゲーショングループから削除されるまで適用されません。

6.1.5 リンクアグリゲーションモード

リンクアグリゲーションは、ダイナミックモードとスタティックモードがあります。

- **スタティックアグリゲーションモード** — アグリゲーションが安定します。スタティックモードのアグリゲーショングループは、スタティックアグリゲーショングループと呼ばれます。メンバポートのアグリゲーションステートは対向先の影響を受けません。
- **ダイナミックアグリゲーションモード** — ダイナミックモードのアグリゲーショングループは、ダイナミックアグリゲーショングループと呼ばれます。ローカルシステムと対向先のシステムはメンバポートのアグリゲーションステートを自動的に管理します。管理者の管理負荷を削減することができます。

6.1.6 スタティックモードのリンクアグリゲーションの動作

I. リファレンスポートの選出

アグリゲーショングループでポートのアグリゲーションステートを設定するとき、システムはリファレンスポートとして自動でメンバポートを選出します。Selected ポートはリファレンスポートとして、同じオペレーショナルキーと属性コンフィグレーションを持つ必要があります。

メンバポートから、アグリゲートインタフェースとして同一の属性を持つ up 状態のリファレンスポートを選択します。

候補となるポートの優先順位は、以下の順番となります。

1) もっとも高いポート優先度
2) 全 2 重/高速
3) 全 2 重/低速
4) 半 2 重/高速

5)　半 2 重/低速

アグリゲートインタフェースと同じ属性コンフィグレーションを持つ候補のポートから、もっとも高い優先度レベルを持つポートがリファレンスポートとして選択されます。

- 同じ優先度を持つポートが複数あり、Selected ポートがある場合、Selected ポートが選ばれます。もし 1 つ以上の最初の Selected ポートがある場合、ポート番号が一番小さい Selected ポートが選択されます。
- 複数のポートに同じ優先度があり、Selected ポートがない場合、ポート番号が一番小さい Selected ポートが選択されます。

II. 各メンバポートのアグリゲーションステートの設定

スタティックアグリゲーショングループが Selected ポートの制限に達した後、グループに加入したポートは、Selected ポートのトラフィックの中断を防ぐため、Unselected ステートに置き換えられます。

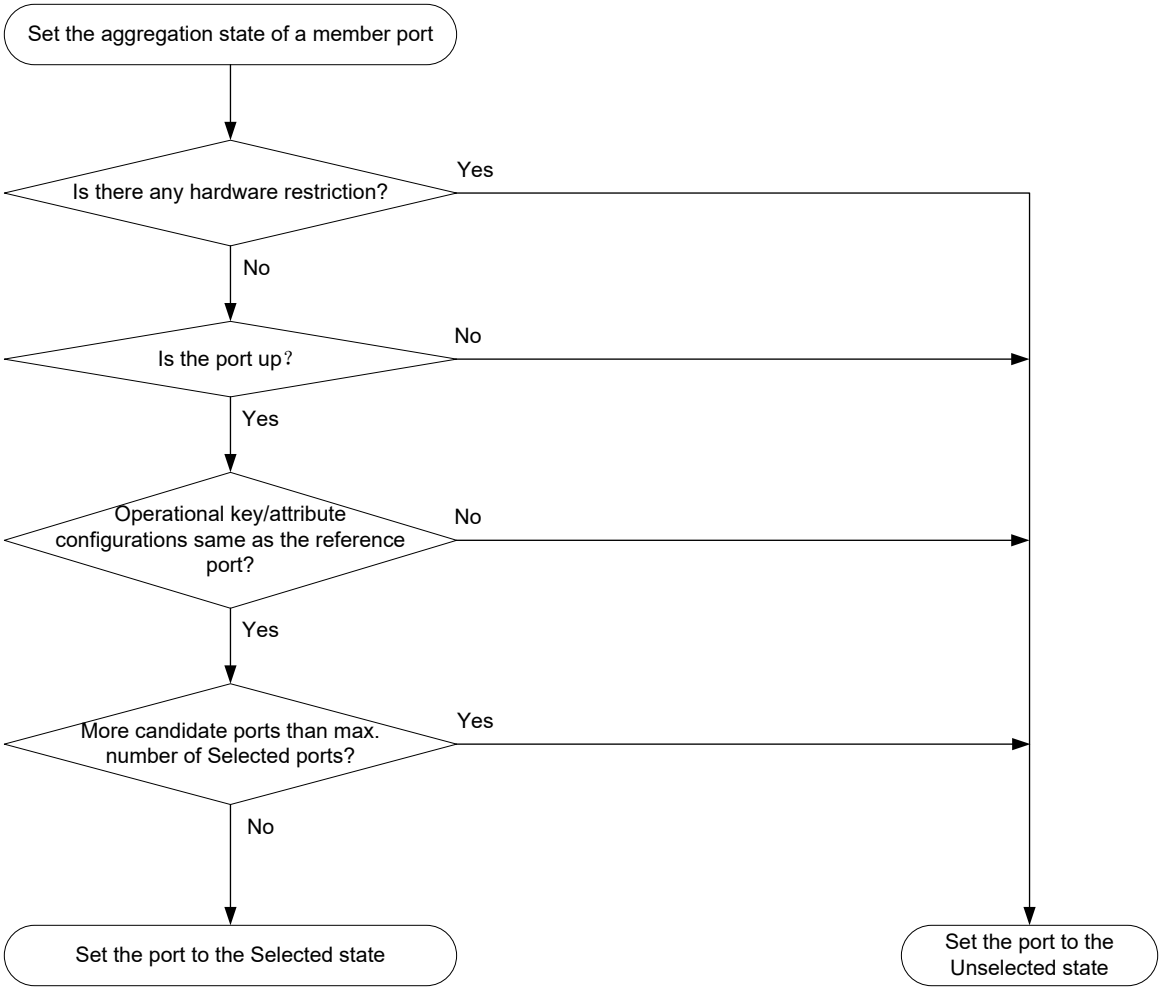


図 6-2 スタティックアグリゲーショングループのアグリゲーションステートの設定

Selected ポートの制限に到達したのち、新しいメンバポートのアグリゲーションの状態は以下の状態によって変わります。

- ポートと Selected ポートが同一の優先度を持つ場合、ポートは Unselected ステートに遷移します。このメカニズムによって既存の Selected ポートでトラフィックの中断を防ぎます。装置の再起動を行うとメンバポートのアグリゲーションステートの再計算が行われます。
- 以下の状態の場合、ポートは Selected ステートに遷移します。
  - □ ポートと Selected ポートが異なる優先度を持つ場合、ポートは少なくとも 1 つの Selected ポートの優先度よりも高い優先度を持ちます。
  - □ アグリゲートインタフェースとして同一の属性コンフィグレーションを持ちます。

オペレーショナルキーと属性コンフィグレーションを変更すると、リンクアグリゲーションメンバポートのアグリゲーションの状態に影響を及ぼす可能性があります。

6.1.7 LACP

ダイナミックアグリゲーションモードは、IEEE802.3ad Link Aggregation Control Protocol（LACP）で規定されています。

LACP は LACP 対応装置と LACPDU（Link Aggregation Control Protocol Data Units）を使用し、情報交換を行います。LACP が有効なアグリゲーショングループのメンバポートは、対向先と情報の交換を行います。メンバポートが LACPDU を受信すると、ほかのメンバポートで受信された情報と受信された情報を比較します。比較することで、2 つのシステム間で Selected ステートになるポートを選定します。

I. LACP 機能

表 6-2に示すように LACP は、基本 LACP 機能と拡張 LACP 機能に分類されます。

表 6-2 基本 LACP 機能と拡張 LACP 機能

カテゴリ	説明
基本LACP機能	システムLACPプライオリティ、システムMACアドレス、ポートLACPプライオリティ、ポート番号、オペレーショナルキーを含む基本的なLACPDUフィールドから実装されます。
拡張LACP機能	新しいType/Length/Value（TLV）フィールドでLACPDUを拡張して実装されます。拡張LACP機能はLACP MADの中間装置で機能させることができます。

II. LACP 動作モード

LACP はアクティブモードあるいはパッシブモードで動作することができます。

LACP がローカルメンバポートとピアのポート上でパッシブモードとして動作するとき、双方のポートは LACPDU を送信することができません。LACP がローカルメンバポートとピアのポート上でアクティブモードとして動作するとき、双方のポートは LACPDU を送信することができます。

QX-S5100G シリーズはアクティブモードのみをサポートしています。

III. LACP プライオリティ

表 6-3に示すように LACP プライオリティには、システム LACP プライオリティとポートプライオリティの 2 種類があります。値が大きいほどプライオリティは高くなります。

表 6-3 LACP プライオリティ

タイプ	説明
システムLACPプライオリティ	リンクアグリゲーションで優勢な装置かを決定するために2つの対向装置（あるいはシステム）で使用します。 ダイナミックリンクアグリゲーションでより高いシステムLACPプライオリティを持つ2つの対向装置（あるいはシステム）がメンバポートのSelectedステートになるポートを最初に設定します。 低いプライオリティを持つシステムはそれぞれの対向先のポートと同様にローカルメンバポートのアグリゲーションステートを設定します。
ポートプライオリティ	システムで選択されるために、メンバポートのプライオリティが決められます。 より高いポートプライオリティを持つメンバポートがSelectedステートになります。

IV. LACP タイムアウト間隔

LACP タイムアウト間隔は、メンバポートが対向のポートから LACPDU を受信するための待ち時間です。もしローカルメンバポートが、LACP タイムアウト間隔時間以内に対向先から LACPDU を受信できない場合、メンバポートは対向先が故障していると認識します。

LACP タイムアウト間隔は、対向先の LACPDU 送信レートも決まります。LACP タイムアウト間隔は以下のタイプを含みます。

- **短いタイムアウト間隔**－タイムアウト間隔は 3 秒です。もし、短いタイムアウト間隔を設定した場合､対向先は LACPDU を早急に送信します｡1 秒ごとに 1 つの LACPDU を送信します。
- **長いタイムアウト間隔**－長いタイムアウト間隔は 90 秒です。もし長いタイムアウト間隔を設定した場合、対向先は LACPDU をロング間隔で送信します。30 秒ごとに 1 つの LACPDU を送信します。

6.1.8 ダイナミックリンクアグリゲーションの動作

I. リファレンスポートの選出

システムは up 状態のインタフェースにある、アグリゲートインタフェースと同じ属性コンフィグレーションを持つメンバポートからリファレンスポートを選出します。Selected ポートはリファレンスポートと同じオペレーショナルキーと属性コンフィグレーションを持つ必要があります。

ローカルシステムは、リファレンスポートを選出するために、リモートシステムと以下の手順が行われます。

1) ローカルシステムのシステム ID をリモートシステムのシステム ID と比較します。システム ID はシステム LACP プライオリティと MAC アドレスが含まれます。

   a) LACPプライオリティの値を比較します。LACPプライオリティの値が低いとシステムIDが小さくなり、優位になります。LACPプライオリティの値が同一の場合、2つのシステムは次のb)に進みます。

   b) MACアドレスを比較します。MACアドレスが低いと、システムIDは小さくなり、優位になります。

2) ポート ID を比較します。ポート ID はポート LACP プライオリティとポート番号から構成されます。

   a) システムはポートLACPプライオリティを比較します。ポートLACPプライオリティが低いポートが優位になります。複数のポートが同じポートLACPプライオリティを持つ場合、次のb)に進みます。

   b) システムはポート番号を比較します。より小さいポート番号のポートが優位になります。もっとも低いポートIDと同一の属性コンフィグレーションを持つポートがリファレンスポートとして選出されます。

II. メンバポートのアグリゲーションステートの設定

リファレンスポートを選出した後、ダイナミックアグリゲーショングループは、個々のメンバポートのアグリゲーションステートを設定します。

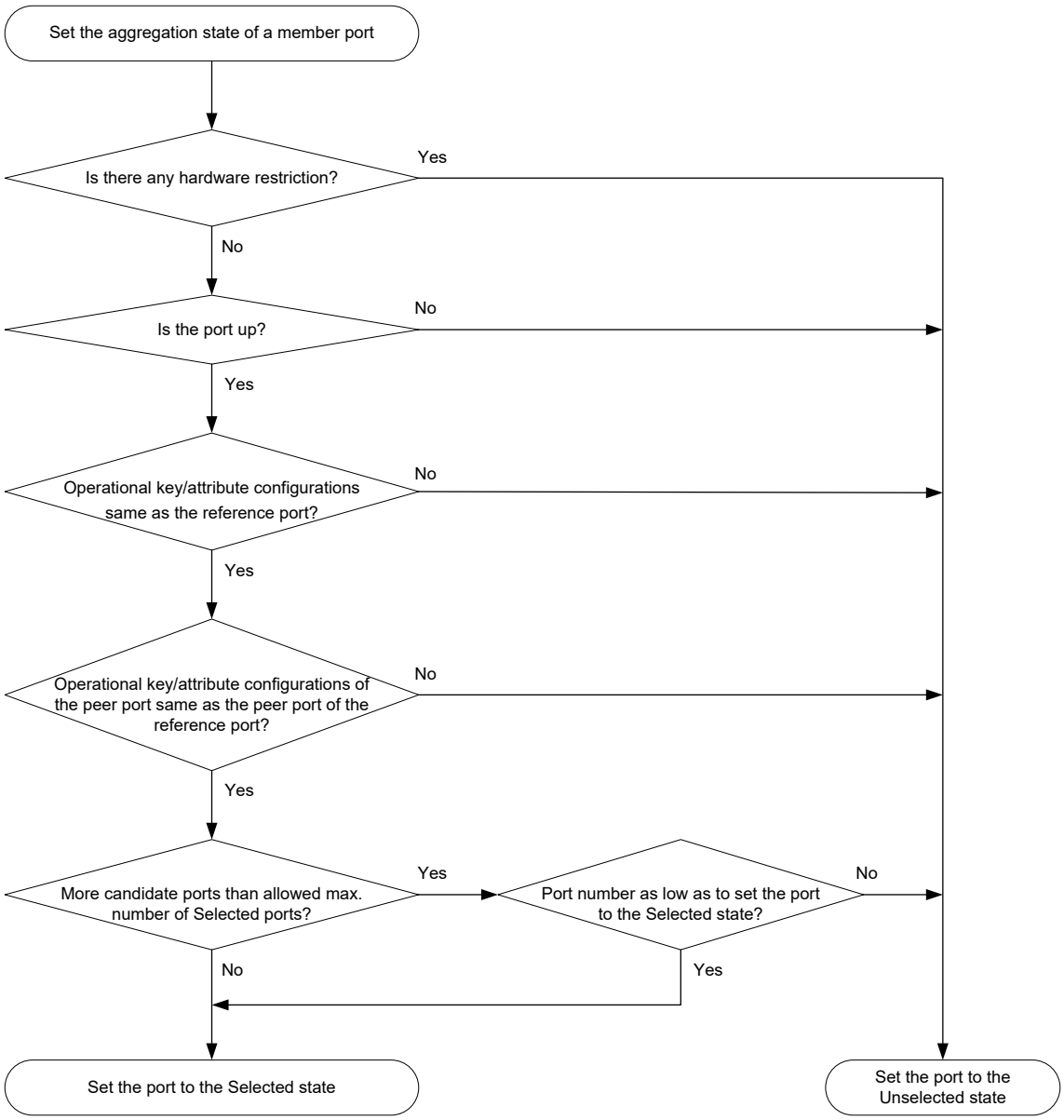


図 6-3 ダイナミックアグリゲーショングループのアグリゲーションステートの設定

高いシステム ID を持つシステムが、リモートシステムのステート状態を認識している間、対向先のポートと同じようにローカルメンバポートのアグリゲーションステートを設定します。

ダイナミックモードでアグリゲートインタフェースを設定するとき、以下のガイドラインに従ってください。

- ダイナミックリンクアグリゲーショングループは、Selected ポートとして全 2 重のみ選択します。
- 安定的なアグリゲーションステートやサービスを中断させないため、メンバポートのオペレーショナルキーや属性コンフィグレーションを変更しないでください。
- Selected ポートが制限に達した後、現在のメンバポートよりも適したポートである場合、ダイナミックアグリゲーショングループに追加されたポートは、Selected ポートになります。

6.1.9 アグリゲーショングループの負荷分散

リンクアグリゲーショングループにおいて、トラフィックは、Selected メンバポートを通り、以下のモードにもとづいて負荷分散が行われます。

- **フローベース負荷分散** — 以下の基準またはその組み合わせによってトラフィックフローが分散され、同じリンクにある同一フローのパケットを転送します。
  - 入力ポート
  - 送信に元あるいは宛先 IP アドレス
  - 送信元あるいは宛先 MAC アドレス
  - 送信元あるいは宛先ポート番号
- **パケットベース負荷分散** — 自動的にパケットタイプ（例 レイヤ 2、IPv4、IPv6）のリンクアグリゲーション負荷分散を選択します。

6.2 リンクアグリゲーション設定作業リスト

作業リスト
（必須設定項目）アグリゲーショングループの設定
（オプション設定項目）アグリゲートインタフェースの設定 • アグリゲートインタフェースの説明の設定 • アグリゲーショングループのSelectedポートの最小と最大数の設定 • アグリゲートインタフェースのシャットダウン
（オプション設定項目）グローバルでのリンクアグリゲーションのロードシェアリングモードの設定
（オプション設定項目）local-firstロードシェアリングモードの有効化

6.3 アグリゲーショングループの設定

この章ではアグリゲーショングループの設定方法について説明します。

6.3.1 設定の制限とガイドライン

I. アグリゲーションメンバインタフェースの制限

インタフェースで表 6-4に示す機能が設定されている場合、アグリゲーショングループにインタフェースを割り当てることができません。

表 6-4 アグリゲーションメンバインタフェースで設定できない機能

インタフェースの機能	参照
MACアドレス認証	オペレーションマニュアルのセクション9 *セキュリティ* “*MACアドレス認証*”を参照してください。

インタフェースの機能	参照
ポートセキュリティ	オペレーションマニュアルのセクション9 *セキュリティ“ポートセキュリティ”*を参照してください。
802.1X	オペレーションマニュアルのセクション9 *セキュリティ“802.1X”*を参照してください。

- ポートミラーリングのリフレクタポートでとして使用されているポートはアグリゲーショングループに割り当てることはできません。リフレクタポートの詳細は、オペレーションマニュアルのセクション 11 *システム管理"ポートミラーリング"*を参照してください。

II. 設定の整合性の要件

- アグリゲーションリンクのエンド間に同じアグリゲーションモードを設定する必要があります。
- スタティックアグリゲーションを正常に動作させるには、各アグリゲーションリンクポートの両端に同じアグリゲーションステートを設定する必要があります。
- ダイナミックアグリゲーションを正常に動作させるには、装置と対向装置でポートがアグリゲートされていることを確認してください。2 つのエンド間で、各メンバポートのアグリゲーションステートを自動的に処理することができます。

III. その他

アグリゲートインタフェースを削除する場合、アグリゲーショングループを削除し、アグリゲーショングループからすべてのメンバポートを削除してください。

6.3.2 アグリゲーショングループの設定

I. スタティックアグリゲーショングループの設定

以下にスタティックアグリゲーショングループの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. アグリゲートインタフェースを作成し、aggregate interface view に移行する	**interface bridge-aggregation** *interface-number*	アグリゲートインタフェースを作成すると、スタティックアグリゲーショングループ番号が、自動的に同一番号で作成されます。
3. system view へ戻る	**quit**	ー

操作	コマンド	補足
4. 指定されたアグリゲーショングループにインタフェースを割り当てる	1. Ethernet interface view に移行する： **interface** *interface-type interface-number* 2. 指定されたアグリゲーショングループにインタフェースを割り当てる： **port link-aggregation group** *group-id*	アグリゲーショングループに複数のインタフェースを割り当てる場合、このステップを繰り返してください。
5. （オプション設定項目）ポート LACP プライオリティを設定する	**link-aggregation port-priority** *priority*	デフォルト：32768

II. ダイナミックアグリゲーショングループの設定

以下にダイナミックアグリゲーショングループの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. システム LACP プライオリティを設定する	**lacp system-priority** *priority*	デフォルト：32768 システムLACPプライオリティの値を変えるとポートの状態（selected/unselected）が変わる可能性があります。
3. アグリゲートインタフェースを作成し、aggregate interface view に移行する	**interface bridge-aggregation** *interface-number*	アグリゲートインタフェースを作成すると、スタティックアグリゲーショングループ番号は、自動的に同一番号で作成されます。
4. ダイナミックアグリゲーションモードで動作するように設定する	**link-aggregation mode dynamic**	デフォルト: スタティックアグリゲーションモード
5. system view へ戻る	**quit**	ー
6. 指定されたアグリゲーショングループにインタフェースを割り当てる	1. Ethernet interface view に移行する： **interface** *interface-type interface-number* 2. 指定されたアグリゲーショングループにインタフェースを割り当てる： **port link-aggregation group** *group-id*	アグリゲーショングループに複数のインタフェースを割り当てる場合、このステップを繰り返してください。
7. ポート LACP プライオリティを設定する	**link-aggregation port-priority** *priority*	デフォルト：32768
8. short LACP タイムアウト間隔（3秒）をインタフェースに設定する	**lacp period short**	デフォルト：90秒 ピアはLACPDUをロング間隔で送信します。

6.4 アグリゲートインタフェースの設定

インタフェースで実行できる設定のほとんどは、アグリゲートインタフェースでも実行できます。

6.4.1 アグリゲートインタフェースの説明の設定

インタフェースの目的などを記載するように、管理者用にアグリゲートインタフェースの説明を記載することができます。

以下にアグリゲートインタフェースの説明の設定する方法を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. aggregate interface view に移行する	**interface bridge-aggregation** *interface-number*	―
3. アグリゲートインタフェースの説明を設定する	**description** *text*	デフォルト：*interface-name* **Interface**

6.4.2 アグリゲーショングループの Selected ポートの最小と最大数の設定

重要：
スタティックアグリゲーショングループに Selected ポートの最小値と最大値を設定した場合、正しい接続を保証するために、対向先のアグリゲーショングループに同じ設定をしてください。

アグリゲートリンクの帯域幅は、Selected メンバポートを増やすことで増加させることができます。アグリゲートリンクの Selected ポートが不足することによる輻輳を防ぐため、アグリゲートインタフェースの Selected メンバポートの最小数を設定できます。

この最小数のしきい値はアグリゲーションメンバポートとアグリゲートインタフェースの両方の状態に影響します。

- 適切なメンバポートが最小数を下回ったとき、以下の処理が行われます。
  - すべてのメンバポートが Unselected ポートに変更します。
  - アグリゲートインタフェースのリンクがダウンします。
- Selected ポートに適切なメンバポートの数が最小数以上になったとき、以下の処理が行われます。
  - 適切なメンバポートが Selected ポートに変更します。
  - アグリゲートインタフェースのリンクがアップします。

アグリゲートグループの Selected ポートの最大数は、設定された最大数あるいはハードウェア性能のいずれか小さいほうで制限されます。

以下の処理を行うことで 2 つのポート間でバックアップを設定することができます。

- アグリゲートグループに 2 つのポートを割り当てます。
- アグリゲートグループの Selected ポートの最大数を 1 に設定します。

このように設定すると、1 つのメンバポートが Selected ポートになります。もう一方のメンバポートが Unselected ポートとなり、バックアップポートとして動作します。

以下に Selected ポートの最小と最大数の設定方法を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. aggregate interface view に移行する	**interface bridge-aggregation** *interface-number*	―
3. アグリゲーショングループの Selected ポートの最小数を設定する	**link-aggregation selected-port minimum** *number*	デフォルト：設定なし
4. アグリゲーショングループの Selected ポートの最大数を設定する	**link-aggregation selected-port maximum** *number*	デフォルト：8

6.4.3 アグリゲートインタフェースのシャットダウン

アグリゲートインタフェースをシャットダウンあるいはアップすると、対応するアグリゲーショングループのステートとリンク状態に以下のような影響があります。

- アグリゲートインタフェースがシャットダウンしたとき、アグリゲーショングループのすべての Selected ポートは Unselected になります。
- アグリゲートインタフェースをアップさせると、対応するアグリゲーショングループのポートの Selected ステートを再計算します。

以下にアグリゲートインタフェースをシャットダウンする方法を示します。

操作	コマンド
1. system view に移行する	**system-view**
2. aggregate interface view に移行する	**interface bridge-aggregation** *interface-number*
3. アグリゲートインタフェースをシャットダウンする	**shutdown**

6.5 グローバルでのリンクアグリゲーションのロードシェアリングモードの設定

リンクアグリゲーションに負荷分散を設定すると、等しいコストのルートに不均衡な方法で共有のトラフィックを負荷させる可能性があります。

ロードシェアリングはグローバルでのみ設定することができます。グローバルでのリンクアグリゲーションモードの設定はすべてのアグリゲーショングループに適用します。

以下にグローバルでのリンクアグリゲーションモードの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. グローバルでのロードシェアリングモードを設定する	**link-aggregation global load-sharing mode** { **destination-ip** | **destination-mac** | **destination-port** | **ingress-port** | **source-ip** | **source-mac** | **source-port** }*	デフォルト: システムはパケットタイプに従い自動でロードシェアリングモードを選択します。

6.6 local-firstロードシェアリングモードの有効化

装置で、メンバポートを越えて優先的にトラフィックを配信するため、複数装置のリンクアグリゲーションで local-first ロードシェアリングを行います。

IRF スタックユニットで異なるメンバデバイスのポートを集約するとき、図 6-4に示すように IRF スタックのトラフィックを軽減するため、local-first ロードシェアリングを使用することができます。IRF スタックの詳細は、オペレーションマニュアルのセクション 2 *IRF スタック"IRF スタックの設定"*を参照してください。

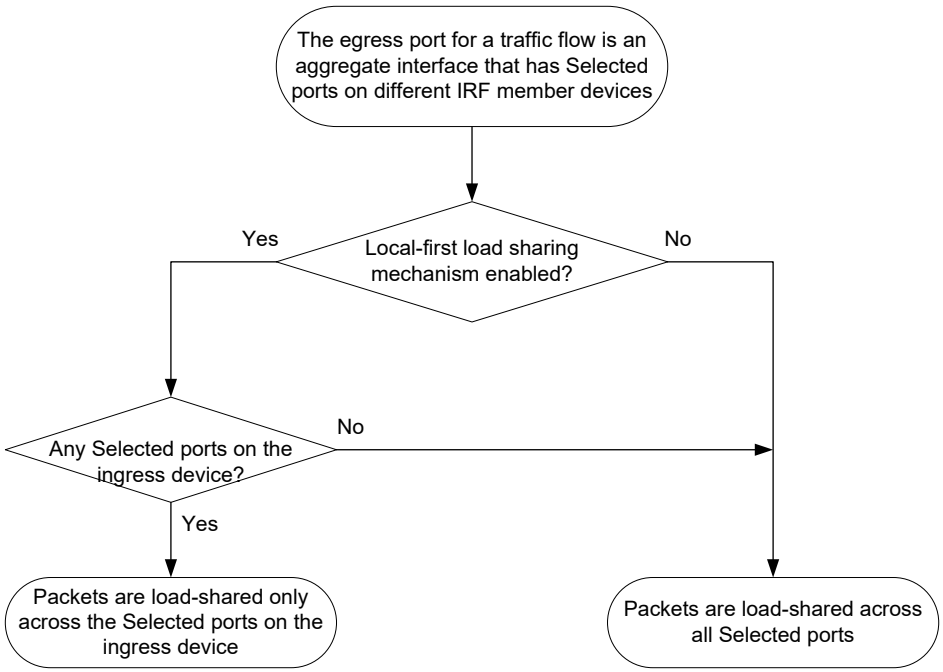


図 6-4 IRF スタックユニットの複数装置での local-firstロードシェアリング

以下にリンクアグリゲーションの local-first ロードシェアリングを有効にする設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. local-first ロードシェアリングを有効にする.	**link-aggregation load-sharing mode local-first**	デフォルト：有効

6.7 リンクアグリゲーションの表示と維持

すべての view で **display** コマンドを実行し、user view で **reset** コマンドを実行できます。

操作	コマンド
1つ以上のアグリゲーションインタフェースを表示する	**display interface** [**bridge-aggregation** [*interface-number*]] [**brief** [**description** | **down**]]
ローカルシステムIDを表示する	**display lacp system-id**
グローバルあるいはグループのロードシェアリングモードを表示する	**display link-aggregation load-sharing mode** [**interface** [**bridge-aggregation** *interface-number*]]
アグリゲーションメンバポートのリンクアグリゲーションの詳細情報を表示する	**display link-aggregation member-port** [*interface-list*]
すべてのアグリゲーショングループの概要を表示する	**display link-aggregation summary**
アグリゲーショングループの詳細情報を表示する	**display link-aggregation verbose** [**bridge-aggregation** [*interface-number*]]
ポートのLACP統計情報をクリアする	**reset lacp statistics** [**interface** *interface-list*]
アグリゲートインタフェース統計情報を削除する	**reset counters interface** [**bridge-aggregation** [*interface-number*]]

6.8 リンクアグリゲーションの設定例

6.8.1 スタティックアグリゲーション設定例

I. ネットワーク要件

図 6-5に示すように以下の要件を設定します。

- Device A と Device B の両方で、スタティックアグリゲーショングループを設定します。
- 片端で VLAN10 を有効にし、VLAN10 でアグリゲートリンクの対向先と通信します。
- 片端で VLAN20 を有効にし、VLAN20 でアグリゲートリンクの対向先と通信します。

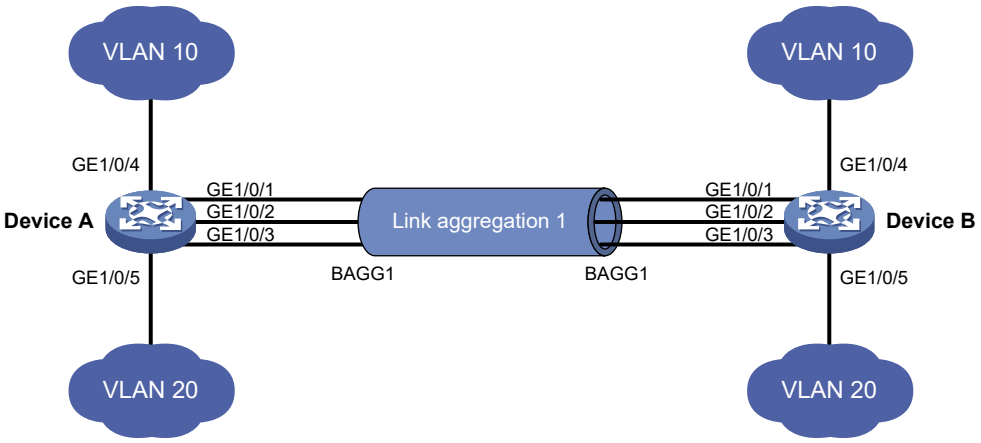


図 6-5 ネットワーク図

II. 設定手順

1)　Device A を設定します。

VLAN 10 を作成し、GigabitEthernet 1/0/4 に割り当てます。

```
<DeviceA> system-view
[DeviceA] vlan 10
[DeviceA-vlan10] port gigabitethernet 1/0/4
[DeviceA-vlan10] quit
```

VLAN 20 を作成し、GigabitEthernet 1/0/5 に割り当てます。

```
[DeviceA] vlan 20
[DeviceA-vlan20] port gigabitethernet 1/0/5
[DeviceA-vlan20] quit
```

アグリゲートインタフェース Bridge-Aggregation 1 を作成します。

```
[DeviceA] interface bridge-aggregation 1
[DeviceA-Bridge-Aggregation1] quit
```

GigabitEthernet 1/0/1～GigabitEthernet 1/0/3 にリングアグリゲーショングループ 1 を割り当てます。

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-aggregation group 1
[DeviceA-GigabitEthernet1/0/1] quit
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port link-aggregation group 1
[DeviceA-GigabitEthernet1/0/2] quit
[DeviceA] interface gigabitethernet 1/0/3
```

```
[DeviceA-GigabitEthernet1/0/3] port link-aggregation group 1
[DeviceA-GigabitEthernet1/0/3] quit
```

アグリゲートインタフェース Bridge-Aggregation 1 をトランクポートとして作成し、VLAN10、VLAN20 を割り当てます。

```
[DeviceA] interface bridge-aggregation 1
[DeviceA-Bridge-Aggregation1] port link-type trunk
[DeviceA-Bridge-Aggregation1] port trunk permit vlan 10 20
[DeviceA-Bridge-Aggregation1] quit
```

2) Device A の設定と同様に Device B を設定します。（詳細は省略します。）

III. 設定の確認

Device A ですべてのアグリゲーショングループの詳細情報を表示します。

```
[DeviceA] display link-aggregation verbose
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected, I -- Individual
Port: A -- Auto port, M -- Management port, R -- Reference port
Flags:  A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
        D -- Synchronization, E -- Collecting, F -- Distributing,
        G -- Defaulted, H -- Expired

Aggregate Interface: Bridge-Aggregation1
Aggregation Mode: Static
Loadsharing Type: NonS
Management VLANs: None
  Port             Status  Priority Oper-Key
  GE1/0/1          S       32768    1
  GE1/0/2          S       32768    1
  GE1/0/3          S       32768    1
```

出力では、リンクアグリゲーション 1 がスタティックアグリゲーショングループで、3 つの Selected ポートがあることを示しています。

6.8.2 ダイナミックアグリゲーション設定例

I. ネットワーク要件

図 6-6に示すように以下の要件を設定します。

- Device A と Device B の両方で、ダイナミックアグリゲーショングループを設定します。
- 片端で VLAN10 を有効にし、VLAN10 でアグリゲートリンクの対向先と通信します。
- 片端で VLAN20 を有効にし、VLAN20 でアグリゲートリンクの対向先と通信します。

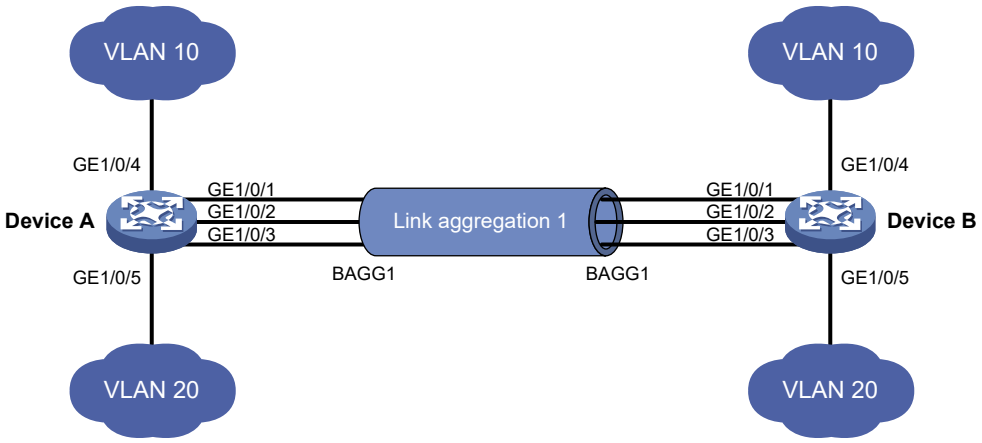


図 6-6 ネットワーク図

II. 設定手順

1)　Device A を設定します。

VLAN 10 を作成し、GigabitEthernet 1/0/4 に割り当てます。

```
<DeviceA> system-view
[DeviceA] vlan 10
[DeviceA-vlan10] port gigabitethernet 1/0/4
[DeviceA-vlan10] quit
```

VLAN 20 を作成し、GigabitEthernet 1/0/5 に割り当てます。

```
[DeviceA] vlan 20
[DeviceA-vlan20] port gigabitethernet 1/0/5
[DeviceA-vlan20] quit
```

アグリゲートインタフェース Bridge-Aggregation 1 を作成し、ダイナミックリンクアグリゲーションモードを設定します。

```
[DeviceA] interface bridge-aggregation 1
[DeviceA-Bridge-Aggregation1] link-aggregation mode dynamic
[DeviceA-Bridge-Aggregation1] quit
```

GigabitEthernet 1/0/1～GigabitEthernet 1/0/3 にリングアグリゲーショングループ 1 を割り当てます。

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-aggregation group 1
[DeviceA-GigabitEthernet1/0/1] quit
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port link-aggregation group 1
```

```
[DeviceA-GigabitEthernet1/0/2] quit
[DeviceA] interface gigabitethernet 1/0/3
[DeviceA-GigabitEthernet1/0/3] port link-aggregation group 1
[DeviceA-GigabitEthernet1/0/3] quit
```

アグリゲートインタフェース Bridge-Aggregation 1 をトランクポートとして作成し、VLAN10、VLAN20 を割り当てます。

```
[DeviceA] interface bridge-aggregation 1
[DeviceA-Bridge-Aggregation1] port link-type trunk
[DeviceA-Bridge-Aggregation1] port trunk permit vlan 10 20
[DeviceA-Bridge-Aggregation1] quit
```

2)　Device A の設定と同様に Device B を設定します。（詳細は省略します。）

III. 設定の確認

Device A ですべてのアグリゲーショングループの詳細情報を表示します。

```
[DeviceA] display link-aggregation verbose
           Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected, I -- Individual
Port: A -- Auto port, M -- Management port, R -- Reference port
Flags:  A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
        D -- Synchronization, E -- Collecting, F -- Distributing,
        G -- Defaulted, H -- Expired

Aggregate Interface: Bridge-Aggregation1
Aggregation Mode: Dynamic
Loadsharing Type: NonS
Management VLANs: None
System ID: 0x8000, 000f-e267-6c6a
Local:
  Port                Status   Priority Index    Oper-Key               Flag
  GE1/0/1(R)          S        32768    11       1                      {ACDEF}
  GE1/0/2             S        32768    12       1                      {ACDEF}
  GE1/0/3             S        32768    13       1                      {ACDEF}
Remote:
  Actor               Priority Index    Oper-Key SystemID               Flag
  GE1/0/1             32768    81       1        0x8000, 000f-e267-57ad {ACDEF}
  GE1/0/2             32768    82       1        0x8000, 000f-e267-57ad {ACDEF}
  GE1/0/3             32768    83       1        0x8000, 000f-e267-57ad {ACDEF}
```

出力では、リンクアグリゲーション 1 がダイナミックアグリゲーショングループで、3 つの Selected ポートがあることを示しています。

目次

このセクションのページは **3-x-x** です。

7 章 Port Isolation..... 7-1
7.1 アイソレーショングループへのポートの追加..... 7-1
7.2 ポートアイソレーションの表示と維持..... 7-2
7.3 ポートアイソレーションの設定例 7-2
7.3.1 ネットワーク要件..... 7-2
7.3.2 設定手順 7-3
7.3.3 設定の確認..... 7-3

7章 Port Isolation

🕮 **メモ：**
QX-S5100G シリーズは、ポートアイソレーションと MLD スヌーピングを同時に使用することができません。

ポートアイソレーション(Port Isolation)機能はデータのプライバシーやセキュリティのために、VLAN を使用することなくレイヤ 2 トラフィックを隔離します。

アイソレーショングループのポートは互いに通信することができませんが、外部のアイソレーショングループのポートと通信することができます。

7.1 アイソレーショングループへのポートの追加

装置は手動で設定することで複数のアイソレーショングループをサポートしています。アイソレーショングループに追加されるポートの数に制限はありません。

以下にアイソレーショングループにポートを割り当てる設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. アイソレーショングループを作成する	**port-isolate group** *group-id*	デフォルト：設定なし
3. interface view に移行する	● Layer 2 Ethernet interface view に移行する： **interface** *interface-type interface-number* ● aggregate interface view に移行する： **interface bridge-aggregation** *interface-number*	● Layer 2 Ethernet interface view に設定すると設定されたインタフェースで適用されます。 ● aggregate interface view に設定するとアグリゲートインタフェースとアグリゲーションメンバポートに適用されます。アグリゲートインタフェースの設定を適用できない場合、アイソレーショングループにメンバポートが割り当てられません。アグリゲーションメンバポートで故障が発生すると、装置はポートをスキップし、他のアイソレーショングループにメンバポートを割り当てることができます。

操作	コマンド	補足
4. アイソレーショングループにポートを追加する	**port-isolate enable group** *group-id*	デフォルト：設定なし ポートは1つのアイソレーショングループに割り当てることができます。**port-isolate enable group**コマンドを複数行った場合、最後に行った設定が適用されます。

7.2 ポートアイソレーションの表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
アイソレーショングループ情報を表示する	**display port-isolate group** [*group-id*]

7.3 ポートアイソレーションの設定例

7.3.1 ネットワーク要件

図 7-1に示すように以下の要件を設定します。

- Host A は GigabitEthernet 1/0/1 に接続されています。Host B は GigabitEthernet 1/0/2 に接続されています。Host C は GigabitEthernet 1/0/3 に接続されています。
- Device は GigabitEthernet 1/0/4 を通してインタネットにアクセスできます。

各 Host はインタネットにアクセスし、レイヤ 2で互いに通信できないように設定します。

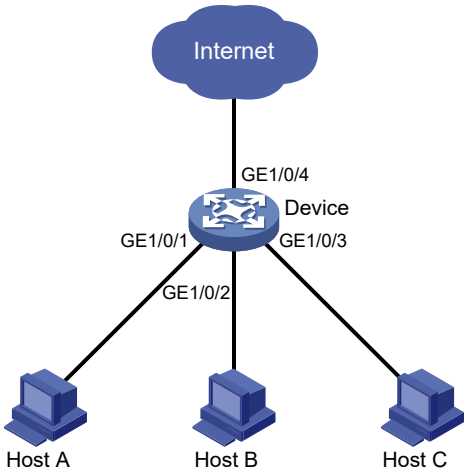


図 7-1 ネットワーク図

7.3.2 設定手順

アイソレーショングループ 1 を作成します。

```
<Device> system-view
[Device] port-isolate group 1
```

GigabitEthernet 1/0/1、GigabitEthernet 1/0/2、GigabitEthernet 1/0/3 をアイソレーショングループ 1 に割り当てます。

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] port-isolate enable group 1
[Device-GigabitEthernet1/0/1] quit
[Device] interface gigabitethernet 1/0/2
[Device-GigabitEthernet1/0/2] port-isolate enable group 1
[Device-GigabitEthernet1/0/2] quit
[Device] interface gigabitethernet 1/0/3
[Device-GigabitEthernet1/0/3] port-isolate enable group 1
[Device-GigabitEthernet1/0/3] quit
```

7.3.3 設定の確認

アイソレーショングループ 1 の情報を表示します。

```
[Device] display port-isolate group 1
 Port isolation group information:
 Group ID: 1
 Group members:
   GigabitEthernet1/0/1     GigabitEthernet1/0/2     GigabitEthernet1/0/3
```

出力は、GigabitEthernet 1/0/1、GigabitEthernet 1/0/2、GigabitEthernet 1/0/3 がアイソレーショングループ 1 に割り当てられていることを示します。その結果、Host A、Host B、Host C はレイヤ 2 で互いに隔離されています。

目次

このセクションのページは**3-x-x** です。

8章 STP 8-1
8.1 STP 8-1
8.1.1 STPのプロトコルフレーム 8-1
8.1.2 STPの基本概念 8-3
8.1.3 STPアルゴリズムの計算プロセス 8-5
8.2 RSTP 8-12
8.2.1 RSTPの基本概念 8-13
8.2.2 RSTPの動作 8-13
8.2.3 RSTPのBPDU処理 8-14
8.3 PVST 8-14
8.3.1 PVSTのプロトコルフレーム 8-15
8.3.2 PVSTの基本概念 8-15
8.3.3 PVSTの動作 8-15
8.4 MSTP 8-16
8.4.1 MSTPの特徴 8-16
8.4.2 MSTPのプロトコルフレーム 8-16
8.4.3 MSTPの基本概念 8-18
8.4.4 MSTPの動作 8-22
8.4.5 装置でのMSTPの実行 8-23
8.4.6 高速収束メカニズム 8-23
8.5 プロトコルと規格 8-26
8.6 スパニングツリー設定作業リスト 8-26
8.6.1 STP設定作業リスト 8-27
8.6.2 RSTP設定作業リスト 8-28
8.6.3 PVST設定作業リスト 8-29
8.6.4 MSTP設定作業リスト 8-30
8.7 動作モードの設定 8-30
8.8 MST regionの設定 8-31
8.9 RootブリッジとSecondary Rootブリッジの設定 8-32
8.9.1 Rootブリッジの設定 8-33
8.9.2 Secondary Rootブリッジの設定 8-33
8.10 ブリッジプライオリティの設定 8-33
8.11 MST regionの最大ホップ数の設定 8-34
8.12 ネットワークダイアメータの設定 8-34
8.13 スパニングツリータイマの設定 8-35
8.14 タイムアウトファクタの設定 8-36
8.15 BPDU最大送出レートの設定 8-37
8.16 Edgeポートの設定 8-37
8.17 ポートパスコストの設定 8-38
8.17.1 デフォルトパスコストの計算時の基準指定 8-38
8.17.2 ポートのパスコストの設定 8-40
8.17.3 設定例 8-40
8.18 ポートプライオリティの設定 8-41
8.19 Point-to-Pointリンクの設定 8-41
8.20 MSTPパケットのフォーマット設定 8-42

8.21 ポート遷移状態情報の出力の有効化 8-42
8.22 スパニングツリー機能の有効化 8-43
8.22.1 STP/RSTP/MSTPモードでのスパニングツリー機能の有効化 8-43
8.22.2 PVSTモードでのスパニングツリー機能の有効化 8-43
8.23 mCheck機能の設定 8-44
8.23.1 制限とガイドライン 8-44
8.23.2 グローバルでのmCheckの設定手順 8-44
8.23.3 interface viewでのmCheckの実行 8-44
8.24 矛盾したPVID 保護の無効化 8-45
8.25 Digest Snoopingの設定 8-45
8.25.1 Digest Snooping設定例 8-47
8.26 No Agreement Checkの設定 8-48
8.26.1 No Agreement Check設定例 8-50
8.27 TC snoopingの設定 8-50
8.28 保護機能の設定 8-51
8.28.1 BPDUガードの有効化 8-52
8.28.2 Rootガードの有効化 8-53
8.28.3 Loopガードの有効化 8-53
8.28.4 ポート役割の制限機能 8-54
8.28.5 TC-BPDUガードの有効化 8-55
8.28.6 BPDUドロップ機能の有効化 8-55
8.28.7 PVST BPDUガード機能の有効化 8-56
8.28.8 disputeガードの無効化 8-56
8.29 TC BPDUの検出、受信イベントのログ作成の有効化 8-58
8.30 BPDUガードによりシャットダウンしたエッジポートの再アクティブ化無効 8-58
8.31 新規ルートブリッジの選択、トポロジ変更イベントによるSNMP notificationの有効化 8-59
8.32 スパニングツリーの表示と維持 8-60
8.33 スパニングツリー設定例 8-60
8.33.1 MSTP設定例 8-60
8.33.2 PVST設定例 8-65

8章 STP

スパニングツリーは、ループ検出時に物理的に通信しないインタフェースを設定することによりループを防止します。

STP は、狭義では、IEEE802.1d STP を意味しており、広義では IEEE802.1d STP と拡張されたスパニングツリープロトコル（RSTP（Rapid Spanning Tree Protocol）、MSTP（Multiple Spanning Tree Protocol）、PVST（Per-VLAN Spanning Tree）など）を含めたものを意味します。

8.1 STP

STP（Spanning Tree Protocol）は、IEEE の 802.1d で規定されている、LAN（local area network）の円環上（ループ状）に形成されたレイヤ 2 プロトコルにおいてデータトラフィックが永続的に流れ続けることを防止するプロトコルです。

STP が動作している装置は、ネットワークでループを検出します。ほかの装置と情報を交換し、ループがないツリー構成にループの構成を設定させ、特定のポートをブロックすることでループを防ぎます。

8.1.1 STP のプロトコルフレーム

スパニングツリープロトコルでは、リンクレイヤパケットの BPDU（Bridge Protocol Data Units）を使用して、情報交換、状態の維持管理を行います。この章ではスパニングツリーのすべてのタイプを代表して BPDU を使用します。

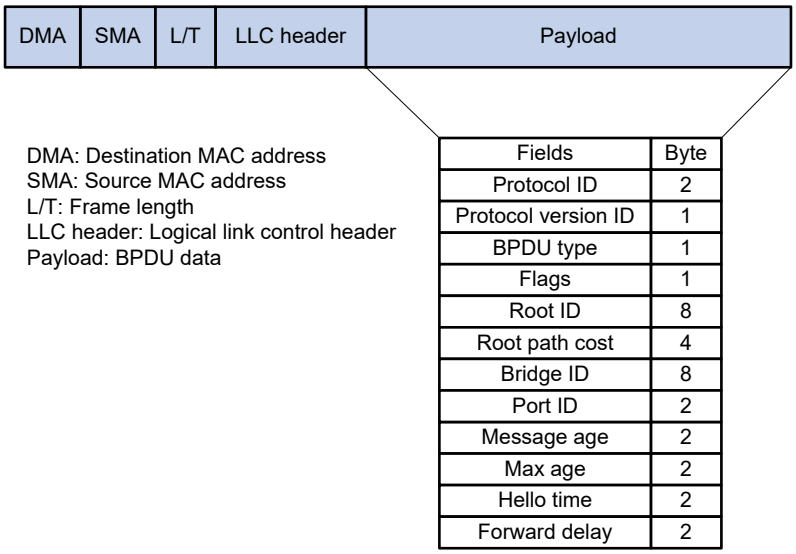
STP が有効なネットワークの装置は BPDU を交換してスパニングツリーを確立します。BPDU はスパニングツリーの計算を行うために十分な情報を含みます。

STP では、以下の 2 種類の BPDU を使用します。

- **Configuration BPDU** — スパニングツリーを構成し、ツリートポロジを維持するために使います。
- **TCN（Topology change notification） BPDU** — ネットワークトポロジの変更を通知するために使います。

I. Configuration BPDU

装置は Root ブリッジを選択し Root ポートを決定するために、ネットワーク内の装置間で Configuration BPDU の交換を行います。図 8-1に Configuration BPDU のフォーマットを示します。



Fields	Byte
Protocol ID	2
Protocol version ID	1
BPDU type	1
Flags	1
Root ID	8
Root path cost	4
Bridge ID	8
Port ID	2
Message age	2
Max age	2
Hello time	2
Forward delay	2

図 8-1 Configuration BPDU のフォーマット

Configuration BPDU には、ネットワークトポロジを構築するための以下のデータが書き込まれています。

- **Protocol ID**– IEEE802.1d を示します。0x0000 で固定です。
- **Protocol version ID**（プロトコルバージョン ID）– スパニングツリーのバージョン ID です。STP のプロトコルバージョン ID は 0x00 です。
- **BPDU type**– BPDU のタイプです。Configuration BPDU の値は 0x00 です。
- **Flags**– BPDU の目的を示します。8 ビットフィールドです。最下位ビットは TC（Topology Change）フラグです。最上位ビットは TCA（Topology Change Acknowledge）フラグです。ほかのビットは予約用です。
- **Root ID**– Root ブリッジの ID です。Root ブリッジのプライオリティと MAC アドレスで構成されます。
- **Root path cost**（ルートパスコスト）– Root ブリッジまでの最短ルートのコストです。
- **Bridge ID**– Designated ブリッジの ID です。Designated ブリッジのプライオリティと MAC アドレスで構成されます。
- **Port ID**– Designated ブリッジのポート ID です。Designated ブリッジのプライオリティとグローバルポート番号で構成されます。
- **Message age**– ネットワーク内で転送された Configuration BPDU の経過時間です。
- **Max age**– 装置に記録された Configuration BPDU の有効時間です。
- **Hello 時間**– Configuration BPDU の転送間隔です。
- **Forward delay**– 装置の状態が遷移するときの遅延時間です。

装置はスパニングツリーの計算を行うため、Root ブリッジ ID（Root ID）、Root パスコスト、Designated ブリッジ ID（Bridge ID）、Designated ポート ID（Port ID）、Message age、Max age、Hello 時間（Hello time）、Forward delay を使用します。

II. TCN BPDU

TCN BPDU には、ネットワークトポロジの変更を通知します。図 8-2に TCN BPDU のフォーマットを示します。

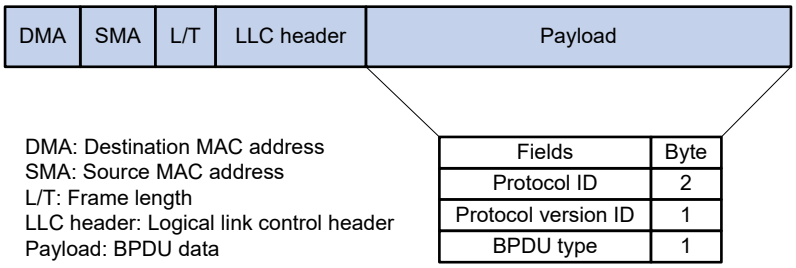


図 8-2 TCN BPDU のフォーマット

TCN BPDU には以下のデータが書き込まれています。

- **Protocol ID**– IEEE802.1d を示します。0x0000 で固定です。
- **Protocol version ID**– スパニングツリーの Version ID です。STP のプロトコルバージョン ID は 0x00 です。
- **BPDU type**– BPDU のタイプです。TCN BPDU の値は 0x80 です。

ブリッジで以下のイベントの 1 つが発生したとき、Root ブリッジ以外のブリッジが TCN BPDU を送信します。

- ポートが Forwarding 状態に遷移し、ブリッジに少なくとも 1 つの Designated ポートがあります。
- ポートが Forwarding 状態あるいは Learning 状態から、Blocking 状態に遷移します。

Root ブリッジ以外のブリッジはネットワークトポロジの変更を 1 回通知するため、TCN BPDU を使用します。そして Root ブリッジは Configuration BPDU の TC フラグを設定し、ほかのブリッジに転送します。

8.1.2 STP の基本概念

I. Root ブリッジ

STP のツリーは、1 つの Root ブリッジと複数のほかのブリッジで構成されます。ほかのブリッジは“Leaf ノード”と呼ばれます。Root ブリッジはトポロジの変化に応じて変更することができます。

ネットワークの初期設定において、各装置は生成し、定期的に Root ブリッジとして Configuration BPDU を送信します。ネットワークの収束後、Root ブリッジのみが定期的に Configuration BPDU を送信します。ほかの装置は、BPDU を転送するのみとなります。

II. Root ポート

Root ブリッジ以外の装置において、Root ブリッジへのパスコストがもっとも低い 1 つのポートが Root ポートとなります。Root ポートは、Root ブリッジの装置と通信を行うポートになります。なお、Root ブリッジの装置には、Root ポートはありません。

III. Designated ブリッジと Designated ポート

分類	Designated ブリッジ	Designated ポート
装置	ローカル装置に直接、接続されている装置でローカルの装置にBPDUの転送を行います。	Designatedブリッジがこのポートにbpduを転送します。
LAN	LANセグメントにBPDUを転送します。	Designatedブリッジが、このLANセグメントにBPDUを転送します。

図 8-3に示すように、Device B と Device C は LAN に直接接続されています。

もし Device A がポート A1 を経由して Device B に BPDU を転送する場合、Designated ブリッジと Designated ポートは以下のようになります。

- Device B の Designated ブリッジは Device A です。
- Device B の Designated ポートは Device A のポート A1 です。

もし Device B が LAN に BPDU を転送する場合、Designated ブリッジと Designated ポートは以下のようになります。

- LAN の Designated ブリッジは Device B です。
- LAN の Designated ポートは Device B のポート B2 です。

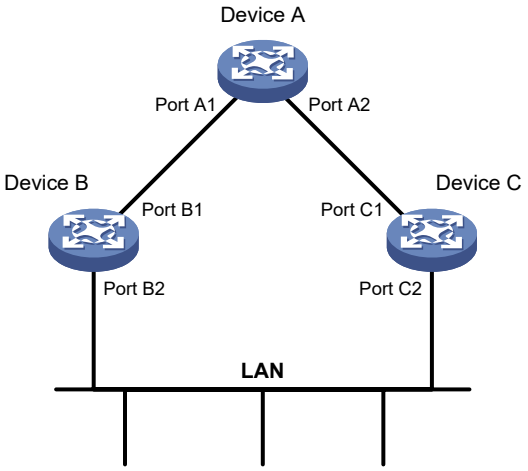


図 8-3 Designated ブリッジと Designated ポート

IV. ポート状態

STP のポート状態を表 8-1に示します。

表 8-1 STP のポート状態

状態	BPDU の送受信	MAC アドレスの学習	データの転送
Disabled	No	No	No
Listening	Yes	No	No
Learning	Yes	Yes	No
Forwarding	Yes	Yes	Yes
Blocking	受信のみ	No	No

V. パスコスト

パスコストは、STP でリンクを選択するのに使用される値です。STP はリンク間のパスコストを比較し、もっともパスコストの小さいリンクを使ったトポロジを構成します。STP はループがないようにネットワークを構成させるため、冗長な STP のリンクをブロックします。

8.1.3 STP アルゴリズムの計算プロセス

スパニングツリーのアルゴリズムは以下の計算プロセスを使用しています。動作をわかりやすくするため、簡単な例をもとに説明します。

I. ネットワークの初期化

STP アルゴリズムは以下のプロセスを使用します。

1)　ネットワークの初期化

装置の初期化として、各ポートは以下の内容で BPDU を作成します。

- □　ポートを Designated ポートとします。
- □　装置自身を Root ブリッジとします。
- □　Root パスコストを 0 とします。
- □　Designated ブリッジ ID を自身の装置 ID とします。

2)　Root ブリッジの選択

最初にネットワーク上の STP が有効な各装置は、自身が Root ブリッジとして仮定し、Root ブリッジを自身の Device ID とします。BPDU の交換を行うことによって、装置は自身の Root ブリッジ ID と、Root ブリッジとなるもっとも小さい Root ブリッジ ID の装置を選択するため、Root ブリッジ ID を比較します。

3)　Root ブリッジでない Root ポートと Designated ポートを選択します。

操作	説明
1	Rootブリッジでない装置は、もっとも優先度の高いConfiguration BPDUを受信したポートをRootポートと認識します。表 8-2にConfiguration BPDUを選択する方法を記載します。
2	Configuration BPDUとRootポートのパスコストをもとにして、装置はほかのポートのDesignatedポートのConfiguration BPDUを計算します。 ● RootブリッジIDをRootポートで受信したConfiguration BPDUのRootブリッジIDに書き換えます。 ● RootポートコストをRootポートで受信するConfiguration BPDUのRootポートコストにRootポートのパスコストを加算した値に書き換えます。 ● DesignatedブリッジIDをその装置のブリッジIDに書き換えます。 ● DesignatedポートIDを出力ポートのIDに書き換えます。

操作	説明
3	書き換えたConfiguration BPDUとそのポートで受信するConfiguration BPDUを比較することで、そのポートの役割が決まります。 ● 書き換えたConfiguration BPDUの優先度が高い場合、装置は以下の処理を行います。 　• ポートはDesignatedポートと認識します。 　• ポートのConfiguration BPDUを計算したConfiguration BPDUに書き換えます。 　• Configuration BPDUを周期的に送信します。 ● そのポートで受信するConfiguration BPDUの優先度が高い場合、そのポートからConfiguration BPDUを送出することを止め、対向装置からのConfiguration BPDUの受信だけを行います。

ネットワークのトポロジが安定している場合、Root ポートと Designated ポートはユーザのトラフィックのみを転送します。ほかのブロックされたポートは BPDU の受信のみを行い、BPDU やトラフィックの転送を行いません。

表 8-2 もっとも優先度の高い Configuration BPDU の選出

操作	アクション
1	ポートでConfiguration BPDUを受信し、装置はポートによって作成されたConfiguration BPDUと受信したConfiguration BPDUの優先度を比較します。 ● もし受信したConfiguration BPDUの優先度が低い場合、装置は受信したConfiguration BPDUを廃棄し、ポートで作成されたConfiguration BPDUを保存します。 ● もし受信したConfiguration BPDUの優先度が高い場合、受信したConfiguration BPDUの内容にもとづいてポートで作成したConfiguration BPDUの内容を書き換えます。
2	装置はすべてのConfiguration BPDUを比較し、もっとも優先度の高いConfiguration BPDUを選出します。

以下に Configuration BPDU の比較順序を示します。

a) RootブリッジIDがもっとも小さいConfiguration BPDUの優先度がもっとも高くなります。

b) すべてのConfiguration BPDUのRootブリッジIDが同じ場合には、次にRootパスコストを比較します。Configuration BPDUのRootパスコストとその受信ポートのパスコストの加算値のもっとも小さいConfiguration BPDUの優先度が高くなります。たとえばConfiguration BPDUのRootパスコストと受信したポートのパスコストがSとします。もっとも小さいSのConfiguration BPDUがもっとも高い優先度となります。

c) すべてのConfiguration BPDUのRootブリッジIDとSが同じ場合、以下の領域を順に比較します。

- □ Designated ブリッジ ID
- □ Designated ポート ID
- □ 受信したポートの ID

Designated ブリッジ ID、Designated ポート ID あるいは受信したポートの ID の小さい Configuration BPDU が選択されます。

Root ブリッジのとき、ツリー構造のトポロジは、Root ポート、Designated ポートが選択されます。

II. STP アルゴリズム計算の例

図 8-4に STP アルゴリズムの計算例を示します。

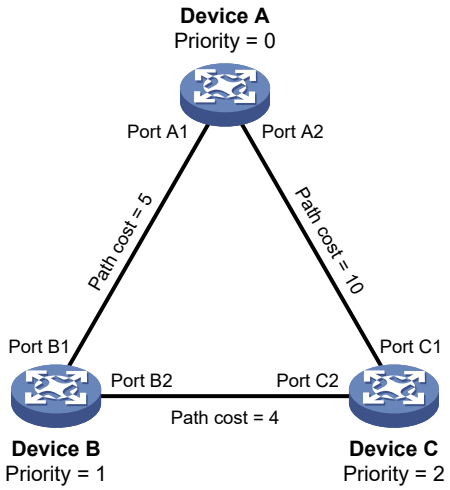


図 8-4 STP アルゴリズム

図 8-4に示すように、Device A、Device B、Device C の優先度の値は、それぞれ 0、1、2 で、3 つの装置間のリンクパスコストは、それぞれ 5、10、4 です。

1)　装置の初期状態

表 8-3に示すように各 Configuration BPDU は Root ブリッジ ID、Root パスコスト、Designated ブリッジ ID、Designated ポート ID を含みます。

表 8-3 各装置の初期状態

装置	ポート名	ポートの Configuration BPDU
Device A	ポートA1	{0, 0, 0, ポートA1}
	ポートA2	{0, 0, 0, ポートA2}
Device B	ポートB1	{1, 0, 1, ポートB1}
	ポートB2	{1, 0, 1, ポートB2}
Device C	ポートC1	{2, 0, 2, ポートC1}
	ポートC2	{2, 0, 2, ポートC2}

2)　各装置の Configuration BPDU を比較します。

表 8-4において、各 Configuration BPDU は Root ブリッジ ID、Root パスコスト、Designated ブリッジ ID、Designated ポート ID を含みます。

表 8-4 各装置の比較プロセスと結果

装置	比較プロセス	比較後のポートの Configuration BPDU
Device A	ポートA1は以下の操作をします。 1． Device B の Configuration BPDU {1,0,1,ポートB1}を受信します。 2． ローカルポートの Configuration BPDU{0,0,0, ポート A1}が設定を受信したメッセージより優位であることを出します。 3． 受信した Configuration BPDU を破棄します。 ポートA2は以下の操作をします。 1． Device C の Configuration BPDU {2,0,2, ポートC1}を受信します。 2． ローカルポートの Configuration BPDU {0,0,0, ポート A2}が受信した Configuration BPDU より優位であることをと検出します。 3． 受信した Configuration BPDU を破棄します。 Device Aは、Device Aの全ポートのConfiguration BPDUのRootブリッジおよびDesignatedブリッジがDevice Aであることを検出するとそれ自体をRootブリッジとみなします。この場合、Device Aは各ポートのConfiguration BPDUに対して何の変更も行わず、定期的にConfiguration BPDUの送信をはじめます。	• ポートA1：{0, 0, 0,ポートA1} • ポートA2：{0, 0, 0,ポートA2}
Device B	ポートB1は以下の操作をします。 1． Device A の Configuration BPDU {0,0,0, ポートA1}を受信します。 2． 受信した Configuration BPDU がローカルポートの Configuration BPDU {1, 0, 1,ポートB1}より優位であることを検出します。 3． ポート B1 の Configuration BPDU を更新します。 ポートB2は以下の操作をします。 1． Device C の Configuration BPDU {2,0,2, ポートC2}を受信します。 2． ローカルポートの Configuration BPDU {1,0,1, ポート B2}が受信した Configuration BPDU より優位であることを検出します。 3． 受信した Configuration BPDU を破棄します。	• ポートB1：{0, 0, 0, ポートA1} • ポートB2：{1, 0, 1, ポートB2}

装置	比較プロセス	比較後のポートの Configuration BPDU
	Device Bは以下の操作をします。 1． すべてのポートの Configuration BPDU を比較します。 2． ポート B1 の Configuration BPDU が最適な Configuration BPDU であると判断します。 3． ポート B1 を Root ポートとして使い、その Configuration BPDU は変更しません。 ポートB1のConfiguration BPDUおよびRootポートのパスコストにもとづき、ポートB2のConfiguration BPDUのDesignated {0,5,1, ポートB2}を計算します。Device Bは計算したConfiguration BPDU {0,5,1, ポートB2}とポートB2のConfiguration BPDUを比較します。計算したConfiguration BPDUが優位であればポートB2はDesignatedポートとなります。このポートのConfiguration BPDUは計算したConfiguration BPDUに置き換えられ、定期的に送信されます。	● Rootポート（ポートB1）: {0, 0, 0, ポートA1} ● Designatedポート（ポートB2）: {0, 5, 1, ポートB2}
Device C	ポートC1は以下の操作をします。 1． Device A の Configuration BPDU{0,0,0, ポート A2}を受信します。 2． 受信した Configuration BPDU がローカルポートの Configuration BPDU{2,0,2, ポート C1}より優位であることを検出します。 3． ポート C1 の Configuration BPDU を更新します。 ポートC2は以下の操作をします。 1． メッセージが更新される前に、Device B のポート B2 の Configuration BPDU{1,0,1, ポート B2}を受信します。 2． 受信した Configuration BPDU がローカルポートの Configuration BPDU{2,0,2, ポート C2}より優位であることを検出します。 3． ポート C2 の Configuration BPDU を更新します。	● ポートC1：{0, 0, 0, ポートA2} ● ポートC2：{1, 0, 1, ポートB2}
	Device Cは以下の操作をします。 1． すべてのポートの Configuration BPDU を比較します。 2． ポート C1 の Configuration BPDU が最適な Configuration BPDU であると判断します。 3． ポート C1 を Root ポートとして使い、その Configuration BPDU は変更しません。 ポートC1のConfiguration BPDUおよびRootポートのパスコストにもとづき、ポートC2のConfiguration BPDUのDesignated {0,10,2, ポートC2}を計算します。Device Cは計算したConfiguration BPDU {1,0,1, ポートB2}とポートC2のConfiguration BPDUを比較します。計算したConfiguration BPDUが優位であればポートC2はDesignatedポートとなります。このポートのConfiguration BPDUは計算したConfiguration BPDUに置き換えられます。	● Rootポート（ポートC1）: {0, 0, 0, ポートA2} ● Designatedポート（ポートC2）: {0, 10, 2, ポートC2}

装置	比較プロセス	比較後のポートの Configuration BPDU
	ポートC2は以下の操作をします。 1． 更新された Device B の Configuration BPDU{0,5,1, ポート B2}を受信します。 2． 受信した Configuration BPDU がローカルポートの Configuration BPDU{0,10,2, ポート C2}より優位であることを検出します。 3． ポート C1 の Configuration BPDU を更新します。 ポートC1は以下の操作をします。 1． Device A から定期的に Configuration BPDU {0,0,0, ポート A2}を受信します。 2． ローカルポートの Configuration BPDU と同じであることを検出します。 3． Configuration BPDU を更新します。	● ポートC1：{0, 0, 0, ポート A2} ● ポートC2：{0, 5, 1, ポート B2}
	Device Cは、ポートC1のルートパスコスト（10）（受信したConfiguration BPDU（0）のルートパスコスト＋ポートC1のパスコスト（10））は、ポートC2のパスコスト（9）よりも大きいと判断し、ポートC2のBPDUが最適なConfiguration BPDUと判断します。ポートC2がルートポートとなり、そのメッセージは変更されません。 Configuration BPDUとルートポートのパスコストにもとづき、Device Cは以下の操作をします。 1． ポート C1 の Designated ポートの Configuration BPDU {0,9,2, ポート C1}を計算します。 2． それをポート C1 の Configuration BPDU {0,0,0, ポート A2}と比較します。 3． 計算された Configuration BPDU よりもローカルポートの Configuration BPDU が優位であることを検出します。ポート C1 はブロックされ、Configuration BPDU はそのまま変更しません。 ポートC1は、たとえば、Device BとDevice Cの間のリンクが切断されるなど、STPの計算プロセスのあらたな契機があるまで、データを転送しません。	● Blockedポート（ポート C1）：{0, 0, 0, ポートA2} ● Rootポート（ポートC2）：{0, 5, 1, ポートB2}

表 8-4に記述した比較プロセス後は、Device A を Root ブリッジとするスパニングツリーが図 8-5のように確立されます。

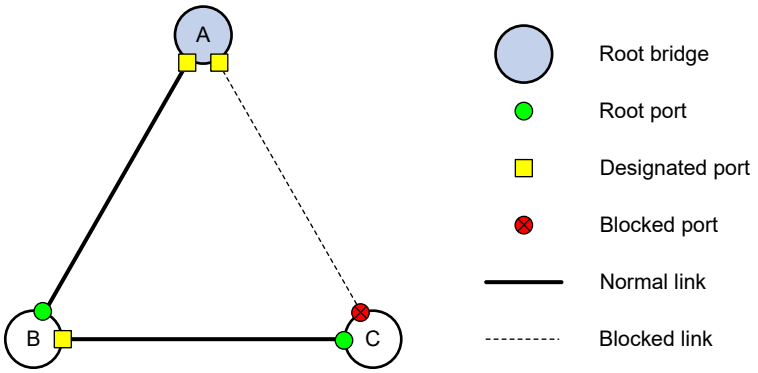


図 8-5 比較プロセス後のスパニングツリー

III. STP の Configuration BPDU 転送メカニズム

STP の Configuration BPDU は以下のガイドラインに従って転送されます。

- ネットワークの初期化をした際、各装置は自身を Root ブリッジとみなします。Configuration BPDU を生成し、Hello 時間の間隔で Configuration BPDU を送信します。
- Configuration BPDU を受信した Root ポートは、受信した Configuration BPDU がポートの Configuration BPDU より優位である場合、装置は以下の操作をします。
  - □ Configuration BPDU の有効時間を延ばします。
  - □ Configuration BPDU の時間を計るタイマをスタートさせます。
  - □ Designated ポートから Configuration BPDU を送信します。
- Designated ポートがローカルポートの Configuration BPDU と比較して優先順位の低い Configuration BPDU を受信した場合、ローカルポートの Configuration BPDU を返信します。
- 通信ができなくなると、Root ポートは、新しい Configuration BPDU を受信せず、古い Configuration BPDU はタイムアウトして破棄されます。このとき、装置は装置自体をルートとする Configuration BPDU を生成し、その BPDU を送信します。これが新しいスパニングツリーを計算する契機になり、ネットワークの接続を回復させます。

新しく計算された Configuration BPDU は、すぐにネットワーク内に広まらないため、トポロジの変更を検出していない古い Root ポートや Designated ポートは古い通信経路でデータの転送を継続します。新しい Root ポートや Designated ポートが選出されてから、すぐにデータの転送を開始すると、ループが発生する可能性があります。

IV. STP タイマ

STP には 3 つの重要なパラメータがあります。

- Forward delay

装置の状態が遷移するときの遅延時間です。

リンク障害等が発生すると、STP トポロジは再構築されます。再構築後の Configuration BPDU は、ネットワーク内にすぐには広まらないため、新しく選出された Root ポートや

Designated ポートがすぐにデータの転送をはじめてしまうと、ループが発生する可能性があります。

このため、新しく選出された Root ポートまたは Designated ポートは、Forwarding 状態に遷移する前に Forward delay タイマの 2 倍の時間を必要とします。これにより、新しい Configuration BPDU をネットワークに広げることができます。

- Hello 時間

装置が周辺の装置に Hello パケットを送信する間隔です。通信が正常であることを確認するものです。デフォルトは 2 秒です。装置がタイムアウト時間以内に Configuration BPDU を受信しない場合、装置はスパニングツリーの再計算を行います。タイムアウト時間を計算する式を以下に示します。

タイムアウト時間 ＝ タイムアウトファクタ × 3 × Hello 時間

- Max age

装置の Configuration BPDU が時間切れになっていないかどうかを判断するのに使うパラメータです。最大有効時間を越えた Configuration BPDU は破棄されます。デフォルトは 20 秒です。MSTP ネットワークの CIST では、装置は、Configuration BPDU 内に記載されている Max Age を経過した BPDU メッセージを廃棄します。最大エージング時間は CIST を除いて MSTI に影響がありません。

ポートがタイムアウト時間以内に Configuration BPDU を受信しない場合、ポートは Listening 状態に遷移します。装置はスパニングツリーを再計算します。ポートが Forwarding 状態に遷移するまで約 50 秒かかります。この値は Max age が 20 秒、Listening 状態が 15 秒、Learning 状態が 15 秒とした値です。

スパニングツリーの状態変更が頻繁に発生するのを回避するには、Hello 時間、Forward Delay、最大エージング時間の設定を次式に満足するよう設定してください。

- 2 ×（Forward delay － 1 秒）≧ Max age
- Max age ≧ 2 ×（Hello 時間 ＋ 1 秒）

8.2 RSTP

RSTP は、新しく選出された Root ポートあるいは Designated ポートを Forwarding 状態にするため、STP よりもネットワークの高速な収束を行います。

- **Protocol version ID**– スパニングツリーの Version ID です。RSTP のプロトコルバージョン ID は 0x02 です。
- **BPDU type**– BPDU のタイプです。RSTP BPDU の値は 0x02 です。
- **Flags**– BPDU の目的を示します。8 ビットフィールドです。
- **Version1 length**– Version 1 のプロトコル情報が存在しないことを示します。値は 0x00 です。

RSTP はトポロジの変更を通知する際に TCN BPDU を使用しません。トポロジの変更を通知する場合、RSTP は TC フラグを設定し、BPDU をフラッディングします。

8.2.1 RSTP の基本概念

I. ポートの役割

- **Alternate ポート**（代替ポート）– Root ポートのバックアップとして動作します。Root ポートがブロックされたとき、Alternate ポートが引き継ぎます。
- **Backup ポート**– Designated ポートのバックアップとして動作します。Designated ポートが無効であるとき、backup ポートは新しい Designated ポートになります。同一のスパニングツリーの 2 つのポートが接続されたとき、ループが発生します。そのため装置はポートの 1 つをブロックします。ブロックされたポートは backup ポートです。
- **Edge ポート**– ネットワークの装置あるいはネットワークセグメントに接続されておらず、ユーザホストに直接接続しているポートです。

II. ポート状態

RSTP は、STP の Disabled 状態、Blocking 状態、Listening 状態が discarding 状態に変わりました。表 8-5に RSTP と STP のポート状態の違いを示します。

表 8-5 STP のポート状態

STP ポート状態	RSTP ポート状態	BPDU の送信	MAC アドレスの学習	データの転送
Disabled	Discarding	No	No	No
Blocking	Discarding	No	No	No
Listening	Discarding	Yes	No	No
Learning	Learning	Yes	Yes	No
Forwarding	Forwarding	Yes	Yes	Yes

8.2.2 RSTP の動作

RSTP の計算中、以下のイベントが発生します。

- discarding 状態のポートが Alternate ポートになる場合、状態を保持します。
- discarding 状態のポートが Root ポートあるいは Designated ポートとして選出された場合、Forward delay 後、Learning 状態に遷移します。ポートは MAC アドレスを学習し、別の Forward delay 後に Forwarding 状態に遷移します。
  - □ 以下の要件に一致した場合、新しく選出された RSTP の Root ポートは即座に Forwarding 状態になります。
    - 装置の古い Root ポートが転送データを止めた場合
    - 上り方向の Designated ポートが転送をはじめた場合
  - □ 以下の要件の 1 つに一致した場合、新しく選出された RSTP の Designed ポートは即座に Forwarding 状態になります。
    - Designed ポートがユーザ端末に直接接続された Edge ポートとして設定された場合
    - Designated ポートが point-to-point リンクに接続し、直接接続された装置からハンドシェイクの応答を受信した場合

8.2.3 RSTP の BPDU 処理

Root ブリッジでないアクティブな装置は、Designated ポートに Hello 時間の間隔で RSTP BPDU を送信します。RSTP BPDU の送信は Root ブリッジを待つことなく行われます。これにより RSTP はリンク障害を早急に検出することができます。装置が Hello 時間の 3 倍以内にポートで RSTP BPDU を受信しない場合、装置はリンク障害が発生したと認識します。記録された Configuration BPDU の有効期限が終了したのち、装置は RSTP の計算を行うため、TC フラグを設定し、RSTP BPDU をフラッディングします。

RSTP では、Blocking 状態のポートは自身の BPDU よりも低いプライオリティで即座に RSTP BPDU に応答することができます。

図 8-6に示すように、Device A は Root ブリッジです。Device B のプライオリティは Device C のプライオリティよりも低いです。Device C のポート C2 はブロックされます。

Device A と Device B 間のリンクに障害が発生した場合、以下のイベントが発生します。

1) Device B は Root ブリッジとして Device B の RSTP BPDU を Device C に送信します。
2) Device C は RSTP BPDU を Device C の BPDU と比較します。
3) Device B からの RSTP BPDU のプライオリティが低いため、Device C は Device C の BPDU を Device B に送信します。
4) Device B はポート B2 が Root ポートと認識し、Device C への RSTP BPDU の送信を停止します。

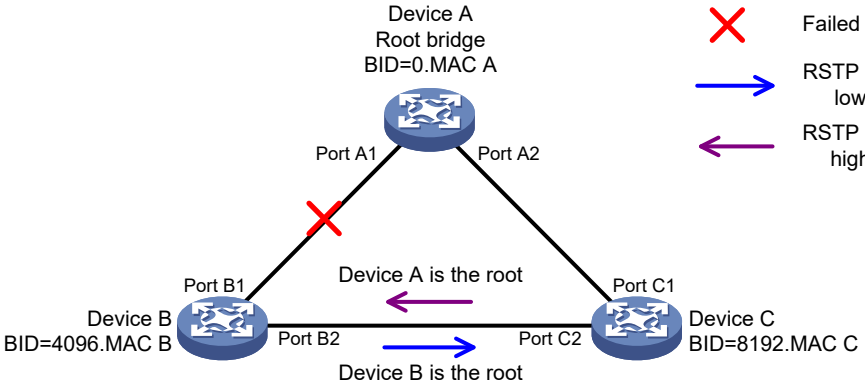


図 8-6 RSTP の BPDU 処理

8.3 PVST

STP あるいは RSTP が有効な LAN ではすべてのブリッジは 1 つのスパニングツリーで共有されます。すべての VLAN からのトラフィックは 1 つのスパニングツリーを経由して転送されます。ループがあった場合、ポートは、VLAN でループをブロックすることができません。

PVST は各 VLAN にそれぞれのスパニングツリーを持たせることができます。スパニングツリーはリンクと帯域幅を増大することができます。各 VLAN が独立して STP または RSTP を動作するため、スパニングツリーは VLAN に対応するだけで動作します。

PVST は、Rapid PVST や PVST が動作するサードパーティ製の装置や NEC の装置と通信することができます。PVST が有効な NEC の装置は、PVST が有効な NEC の装置ある

いは Rapid PVST が有効なサードパーティ製の装置と接続したとき、RSTP のように早急なネットワークの収束をサポートします。

8.3.1 PVST のプロトコルフレーム

図 8-7に示すように PVST BPDU は以下の相違点を除いて RSTP BPDU と同一のフォーマットを使用します。

- PVST BPDU の宛先 MAC アドレスはプライベート MAC アドレスの 01-00-0c-cc-cc-cd です。
- 各 PVST BPDU は VLAN タグを転送します。VLAN タグは PVST BPDU が所属する VLAN を識別します。
- 組織コード、PID フィールドは PVST BPDU の LLC ヘッダに追加されています。

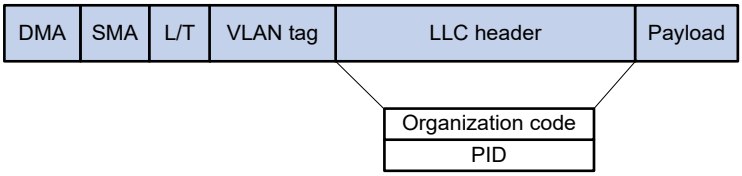


図 8-7 PVST BPDU フォーマット

ポートのリンクタイプは、ポートが送信する BPDU タイプを決定します。

- アクセスポートは RSTP BPDU を送信します。
- トランクあるいはハイブリッドポートはデフォルト VLAN では RSTP BPDU を送信します。ほかの VLAN では PVST BPDU を送信します。

8.3.2 PVST の基本概念

PVST は高速収束を行うため、RSTP と同一のポートの役割とポート状態を使用します。詳細はオペレーションマニュアルのセクション 3 *アクセス*“*STP*”の“*RSTP*”の“*RSTP の基本概念*”を参照してください。

8.3.3 PVST の動作

PVST では各 VLAN はほかのスパニングツリーに影響せずに、自身のスパニングツリーを独立して維持します。これにより各 VLAN のループは除去され、異なる VLAN のトラフィックがリンクを超えて共有されます。PVST は計算を行うため、デフォルト VLAN では RSTP BPDU を使用し、ほかの VLAN では PVST BPDU を使用します。QX シリーズの PVST は、各 VLAN を MSTI にマッピングすることで VLAN ごとのスパニングツリーの計算を行います。

8.4 MSTP

MSTP は以下の STP、RSTP、PVST の制限を克服したものです。

- **STP の制限**– STP は、ポートの高速な状態遷移には対応できません。新しく選出されたポートは、Forwarding 状態に遷移する前に 2 倍の Forward delay を待たなければなりません。
- **RSTP の制限**– RSTP（rapid spanning tree protocol）は、STP よりも収束時間を早くしたにもかかわらず、STP 同様 VLAN 上の全ネットワークブリッジがスパニングツリーを共有するため、冗長リンクを VLAN ごとにブロックできない欠点があります。
- **PVST の制限**– 各 VLAN はスパニングツリーを持つため、PVST BPDU の量は、トランクあるいはハイブリッドポートの VLAN の数に比例して増加します。トランクあるいはハイブリッドポートが多くの VLAN を許可しているとき、VLAN スパニングツリーを維持するリソースと計算を行うリソースの両方が劇的に増加します。複数の VLAN があるトランクあるいはハイブリッドポートでステータスの変更がある場合、装置の CPU は影響するスパニングツリーを再計算するために負担がかかります。その結果、ネットワークの性能が低下します。

8.4.1 MSTP の特徴

IEEE802.1s をもとに発展させた MSTP（multiple spanning tree protocol）は、STP、RSTP、PVST の制限を克服します。ネットワークを高速に収束させるだけでなく、VLAN ごとにデータフローがそれぞれのパスに転送されるので、冗長リンクの負荷分散ができます。

MSTP には以下のような特徴があります。

- MSTP によりスイッチネットワークは複数の領域に分けられ、それぞれの領域が独立した複数のスパニングツリーで構成されます。
- MSTP は、マッピングテーブルを使用し、MST インスタンスへの VLAN のマッピングを行います。MSTP は、複数の VLAN を 1 つの MST インスタンスにマッピングすることで、通信帯域やリソースの使用を節約できます。
- MSTP はループのあるネットワークをループのないツリー構造に変え、ループネットワーク内でのループを回避します。さらに、MSTP はデータ転送用の冗長パスを複数提供し、データ転送プロセスにおける VLAN データの負荷分散を行います。
- MSTP は STP、RSTP と一部の PVST に互換性があります。

8.4.2 MSTP のプロトコルフレーム

図 8-8に MSTP BPDU のフォーマットを示します。

Fields	Byte
Protocol ID	2
Protocol version ID	1
BPDU type	1
Flags	1
Root ID	8
Root path cost	4
Bridge ID	8
Port ID	2
Message age	2
Max age	2
Hello time	2
Forward delay	2
Version1 length=0	1
Version3 length	2
MST configuration ID	51
CIST IRPC	4
CIST bridge ID	8
CIST remaining ID	1
MSTI configuration messages	LEN

MSTP-specific fields

図 8-8 MSTP BPDU のフォーマット

MSTP BPDU の最初の 13 フィールドは RSTP BPDU と同一です。ほかの 6 つのフィールドは MSTP で固有です。

- **Protocol version ID**（プロトコルバージョン ID）– スパニングツリーのバージョン ID です。MSTP のプロトコルバージョン ID は 0x02 です。
- **BPDU type**– BPDU のタイプです。RSTP BPDU、MSTP BPDU の値は 0x02 です。
- **Root ID**– 共通 Root ブリッジの ID です。
- **Root path cost**（ルートパスコスト）– CIST（common and internal spanning tree）の外部のパスコストです。
- **Bridge ID**– IST（Internal spanning tree）あるいは MSTI（Multiple Spanning Tree Instance）の regional Root の ID です。
- **Port ID**– CIST の Designated ブリッジの ID です。Designated ブリッジのプライオリティとグローバルポート番号で構成されます。
- **Version3 length**– MSTI 指定フィールドの長さです。装置は MSTP BPDU の受信を確認するために、このフィールドを使います。
- **MST Configuration ID**– フォーマットセレクタ、Configuration 名、revision レベル、Configuration ダイジェストが含まれます。フォーマットセレクタは 0x00 で固定です。ほかのパラメータはもとのブリッジで MST region を識別するために使用します。
- **CIST IRPC**– もとのブリッジから MST region のルートへの内部ルートパス（IRPC：Internal root path cost）です。
- **CIST bridge ID**– MSTP BPDU を送信するブリッジの ID です。
- **CIST remaining ID**– 残りホップ数です。このフィールドは MST region の規模を制限します。regional Root は残りホップ数を最大値に設定し、BPDU を送信します。BPDU を受信する各装置はスパニングツリーを構成する装置を経由するたびに、-1 します。ホップ数が 0 になったとき、BPDU を廃棄します。MST region の最大ホップ数を超える装置はスパニングツリーの計算に参加することができません。デフォルトの残りホップ数は 20 です。
- **MSTI Configuration messages**– MSTI の Configuration メッセージが含まれます。各 MSTI Configuration メッセージは 16 バイトです。このフィールドは 0～64 まで含

むことができます。MSTI Configuration メッセージの数は MST region の MSTI の数によって決まります。

8.4.3 MSTP の基本概念

図 8-9は 4 つの MST region から構成され、各 MST region は 4 つの MSTP 装置から構成されます。図 8-10は MST region3 のネットワークトポロジを示します。

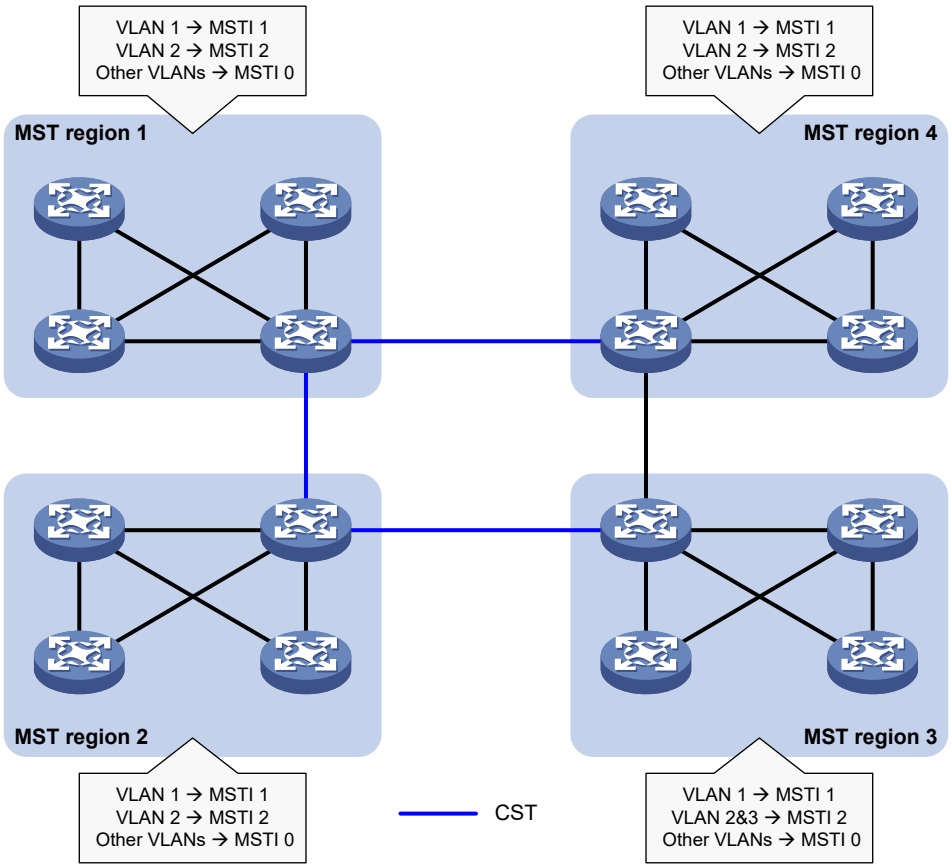


図 8-9 MSTP の基本概念

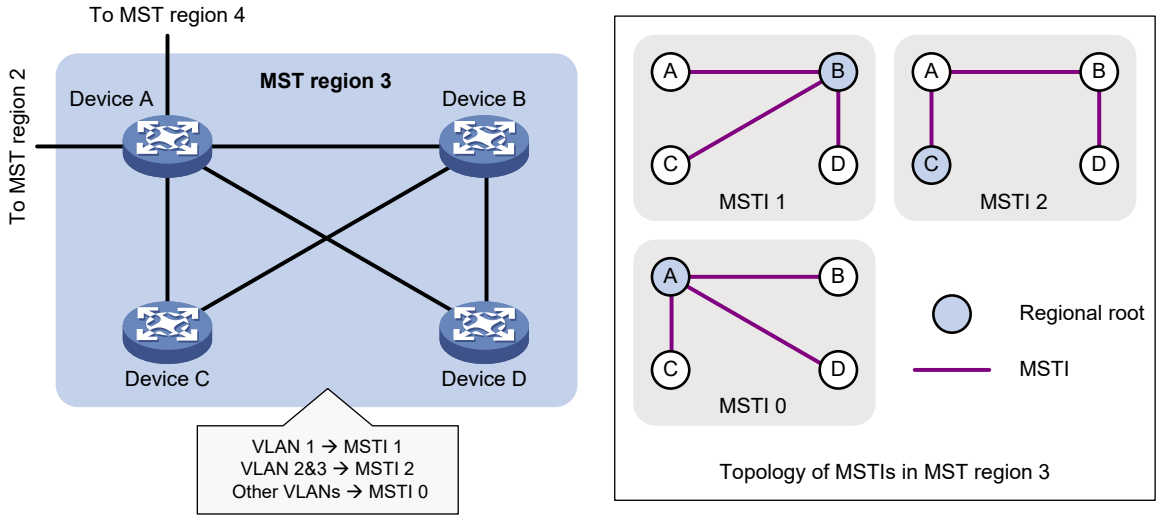


図 8-10 MST region 3 のネットワーク図とトポロジ

I. MST region

複数のスパニングツリーregion（MST region）は、スイッチネットワークの複数の装置と装置間のネットワークセグメントで構成されています。これらの装置には、以下のような特性があります。

- すべて MSTP を有効にしています。
- 同じ region 名を持っています。
- VLAN インスタンスマッピングの設定が同じです。
- MSTP リビジョンレベルの設定が同じです。
- 物理的に相互にリンクしています。

複数の MST region はスイッチネットワークで使われます。同じ MST region に装置を割り当てることができます。図 8-9は以下のようになっています。

- スイッチネットワークは MST region1～4 の 4 つの MST region から構成されます。
- 各 MST region のすべての装置は同じ MST region 設定を持ちます。

II. MSTI

MSTP により、複数のスパニングツリーを、ほかから独立したスパニングツリーとして、1 つの MST region で生成でき、VLAN を指定するために各スパニングツリーでマッピングされます。それぞれのスパニングツリーは 1 つの MST インスタンス（MSTI（Multiple Spanning Tree Instance））とみなされます。

図 8-10では、MSTI1、MSTI2、MSTI0 の 3 つの MSTI があります。

III. VLAN インスタンスマッピングテーブル

VLAN インスタンスマッピングテーブルは VLAN と MST インスタンス間のマッピングの関係ついて、MST region ごとに記載されています。

図 8-10では、MST region 3 の VLAN インスタンスマッピングテーブルは以下のようになっています。

- VLAN 1 は MSTI 1 にマッピングされています。
- VLAN 2 は MSTI 2 にマッピングされています。
- 残りは MSTI0 にマッピングされています。

MSTP は、VLAN インスタンスマッピングテーブルを使って負荷分散を行います。

IV. CST

CST は、スイッチネットワークのすべての MST region に接続する 1 つのスパニングツリーです。MST region をそれぞれ装置とみなすと、CST はこれらの装置が STP または RSTP で計算したスパニングツリーです。図 8-9の青い線は CST を示しています。

V. IST

IST（Internal spanning tree）は、MST region で動作するスパニングツリーです。特別な MSTI で MSTI0 と呼ばれます。デフォルトではすべての VLAN は MSTI0 にマッピングされています。図 8-9では、MSTI 0 は MST region3 の IST です。

VI. CIST

CIST（common and internal spanning tree）はスイッチネットワークですべての装置に接続する 1 つのスパニングツリーです。CIST は、すべての MST region にある IST と CST で構成されます。図 8-9では、すべての MST region と inter-region CST を加えた IST（MSTI 0）は、全体の CIST を構成します。

VII. Regional Root

MST region 内の IST または MSTI の Root ブリッジは、MST またはその MSTI の regional Root ブリッジです。トポロジをベースに、MST region のそれぞれのスパニングツリーが異なる region ルートを持つ場合があります。

図 8-10の MST region3 では、以下のようになっています。

- MSTI1 の regional ルートは Device B です。
- MSTI2 の regional ルートは Device C です。
- MSTI0（IST）の regional ルートは Device A です。

VIII. 共通 Root ブリッジ

共通 Root ブリッジは、CIST の Root ブリッジです。

図 8-9では、MST Region 1 のスイッチが共通 Root ブリッジです。

IX. ポートの役割

異なる MSTI で、ポートは異なる役割を行います。図 8-11に示すように MST region は Device A、Device B、Device C、Device D があります。Device A のポート A1 とポート A2 は共通 Root ブリッジに接続されています。Device B のポート B2、ポート B3 はループしています。Device C のポート C3、ポート C4 はほかの MST region に接続されています。Device D のポート D3 はホストに接続されています。

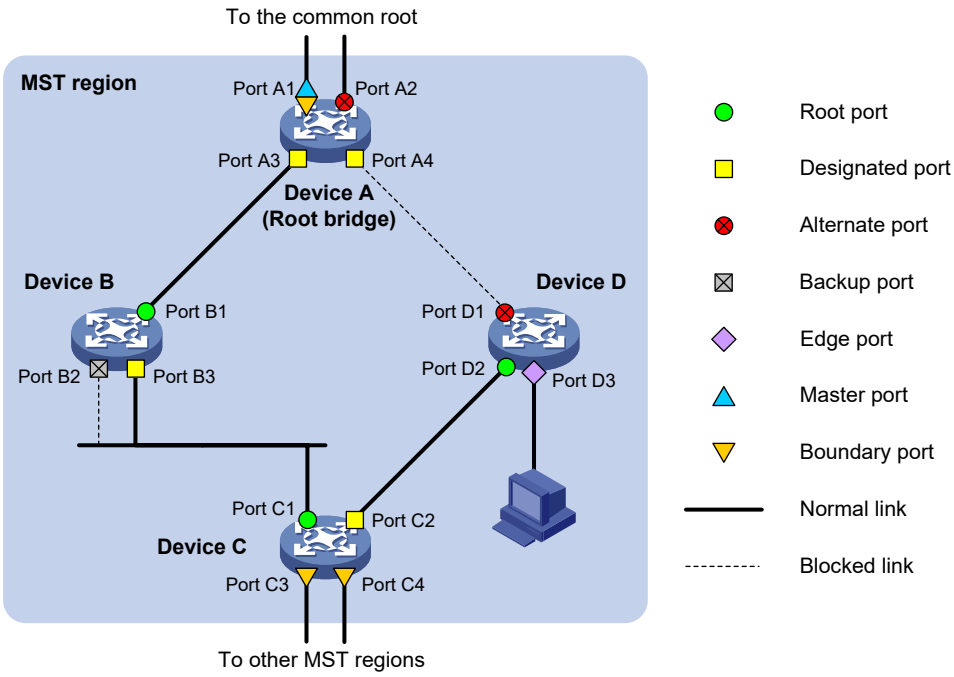


図 8-11 ポートの役割

MSTP では、以下のポートの計算を行っています。

- **Root** ポート– 非 Root ブリッジ用にデータを Root ブリッジに転送します。Root ブリッジは Root ポートを持っていません。
- **Designated** ポート– データを下流方向のネットワークセグメントや装置に転送するポートです。
- **Alternate** ポート– Root ポートもしくは Master ポートの代替ポートです。Root ポートもしくは Master ポートがブロッキング状態になると、その代わりに Root ポートもしくは Master ポートになるポートです。
- **Backup** ポート– Designated ポートの代替ポートで、高速な切り替えのために使われます。Designated ポートがブロッキング状態になると、即座にその代わりに Designated ポートになり、データの転送を開始できます。
- **Edge** ポート– ネットワーク装置あるいはネットワークセグメントに接続されていないポートで、ユーザホストに直接接続されています。
- **Master** ポート– MST Region を共通 Root ブリッジに接続するポートで、その MST Region における Root ポートでもあります。Master ポートから共通 Root ブリッジへのパスは、最短パスとなります。Master ポートはいつも regional Root にあるわけではありません。IST や CIST の Root ポートは Root ポートで、ほかの MSTI の Master ポートです。
- **Boundary** ポート– MST Region の端点のポートで、ほかの MST Region や STP/RSTP で制御される装置と接続します。MSTP の計算を行うとき、MSTI の

boundary ポートの役割は CIST の役割と同一です。Master ポートになるわけではありません。MSTI の Master ポートは CIST の Root ポートです。

X. ポートの状態

MSTP では、ポートは以下のいずれかの状態になっています。

- **Forwarding**ーこの状態のポートは、BPDU の送受信が可能で、MAC アドレスを学習し、ユーザトラフィックを転送できます。
- **Learning**ーこの状態のポートは、BPDU の送受信が可能で、MAC アドレスを学習しますが、ユーザトラフィックを転送できません。
- **Discarding**ーこの状態のポートは、BPDU の受信のみ可能です。MAC アドレスの学習やユーザトラフィックを転送できません。

🕮 **メモ：**

MSTI が異なると、ポートの状態も異なります。

ポートの状態はポートの役割と排他的ではありません。表 8-6にポートの役割と、成り得るポート状態の関係を示します。“〇”はポートがこの状態に対応することを示し、“×”ポートがこの状態に対応しないことを示します。

表 8-6 ポートの役割とポート状態の関係

ポートの役割（右） ポートの状態（下）	Root ポート /master ポート	Designated ポート	Alternate ポート	Backup ポート
Forwarding	〇	〇	×	×
Learning	〇	〇	×	×
Discarding	〇	〇	〇	〇

8.4.4 MSTP の動作

MSTP はレイヤ 2 ネットワーク全体を複数の MST Region に分割します。MST Region 間で CST を生成し、各 MST Region 内に MSTI と呼ばれる複数のスパニングツリーを生成します。MSTI が 0 の MSTI は IST です。

MSTP では、STP と同様に、スパニングツリーを構成するための情報転送に BPDU を使用します。MSTP 用の BPDU との違いは、MSTP の BPDU に加えて、MSTI 用のパラメータを付加します。

I. CIST の構築

CIST の構築では、以下の処理が行われます

- もっとも優先度の高い装置を、CIST の Root として選出します。
- 各 MST Region では IST が構築されます。
- MSTP はそれぞれの MST Region を 1 つの装置とみなして、ネットワークの CST を構築します。

構築された IST と CST で CIST が構成されます。

II. MSTI の構築

MST Region 内では、VLAN マッピングテーブルの情報によって VLAN グループごとの MSTI を構築します。それぞれの MSTI では、STP と同様にスパニングツリーを構成します。詳細は、オペレーションマニュアルのセクション 3 *アクセス "STP"の"STP アルゴリズムの計算プロセス"*を参照してください。

MSTP では、VLAN パケットは以下のパスに沿って転送されます。

- MST region 内ではパケットは対応する MSTI に沿って転送されます。
- MST region 間ではパケットは CST に沿って転送されます。

8.4.5 装置での MSTP の実行

MSTP は STP および RSTP と互換性があります。STP および RSTP プロトコルパケットは、MSTP を実行している装置に認識され、スパニングツリーの計算に使用されます。

基本的な MSTP 機能に加え、以下のような特別な機能を提供することで、管理を容易にします。

- Root ブリッジの保持
- Root ブリッジのバックアップ
- Root ガード
- BPDU ガード
- Loop ガード
- TC-BPDU ガード
- ポート役割制限
- TC-BPDU 転送制限機能

8.4.6 高速収束メカニズム

STP ではポートは Blocking 状態から Forwarding 状態に遷移する前、Forward delay（デフォルトで 30 秒です）の 2 倍待つ必要があります。Forward delay は Hello 時間とネットワークダイアメータに関連します。Forward delay が短すぎる場合、ループが発生する可能性があります。これはネットワークの安定性に影響します。

RSTP、PVST、MSTP は Edge ポート、Root ポート、Designated ポートのポート状態の遷移を早く行う高速収束メカニズムを使用します。Designated ポートの高速収束メカニズムは P/A transition（proposal/agreement_transition）として知られます。

I. Edge ポートの高速収束

図 8-12に示すようにポート C3 はホストに接続された Edge ポートです。ネットワークトポロジの変更が発生したとき、ループが発生しないため、ポートは即座に Blocking 状態から Forwarding 状態に遷移します。

装置はポートが端末に直接接続されているか決定することができないため、Edge ポートとしてポートを手動で設定する必要があります。

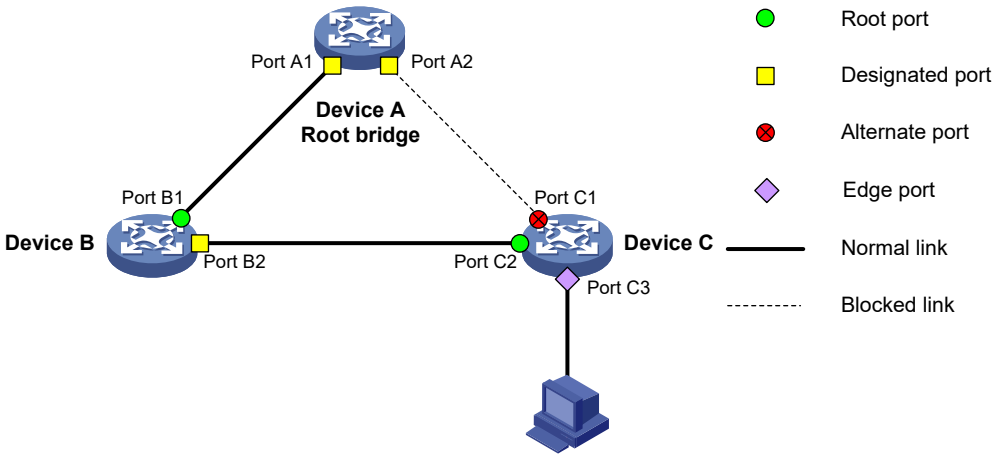


図 8-12 Edge ポートの高速収束

II. Root ポートの高速収束

Root ポートがブロックされたとき、ブリッジは新しい Root ポートとしてもっともプライオリティが高い Alternate ポートを選出します。新しい Root ポートの対向先が Forwarding 状態である場合、新しい Root ポートは即座に Forwarding 状態に遷移します。

図 8-13に示すように Device C のポート C2 は Root ポートで、ポート C1 は Alternate ポートです。ポート C2 が Blocking 状態に遷移した場合、ポート C1 は Root ポートとして選出され、即座に Forwarding 状態に遷移します。

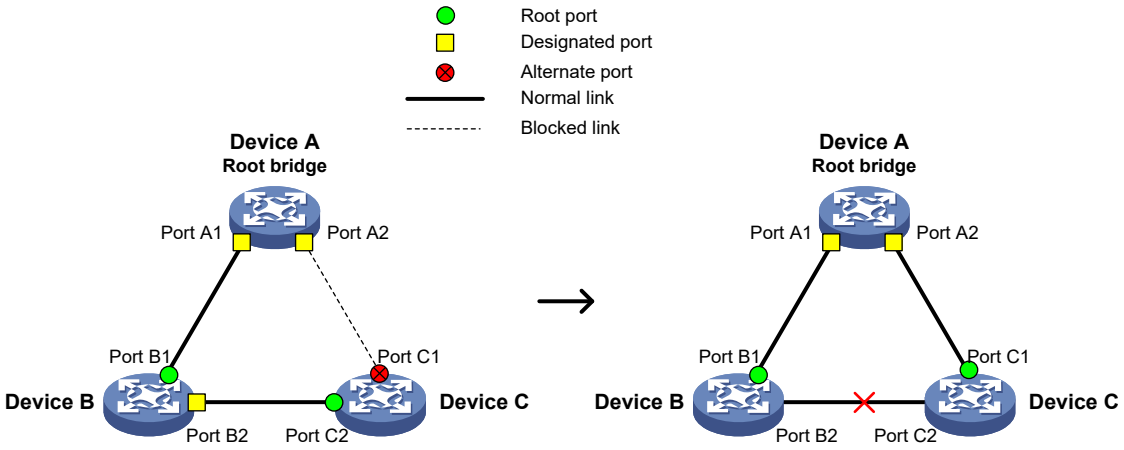


図 8-13 Root ポートの高速収束

III. P/A transition

P/A transition は対向先とハンドシェイクを行った後、Designated ポートが高速に Forwarding 状態に遷移することを有効にします。P/A transition はポイント—ポイントリンクでのみ適用します。

- RSTP と PVST の P/A transition

RSTP あるいは PVST では、新しいリンクあるいは回復したリンクのポートは Blocking 状態の Designated ポートです。

Designated ポートの 1 つが discarding 状態あるいは Learning 状態に遷移したとき、BPDU の proposal フラグを設定します。対向先の装置は BPDU を受信し、受信ポートが Root ポートであるかどうかを決定します。そしてブリッジは Designated ポートに agreement BPDU を応答します。agreement BPDU を受信すると、Designated ポートは即座に Forwarding 状態に遷移します。Designated ポートが agreement BPDU を受信しない場合、Forwarding 状態に遷移するために Forward delay の 2 倍を待ちます。

図 8-14に示すように、P/A transition の動作を示します。

1) Device A はポート A1 を通して Device B に proposal BPDU の送信を行います。
2) Device B はポート B2 で proposal BPDU を受信します。ポート 2 は Root ポートとして選出されます。
3) Device B はループを取り除くため Designated ポート B2 と Alternate ポート B3 をブロックします。
4) Root ポート B2 は Forwarding 状態に遷移し、Device A に agreement BPDU を送信します。
5) agreement BPDU を受信したのち、Device A の Designated ポート A1 は即座に Forwarding 状態に遷移します。

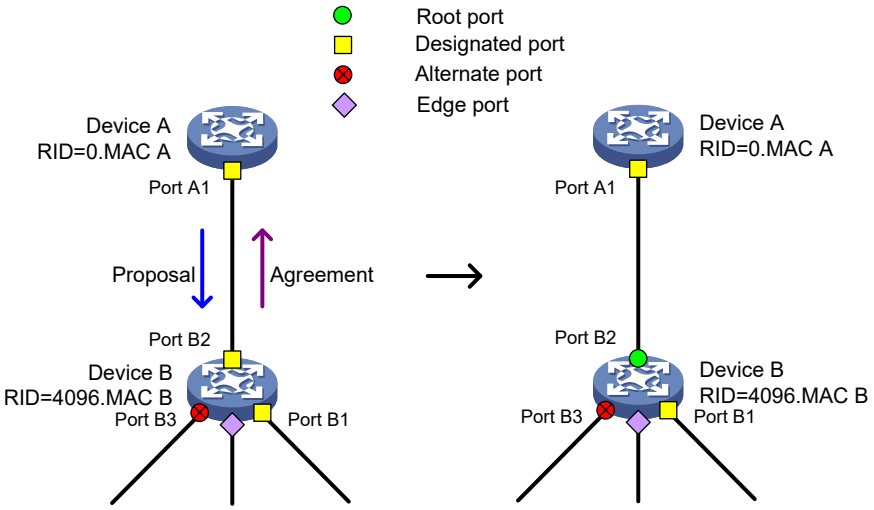


図 8-14 RSTP と PVST の P/A transition

- MSTP の P/A transition

MSTP では上流のブリッジは BPDU の proposal フラグと agreement フラグの両方を設定します。下流のブリッジが BPDU を受信し、受信ポートが Root ポートとして選出された場合、ブリッジは Edge ポートを除くほかのすべてのポートをブロックします。下流のブリッジは上流のブリッジに agreement BPDU を応答します。agreement BPDU を受信すると、上流のポートは即座に Forwarding 状態に遷移します。上流のポートが agreement BPDU を受信しない場合、Forwarding 状態に遷移するために Forward delay の 2 倍を待ちます。

図 8-15に示すように、P/A transition の動作を示します。

1) Device A は BPDU の proposal フラグと agreement フラグの両方を設定し、ポート A1 を通して Device B に BPDU の送信を行います。

2) Device B は BPDU を受信します。Device B のポート B1 は Root ポートとして選出されます。
3) Device B は Edge ポートを除くほかのすべてのポートをブロックします。
4) Device B の Root ポート B1 は Forwarding 状態に遷移し、Device A に agreement BPDU を送信します。
5) agreement BPDU を受信すると、Device A のポート A1 は即座に Forwarding 状態に遷移します。

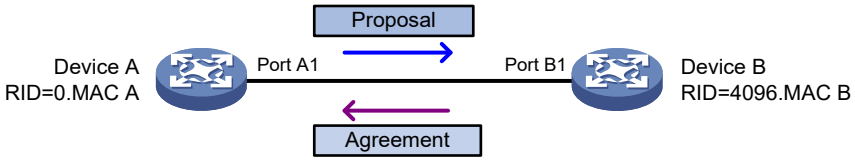


図 8-15 MSTP の P/A transition

8.5 プロトコルと規格

MSTP は以下に示すプロトコルと規格に記載されています。

- IEEE 802.1d, *Media Access Control (MAC) Bridges*
- IEEE 802.1w, *Part 3: Media Access Control (MAC) Bridges− Amendment 2: Rapid Reconfiguration*
- IEEE 802.1s, *Virtual Bridged Local Area Networks− Amendment 3: Multiple Spanning Trees*
- IEEE 802.1Q-REV/D1.3, *Media Access Control (MAC) Bridges and Virtual Bridged Local Area Networks − Clause 13: Spanning tree Protocols*

8.6 スパニングツリー設定作業リスト

スパニングツリーを設定する前に、以下の作業を完了してください。

- 各 MST インスタンス内のそれぞれの装置で使用するプロトコル（STP、RSTP、MSTP、PVST）を定義してください。
- 装置の役割（Root ブリッジまたは Leaf ノード）を定義してください。

スパニングツリーを設定するとき、以下の制限とガイドラインに従ってください。

- スパニングツリーの設定は、RRPP、Smart Link と一緒に設定できません。
- system view で行った設定は全体に適用されます。Ethernet interface view で行った設定は、インタフェースでのみ適用されます。aggregate interface view で行った設定は、アグリゲートインタフェースでのみ適用されます。アグリゲーションメンバポートで行った設定は、アグリゲーショングループから取り除かれた後に有効になります。
- アグリゲートインタフェースでスパニングツリーを有効にした後、アグリゲートインタフェースでアルゴリズムの計算が行われます。アグリゲーションメンバポートでは行われません。スパニングツリーは、状態を有効にすることに加えて、対応するアグリゲートインタフェースに一致する各選択されたメンバポートの Forwarding 状態を有効にします。

- アグリゲーショングループのメンバポートはスパニングツリーの計算に関与しませんが、ポートは、アグリゲーショングループから取り除かれた後に、MSTP 計算に参加するために、その MSTP 設定を確保しています。

8.6.1 STP 設定作業リスト

作業リスト
Rootブリッジの設定： ● （必須設定項目）動作モードの設定 ● （オプション設定項目）RootブリッジとSecondary Rootブリッジの設定 ● （オプション設定項目）ブリッジプライオリティの設定 ● （オプション設定項目）ネットワークダイアメータの設定 ● （オプション設定項目）スパニングツリータイマの設定 ● （オプション設定項目）タイムアウトファクタの設定 ● （オプション設定項目）BPDU最大送出レートの設定 ● （オプション設定項目）ポート遷移状態情報の出力の有効化 ● （必須設定項目）スパニングツリー機能の有効化
Leafノードの設定： ● （必須設定項目）動作モードの設定 ● （オプション設定項目）ブリッジプライオリティの設定 ● （オプション設定項目）タイムアウトファクタの設定 ● （オプション設定項目）BPDU最大送出レートの設定 ● （オプション設定項目）ポートパスコストの設定 ● （オプション設定項目）ポートプライオリティの設定 ● （オプション設定項目）ポート遷移状態情報の出力の有効化 ● （必須設定項目）スパニングツリー機能の有効化
（オプション設定項目）TC snoopingの設定
（オプション設定項目）保護機能の設定
（オプション設定項目）新しいRootの選出とトポロジ変更によるSNMP notificationの有効化

8.6.2 RSTP 設定作業リスト

作業リスト
Rootブリッジの設定： ● （必須設定項目）動作モードの設定 ● （オプション設定項目）RootブリッジとSecondary Rootブリッジの設定 ● （オプション設定項目）ブリッジプライオリティの設定 ● （オプション設定項目）ネットワークダイアメータの設定 ● （オプション設定項目）スパニングツリータイマの設定 ● （オプション設定項目）タイムアウトファクタの設定 ● （オプション設定項目）BPDU最大送出レートの設定 ● （オプション設定項目）Edgeポートの設定 ● （オプション設定項目）Point-to-Pointリンクの設定 ● （オプション設定項目）ポート遷移状態情報の出力の有効化 ● （必須設定項目）スパニングツリー機能の有効化
Leafノードの設定： ● （必須設定項目）動作モードの設定 ● （オプション設定項目）ブリッジプライオリティの設定 ● （オプション設定項目）タイムアウトファクタの設定 ● （オプション設定項目）BPDU最大送出レートの設定 ● （オプション設定項目）Edgeポートの設定 ● （オプション設定項目）ポートパスコストの設定 ● （オプション設定項目）ポートプライオリティの設定 ● （オプション設定項目）Point-to-Pointリンクの設定 ● （オプション設定項目）ポート遷移状態情報の出力の有効化 ● （必須設定項目）スパニングツリー機能の有効化
（オプション設定項目）mCheck機能の設定
（オプション設定項目）TC snoopingの設定
（オプション設定項目）保護機能の設定
（オプション設定項目）新しいRootの選出とトポロジ変更によるSNMP notificationの有効化

8.6.3 PVST 設定作業リスト

作業リスト
Rootブリッジの設定： ● （必須設定項目）動作モードの設定 ● （オプション設定項目）RootブリッジとSecondary Rootブリッジの設定 ● （オプション設定項目）ブリッジプライオリティの設定 ● （オプション設定項目）ネットワークダイアメータの設定 ● （オプション設定項目）スパニングツリータイマの設定 ● （オプション設定項目）タイムアウトファクタの設定 ● （オプション設定項目）BPDU最大送出レートの設定 ● （オプション設定項目）Edgeポートの設定 ● （オプション設定項目）Point-to-Pointリンクの設定 ● （オプション設定項目）ポート遷移状態情報の出力の有効化 ● （必須設定項目）スパニングツリー機能の有効化 ● （オプション設定項目）矛盾したPVID 保護の無効化
Leafノードの設定： ● （必須設定項目）動作モードの設定 ● （オプション設定項目）ブリッジプライオリティの設定 ● （オプション設定項目）タイムアウトファクタの設定 ● （オプション設定項目）BPDU最大送出レートの設定 ● （オプション設定項目）Edgeポートの設定 ● （オプション設定項目）ポートパスコストの設定 ● （オプション設定項目）ポートプライオリティの設定 ● （オプション設定項目）Point-to-Pointリンクの設定 ● （オプション設定項目）ポート遷移状態情報の出力の有効化 ● （必須設定項目）スパニングツリー機能の有効化
（オプション設定項目）mCheck機能の設定
（オプション設定項目）矛盾したPVID 保護の無効化
（オプション設定項目）保護機能の設定
（オプション設定項目）TC BPDUの検出、受信イベントのログ作成の有効化
（オプション設定項目）新しいRootの選出とトポロジ変更によるSNMP notificationの有効化

8.6.4 MSTP 設定作業リスト

作業リスト
Rootブリッジの設定： • （必須設定項目）動作モードの設定 • （必須設定項目）MST regionの設定 • （オプション設定項目）RootブリッジとSecondary Rootブリッジの設定 • （オプション設定項目）ブリッジプライオリティの設定 • （オプション設定項目）MST regionの最大ホップ数の設定 • （オプション設定項目）ネットワークダイアメータの設定 • （オプション設定項目）スパニングツリータイマの設定 • （オプション設定項目）タイムアウトファクタの設定 • （オプション設定項目）BPDU最大送出レートの設定 • （オプション設定項目）Edgeポートの設定 • （オプション設定項目）Point-to-Pointリンクの設定 • （オプション設定項目）MSTPパケットのフォーマット設定 • （オプション設定項目）ポート遷移状態情報の出力の有効化 • （必須設定項目）スパニングツリー機能の有効化
Leafノードの設定： • （必須設定項目）動作モードの設定 • （必須設定項目）MST regionの設定 • （オプション設定項目）ブリッジプライオリティの設定 • （オプション設定項目）タイムアウトファクタの設定 • （オプション設定項目）BPDU最大送出レートの設定 • （オプション設定項目）Edgeポートの設定 • （オプション設定項目）ポートパスコストの設定 • （オプション設定項目）ポートプライオリティの設定 • （オプション設定項目）Point-to-Pointリンクの設定 • （オプション設定項目）MSTPパケットのフォーマット設定 • （オプション設定項目）ポート遷移状態情報の出力の有効化 • （必須設定項目）スパニングツリー機能の有効化
（オプション設定項目）mCheck機能の設定
（オプション設定項目）Digest Snoopingの設定
（オプション設定項目）No AgreementCheckの設定
（オプション設定項目）TC snoopingの設定
（オプション設定項目）保護機能の設定
（オプション設定項目）新しいRootの選出とトポロジ変更によるSNMP notificationの有効化

8.7 動作モードの設定

スパニングツリーの動作モードは以下があります。

- **STP モード**– 装置のすべてのポートは STP BPDU を送信します。ポートの対向装置が STP のみをサポートしている場合、このモードを選択します。

- **RSTP モード**– 装置のすべてのポートは RSTP BPDU を送信します。対向装置から STP BPDU を受信した場合、ポートは自動で STP モードに遷移します。対向装置から MSTP BPDU を受信した場合、ポートは MSTP モードに遷移しません。
- **PVST モード**－装置のすべてのポートは PVST BPDU を送信します。各 VLAN はスパニングツリーを維持します。スパニングツリーの容量は PVST が有効なポートと、PVST が有効な VLAN を掛け合わせた数になります。もしネットワークの容量がスパニングツリーの容量を超えるとき、装置の CPU に負荷がかかります。パケット転送が中断され、ネットワークが不安定になります。スパニングツリーの数は最大 128 にしてください。
- **MSTP モード**– 装置のすべてのポートは MSTP BPDU を送信します。対向装置から STP BPDU を受信した場合、ポートは自動で STP モードに遷移します。対向装置から RSTP BPDU を受信した場合、ポートは RSTP モードに遷移しません。

MSTP モードは、RSTP モードと互換性があり、RSTP モードは STP モードと互換性があります。

PVST モードの互換性はポートのリンクタイプに依存します。

- アクセスポートでは、PVST モードはすべての VLAN でほかのスパニングツリーと互換性があります。
- トランクポートあるいはハイブリッドポートでは、PVST モードは、VLAN1 でほかのスパニングツリーと互換性があります。

以下に動作モードの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． 動作モードを設定する	**stp mode** { **mstp** | **pvst** | **rstp** | **stp** }	デフォルト：MSTP

8.8 MST regionの設定

2 つスパニングツリーの装置が物理的に接続され、以下が同じ設定の場合、スパニングツリーの装置は同じ MST region に属します。

- フォーマットセレクタ（デフォルトは 0 で設定不可）
- MST region 名
- MST region revision レベル
- MST region の同一 VLAN-to-instance マッピングエントリ

MST region に関連したパラメータ（特に VLAN-to-instance マッピングテーブル）の設定は、MSTI に新しいスパニングツリーの計算の原因になり、ネットワークトポロジが不安定になる可能性があります。ネットワークトポロジが不安定になる可能性を減らすために、以下のいずれかの設定をしてから MST region の設定を適用してください。

- **active region-configuration** コマンドで MST region 関連のパラメータをアクティブにします。
- スパニングツリーが無効な状態では、**stp global enable** コマンドで MSTP を有効にします。

STP、RSTP、PVST モードでは MST region の設定は適用されません。

以下に MST region の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―

操作	コマンド	補足
2． MST region view に移行する	**stp region-configuration**	―
3． MST region 名を設定する	**region-name** *name*	デフォルト：装置のMACアドレス
4． VLAN-to-instanceマッピングテーブルを作成する	• **instance** *instance-id* **vlan** *vlan-id-list* • **vlan-mapping modulo** *modulo*	どちらかの設定を使用します。 デフォルト：全VLANがCIST（あるいはMSTI 0）にマッピングされています。
5． MST region の MSTP Revision レベルを設定する	**revision-level** *level*	デフォルト：0
6． （オプション設定項目）MST Region の設定がアクティブ化されていないことを表示する	**check region-configuration**	―
7． 手動で MST Region の設定を有効にする	**active region-configuration**	―

8.9 RootブリッジとSecondary Rootブリッジの設定

MSTP は、MSTP 計算でスパニングツリーの Root ブリッジを指定できます。あるいは、Root ブリッジあるいは Secondary Root ブリッジとして装置を指定することができます。

装置は、異なるスパニングツリーと独立しています。あるスパニングツリーの Root ブリッジや Secondary Root ブリッジは、別のスパニングツリーの Root ブリッジや Secondary Root ブリッジにすることができます。しかし 1 つの装置を同じスパニングツリーの Root ブリッジや Secondary Root ブリッジにすることはできません。

スパニングツリーは 1 つの Root ブリッジのみ持ちます。もし同一時間に、スパニングツリーで複数の Root ブリッジが選択された場合、もっとも小さい MAC アドレスの装置が選択されます。

インスタンスの Root ブリッジが故障あるいはシャットダウンしたとき、以下のようになります。

- 1 つの Secondary Root ブリッジのみが指定されている場合、Root ブリッジになります。
- インスタンスに複数の Secondary Root ブリッジを指定していた場合、MSTP が MAC アドレスのもっとも小さい Secondary Root ブリッジを新しい Root ブリッジに指定します。
- Secondary Root ブリッジが指定されていない場合、新しい Root ブリッジを選出します。

装置のプライオリティの設定に関係なく、各スパニングツリーに 1 つの Root ブリッジを指定することができます。装置を Root ブリッジあるいは Secondary Root ブリッジに指定した後は、装置のプライオリティを変更することはできません。

装置のプライオリティを 0 に設定し、Root ブリッジに指定することもできます。装置のプライオリティの設定につきましては、オペレーションマニュアルのセクション 3 *アクセス "STP"の" ブリッジプライオリティの設定"*を参照してください。

8.9.1 Root ブリッジの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． Root ブリッジを設定する	• STP/RSTPモード： **stp root primary** • PVSTモード： **stp vlan** *vlan-id-list* **root primary** • MSTPモード： **stp** [**instance** *instance-list*] **root primary**	デフォルト：Rootブリッジとして機能しません。

8.9.2 Secondary Root ブリッジの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． Secondary Root ブリッジを設定する	• STP/RSTPモード： **stp root secondary** • PVSTモード： **stp vlan** *vlan-id-list* **root secondary** • MSTPモード： **stp** [**instance** *instance-list*] **root secondary**	デフォルト：Secondary Root ブリッジとして機能しません。

8.10 ブリッジプライオリティの設定

スパニングツリーでは、ブリッジプライオリティのパラメータを用いて、Root ブリッジを決定します。この際に使用するブリッジプライオリティの値を、以下のコマンドを使用して設定します。もっとも小さい値のブリッジプライオリティを設定することで、その装置を Root ブリッジにすることができます。異なるスパニングツリーには異なるブリッジプライオリティを設定することができます。

Root ブリッジの選出とき、スパニングツリーのすべての装置が、同じプライオリティの値である場合、もっとも小さい MAC アドレスの装置が Root ブリッジとして選択されます。Root ブリッジもしくは Secondary Root ブリッジを指定した後に、装置のブリッジプライオリティを変更することはできません。

以下に指定された MSTI のブリッジプライオリティの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー

操作	コマンド	補足
2． ブリッジプライオリティを設定する	● STP/RSTPモード： **stp priority** *priority* ● PVSTモード： **stp vlan** *vlan-id-list* **priority** *priority* ● MSTPモード： **stp** [**instance** *instance-list*] **priority** *priority*	デフォルト：32768

8.11 MST regionの最大ホップ数の設定

MST Region における最大ホップ数は、MST Region の最大範囲を制限するために使用します。

regional Root ブリッジによって送信された Configuration BPDU は最大値に設定されたホップカウントがあります。装置が Configuration BPDU を受信した場合、ホップカウントを 1 ずつマイナスします。転送される BPDU に新しいホップカウントを使用します。装置が BPDU のホップカウントが 0 の Configuration BPDU を受信した場合、装置は Configuration BPDU 廃棄します。最大ホップを超過する装置はスパニングツリーの計算を行うことができないため、MST region のサイズは制限されます。

この設定は Root ブリッジのみ設定できます。MST region 内にあるほかのすべての装置は、Root ブリッジで設定された値を使用します。

STP ネットワークサイズにもとづいて、MST Region の最大ホップ数を設定することができます。ルートブリッジの最大ホップ数の設定は、Edge ポートの最大ホップ数よりも大きい値にすることを推奨します。

以下に MST region の最大ホップ数の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． MST Region の最大ホップ数を設定する	**stp max-hops** *hops*	デフォルト：20

8.12 ネットワークダイアメータの設定

ネットワークにおける任意の 2 台の装置を結ぶもっとも遠いパス上にある装置の数を、ネットワークの大きさを示す 1 つの指標として設定します。ネットワークダイアメータが大きいと、ネットワークが大きいことを示します。

ネットワークダイアメータの設定に従って、装置は MSTP の Hello 時間、転送遅延、最大エージング時間を適切な値に自動的に設定します。

STP、RSTP、MSTP モードでは、以下のようになります。

- 各 MST region は装置とみなされます。
- 設定したネットワークダイアメータは、CIST（あるいは Root ブリッジ）でのみ有効で、MSTI では無効です。

PVST モードでは、設定されたネットワークダイアメータは指定された VLAN の Root ブリッジでのみ有効です。

以下にネットワークダイアメータの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． ネットワークダイアメータを設定する	● STP/RSTP/MSTPモード： **stp bridge-diameter** *diameter* ● PVSTモード： **stp vlan** *vlan-id-list* **bridge-diameter** *diameter*	デフォルト：7

8.13 スパニングツリータイマの設定

設定可能なスパニングツリー関連タイマには、以下のタイマがあります。

- **Forward delay**– ポートが状態遷移に要する時間です。ネットワークで一時的なループの発生を防ぐため、スパニングツリーは discarding 状態から Forwarding 状態に遷移する前に、中間状態（Learning 状態）に設定します。また Forward delay が終了したのち、ポートが Forwarding 状態に遷移するように要求します。これにより対向先とローカルポートの状態が同期化されることを保証します。
- **Hello 時間**– リンク障害等を検出するために、Hello 時間に設定された間隔で Configuration BPDU（Hello パケット）を定期的に送信します。
- タイムアウト時間以内に Configuration BPDU を受信しない場合、スパニングツリーを再計算します。タイムアウト期間の式は以下となります。

  タイムアウト時間＝タイムアウトファクタ × 3 × Hello 時間
- **Max age**– MSTP ネットワークの CIST で、装置の Configuration BPDU が時間切れになっていないかどうかを判断するのに使うパラメータです。最大有効時間を越えた Configuration BPDU は破棄されます。時間切れになった場合、新しくスパニングツリーの計算を行います。最大エージング時間は MSTI に影響しません。

スパニングツリーの状態変更が頻繁に発生するのを回避するには、Hello 時間、Forward Delay、最大エージング時間の設定を次式に満足するよう設定してください。

- 2 ×（Forward delay － 1 秒）≧ Max age
- Max age ≧ 2 ×（Hello 時間 ＋ 1 秒）

スパニングツリーのタイマは手動ではなく自動で設定することを推奨します。ネットワークダイアメータの設定にもとづいて、自動的に計算します。ネットワークダイアメータがデフォルトである場合、スパニングツリーのタイマはデフォルト値となります。

Root ブリッジに設定されるタイマは、ネットワーク全体のすべての装置で適用されます。

I. 制限とガイドライン

- ネットワークのダイアメータに応じて、Forward Delay の設定値は変更します。一般的に、ネットワークのダイアメータが大きい程、転送遅延は長く設定してください。転送遅延を極端に短く設定すると一時的に冗長パスが発生してしまい、転送遅延を極端に長くするとネットワーク接続が再開するまでの時間が長くなります。よって、一般的なネットワークにおいては、デフォルト値で使用することを推奨します。
- Hello 時間を適切に設定するとで、リンク障害等を適切に検出しリンクの切り替えを行えます。Hello 時間を極端に短く設定すると、消費されるネットワークリソースが

増えると共に装置での処理も大きくなります。また Hello 時間を極端に長く設定すると、リンク上でパケットロスが発生すると、装置はそれをリンク障害と認識するためスパニングツリーの再構築が発生してしまいます。よって、一般的なネットワークにおいては、デフォルト値で使用することを推奨します。

- スパニングツリーの段数および構成する装置での処理能力に応じて、最大エージング時間の設定値は変更します。極端に小さい設定を行うと、ネットワークの輻輳発生によってスパニングツリーの再構築が発生する可能性があります。また、極端に大きい設定を行うと、リンク障害を所定の時間内に検出し、スパニングツリーを再構築できなくなります。よって、一般的なネットワークにおいては、デフォルト値で使用することを推奨します。

II. 設定手順

以下にスパニングツリータイマの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． Forward delay タイマを設定する	• STP/RSTP/MSTPモード： **stp timer forward-delay** *time* • PVSTモード： **stp vlan** *vlan-id-list* **timer forward-delay** *time*	デフォルト：15秒
3． Hello 時間を設定する	• STP/RSTP/MSTPモード： **stp timer hello** *time* • PVSTモード： **stp vlan** *vlan-id-list* **timer hello** *time*	デフォルト：2秒
4． Max age タイマを設定する	• STP/RSTP/MSTPモード： **stp timer max-age** *time* • PVSTモード： **stp vlan** *vlan-id-list* **timer max-age** *time*	デフォルト：20秒

8.14 タイムアウトファクタの設定

タイムアウトファクタは、以下の式で表されるタイムアウト時間を決めるために使用されるパラメータです。

タイムアウト時間 ＝ タイムアウトファクタ × 3 × Hello 時間

スパニングツリーの状態が安定しているとき、Root ブリッジでない装置は Hello パケット（Configuration BPDU）を Hello 間隔で下流の装置にリンクの故障を検知するため、転送します。もし通常、Hello タイマの 9 倍の時間、上流の装置から Hello パケットを受信しないと、上流の装置が故障しているとみなし、ネットワークのトポロジの再構築を開始します。

ネットワークの安定性を保つために、タイムアウトファクタを 5、6、7 に設定することを推奨します。

- 予期しないスパニングツリーの再構築を防ぎます。安定したネットワークにおいても、上流の装置の処理能力がビジーのときに、ネットワークのトポロジの再構築が行われる可能性があります。たとえば、多くのレイヤ 2 インタフェースが上流の装置で設定

されているとします。下流の装置がタイムアウト時間内に BPDU の受信に失敗し、予期せずスパニングツリーの再構築が行われます。

- 安定したネットワークでネットワークリソースを削減します。

以下にタイムアウトファクタの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． タイムアウトファクタを設定する	**stp timer-factor** *factor*	デフォルト：3

8.15 BPDU最大送出レートの設定

各 Hello 時間以内にポートが送信できる BPDU の最大数は、BPDU 転送レートと Hello 時間の合計に等しいです。ポートの物理状態とネットワークの構成にもとづいて適切な BPDU 転送レートを設定してください。

BPDU 転送レートを大きくするとは多くのシステムリソースが必要となります。最大 BPDU 転送レートを適切に設定することにより、ポートが BPDU を送信するスピードを制限し、ネットワークトポロジが変更した際に過剰な帯域リソースを使用しないようにできます。デフォルト値を使うことを推奨します。

以下に BPDU 最大送出レートの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． Ethernet interface view あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	―
3． BPDU 最大送出レートを設定する	**stp transmit-limit** *limit*	デフォルト：10

8.16 Edgeポートの設定

Edge ポートとは、ほかの Ethernet スイッチや共有ネットワークセグメントに接続されず、ユーザ端末等に直接接続しているポートを示します。ネットワークトポロジが変化した場合、Edge ポートは一時的なループを起こしません。装置はポートが端末に直接接続されているかどうかを認識しないため、Edge ポートを手動で設定する必要があります。Edge ポートと設定することによって、接続装置が STP をサポートしていない場合には、ポートがリンクアップすると即座に Forwarding 状態に遷移させることができます。

I. 制限とガイドライン

- BPDU ガード機能が無効であるとき、Edge ポートが別のポートから BPDU を受信した場合、Edge ポートは非 Edge ポートになります。Edge ポートに戻す場合、再度有効化を行う必要があります。
- ポートがユーザ端末に接続されている場合、Edge ポートとして設定し、BPDU ガードを有効にします。この機能によってネットワークのセキュリティを保持しながら Forwarding 状態を早急に収束させることができます。

- ループガード、Edge ポートの機能を、ポートに同時に設定することはできません。

II. 設定手順

以下に Edge ポートの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Ethernet あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	―
3. Edge ポートを設定する	**stp edged-port**	デフォルト : すべてのポートは非エッジポートです。

8.17 ポートパスコストの設定

パスコストは、ポートに接続するリンクの速度に関係するパラメータです。MSTP 対応の装置では、ポートは MSTI ごとに異なるパスコストを持つことができます。パスコストを適切に設定することで、VLAN トラフィックフローが別々の物理リンクで転送されるので、VLAN ごとの負荷分散が可能です。

装置は自動的にデフォルトのパスコストを計算でき、一方でユーザはポートのパスコストを設定できます。

8.17.1 デフォルトパスコストの計算時の基準指定

⚠ **注意**：
装置がデフォルトパスコストを計算する際に使用する基準を変更した際は、デフォルトにパスコストを戻してください。

ポートパスコストのデフォルト値には以下のモードがあります。設定の標準から選択できます。

- **dot1d-1998**– IEEE 802.1d-1998 で規定されているポートパスコストの対応値を使用します。
- **dot1t**– IEEE 802.1t で規定されているポートパスコストの対応値を使用します。
- **legacy**– QX シリーズ独自のポートパスコストの対応値を使用します。

デフォルトのパスコストを計算する際に、基準を設定する場合、以下のガイドラインに従ってください。

- アグリゲーションリンクのパスコストの計算は、IEEE 802.1d-1998 の場合、アグリゲーションリンクのポートの数を考慮しません。IEEE 802.1t は、アグリゲーションリンクのポートの数を考慮にします。計算式は、パスコスト＝ 200,000,000/リンク速度（100kbps 単位）で、リンク速度はアグリゲーションリンクがブロックされていないポートのリンク速度の合計です。
- IEEE 802.1d-1998 あるいは QX シリーズ独自の基準は、ポートあるいはインタフェースのリンク速度が 10Gbps を超えたとき、単一ポートあるいはアグリゲートインタ

フェースに設定可能なもっとも小さい値を指定してください。この基準にもとづいて転送するパスは、最適なパスにならない可能性があります。この問題に対応するため、以下のいずれかを行ってください。

- □ デフォルトパスコスト計算の基準として、**dot1t** を使用します。
- □ ポートのパスコストを手動で設定します。（オペレーションマニュアルのセクション 3 *アクセス "STP"の"パスコストの設定"*を参照してください。）

以下にデフォルトパスコストを計算するときに装置に使用する基準を指定する方法を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． パスコストの計算基準を設定する	**stp pathcost-standard** { **dot1d-1998** | **dot1t** | **legacy** }	デフォルト：**legacy**

表 8-7 リンク速度とパスコスト間のマッピング

リンク速度	ポートタイプ	パスコスト		
		IEEE 802.1d-1998	IEEE 802.1t	QX シリーズ独自
0	―	65535	200000000	200000
10 Mbps	単一ポート	100	2000000	2000
	集約リンク2ポート		1000000	1800
	集約リンク3ポート		666666	1600
	集約リンク4ポート		500000	1400
100 Mbps	単一ポート	19	200000	200
	集約リンク2ポート		100000	180
	集約リンク3ポート		66666	160
	集約リンク4ポート		50000	140
1000 Mbps	単一ポート	4	20000	20
	集約リンク2ポート		10000	18
	集約リンク3ポート		6666	16
	集約リンク4ポート		5000	14
10 Gbps	単一ポート	2	2000	2
	集約リンク2ポート		1000	1
	集約リンク3ポート		666	1
	集約リンク4ポート		500	1
20 Gbps	単一ポート	1	1000	1
	集約リンク2ポート		500	1
	集約リンク3ポート		333	1
	集約リンク4ポート		250	1
40 Gbps	単一ポート	1	500	1
	集約リンク2ポート		250	1
	集約リンク3ポート		166	1
	集約リンク4ポート		125	1
100 Gbps	単一ポート	1	200	1
	集約リンク2ポート		100	1
	集約リンク3ポート		66	1
	集約リンク4ポート		50	1

8.17.2 ポートのパスコストの設定

ポートのパスコストを変更したとき、ポートの役割を再計算し、状態遷移を初期化します。

以下にポートのパスコストの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． Ethernet あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	―
3． パスコストを設定する	● STP/RSTPモード： **stp cost** *cost* ● PVSTモード： **stp vlan** *vlan-id-list* **cost** *cost* ● MSTPモード： **stp** [**instance** *instance-list*] **cost** *cost*	デフォルト：システムがパスコストを自動計算します。

8.17.3 設定例

MSTP モードで、以下の設定をします。

- IEEE 802.1d-1998 の計算基準を使用します。
- MSTI 2 の GigabitEthernet 1/0/3 のパスコストを 200 に設定します。

```
<Switch> system-view
[Switch] stp pathcost-standard dot1d-1998
Cost of every port will be reset and automatically re-calculated after you change
the current pathcost standard. Continue?[Y/N]:y
Cost of every port has been re-calculated.
[Switch] interface gigabitethernet 1/0/3
[Switch-GigabitEthernet1/0/3] stp instance 2 cost 200
```

PVST モードで以下を設定します。

- IEEE 802.1d-1998 の計算基準を使用します。
- VLAN20～VLAN30 の GigabitEthernet 1/0/3 のパスコストを 2000 に設定します。

```
<Switch> system-view
[Switch] stp pathcost-standard dot1d-1998
Cost of every port will be reset and automatically re-calculated after you change
the current pathcost standard. Continue?[Y/N]:y
Cost of every port has been re-calculated
[Switch] interface gigabitethernet 1/0/3
[Switch-GigabitEthernet1/0/3] stp vlan 20 to 30 cost 2000
```

8.18 ポートプライオリティの設定

Root ポートを選出する際、ポートのポートプライオリティが重要な役割を果たします。ほかのパラメータが同じ場合、ポートプライオリティの高いポート（ポートプライオリティ値が小さいポート）が Root ポートに選出されます。

スパニングツリーでは異なるパスごとに異なるポートプライオリティを設定でき、スパニングツリーごとに役割を指定できます。そのため、VLAN 単位で異なる物理ポートを介してデータを流すことができるため、VLAN ベースで負荷分散が可能となります。正確なネットワーク要件にもとづいてポートプライオリティを設定することができます。

ポートのプライオリティを変更したとき、システムはポートの役割を再計算し、状態遷移を開始します。

以下にポートプライオリティの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Ethernet interface view あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	―
3. ポート priority を設定する	• STP/RSTPモード： **stp port priority** *priority* • PVSTモード： **stp vlan** *vlan-id-list* **port priority** *priority* • MSTPモード： **stp** [**instance** *instance-list*] **port priority** *priority*	デフォルト：128

8.19 Point-to-Pointリンクの設定

Point-to-Point リンクは、2 台の装置を直結するリンクです。2 つの Root ポートや Designated ポートが Point-to-Point リンクである場合、そのリンクの両端に Point-to-Point リンクと設定することで、ポート間で同期のためのパケットを使用して、即座に Forwarding 状態に遷移させることができます。

I. 制限とガイドライン

- リンクアグリゲーションを設定している場合や全 2 重モードを設定している場合、Point-to-Point リンクとして設定することができます。NEC ではデフォルトの設定を使用し、リンクタイプを自動的に設定した値とすることを推奨します。
- MSTP あるいは PVST モードのポートに **stp point-to-point force-false** コマンドあるいは **stp point-to-point force-true** コマンドを設定した場合、設定はすべての VLAN あるいは MSTI に適用されます。
- 実際には Point-to-Point でないポートに対して、Point-to-Point の設定を行うと、一時的にループが発生する可能性がありますので、注意してください。

II. 設定手順

以下に Point-to-Point リンクの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Ethernet あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	―
3. Point-to-Point リンクを設定する	**stp point-to-point** { **auto** | **force-false** | **force-true** }	デフォルト：**auto** autoではポートが自動的にリンクタイプを決定します。

8.20 MSTPパケットのフォーマット設定

ポートは以下のフォーマットで MSTP パケットの送受信を行うことができます。

- **dot1s** – IEEE802.1s で規定された形式です。
- **legacy** – QX シリーズ独自形式（IEEE802.1s ドラフト版で規定された形式）です。対向装置は、QX シリーズの製品のみです。

デフォルトの MSTP のパケットフォーマットは **auto** です。ポートは自動で 2 つの MSTP パケットのフォーマットを区別します。対向装置からの BPDU に合わせて、自動でフォーマットを選択し、送信します

MSTP パケットフォーマットをポートに設定できます。設定後、MSTP モードで動作しているときは、ポートは設定しているフォーマットのパケットのみ送受信し、同じフォーマットのパケットを送信する装置と通信します。

モードのポートはデフォルトで IEEE 802.1s MSTP パケットのみ送信します。ポートが legacy フォーマットの MSTP パケットを受信したときポートは **legacy** フォーマットのパケットのみ送信を行います。これは、ポートがパケットのフォーマットが頻繁に変更することを防ぎます。IEEE 802.1s MSTP パケットを送信するように設定するために、ポートをシャットダウンし、その後、ポートをアップ状態にします。

MSTI 数が 48 を超えたとき、ポートは IEEE 802.1s のみ送信することができます。

以下にポートでサポートされる MSTP パケットフォーマットの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Ethernet あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	―
3. MSTP パケットフォーマットを設定する	**stp compliance** { **auto** | **dot1s** | **legacy** }	デフォルト：**auto**

8.21 ポート遷移状態情報の出力の有効化

大規模なスパニングツリーネットワークでは、MSTI のポート状態の遷移に関する情報を出力できるように設定し、リアルタイムでポート状態をモニタリングできます。

以下にポート状態の遷移に関する情報を出力する設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． ポート遷移状態の情報を出力するように設定を有効にする	• STP/RSTPモード： **stp port-log instance 0** • PVSTモード： **stp port-log vlan** *vlan-id-list* • MSTPモード： **stp port-log** { **all** | **instance** *instance-list* }	デフォルト：無効

8.22 スパニングツリー機能の有効化

ほかのスパニングツリー機能に関連した設定を有効にする前に、装置でスパニングツリー機能を有効化にする必要があります。STP、RSTP、MSTP モードではスパニングツリー機能がグローバルと設定したポートで有効化されることを確認してください。PVST モードではスパニングツリー機能がグローバル、指定した VLAN および設定したポートで有効化されることを確認してください。

ポートでのスパニングツリーの計算と装置の CPU のリソースを節約するため、**undo stp enable** コマンドを使用して、ポートでスパニングツリー機能を無効にすることができます。スパニングツリー機能を無効にしたら、ループが発生していないことを確認してください。

8.22.1 STP/RSTP/MSTP モードでのスパニングツリー機能の有効化

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． スパニングツリー機能を有効にする	**stp global enable**	デフォルト：無効
3． Ethernet interface view あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	―
4． （オプション設定項目）ポートでスパニングツリー機能を有効にする	**stp enable**	デフォルト：すべてのポートで有効

8.22.2 PVST モードでのスパニングツリー機能の有効化

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． スパニングツリー機能を有効にする	**stp global enable**	デフォルト：無効
3． VLAN でスパニングツリー機能を有効にする	**stp vlan** *vlan-id-list* **enable**	デフォルト：すべてのVLANで有効

操作	コマンド	補足
4． Ethernet interface view あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	―
5． ポートでスパニングツリー機能を有効にする	**stp enable**	デフォルト : すべてのポートで有効

8.23 mCheck機能の設定

mCheck 機能はポート状態転送プロセスをユーザが設定できるようにする機能です。

MSTP、MSTP あるいは PVST が動作している装置のポートが STP で動作する装置に接続し STP BPDU を受信した場合、ポートは STP モードに自動的に変更します。しかし以下の場合は、ポートは自動的にもとのモードに戻ることができません。

- 対向の STP 装置がシャットダウンあるいは取り外された場合
- ローカルの装置が変更を検出できない場合

もとのモードで動作するようにポートの設定を強制的に変更するために、mCheck 機能の設定を行うことができます。

たとえば Device A、Device B、Device C が順に接続されています。Device A は STP が動作し、Device B はスパニングツリーが動作しておらず、Device C は RSTP、MSTP あるいは PVST で動作しています。このとき、Device C は、Device B によって透過的に転送された STP BPDU を受信するとき、受信したポートは STP モードに変更します。もし Device B が Device C と RSTP､MSTP あるいは PVST で動作するように設定された場合、Device B と Device C で相互に接続されているポートは mCheck を動作させる必要があります。

8.23.1 制限とガイドライン

mCheck 機能は MSTP、RSTP あるいは PVST モードで動作する装置で適用されます。

8.23.2 グローバルでの mCheck の設定手順

操作	コマンド
1． system view に移行する	**system-view**
2． mCheck を実行する	**stp global mcheck**

8.23.3 interface view での mCheck の実行

操作	コマンド
1． system view に移行する	**system-view**

操作	コマンド
2． Ethernet あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*
3． mCheck を実行する	**stp mcheck**

8.24 矛盾したPVID 保護の無効化

PVST では、接続されている 2 つのポートが異なる PVID を使用している場合、PVST 計算エラーが発生する可能性があります。デフォルトでは、矛盾した PVID 保護は、PVST 計算エラーを回避するために有効になっています。PVID の不一致がポートで検出されると、システムはポートをブロックします。

I. 制限とガイドライン

接続された 2 つのポートで異なる PVID が必要な場合は、ポートをホストする装置で矛盾する PVID 保護を無効にします。PVST 計算エラーを回避するには、次の要件が満たされていることを確認してください。

- ある装置上の VLAN が、別の装置上のピアポートの PVID (デフォルト VLAN を除く) と同じ ID を使用していないことを確認します。
- ローカルポートまたはそのピアがハイブリッドポートである場合は、ローカルポートとピアポートを同じ VLAN のタグ無メンバとして設定しないでください。
- ローカル装置とピア装置の両方で矛盾した PVID 保護を無効にします。

この機能は、装置が PVST モードで動作している場合にだけ有効です。

II. 設定手順

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． 矛盾した PVID 保護機能を無効にする	**stp ignore-pvid-inconsistency**	デフォルト：有効

8.25 Digest Snoopingの設定

注意：

以下に示す状況において、グローバルで Digest Snooping を設定する場合、注意してください。

- VLAN インスタンスマッピングを変更します。
- デフォルトの MST region の設定を復元します。

VLAN インスタンスマッピングが隣り合う装置と異なる場合、ループあるいは通信断が発生します。

IEEE 802.1s で定義されているように、同じ region で接続された装置は、MST region 関連の設定が一致します。MST region 関連の設定は以下が含まれます。

- region 名
- リビジョンレベル
- VLAN インスタンスマッピング

MSTP 対応の装置は、BPDU パケットの Configuration ID をチェックすることで、同じ MST region の装置かを識別します。Configuration ID は、region 名、リビジョンレベル、設定ダイジェスト（16 バイト長、VLAN インスタンスマッピングにもとづく HMAC-MD5 アルゴリズムによる計算結果）で構成されています。

MSTP の実装はベンダによって異なり、プライベートキーを使用して計算する設定ダイジェストも異なります。同じ MST region でも装置を提供するベンダが異なると、互いに通信することができません。

NEC の装置とほかのベンダの装置間で通信を行う場合、同じ MST region で接続するポートで Digest snooping 機能を有効にします。

I. 制限とガイドライン

Digest snooping の設定を行うとき以下のガイドラインに従ってください。

- Digest snooping を有効にする前に、別のベンダの装置がスパニングツリーに接続され、動作していることを確認してください。
- Digest Snooping 機能が有効になっている場合、同じ region（in-the-same-region）チェックに設定ダイジェストの比較は行われないため、関連するポートでは VLAN インスタンスマッピングを同じにしなければなりません。
- Digest snooping 機能を適用するためには、グローバルと設定ポートの両方で Digest snooping 機能を有効にしてください。まず、関連するすべてのポートで Digest snooping 機能を有効にし、それからグローバルでも有効にすることを推奨します。これにより設定がすべてのポートに適用され、ネットワークへの影響を減らすことができます。
- ループを防ぐため、MST region の Edge ポートで Digest snooping を有効にしないでください。
- Digest snooping を有効にした後、スパニングツリー機能を有効にしてください。ネットワークの動作が安定しているときは、トラフィックの中断を避けるため、Digest snooping を有効にしないでください。

II. 設定手順

設定 Digest を計算するために秘密鍵を使用している他ベンダの装置が、NEC の装置に接続されている場合、NEC の装置でのみ Digest snooping の設定を有効にすることができます。

以下に Digest snooping の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Ethernet あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	―
3. インタフェースで Digest Snooping を有効にする	**stp config-digest-snooping**	デフォルト：無効
4. system view から戻る	**quit**	―

操作	コマンド	補足
5． グローバルで Digest Snooping を有効にする	**stp global config-digest-snooping**	デフォルト：無効

8.25.1 Digest Snooping 設定例

I. ネットワーク要件

図 8-16に示すように、Device A、Device B が Device C に接続されています。Device C はほかベンダの装置で、すべての装置は同じ region を使用しています。

3 つの装置が互いに通信できるように、Device C に接続されている Device A、Device B のポートで Digest snooping を有効にします。

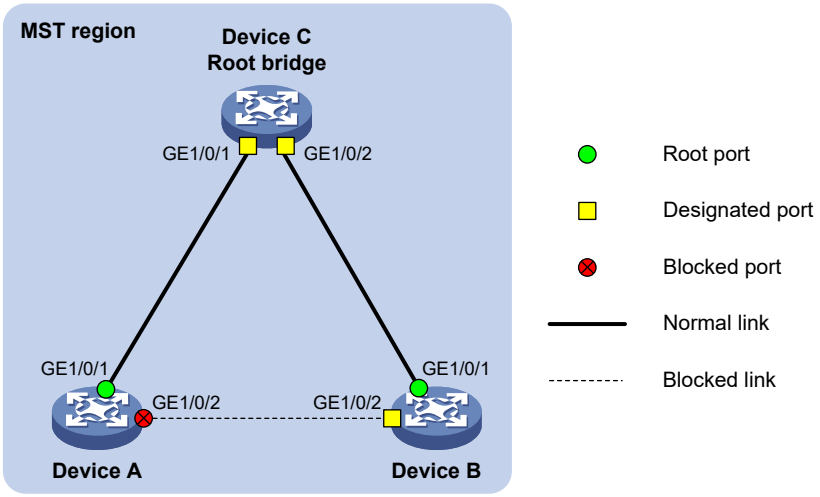


図 8-16 ネットワーク図

II. 設定手順

Device A の GigabitEthernet 1/0/1 で Digest snooping を有効にし、Device A のグローバルで Digest snooping を有効にします。

```
<DeviceA> system-view
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] stp config-digest-snooping
[DeviceA-GigabitEthernet1/0/1] quit
[DeviceA] stp global config-digest-snooping
```

Device B の GigabitEthernet 1/0/1 で Digest snooping を有効にし、Device B のグローバルで Digest snooping を有効にします。

```
<DeviceB> system-view
```

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] stp config-digest-snooping
[DeviceB-GigabitEthernet1/0/1] quit
[DeviceB] stp global config-digest-snooping
```

8.26 No Agreement Checkの設定

RSTP と MSTP の Designated ポートの高速な状態遷移には、2 つのタイプのメッセージが使用されています。

- **Proposal** – Designated ポートから送信される高速遷移リクエスト
- **Agreement** – 高速遷移リクエストの応答（acknowledge）パケット

RSTP、MSTP が動作している装置のポートが下流の装置から、agreement パケットを受信したときにのみ、Designated ポートで高速遷移を実行できます。RSTP 装置と MSTP 装置の相違点は以下のとおりです。

- MSTP 装置は、下流装置の Root ポートが上流の装置から agreement パケットを受信した後にのみ、agreement パケットを送信します。
- RSTP 装置は、下流装置の Root ポートが上流の装置から agreement パケットを受信したかに関わらず、agreement パケットを送信します。

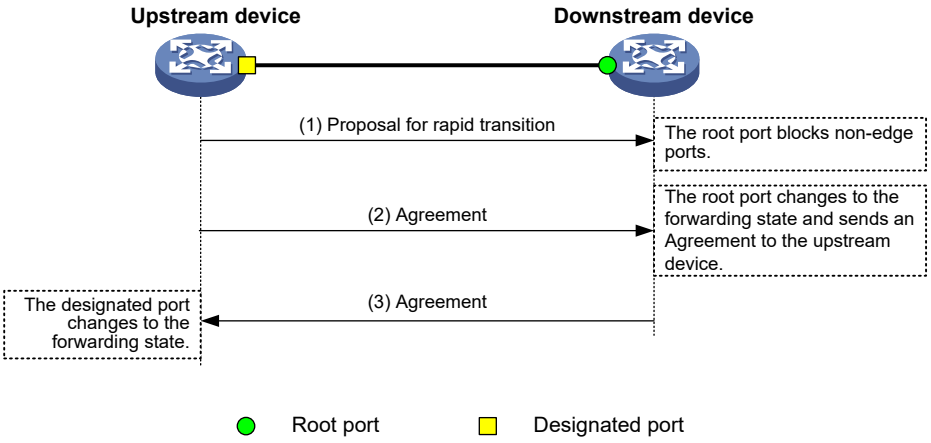


図 8-17 MSTP の Designated ポートの高速状態遷移のメカニズム

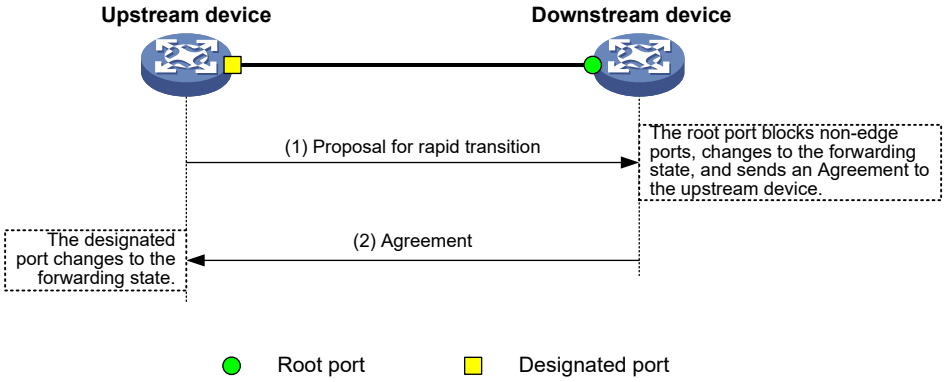


図 8-18 RSTP の Designated ポートの高速状態遷移のメカニズム

上流装置がほかベンダの装置である場合、高速状態遷移の実行が以下のように制限される可能性があります。

- 上流装置が RSTP と類似の高速遷移メカニズムを使用します。
- 下流装置が MSTP を使用し、RSTP モードをサポートしません。

この場合、以下の事象が発生します。

1) 下流装置の Root ポートは上流装置から agreement パケットを受信しません。
2) 上流装置に no agreement パケットを送信します。

その結果、上流装置の Designated ポートは 2 回分の転送遅延の後、Forwarding 状態に遷移します。

このような場合に下流装置のポートで No Agreement Check 機能を有効にすることで、高速状態遷移を実行できます。

I. 設定要件

No Agreement Check 機能を設定する前に、以下の作業を行う必要があります。

- 装置は、スパニングツリーに対応している他ベンダの装置と point-to-point リンクによって接続しています。
- 2 台の装置に同じ region 名、リビジョンレベル、VLAN インスタンスマッピングを設定し、同じ region に所属させます。

II. 設定手順

Root ポートで No Agreement Check 機能を有効にすることができます。

以下に No Agreement Check の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. Ethernet interface view あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	—
3. No Agreement Check 機能を有効にする	**stp no-agreement-check**	デフォルト：無効

8.26.1 No Agreement Check 設定例

I. ネットワーク要件

図 8-19に示すように、以下の要件に従います。

- Device A は、同じ region に属し、異なる MSTP を実装した他ベンダの装置に接続しています。
- ほかのベンダの装置（Device B）は Regional Root ブリッジで、Device A は下流装置です。

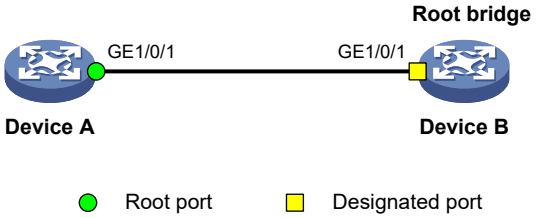


図 8-19 ネットワーク図

II. 設定手順

Device A の GigabitEthernet 1/0/1 で、No Agreement Check 機能を有効にします。

```
<DeviceA> system-view
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] stp no-agreement-check
```

8.27 TC snoopingの設定

図 8-20に示すように、IRF スタックユニットは 2 重のポートで 2 つのユーザネットワークに接続します。

以下の要件に従います。

- Device A と Device B は、IRF スタックを構成します。
- スパニングツリー機能は、Device A と Device B では無効にし、ユーザネットワーク 1 とユーザネットワーク 2 のすべての装置では有効にします。
- IRF スタックユニットはユーザネットワークにスパニングツリーの計算をせずに BPDU を送信します。

ネットワーク構成に変更が生じると、IRF スタックユニットは MAC アドレステーブルと ARP テーブルを更新するのに時間を要します。この間、ネットワークの通信断が発生します。

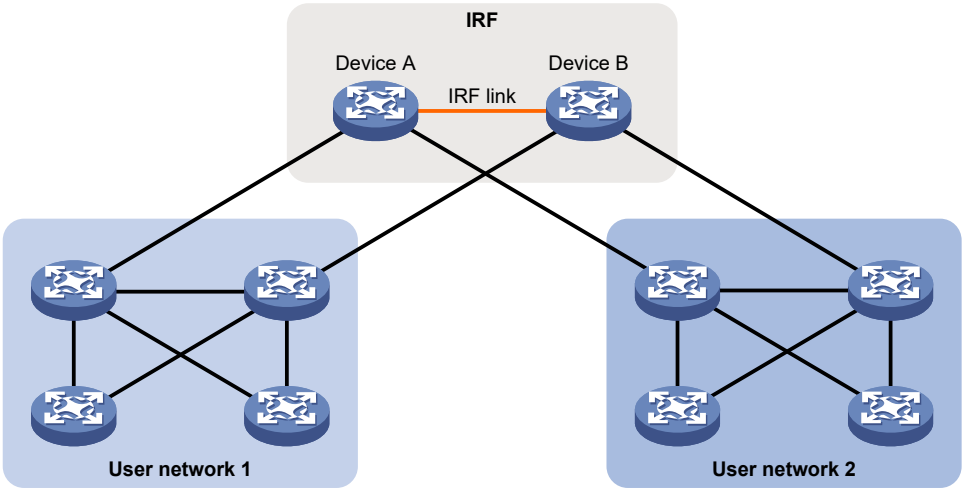


図 8-20 TC snooping ネットワーク

トラフィックの中断を防ぐため、IRF スタックユニットに TC snooping を設定することができます。ポートから TC-BPDU を受信したのち、IRF スタックユニットはポートの VLAN に関連する MAC アドレステーブルと ARP テーブルのエントリを更新します。こうして、TC snooping はネットワーク構成の変更からネットワーク内の通信断を避けることができます。ARP テーブルの詳細は、オペレーションマニュアルのセクション 4 *IP サービス* "*ARP*"を参照してください。

I. 制限とガイドライン

TC snooping の設定を行うとき以下のガイドラインに従ってください。

- TC snooping とスパニングツリー機能を同時に設定できません。TC snooping 機能を有効化する前に、グローバルでスパニングツリー機能を無効にしてください。
- TC snooping は PVST モードではサポートしておりません。

II. 設定手順

以下に TC snooping の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. スパニングツリー機能を無効にする	**undo stp global enable**	デフォルト：無効
3. TC snooping 機能を有効にする	**stp tc-snooping**	デフォルト：無効

8.28 保護機能の設定

スパニングツリーの装置は以下の保護機能をサポートしています。

- BPDU ガード
- Root ガード
- Loop ガード

- ポート役割の制限機能
- TC-BPDU ガード
- BPDU ドロップ機能
- PVST BPDU ガード

8.28.1 BPDU ガードの有効化

アクセスポートは通常、ユーザ端末（PC など）やファイルサーバに直接接続されており、高速な遷移を実現するために、Edge ポートに設定されています。こうしたポートで BPDU パケットを受信すると、装置はそのポートを自動的に非 Edge ポートにし、スパニングツリーの再計算を開始します。その結果、ネットワーク全体でトポロジ変更が発生する可能性があります。通常の状況下ではこれらのポートは Configuration BPDU を受信すべきではありません。しかし不正な装置への攻撃によって Configuration BPDU を偽造した場合、ネットワークは不安定となります。

この点を狙った悪意のあるユーザの攻撃を防止するための機能として、BPDU ガード機能をサポートします。BPDU ガード機能を設定することで、Edge ポートに設定しているポートで Configuration BPDU パケットを受信すると、装置は以下の操作をします。

- そのポートを shutdown 状態にします。
- NMS に shutdown 状態であることを通知します。

装置は検出の間隔後に、shutdown 状態のポートの解除を行います。検出の間隔は **shutdown-interval** コマンドを使用して設定することができます。
検出の間隔についての詳細は、オペレーションマニュアルのセクション 1 *はじめに* "*装置管理*"を参照してください。

BPDU ガードは、グローバルあるいは Edge ポートで設定します。

loopback test が設定されたポートでは、BPDU ガードを有効にすることができません。loopback test についての詳細は、オペレーションマニュアルのセクション 3 *アクセス* "*Ethernet インタフェース*"を参照してください。

I. グローバルでの BPDU ガードの有効化

グローバルでの BPDU ガードの設定はすべての Edge ポートで適用されます。

以下に BPDU ガードの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. BPDU ガードを有効にする	**stp bpdu-protection**	デフォルト：無効

II. インタフェースでの BPDU ガードの有効化

Edge ポートはインタフェースで設定された BPDU ガードを優先します。インタフェースで BPDU ガードの設定が行われていない場合、グローバルでの BPDU ガードの設定が適用されます。

以下にインタフェースでの BPDU ガードの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． Ethernet interface view あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	―
3． BPDU ガードを有効にする	**stp port bpdu-protection** { **enable** | **disable** }	edgeポートに設定されていません。インタフェースのBPDUガード機能の状態はグローバルでのBPDUガード機能と同一です。

8.28.2 Root ガードの有効化

スパニングツリーの Root ブリッジと Secondary Root ブリッジは、同一 MST region に割り当てられることを推奨します。特に CIST では、Root ブリッジと Secondary Root ブリッジは、ネットワーク設計で、高帯域幅を持つ領域に配置されます。しかし設定ミスや攻撃により、不正な装置がより高い優先度を持った Configuration BPDU を配信すると、本来意図されるスパニングツリーのトポロジが構成されないだけでなく、ネットワークトポロジの変更が多発します。トラフィックが高帯域幅のリンクから低帯域幅のリンクに切り替えられてしまい、ネットワークを安定して使用できなくなります。

この状況を防止するための機能として、Root ガードをサポートします。もし Root ガードが Root ブリッジのポートで有効である場合、ポートはすべてのポートの Designated ポートの役割を実行します。MSTI から高い優先度の Configuration BPDU を受信した後、以下の操作を行います。

- すぐさま MSTI の Listening 状態にポートを切り替えます。
- 受信した Configuration BPDU を転送しません。

もしポートが 2 倍の Forward delay 内に高い優先度の BPDU を受信しない場合、もとの状態に戻ります。

ポートで Loop ガード、Root ガードの設定を同時に設定することができません。

Root ガードは、Designated ポートで設定します。

以下に Root ガードの設定を示します。

操作	コマンド	補足
4． system view に移行する	**system-view**	―
5． Ethernet interface view あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	―
6． Root ガードを有効にする	**stp root-protection**	デフォルト：無効

8.28.3 Loop ガードの有効化

上流の装置から BPDU を受信し続けることによって、Root ポートと Blocking ポートの状態を維持することができます。対向装置での障害もしくはリンク障害が発生すると、ポー

トは上流の装置から BPDU を受信できなくなる可能性があります。この場合、装置はポートの状態を以下のように変更します。

- 上流の BPDU の受信に失敗した Forwarding 状態のポートは Designated ポートになります。
- Blocked ポートは Forwarding 状態に遷移します。

この結果、スイッチネットワークでリンクループが発生します。Loop ガード機能はこのループを防止します。

Loop ガード機能を有効にすると、Loop ガード機能が有効なポートは初期状態で MSTI ごとに廃棄します。ポートが BPDU を受信し、正常状態になっても、そのポートを Designated ポートとして Forwarding 状態に遷移しません。Blocking 状態でパケットを転送しないため、一時的なリンクのループを回避できます。

ユーザの端末を接続したポートで Loop ガードを有効にしないでください。BPDU を受信できないため、すべての MSTI で discard 状態になったままとなります。

ポートの Loop ガード機能は Root ガード機能あるいは Edge ポートの設定を同時に設定することはできません。

装置の Root ポートと、Alternate ポートで Loop ガードを設定します。

以下に Loop ガードの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Ethernet interface view あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	―
3. Loop ガードを有効にする	**stp loop-protection**	デフォルト：無効

8.28.4 ポート役割の制限機能

注意：

この機能を使用することで、スパニングツリーのトポロジの接続に影響する可能性がありますので、注意して設定してください。

ユーザアクセスネットワークの装置のブリッジ ID を変更すると、コアネットワークのスパニングツリーのトポロジが変更する可能性があります。この問題を回避するため、ポート役割の制限機能を有効にすることができます。この機能を有効にすることで、ポートが上位の BPDU を受信したとき、ルートポートではなく Alternate ポートになります。

この機能はユーザアクセスネットワークに接続するポートに設定してください。

以下にポート役割の制限機能の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―

操作	コマンド	補足
2． Ethernet interface view あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	―
3． ポート役割の制限機能を有効にする	**stp role-restriction**	デフォルト：無効

8.28.5 TC-BPDU ガードの有効化

装置はトポロジ変更（TC）の BPDU（BPDU はトポロジ変更を装置に通知します）パケットを受信すると、MAC アドレステーブルのエントリを削除します。しかし、悪意のユーザから偽装した TC-BPDU パケットの攻撃を受けた場合、装置は非常に短い時間内に大量の TC-BPDU パケットを受信することになります。頻繁に削除オペレーション（MAC アドレステーブルの更新）を実行すると、装置のリソースを浪費し、ネットワークの安定性に大きな被害をもたらす可能性があります。

TC-BPDU ガードを有効にすると、最初に TC-BPDU を受信した後、指定時間内（10 秒）の間に、転送アドレスエントリを即座に削除する最大数を設定することができます。TC-BPDU を制限以上受信した場合、装置は、一定の期間の満了後に、転送アドレスエントリを削除します。これにより、頻繁に転送アドレスエントリの削除オペレーションを行うことを防ぐことができます。NEC は TC-BPDU ガードを有効にすることを推奨します。

以下に TC-BPDU ガードの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． TC-BPDU ガードを有効にする	**stp tc-protection**	デフォルト：有効 無効にすることを推奨しません。
3． （オプション設定項目）10 秒ごとに、装置が即座に転送アドレスエントリを削除する最大の回数を設定する	**stp tc-protection threshold** *number*	デフォルト：6

8.28.6 BPDU ドロップ機能の有効化

I. BPDU ドロップ機能

スパニングツリーネットワークにおいて、装置に到着した各 BPDU は、STP 計算プロセスを行い、ネットワークのほかの装置に転送を行います。偽の攻撃者が捏造した BPDU をネットワークに攻撃する脆弱性を使用する可能性があります。捏造された BPDU を連続して送信することにより、ネットワークのすべての装置が STP の計算を計算し続けることになり、結果として CPU が過負荷になるような問題によって、BPDU プロトコルの状態エラーが発生します。

この問題を回避するため、ポートで BPDU ドロップ機能を有効にします。BPDU ドロップ機能が有効になったポートでは、BPDU の受信を行わず、BPDU 攻撃による影響を受けません。

II. 制限とガイドライン

この機能を使用することで、装置は以下の BPDU パケットをドロップします。

- EOAM
- GVRP
- LACP
- LLDP
- PVST
- STP（STP、RSTP、MSTP を含みます）

III. 設定手順

以下に BPDU ドロップ機能の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. Ethernet interface view に移行する	**interface** *interface-type interface-number*	—
3. BPDU ドロップ機能を設定する	**bpdu-drop any**	デフォルト：無効

8.28.7 PVST BPDU ガード機能の有効化

MSTP が有効な装置は PVST BPDU を認識できないため、データトラフィックとして PVST BPDU を転送します。別の独立したネットワークにある PVST が有効な装置で PVST BPDU を受信した場合、PVST の計算に失敗する可能性があります。PVST の計算を失敗させないため、MSTP が有効な装置で PVST BPDU ガード機能を有効にします。ポートで PVST BPDU を受信した場合、装置はポートをシャットダウンします。

以下に PVST BPDU ガード機能の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. PVST BPDU ガード機能を有効にする	**stp pvst-bpdu-protection**	デフォルト：無効

8.28.8 dispute ガードの無効化

I. dispute ガード

片方向リンク障害により、Dispute ガードが開始します。上流ポートが、片方向リンク障害のために、下流の designated ポートから下位の BPDU を forwarding または learning 状態に受信すると、ループが表示されます。Dispute ガードは、上流の designated ポートをブロックしてループを防止します。

図 8-21に示すように、通常の状態ではスパニングツリーの計算結果は次のようになります。

- Device A はルートブリッジで、Port A1 は指定ポートです。
- Port B1 がブロックされます。

Port A1 と Port B1 の間のリンクが Port A1 から Port B1 の方向に障害が発生し、片方向になると、次のイベントが発生します。

1) Port A1 は BPDU のみを受信でき、BPDU を Port B1 に送信できません。
2) Port B1 は、一定期間 Port A1 から BPDU を受信しません。
3) Device B は、自身を root ブリッジとして決定します。
4) Port B1 は BPDU を Port A1 に送信します。
5) Port A1 は、受信した BPDU が自身の BPDU より下位であることを判断します。Dispute が検出されます。
6) Dispute ガードを開始し、Port A1 を起動してブロックし、ループを防止します。

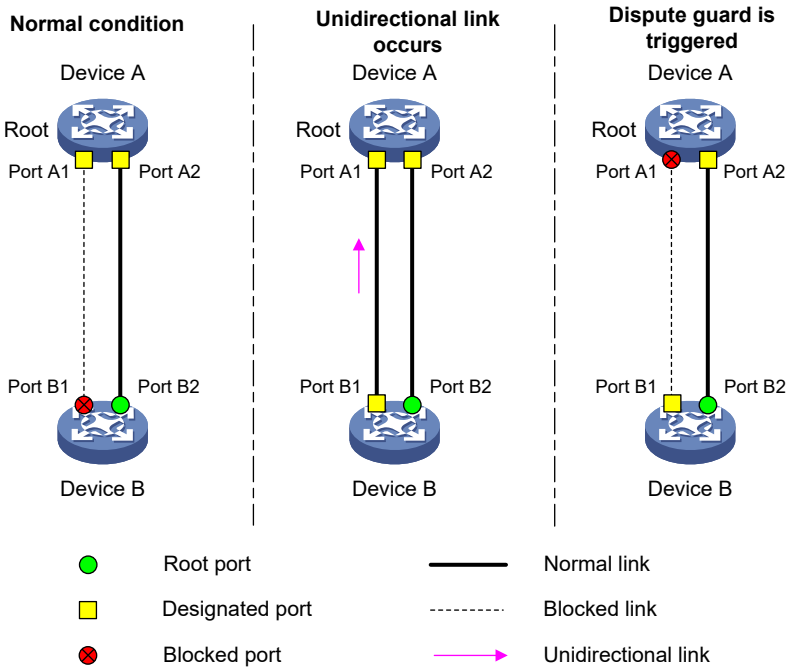


図 8-21 Dispute ガードの開始シナリオ

しかし、Dispute ガードはネットワーク接続を妨害する可能性があります。 VLAN ネットワークでの接続損失を回避するために、Dispute ガードを無効にできます。図 8-22に示すようにスパニングツリー機能は Device B 上で無効にされます。スパニングツリー機能は Device A および Device C で有効になっているため、BPDU をトランスペアレントに送信します。

Device C の Port B1 は VLAN1 のパケットを拒否するように構成されているため、Device C は Device A から VLAN1 の優れた BPDU を受信できません。Device C は、一定期間後に Root ブリッジとして自身を決定します。次に、Port C1 は、VLAN 100 の下位の BPDU を Device A に送信します。

Device A が下位の BPDU を受信すると、Dispute ガードは Port A1 をブロックし、トラフィックの中断を引き起こします。サービス継続性を確保するために、Device A の Dispute ガードを無効にして、リンクがブロックされないようにすることができます。

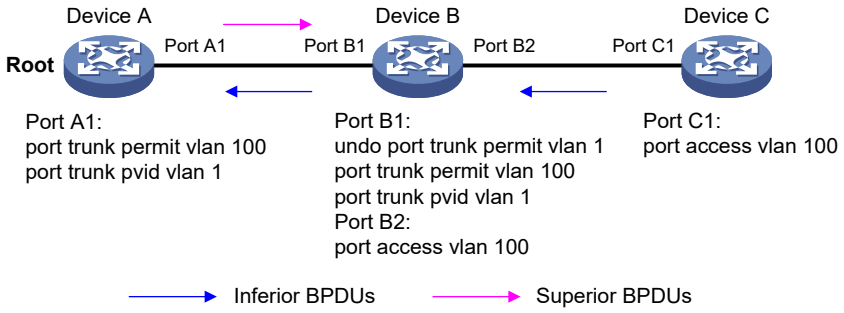


図 8-22 Dispute ガードの無効化シナリオ

I. 制限とガイドライン

ネットワークに片方向リンク障害がない場合、Dispute ガードを無効にできます。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Dispute ガードを無効にする	**undo stp dispute-protection**	デフォルト：有効

8.29 TC BPDUの検出、受信イベントのログ作成の有効化

TC BPDU を検出したとき、あるいは受信したとき、装置でログを作成します。この機能は PVST モードでのみ有効です。

以下に TC BPDU の検出、受信イベントの作成の有効化の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. TC BPDU を検出したとき、あるいは受信したとき、装置でログを作成する	**stp log enable tc**	デフォルト：無効

8.30 BPDUガードによりシャットダウンしたエッジポートの再アクティブ化無効

BPDU ガードは、BPDU を受信したエッジポートをシャットダウンし、NMS にシャットダウンを通知します。

shutdown-interval で設定した時間が経過すると、シャットダウンされていたポートを再度アクティブにします。

この機能は、BPDU ガードによってシャットダウンされたエッジポートを再アクティブ化するのを防ぎます。この機能によってシャットダウンされたエッジポートを起動するには、undo shutdown コマンドを使用します。

以下に BPDU ガードによりシャットダウンしたエッジポートの再アクティブ化を無効の設定手順を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． T BPDU ガードによりシャットダウンしたエッジポートの再アクティブ化を無効にする	stp port shutdown permanent	デフォルト：無効

8.31 新規ルートブリッジの選択、トポロジ変更イベントによるSNMP notificationの有効化

この機能を有効にすると、新規ルートブリッジの選択、あるいはスパニングツリーのトポロジ変更イベントが発生した場合、装置はログを作成し、SNMP に通知します。正常にイベントの notification を送信するため、装置で SNMP を設定する必要があります。SNMP の設定の詳細は、オペレーションマニュアルのセクション 11 *システム管理*”*SNMP*”を参照してください。

snmp-agent trap enable stp [**new-root** | **tc**]コマンドを使用するとき、以下のガイドラインに従ってください。

- **new-root** パラメータは STP、MSTP、RSTP モードでのみ適用します。
- **tc** パラメータは PVST モードでのみ適用します。
- STP、MSTP、RSTP モードでは、**snmp-agent trap enable stp** コマンドは、新規ルートブリッジの選択イベントが発生した場合、SNMP notification の送信を有効にします。
- PVST モードでは、**snmp-agent trap enable stp** コマンドは、スパニングツリーのトポロジ変更が発生した場合、SNMP notification の送信を有効にします。

以下に新規ルートブリッジの選択イベント、スパニングツリーのトポロジ変更イベントによる SNMP notification の送信の有効化の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． 新規ルートブリッジの選択イベントによる SNMP notification の送信を有効にする	STP、MSTP、RSTPモード： ● **snmp-agent trap enable stp new-root** ● **snmp-agent trap enable stp**	デフォルト： ● 新規ルートブリッジの選択イベントによるSNMP notificationの送信は無効です。 ● MSTPモードではスパニングツリーのトポロジの変更が発生した場合、MSTI 0のSNMP notificationの送信は有効です。ほかのMSTIのSNMP notificationの送信は無効です。 ● PVSTモードではすべての
3． スパニングツリーのトポロジ変更イベントによる SNMP notification の送信を有効にする	PVSTモード： **snmp-agent trap enable stp tc**	

操作	コマンド	補足
		VLANのスパニングツリーのトポロジの変更が発生した場合、SNMP notificationの送信は無効です。

8.32 スパニングツリーの表示と維持

すべての view で **display** コマンドを実行し、user view で **reset** コマンドを実行できます。

操作	コマンド
STPのガード機能によってブロッキング状態にあるポートの表示する	**display stp abnormal-port**
ポートのBPDU統計情報を表示する	**display stp bpdu-statistics** [**interface** *interface-type interface-number* [**instance** *instance-list*]]
STPの保護機能によってダウンしているポートを表示する	**display stp down-port**
MSTIポートの役割計算の履歴を表示する	**display stp** [**instance** *instance-list* | **vlan** *vlan-id-list*] **history** [**slot** *slot-number*]
MSTIの全ポートで送受信されたTC/TCN BPDUの統計情報を表示する	**display stp** [**instance** *instance-list* | **vlan** *vlan-id-list*] **tc** [**slot** *slot-number*]
スパニングツリーの状態および統計情報を表示する	**display stp** [**instance** *instance-list* | **vlan** *vlan-id-list*] [**interface** *interface-list* | **slot** *slot-number*] [**brief**]
有効なMST regionの設定情報を表示する	**display stp region-configuration**
MSTIのRootブリッジの情報を表示する	**display stp root**
スパニングツリーの統計情報を削除する	**reset stp** [**interface** *interface-list*]

8.33 スパニングツリー設定例

8.33.1 MSTP 設定例

I. ネットワーク要件

図 8-23に示すようにすべての装置は同じ MST region にあります。Device A、Device B はディストリビューション層にあり、Device C、Device D はアクセス層にあります。

異なる VLAN のパケットが異なるスパニングツリーに転送されるように MSTP を設定します。

- VLAN 10 のパケットは MSTI1 で転送されます。
- VLAN 30 のパケットは MSTI3 で転送されます。
- VLAN 40 のパケットは MSTI4 で転送されます。
- VLAN 20 のパケットは MSTI0 で転送されます。

VLAN 10 と VLAN 30 はディストリビューション層の装置のみ、VLAN 40 はアクセス層の装置のみで通信します。MSTI1 と MSTI3 の Root ブリッジは Device A、Device B となり、MSTI4 の Root ブリッジは Device C となります

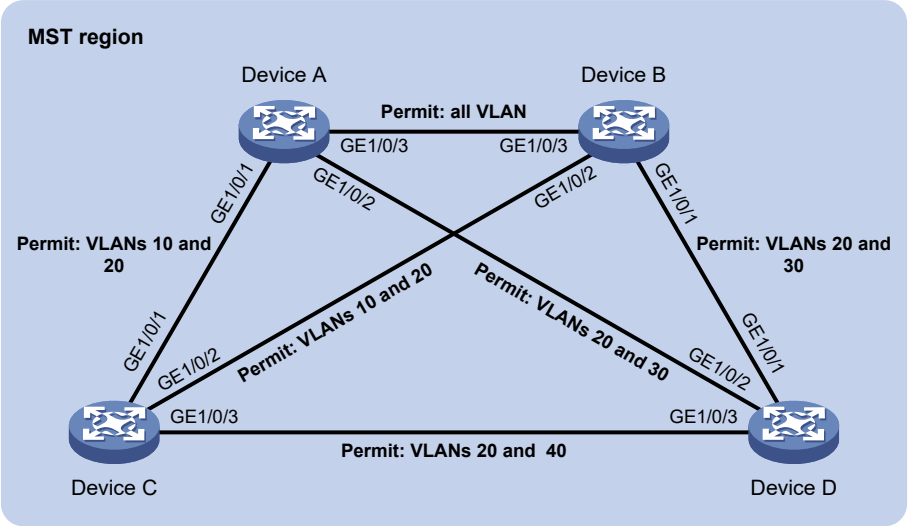


図 8-23 ネットワーク図

II. 設定手順

1)　VLAN を作成し、VLAN メンバポートを設定します。（詳細は省略します）
- □　Device A、Device B の両方で VLAN 10、VLAN 20、VLAN 30 を作成します。
- □　Device C で VLAN 10、VLAN 20、VLAN 40 を作成します。
- □　Device D で VLAN 20、VLAN 30、VLAN 40 を作成します。
- □　装置のポートをトランクポートに設定し、関連する VLAN を割り当てます。

2)　Device A を設定します。

MST region view に移行し、MST region 名 example を設定します。

```
<DeviceA> system-view
[DeviceA] stp region-configuration
[DeviceA-mst-region] region-name example
```

VLAN 10、VLAN 30、VLAN 40 をそれぞれ MSTI1、MSTI3、MSTI4 に割り当てます。

```
[DeviceA-mst-region] instance 1 vlan 10
[DeviceA-mst-region] instance 3 vlan 30
[DeviceA-mst-region] instance 4 vlan 40
```

MST region レベルを 0 とします。

```
[DeviceA-mst-region] revision-level 0
```

MST region の設定をアクティブにします。

```
[DeviceA-mst-region] active region-configuration
[DeviceA-mst-region] quit
```

MSTI1 の Root ブリッジとして Device A を設定します。

```
[DeviceA] stp instance 1 root primary
```

グローバルにスパニングツリーを有効にします。

```
[DeviceA] stp global enable
```

3) Device B を設定します。

MST region view に移行し、MST region 名 example を設定します。

```
<DeviceB> system-view
[DeviceB] stp region-configuration
[DeviceB-mst-region] region-name example
```

VLAN 10、VLAN 30、VLAN 40 をそれぞれ MSTI1、MSTI3、MSTI4 に割り当てます。

```
[DeviceB-mst-region] instance 1 vlan 10
[DeviceB-mst-region] instance 3 vlan 30
[DeviceB-mst-region] instance 4 vlan 40
```

MST region レベルを 0 とします。

```
[DeviceB-mst-region] revision-level 0
```

MST region の設定をアクティブにします。

```
[DeviceB-mst-region] active region-configuration
[DeviceB-mst-region] quit
```

MSTI3 の Root ブリッジとして Device B を設定します。

```
[DeviceB] stp instance 3 root primary
```

グローバルにスパニングツリーを有効にします。

```
[DeviceB] stp global enable
```

4) Device C を設定します。

MST region view に移行し、MST region 名 example を設定します。

```
<DeviceC> system-view
[DeviceC] stp region-configuration
[DeviceC-mst-region] region-name example
```

VLAN 10、VLAN 30、VLAN 40 をそれぞれ MSTI1、MSTI3、MSTI4 に割り当てます。

```
[DeviceC-mst-region] instance 1 vlan 10
[DeviceC-mst-region] instance 3 vlan 30
[DeviceC-mst-region] instance 4 vlan 40
```

MST region レベルを 0 とします。

```
[DeviceC-mst-region] revision-level 0
```

MST region の設定をアクティブにします。

```
[DeviceC-mst-region] active region-configuration
[DeviceC-mst-region] quit
```

MSTI4 の Root ブリッジとして Device C を設定します。

```
[DeviceC] stp instance 4 root primary
```

グローバルにスパニングツリーを有効にします。

```
[DeviceC] stp global enable
```

5) Device D を設定します。

MST region view に移行し、MST region 名 example を設定します。

```
<DeviceD> system-view
[DeviceD] stp region-configuration
[DeviceD-mst-region] region-name example
```

VLAN 10、VLAN 30、VLAN 40 をそれぞれ MSTI1、MSTI3、MSTI4 に割り当てます。

```
[DeviceD-mst-region] instance 1 vlan 10
[DeviceD-mst-region] instance 3 vlan 30
[DeviceD-mst-region] instance 4 vlan 40
```

MST region レベルを 0 とします。

```
[DeviceD-mst-region] revision-level 0
```

MST region の設定をアクティブにします。

```
[DeviceD-mst-region] active region-configuration
[DeviceD-mst-region] quit
```

グローバルにスパニングツリーを有効にします。

```
[DeviceD] stp global enable
```

III. 設定の確認

この例では Device B がもっとも小さい Root ブリッジ ID を持っています。結果として、Device B が MSTI 0 の Root ブリッジとなります。

ネットワークが安定したのち、**display stp brief** コマンドで、各装置で STP の概要情報を表示し、設定の確認を行います。

Device A のスパニングツリーの概要情報を表示します。

```
[DeviceA] display stp brief
 MST ID      Port                        Role  STP State     Protection
 0           GigabitEthernet1/0/1        ALTE  DISCARDING    NONE
 0           GigabitEthernet1/0/2        DESI  FORWARDING    NONE
 0           GigabitEthernet1/0/3        ROOT  FORWARDING    NONE
 1           GigabitEthernet1/0/1        DESI  FORWARDING    NONE
 1           GigabitEthernet1/0/3        DESI  FORWARDING    NONE
 3           GigabitEthernet1/0/2        DESI  FORWARDING    NONE
 3           GigabitEthernet1/0/3        ROOT  FORWARDING    NONE
```

Device B のスパニングツリーの概要情報を表示します。

```
[DeviceB] display stp brief
 MST ID      Port                        Role  STP State     Protection
 0           GigabitEthernet1/0/1        DESI  FORWARDING    NONE
```

```
 0           GigabitEthernet1/0/2          DESI  FORWARDING    NONE
 0           GigabitEthernet1/0/3          DESI  FORWARDING    NONE
 1           GigabitEthernet1/0/2          DESI  FORWARDING    NONE
 1           GigabitEthernet1/0/3          ROOT  FORWARDING    NONE
 3           GigabitEthernet1/0/1          DESI  FORWARDING    NONE
 3           GigabitEthernet1/0/3          DESI  FORWARDING    NONE
```

Device C のスパニングツリーの概要情報を表示します。

```
[DeviceC] display stp brief
 MST ID      Port                          Role  STP State     Protection
 0           GigabitEthernet1/0/1          DESI  FORWARDING    NONE
 0           GigabitEthernet1/0/2          ROOT  FORWARDING    NONE
 0           GigabitEthernet1/0/3          DESI  FORWARDING    NONE
 1           GigabitEthernet1/0/1          ROOT  FORWARDING    NONE
 1           GigabitEthernet1/0/2          ALTE  DISCARDING    NONE
 4           GigabitEthernet1/0/3          DESI  FORWARDING    NONE
```

Device D のスパニングツリーの概要情報を表示します。

```
[DeviceD] display stp brief
 MST ID      Port                          Role  STP State     Protection
 0           GigabitEthernet1/0/1          ROOT  FORWARDING    NONE
 0           GigabitEthernet1/0/2          ALTE  DISCARDING    NONE
 0           GigabitEthernet1/0/3          ALTE  DISCARDING    NONE
 3           GigabitEthernet1/0/1          ROOT  FORWARDING    NONE
 3           GigabitEthernet1/0/2          ALTE  DISCARDING    NONE
 4           GigabitEthernet1/0/3          ROOT  FORWARDING    NONE
```

出力情報から、図 8-24のように VLAN の MSTI マッピングの設定を行っていることがわかります。

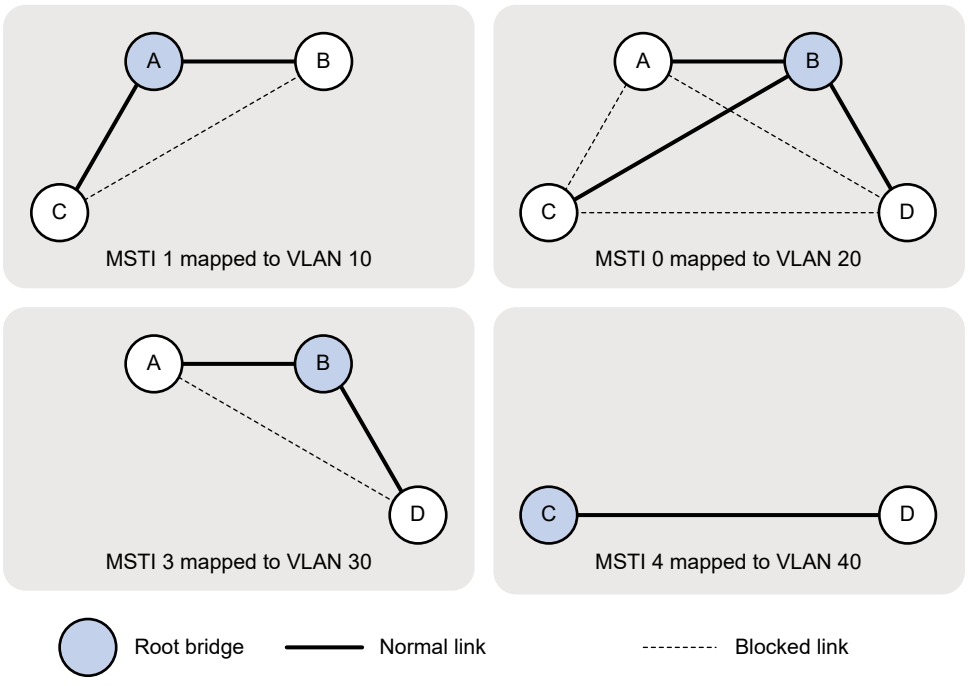


図 8-24 異なる VLAN への MSTI のマッピングの設定

8.33.2 PVST 設定例

I. ネットワーク要件

図 8-25に示すように、Device A、Device B はディストリビューション層にあり、Device C、Device D はアクセス層にあります。

以下の要件を満たすように PVST を設定します。

- VLAN のスパニングツリー間で VLAN パケットを転送します。
- VLAN 10、VLAN 20、VLA N30 はディストリビューション層の装置で終端し、VLAN 40 はアクセス層で終端します。
- VLAN 10、VLAN 20 の Root ブリッジは Device A です。
- VLAN 30 の Root ブリッジは Device B です。
- VLAN 40 の Root ブリッジは Device C です。

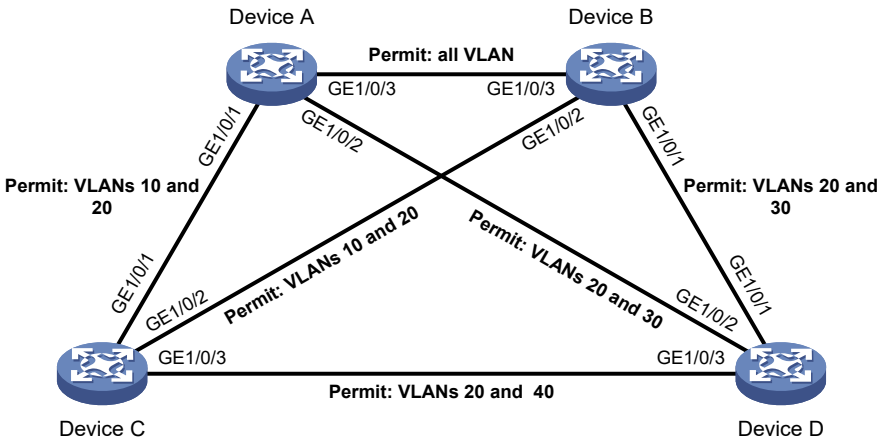


図 8-25 ネットワーク図

II. 設定手順

1)　VLAN、VLAN メンバポートを設定します。（詳細は省略します）
   - □　Device A、Device B の両方で VLAN 10、VLAN 20、VLAN 30 を作成します。
   - □　Device C で VLAN 10、VLAN 20、VLAN 40 を作成します。
   - □　Device D で VLAN 20、VLAN 30、VLAN 40 を作成します。
   - □　トランクポートとして Device のポートを設定し、関連する VLAN に割り当てます。

2)　Device A を設定します。

動作モードを PVST に設定します。

```
<DeviceA> system-view
[DeviceA] stp mode pvst
```

VLAN 10、VLAN 20 の Root ブリッジとして Device を設定します。

```
[DeviceA] stp vlan 10 20 root primary
```

グローバル、VLAN 10、VLAN 20、VLAN 30 でスパニングツリーを有効にします。

```
[DeviceA] stp global enable
```

```
[DeviceA] stp vlan 10 20 30 enable
```

3)　Device B を設定します。

動作モードを PVST に設定します。

```
<DeviceB> system-view
[DeviceB] stp mode pvst
```

VLAN 30 の Root ブリッジとして Device を設定します。

```
[DeviceB] stp vlan 30 root primary
```

グローバル、VLAN 10、VLAN 20、VLAN 30 でスパニングツリーを有効にします。

```
[DeviceB] stp global enable
[DeviceB] stp vlan 10 20 30 enable
```

4)　Device C を設定します。

動作モードを PVST に設定します。

```
<DeviceC> system-view
[DeviceC] stp mode pvst
```

VLAN 40 の Root ブリッジとして Device を設定します。

```
[DeviceC] stp vlan 40 root primary
```

グローバル、VLAN 10、VLAN 20、VLAN 40 でスパニングツリーを有効にします。

```
[DeviceC] stp global enable
[DeviceC] stp vlan 10 20 40 enable
```

5)　Device D を設定します。

動作モードを PVST に設定します。

```
<DeviceD> system-view
[DeviceD] stp mode pvst
```

グローバル、VLAN 20、VLAN 30、VLAN 40 でスパニングツリーを有効にします。

```
[DeviceD] stp global enable
[DeviceD] stp vlan 20 30 40 enable
```

III. 設定の確認

ネットワークが安定したのち、**display stp brief** コマンドで、各装置の STP の概要情報を表示し、設定の確認を行います。

Device A のスパニングツリーの概要情報を表示します。

```
[DeviceA] display stp brief
 VLAN ID     Port                        Role  STP State     Protection
 10          GigabitEthernet1/0/1        DESI  FORWARDING    NONE
 10          GigabitEthernet1/0/3        DESI  FORWARDING    NONE
 20          GigabitEthernet1/0/1        DESI  FORWARDING    NONE
 20          GigabitEthernet1/0/2        DESI  FORWARDING    NONE
 20          GigabitEthernet1/0/3        DESI  FORWARDING    NONE
```

```
 30          GigabitEthernet1/0/2          DESI  FORWARDING    NONE
 30          GigabitEthernet1/0/3          ROOT  FORWARDING    NONE
```

Device B のスパニングツリーの概要情報を表示します。

```
[DeviceB] display stp brief
 VLAN ID     Port                          Role  STP State     Protection
 10          GigabitEthernet1/0/2          DESI  FORWARDING    NONE
 10          GigabitEthernet1/0/3          ROOT  FORWARDING    NONE
 20          GigabitEthernet1/0/1          DESI  FORWARDING    NONE
 20          GigabitEthernet1/0/2          DESI  FORWARDING    NONE
 20          GigabitEthernet1/0/3          ROOT  FORWARDING    NONE
 30          GigabitEthernet1/0/1          DESI  FORWARDING    NONE
 30          GigabitEthernet1/0/3          DESI  FORWARDING    NONE
```

Device C のスパニングツリーの概要情報を表示します。

```
[DeviceC] display stp brief
 VLAN ID     Port                          Role  STP State     Protection
 10          GigabitEthernet1/0/1          ROOT  FORWARDING    NONE
 10          GigabitEthernet1/0/2          ALTE  DISCARDING    NONE
 20          GigabitEthernet1/0/1          ROOT  FORWARDING    NONE
 20          GigabitEthernet1/0/2          ALTE  DISCARDING    NONE
 20          GigabitEthernet1/0/3          DESI  FORWARDING    NONE
 40          GigabitEthernet1/0/3          DESI  FORWARDING    NONE
```

Device D のスパニングツリーの概要情報を表示します。

```
[DeviceD] display stp brief
 VLAN ID     Port                          Role  STP State     Protection
 20          GigabitEthernet1/0/1          ALTE  DISCARDING    NONE
 20          GigabitEthernet1/0/2          ROOT  FORWARDING    NONE
 20          GigabitEthernet1/0/3          ALTE  DISCARDING    NONE
 30          GigabitEthernet1/0/1          ROOT  FORWARDING    NONE
 30          GigabitEthernet1/0/2          ALTE  DISCARDING    NONE
 40          GigabitEthernet1/0/3          ROOT  FORWARDING    NONE
```

出力情報から、図 8-26のように各 VLAN のスパニングツリーのトポロジの設定を行っていることがわかります。

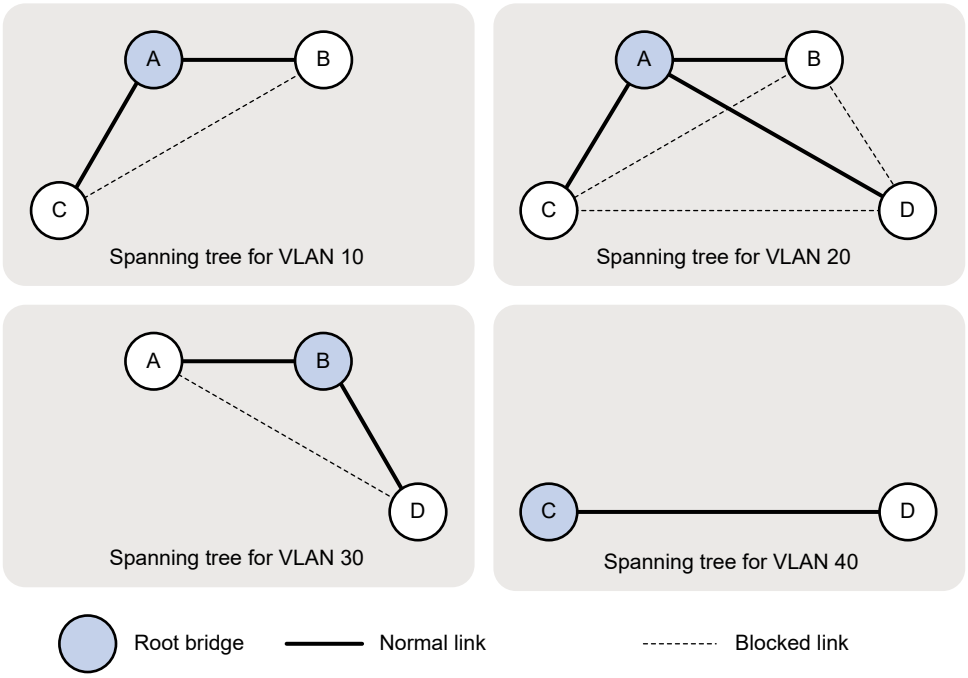


図 8-26 VLAN のスパニングツリーのトポロジ

目次

このセクションのページは**3-x-x** です。

9章 ループ検出 9-1
9.1 概要 9-1
9.1.1 ループ検出メカニズム 9-1
9.1.2 ループ検出間隔 9-2
9.1.3 ループ保護アクション 9-3
9.1.4 ポート状態自動回復 9-3
9.2 ループ検出設定作業リスト 9-3
9.3 ループ検出の有効化 9-4
9.3.1 制限とガイドライン 9-4
9.3.2 グローバルでのループ検出の有効化 9-4
9.3.3 インタフェースでのループ検出の有効化 9-4
9.4 ループ保護アクションの設定 9-5
9.4.1 グローバルでのループ保護アクションの設定 9-5
9.4.2 Ethernetインタフェースでのループ保護アクションの設定 9-5
9.4.3 アグリゲートインタフェースでのループ保護アクションの設定 9-5
9.5 ループ検出間隔の設定 9-6
9.6 ループ検出の表示と維持 9-6
9.7 ループ検出設定例 9-6
9.7.1 ネットワーク要件 9-6
9.7.2 設定手順 9-7
9.7.3 設定の確認 9-8

9章 ループ検出

🕮 **メモ：**
QX-S5100G シリーズはデフォルトでブロックアクションが動作します。

9.1 概要

不正なネットワークの接続あるいは設定は、レイヤ 2 のループを発生させます。ループができると送信されたデータがループ内を無限に巡り続け、回線が圧迫されて通信ができなくなり、ネットワーク機器が過負荷になって性能が低下するなどの、ネットワーク障害を引き起こす原因となります。

ループ検出機能は、ループが発生した場合、ネットワークの接続と設定に対応するように通知させるため、すぐさまログを作成します。ループ検出はネットワークの接続と設定をシャットダウンすることができます。ログは Information center で維持されます。詳細はオペレーションマニュアルのセクション 11 *システム管理*"*Information Center*"を参照してください。

9.1.1 ループ検出メカニズム

装置は検出フレームを送信し、装置のポートからフレームが戻るかどうかを確認することでループを検出します。検出した場合、装置はループされたリンクに接続されていると認識します。

ループ検出は通常 VLAN 内で動作します。検出フレームに送信されたフレームと異なる VLAN タグが付いている場合、内部 VLAN ループが発生しています。ループを取り除くため、正しい設定の QinQ あるいは VLAN マッピングの設定を行います。QinQ、VLAN マッピングの詳細は、オペレーションマニュアルのセクション 3 *アクセス* ”*QinQ*”、“*VLAN マッピング*”を参照してください。

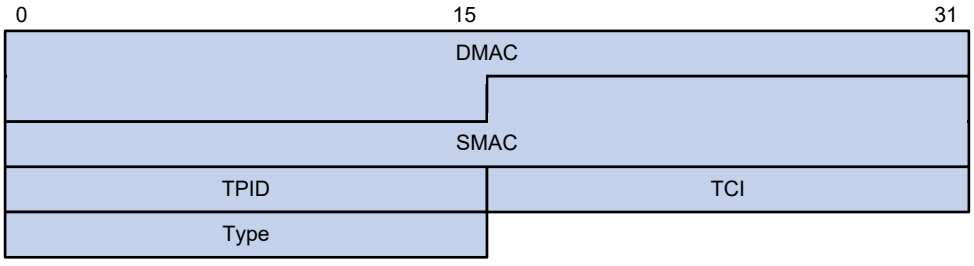


図 9-1 ループ検出のイーサネットフレームヘッダ

ループ検出のイーサネットフレームヘッダは以下のフィールドがあります。

- **DMAC** – フレームの宛先 MAC アドレスです。MAC アドレスは、マルチキャスト MAC アドレス 010F-E200-0007 です。ループ検出機能が有効で、この宛先 MAC アドレスのフレームを受信したとき、以下の処理を行います。
  - □ CPU にフレームを送信します。
  - □ フレームを最初に受信した VLAN にフラッドします。
- **SMAC** – フレームの送信元 MAC アドレスで、送信している装置の MAC アドレスです。
- **TPID** – VLAN タグのタイプで、0x8100 です。
- **TCI** – VLAN タグの情報で優先度と VLAN ID が含まれます。
- **Type** – プロトコルタイプで、0x8918 です。

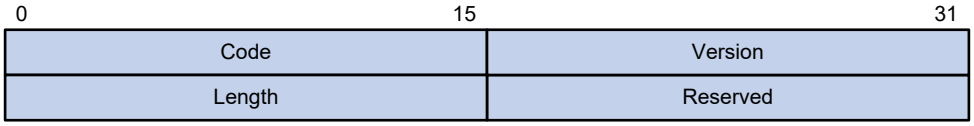


図 9-2 ループ検出の内部フレームヘッダ

ループ検出の内部フレームヘッダは以下のフィールドがあります。

- **Code** – プロトコルサブタイプで、0x0001 です。ループ検出プロトコルを含みます。
- **Version** – プロトコルバージョンで、0x0000 です。
- **Length** – フレーム長です。値は内部ヘッダを含みますが、イーサネットヘッダは含みません。
- **Reserved** – 予約されたフィールドです。

ループ検出のフレームは TLV（タイプ、長さ、値）としてカプセル化されます。

表 9-1 ループ検出でサポートされる TLV

TLV	説明	補足
End of PDU	PDUの最後	オプション
Device ID	送信装置のBridge MACアドレス	必須
Port ID	ポートを送信するPDUのID	オプション
Port Name	ポートを送信するPDU名	オプション
System Name	装置名	オプション
Chassis ID	ポートを送信するシャーシID	オプション
Slot ID	ポートを送信するスロットID	オプション
Sub Slot ID	ポートを送信するサブスロットID	オプション

9.1.2 ループ検出間隔

ループ検出は、ネットワークの変化に対して連続して対応します。ループ検出フレームは、指定された間隔（ループ検出間隔と呼ばれます）で、ポートにループが発生したかどうか、ループが取り除かれたかどうかを確認するために送信されます。

9.1.3 ループ保護アクション

装置がポートを検出したとき、ログを作成しますが、デフォルトでポートに何らかのアクションは実行しません。以下のアクションのうちの 1 つのアクションを行うように設定することができます。

- **Block** – ポートが MAC アドレスを学習することを無効にし、ポートに受信されるトラフィックをブロックします。
- **No-learning** – ポートが MAC アドレスを学習することを無効にします。
- **Shutdown** – すべてのフレームの送受信を無効にするため、ポートをシャットダウンします。

9.1.4 ポート状態自動回復

block、**no-learning** ポートを設定した装置がポートでループを検出すると、アクションを開始しループ検出間隔の 3 倍の時間待ちます。もしポートでループを検出してからループ検出間隔の 3 倍の期間内にループ検出フレームを受信しない場合、以下の動作をします。

- 装置は自動的にポートを転送状態に設定します。
- ユーザにイベントを通知します。

loopback-detection action shutdown コマンドが使用されたとき、装置は以下の動作をします。

1) 装置は自動的にポートをシャットダウンします。
2) **shutdown-interval** コマンドで設定された検出タイマが満了したのち、装置は自動的にポートを転送状態に設定します。
3) 検出タイマが満了するときにループが検出されると、装置は再びポートをシャットダウンします。

この処理はループが削除されるまで繰り返されます。

🕮 **メモ：**

ループ検出フレームが負荷抑制機能などで削除されることによって、ループが継続していても誤って回復する場合があります。この現象を避けるためには、**shutdown** アクションを使用するか、手動でループを取り除いてください。

9.2 ループ検出設定作業リスト

作業リスト
（必須設定項目）ループ検出の有効化
（オプション設定項目）ループ保護アクションの設定
（オプション設定項目）ループ検出間隔の設定

9.3 ループ検出の有効化

9.3.1 制限とガイドライン

ループ検出を有効にするときは、次の制限事項とガイドラインに従ってください。

- ループ検出はグローバルあるいはポート単位で有効にすることができます。指定のポートのみループ検出を有効化する場合は、グローバルの設定を無効に設定してください。
- ループ検出はポートで有効化されている VLAN の検出フレームを受信すると、受信したポートのループ検出が有効かどうかに関係なく、そのポートで指定したループ保護アクションが動作します。
- リンクアグリゲーションポート単位にループ検出を有効化する場合は、リンクアグリゲーショングループの論理ポート（aggregate interface view）にループ検出の設定をする必要があります。メンバポートに設定しても動作しません。

🕮 **メモ：**

ループ検出を有効化する VLAN は、必要な VLAN のみ設定することを推奨します。
複数の VLAN でループ検出を有効にした場合、それぞれの VLAN 宛にループ検出パケットが送信されます。例えば、すべての VLAN を許可しているトランクポートでループ検出をすべての VLAN で有効にした場合、ネットワークに存在する装置では 4094 個の MAC アドレスが学習されます。その結果、周辺装置の MAC アドレステーブルのリソースが足りなくなる可能性があります。

9.3.2 グローバルでのループ検出の有効化

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. グローバルでループ検出を有効にする	**loopback-detection global enable vlan** { *vlan-id-list* | **all** }	デフォルト：無効

9.3.3 インタフェースでのループ検出の有効化

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Ethernet interface view あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	―
3. ポートでループ検出を有効にする	**loopback-detection enable vlan** { *vlan-id-list* | **all** }	デフォルト： Ethernetインタフェースでは VLAN1のループ検出が有効です。アグリゲートインタフェースではループ検出は無効です。

9.4 ループ保護アクションの設定

ループ保護アクションはグローバルあるいは指定されたポートで有効にすることができます。グローバルの設定は、指定された VLAN のすべてのポートに適用されます。ポート毎の設定は、グローバルの設定よりも優先されます。

🕮 **メモ：**

- **shutdown** アクションを設定し、ポートでループが検出された場合、ポートをシャットダウンする際、ループ状態を解除するため、RECOVERED のログも出力します。
- **shutdown** アクションによるポートのシャットダウンが行われると、**display interface** コマンドの Current state フィールドが DOWN（Loopback detection down）と表示されます。

9.4.1 グローバルでのループ保護アクションの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. グローバルでループ保護アクションを設定する	**loopback-detection global action shutdown**	デフォルト : ループを検出したときアクションは実行しませんがログを出力します。

9.4.2 Ethernet インタフェースでのループ保護アクションの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Ethernet interface view に移行する	**interface** *interface-type interface-number*	―
3. インタフェースでループ保護アクションを設定する	**loopback-detection action** { **block** | **no-learning** | **shutdown** }	デフォルト : ループを検出したときブロックアクションを実行します。

9.4.3 アグリゲートインタフェースでのループ保護アクションの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. aggregate interface view に移行する	**interface bridge-aggregation** *interface-number*	―
3. アグリゲートインタフェースでループ保護アクションを設定する.	**loopback-detection action shutdown**	デフォルト : ループを検出したときアクションは実行しませんがログを出力します。

9.5 ループ検出間隔の設定

ループ検出が有効であるとき、装置は、指定された間隔でループ検出フレームを送信します。短い間隔では検出感度が上がりますが、より多くのリソースが消費されます。ループ検出間隔の設定を行うときには、システムのパフォーマンスとループ検出速度を考慮してください。

以下にループ検出間隔の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． ループ検出間隔を設定する	**loopback-detection interval-time** *interval*	デフォルト：5秒

9.6 ループ検出の表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
ループ検出の設定と状態を表示する	**display loopback-detection**

9.7 ループ検出設定例

🕮 **メモ：**

STP 機能によってブロッキング状態のポートでは、ループ検出パケットの送受信はできません。

9.7.1 ネットワーク要件

図 9-3に示すように、ループを検出したとき、Device A がログを作成し、自動的にポートのシャットダウンを行うようにループ検出の設定を行います。

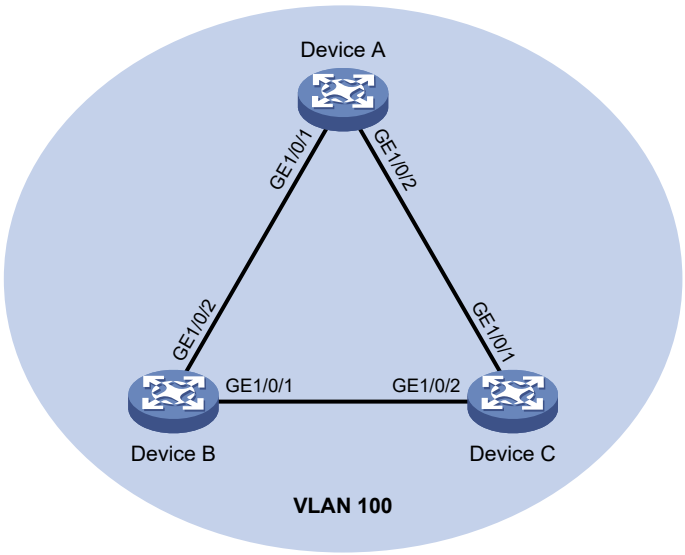


図 9-3 ネットワーク図

9.7.2 設定手順

1)　Device A を設定します。

VLAN 100 を作成し、グローバルにループ検出を設定します。

```
<DeviceA> system-view
[DeviceA] vlan 100
[DeviceA-vlan100] quit
[DeviceA] loopback-detection global enable vlan 100
```

GigabitEthernet 1/0/1、GigabitEthernet 1/0/2 をトランクポートとして設定し、VLAN 100 を割り当てます。

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-type trunk
[DeviceA-GigabitEthernet1/0/1] port trunk permit vlan 100
[DeviceA-GigabitEthernet1/0/1] quit
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port link-type trunk
[DeviceA-GigabitEthernet1/0/2] port trunk permit vlan 100
[DeviceA-GigabitEthernet1/0/2] quit
```

シャットダウンを行うループ保護アクションをグローバルで設定します。

```
[DeviceA] loopback-detection global action shutdown
```

ループ検出間隔を 35 秒に設定します。

```
[DeviceA] loopback-detection interval-time 35
```

2)　Device B を設定します。

VLAN 100 を作成します。

```
<DeviceB> system-view
[DeviceB] vlan 100
[DeviceB- vlan100] quit
```

GigabitEthernet 1/0/1、GigabitEthernet 1/0/2 をトランクポートとして設定し、VLAN 100 を割り当てます。

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port link-type trunk
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 100
[DeviceB-GigabitEthernet1/0/1] quit
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] port link-type trunk
[DeviceB-GigabitEthernet1/0/2] port trunk permit vlan 100
[DeviceB-GigabitEthernet1/0/2] quit
```

3)　Device C を設定します。

VLAN 100 を作成します。

```
<DeviceC> system-view
[DeviceC] vlan 100
[DeviceC- vlan100] quit
```

GigabitEthernet 1/0/1、GigabitEthernet 1/0/2 をトランクポートとして設定し、VLAN 100 を割り当てます。

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] port link-type trunk
[DeviceC-GigabitEthernet1/0/1] port trunk permit vlan 100
[DeviceC-GigabitEthernet1/0/1] quit
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] port link-type trunk
[DeviceC-GigabitEthernet1/0/2] port trunk permit vlan 100
[DeviceC-GigabitEthernet1/0/2] quit
```

9.7.3 設定の確認

Device A のログを確認します。

```
[DeviceA]
%Feb 24 15:04:29:663 2013 DeviceA LPDT/4/LPDT LOOPED: Loopback exists on
GigabitEthernet1/0/1.
%Feb 24 15:04:29:667 2013 DeviceA LPDT/4/LPDT LOOPED: Loopback exists on
GigabitEthernet1/0/2.
%Feb 24 15:04:44:243 2013 DeviceA LPDT/5/LPDT RECOVERED: Loopback on
GigabitEthernet1/0/1 recovered.
%Feb 24 15:04:44:248 2013 DeviceA LPDT/5/LPDT RECOVERED: Loopback on
GigabitEthernet1/0/2 recovered.
```

出力内容は、以下のことを示します。

- Device A はループ検出間隔内に GigabitEthernet 1/0/1、GigabitEthernet 1/0/2 のポートでループを検出しました。
- Device A は自動的に GigabitEthernet 1/0/1、GigabitEthernet 1/0/2 をシャットダウンしました。

display loopback-detection コマンドを使用して Device A のループ検出の設定と情報を表示します。

```
[DeviceA] display loopback-detection
Loop detection is enabled.
Loop detection interval is 35 second(s).
No loopback is detected.
```

出力はシャットダウンアクションに従って、GigabitEthernet 1/0/1、GigabitEthernet 1/0/2 ポートがループから開放されたことを示しています。

Device A の GigabitEthernet 1/0/1 の状態を表示します。

```
[DeviceA] display interface gigabitethernet 1/0/1
GigabitEthernet1/0/1 current state: DOWN (Loop detection down)
...
```

出力は、GigabitEthernet 1/0/1 がループ検出アクションによってシャットダウンしていることを示しています。

Device A の GigabitEthernet 1/0/2 の状態を表示します。

```
[DeviceA] display interface gigabitethernet 1/0/2
GigabitEthernet1/0/2 current state: DOWN (Loop detection down)
...
```

出力は、GigabitEthernet 1/0/2 がループ検出アクションによってシャットダウンしていることを示しています。

目次

このセクションのページは **3-x-x** です。

10 章 VLAN 10-1
10.1 概要 10-1
10.1.1 VLAN フレームのカプセル化 10-1
10.1.2 プロトコルと標準 10-2
10.2 VLAN の設定 10-2
10.2.1 制限とガイドライン 10-2
10.3 VLAN インタフェースの設定 10-3
10.3.1 制限とガイドライン 10-3
10.3.2 VLAN インタフェースの基本設定 10-4
10.4 ポートベース VLAN の設定 10-4
10.4.1 概要 10-4
10.4.2 アクセスポート VLAN の設定 10-6
10.4.3 トランクポート VLAN の設定 10-6
10.4.4 ハイブリッドポート VLAN の設定 10-7
10.5 MAC ベース VLAN 10-8
10.5.1 概要 10-8
10.5.2 設定の一般的な制限とガイドライン 10-11
10.5.3 スタティック MAC ベース VLAN の設定 10-11
10.5.4 ダイナミック MAC ベース VLAN の設定 10-12
10.5.5 サーバ割り当て MAC ベース VLAN 10-13
10.6 IP サブネットベース VLAN の設定 10-13
10.7 プロトコルベース VLAN 10-14
10.7.1 概要 10-14
10.8 VLAN の表示と維持 10-15
10.9 VLAN 設定例 10-16
10.9.1 ポートベース VLAN 設定例 10-16
10.9.2 MAC ベース VLAN 設定例 10-18
10.9.3 IP サブネットベース VLAN 設定例 10-20
10.9.4 プロトコルベース VLAN 設定例 10-22

10章 VLAN

10.1 概要

VLAN（Virtual Local Area Network）テクノロジは、物理 LAN を複数の論理 LAN に分割することで、スイッチ内を仮想的なグループに分けます。次の利点があります。

- **セキュリティ**－同じ VLAN 内のホストはレイヤ 2 で相互に通信できますが、レイヤ 2 の他の VLAN のホストから隔離され、直接通信できる範囲を限定します。
- **ブロードキャストトラフィックの分離**－グループの範囲内でのみ直接通信するため、ブロードキャストフレームによる回線の混雑を緩和します。
- **柔軟性**－VLAN は、ワークグループごとに論理的に分割できます。同じワークグループ内のホストは、物理的な場所に関係なく、ネットワーク構成を決めることができます。

図 10-1のように VLAN を使用して、LAN を小さく分割することで、ブロードキャストドメインの影響を少なくすることができます。

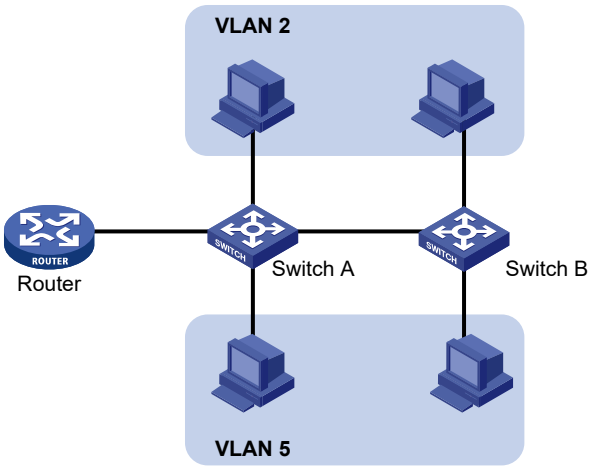


図 10-1 VLAN ネットワーク図

VLAN は物理的な要素からは制限を受けません。たとえば、特定のワークグループによって使用されるすべてのワークステーションとサーバは物理的な位置に関係なく、同じ LAN に接続することができます。異なる VLAN 間と通信するためにはルータやレイヤ 3 スイッチが必要となります。

10.1.1 VLAN フレームのカプセル化

異なる VLAN からイーサネットフレームを認識するため、図 10-2に示すように IEEE802.1Q では、宛先/送信元 MAC アドレス（DA&SA）フィールドと上位プロトコルタイプフィールドの間に 4byte の VLAN タグを追加しました。

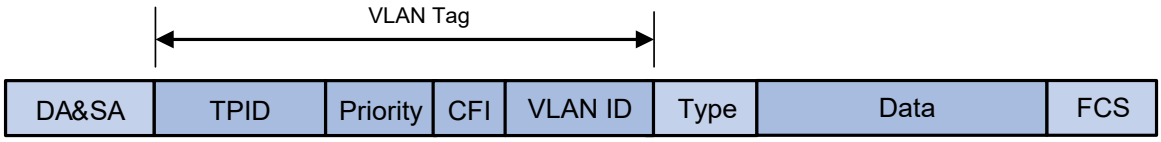


図 10-2 VLAN タグの位置とフォーマット

VLAN タグは以下のフィールドが含まれます。

- **TPID**– フレームに VLAN タグが付いているかどうかを識別するためのプロトコル識別子です。このフィールドは 16 ビット長です。デフォルトで TPID は 0x8100 で VLAN タグが付いています。
- **Priority**– フレームの 802.1p 優先度を示します。このフィールドは 3 ビット長です。詳細はオペレーションマニュアルのセクション 8 *ACL and QoS "プライオリティマッピング"*を参照してください。
- **CFI**– 標準フォーマットを示すフィールドです。このフィールドは 1 ビット長です。パケットが異なるメディアを跨いで転送されるとき、MAC アドレスは標準フォーマットでカプセル化されます。以下の値が設定できます。
  - **0（デフォルト）**– MAC アドレスは標準フォーマットでカプセル化されます。
  - **1**– MAC アドレスは非標準フォーマットでカプセル化されます。
- **VLAN ID**– フレームが所属する VLAN を示します。このフィールドは 12 ビット長です。VLAN-ID の範囲は 0～4095 です。0 と 4095 はプロトコルによって予約されているので、実際に使える値は 1～4094 となります。

フレームを受信したとき、ネットワーク装置はフレームに VLAN タグが付いているか、そして VLAN タグの値を確認して処理を決定します。詳細はオペレーションマニュアルのセクション 3 *アクセス "VLAN"の"ポートベース VLAN の設定"*を参照してください。

イーサネットは Ethernet II、802.3/802.2 LLC、802.3/802.2 SNAP、802.3 raw などのカプセル化フォーマットをサポートしています。ここでは Ethernet II カプセル化フォーマットを使用しています。VLAN タグフィールドは VLAN を識別するために、これらのカプセル化フォーマットにも付与されます。詳細は関連するプロトコルと標準を参照してください。

複数のタグ付きフレームのために、装置はもっとも外側の VLAN タグに従って処理し、ペイロードとしてその内部の VLAN タグを送信します。

10.1.2 プロトコルと標準

IEEE 802.1Q, *IEEE Standard for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks*

10.2 VLANの設定

10.2.1 制限とガイドライン

VLAN を設定する場合、以下の制限とガイドラインに従ってください。

- デフォルト VLAN である VLAN1 は作成または削除できません。
- ダイナミック VLAN、あるいはアプリケーションで設定されている VLAN は **undo vlan** コマンドで削除することはできません。最初に各設定から VLAN の設定を削除してください。

以下に VLAN の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. （オプション設定項目）VLAN を作成し、view へ移行あるいは VLAN リストを作成する	**vlan** { *vlan-id1* [**to** *vlan-id2*] | **all** }	デフォルト： デフォルト VLAN（VLAN1）のみ
3. VLAN view に移行する	**vlan** *vlan-id*	VLAN リストを作成した後、指定した VLAN を設定するには、この操作を実行してください。
4. VLAN の名前を設定する	**name** *text*	デフォルト：**VLAN** *vlan-id* たとえば VLAN 100 の VLAN 名は **VLAN 0100** です。
5. VLAN の説明を設定する	**description** *text*	デフォルト：**VLAN** *vlan-id* *vlan-id* は VLAN の ID です。 たとえば VLAN 100 の説明は **VLAN 0100** です。

10.3 VLANインタフェースの設定

VLAN の異なるホスト間で通信を行うには、ルータまたはレイヤ 3 スイッチでレイヤ 3 転送を行う必要があります。これを実現するために、VLAN インタフェースが使用されます。VLAN インタフェースは異なる VLAN 間でレイヤ 3 通信を行うための仮想インタフェースです。装置上の VLAN インタフェースは物理的には存在しません。各 VLAN は、1 つの VLAN インタフェースを作成することができます。VLAN インタフェースには IP アドレスを割り当てることができ、そしてそれをゲートウェイとすることで、異なる IP ネットワークセグメントへのトラフィックを転送することが可能となります。

10.3.1 制限とガイドライン

VLAN インタフェースを設定する場合、以下の制限とガイドラインに従ってください。

以下に記載するセカンダリ VLAN には VLAN インタフェースを作成できません。

- 同じプライマリ VLAN に関連付けられています。
- プライマリ VLAN インタフェースの VLAN interface view でレイヤ 3 通信が有効になっています。

セカンダリ VLAN の詳細は、オペレーションマニュアルのセクション 3 *アクセス”Private VLAN”* を参照してください。

10.3.2 VLAN インタフェースの基本設定

VLANインタフェースを作成する前に、対応するVLANが作成されている必要があります。

以下に VLAN インタフェースの基本設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. VLAN インタフェースを作成し、VLAN interface view に移行する	**interface vlan-interface** *vlan-interface-id*	デフォルト：設定なし VLANが存在する場合、直接そのviewに移行します。
3. VLAN インタフェースに IP アドレスを割り当てる	**ip address** *ip-address* { *mask* | *mask-length* } [**sub**]	デフォルト：設定なし
4. VLAN インタフェースの説明を設定する	**description** *text*	デフォルト：VLANインタフェース名。 たとえば**Vlan-interface1 Interface**です。
5. （オプション設定項目）VLAN インタフェースをアップ状態にする	**undo shutdown**	デフォルト：手動でシャットダウン状態になっていません。 ● VLANのすべてのポートがdownしている場合、VLANインタフェースはdownになります。 ● 1つ以上のVLANがupである場合、VLANインタフェースはupになります。

10.4 ポートベースVLANの設定

10.4.1 概要

ポートベース VLAN はポートに VLAN を割り当てます。VLAN を割り当てられたポートはその VLAN のトラフィックだけを転送します。

I. ポートリンクタイプ

ポートリンクタイプはアクセス、トランク、ハイブリッドに設定することができます。3つのリンクタイプは、異なる VLAN タグの処理方法を使用します。

- **アクセス**－アクセスポートは 1 つの VLAN にのみ所属することができます。タグが付与されずにパケットを送信します。通常、PC が直接接続されるポートはアクセスポートに設定します。アクセスポートは、以下の場合に使用されます。
  - □ VLAN パケットをサポートしない端末に接続します。
  - □ VLAN を区別できない装置に接続します。
- **トランク**－トランクポートは複数の VLAN に所属することができ、複数の VLAN のトラフィックを送受信可能です。デフォルト VLAN（PVID）以外のトラフィックがトランクポートを通過するとき、そのトラフィックには VLAN タグが付与されます。

トランクポートは通常、同じ VLAN を持つネットワーク装置と接続するのに使用されます。

- **ハイブリッド**－ハイブリッドポートは複数の VLAN からパケットを転送することができます。ハイブリッドポートに転送されたパケットのタグの状態はポートの設定に依存します。ハイブリッドポートは一般的に SVLAN タグを削除するため、one-to-two VLAN マッピングで使用されます。one-to-two VLAN マッピングの詳細は、オペレーションマニュアルのセクション 3 *アクセス" VLAN マッピング"* を参照してください。

II. PVID

PVID は、ポートのデフォルト VLAN です。ポートで受信されたタグなしパケットは PVID のポートから受信されたパケットとして認識されます。

ポートに PVID を設定する際は、以下の制限とガイドラインに従ってください。

- アクセスポートは 1 つの VLAN にのみ属しているため、その VLAN 以外へ PVID を変更することはできません。
- トランクまたはハイブリッドポートは複数の VLAN と PVID 設定をサポートします。
- アクセスポートで **undo vlan** コマンドで PVID を削除すると、ポートのタイプによって以下のいずれかの動作をします。
  - □ アクセスポートでは、PVID は VLAN1 になります。
  - □ トランクまたはハイブリッドポートでは、PVID の設定に影響はありません。

  トランクまたはハイブリッドポートでは存在しない VLAN を PVID として設定することができますが、アクセスポートではできません。
- ローカルとリモートで同じ PVID を設定することを推奨します。
- ポートで PVID からのパケットとタグなしパケットを廃棄しないように、ポートを PVID に割り当ててください。

III. 異なるリンクタイプの処理方法

アクション	アクセス	トランク	ハイブリッド
VLANタグなしフレームの入力フレーム処理	PVIDのタグを各フレームに付与します。	• PVIDがポートで許可されている場合、PVIDのタグを各フレームに付与します。 • PVIDがポートで許可されていない場合、フレームを廃棄します。	
VLANタグ付きフレームの入力フレーム処理	• PVIDのタグが付いたフレームのみ受信します。 • PVID以外のタグ付きフレームは破棄します。	• VLANがポートで許可されている場合、フレームを受信します。 • VLANがポートで許可されていない場合、フレームを廃棄します。	
出力フレーム処理	VLANのタグを外して送信します。	• PVIDのタグが付いたフレームはタグを外して送信します。 • PVID以外の許可されているVLANの場合、タグを付けたまま送信します。	PVIDを含めた**port hybrid vlan**コマンドの設定に従います。タグを付けたまま送信するか、タグを外して送信します。

VLAN ネットワークでは、タグなしパケットが処理される順番は以下の通りです。

- MAC ベース VLAN
- プロトコルベース VLAN
- ポートベース VLAN

10.4.2 アクセスポート VLAN の設定

VLAN view あるいは interface view でアクセスポートを VLAN に割り当てることができます。

アクセスポートを VLAN に割り当てる前に、対応する VLAN が作成されている必要があります。

I. VLAN view でのアクセス VLAN の設定方法

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. VLAN view 移行する	**vlan** *vlan-id*	ー
3. アクセスポートを VLAN に割り当てる	**port** *interface-list*	デフォルト：VLAN 1

II. interface view でのアクセス VLAN の設定方法

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. interface view に移行する	● Ethernet interface view に移行する： **interface** *interface-type interface-number* ● aggregate interface view に移行する： **interface bridge-aggregation** *interface-number*	ー
3. リンクタイプをアクセスに設定する	**port link-type access**	デフォルト：アクセス
4. （オプション設定項目）アクセスポートを VLAN に割り当てる	**port access vlan** *vlan-id*	デフォルト：VLAN1に属します。

10.4.3 トランクポート VLAN の設定

トランクポートは複数の VLAN に所属することができます。トランクポート VLAN の設定は、interface view で VLAN に割り当てることができます。

VLAN にトランクポートを割り当てるとき、以下の制限とガイドラインに従ってください。

- ポートリンクタイプをトランクからハイブリッド（またはその逆）に直接変更することはできません。最初にリンクタイプをアクセスにしてから目的のタイプへ変更してください。
- PVID からのパケットを転送するために、トランクポートに PVID を設定した後に、**port trunk permit vlan** コマンドで PVID を許可する必要があります。

以下にトランクポートを VLAN に割り当てる設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. interface view に移行する	● interface viewに移行する：**interface** *interface-type interface-number* ● aggregate interface viewに移行する：**interface bridge-aggregation** *interface-number*	―
3. リンクタイプをトランクに設定する	**port link-type trunk**	デフォルト：アクセス
4. トランクポートで許可する VLAN を設定する	**port trunk permit vlan** {*vlan-id-list* | **all** }	デフォルト：vlan1のみ許可
5. （オプション設定項目）トランクポートの PVID を設定する	**port trunk pvid vlan** *vlan-id*	デフォルト： VLAN 1

10.4.4 ハイブリッドポート VLAN の設定

ハイブリッドポートは複数の VLAN に所属することができます。ハイブリッドポート VLAN の設定は、interface view で VLAN に割り当てることができます。ハイブリッドポートを VLAN に割り当てる前に、対応する VLAN が作成されている必要があります。

VLAN にハイブリッドポートを割り当てるとき、以下のガイドラインに従ってください。

- ポートリンクタイプをトランクからハイブリッド（またはその逆）に直接変更することはできません。最初にリンクタイプをアクセスにしてから目的のタイプへ変更してください。
- PVID からのパケットを転送するためには、トランクポートに PVID を設定した後に、**port hybrid vlan** コマンドで PVID を許可する必要があります。

以下にハイブリッドポートを VLAN に割り当てる設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. interface view に移行する	● interface viewに移行する：**interface** *interface-type interface-number* ● aggregate interface viewに移行する：**interface bridge-aggregation** *interface-number*	―
3. リンクタイプをハイブリッドに設定する	**port link-type hybrid**	デフォルト：アクセス

操作	コマンド	補足
4. ハイブリッドポートで許可する VLAN を設定する	**port hybrid vlan** *vlan-id-list* { **tagged** | **untagged** }	デフォルト : リンクタイプがアクセスであるとき、ハイブリッドポートのPVIDはポートが所属しているVLANのIDです。
5. （オプション設定項目）ハイブリッドポートの PVID を設定する	**port hybrid pvid vlan** *vlan-id*	デフォルト : リンクタイプがアクセスであるとき、ハイブリッドポートはポートが所属しているVLANのタグなしメンバです。

10.5 MACベースVLAN

10.5.1 概要

この機能はハイブリッドポートでのみ有効です。

MAC ベース VLAN は MAC アドレスをもとにして VLAN にホストを割り当てます。この機能は VLAN の設定がユーザの位置情報にかかわらず同一であるため、ユーザベース VLAN とも呼ばれます。

I. スタティック MAC ベース VLAN の割り当て

VLANユーザが少ないネットワークでは、スタティック MACベース VLANを使用します。ポートでスタティック MAC ベース VLAN を設定するため、以下の作業を行う必要があります。

1) MAC-VLAN エントリを作成します。
2) ポートで MAC ベース VLAN を有効にします。
3) MAC ベース VLAN にポートを割り当てます。

スタティック MAC ベース VLAN の割り当てが完了したのち、ポートは受信したフレームを以下のように処理します。

- タグなしフレームの場合、ポートは以下の作業で VLAN ID を決定します。

a) 最初にポートは完全一致を実行します。マスクをすべてFに設定し、MAC-VLANエントリを検索します。フレームの送信元MACアドレスがMAC-VLANエントリのMACアドレスと完全に一致する場合、ポートはエントリに特定なVLAN IDのタグをフレームに付与します。

b) フレームの送信元MACアドレスがMAC-VLANエントリのMACアドレスと完全に一致しない場合、ポートはあいまい一致を実行します。
   - □ ALL-F ではないマスクで MAC-VLAN マッピングリストを検索します。
   - □ 検索キーワードと各マスクの上の論理積演算を実行します。論理積演算の結果がMACアドレスと完全に一致している場合、装置は検索を終了して、対応する VLAN タグをパケットに追加します。

c) VLAN IDが一致しない場合、ポートは以下の順番でVLANを決定します。
   - □ プロトコルベース VLAN

□ ポートベース VLAN

一致している場合、ポートは対応する VLAN タグをフレームに付与します。

- タグづけフレームを受信したとき、フレームの VLAN ID がポートで許可されているか確認します。
  - □ フレームの VLAN ID がポートで許可されている場合、ポートはフレームを転送します。
  - □ フレームの VLAN ID がポートで許可されていない場合、ポートはフレームを廃棄します。

II. ダイナミック MAC ベース VLAN の割り当て

対象のポートの MAC ベース VLAN を決定することができない場合、ダイナミック MAC ベース VLAN を割り当てることができます。ダイナミック MAC ベース VLAN の割り当てを行う場合、以下の作業を行う必要があります。

1) MAC-VLAN エントリを作成します。
2) ポートで MAC ベース VLAN を有効にします。
3) ポートでダイナミック MAC ベース VLAN を有効にします。

図 10-3に示すように、ダイナミック MAC ベース VLAN の割り当てを以下のように処理します。

4) ポートでフレームを受信したとき、ポートはフレームがタグづけされているか確認します。
   - □ もしタグづけされている場合、ポートはフレームの送信元 MAC アドレスに通知します。
   - □ もしタグづけされていない場合、ポートは以下の順番でフレームの VLAN を選択します。
     - □ MAC ベース VLAN（あいまい一致、完全一致）
     - □ プロトコルベース VLAN
     - □ ポートベース VLAN

   選択した VLAN をフレームにタグづけしたのち、ポートはフレームの送信元 MAC アドレスに通知します。
5) ポートは MAC-VLAN エントリに一致するフレームの送信元アドレスと VLAN ID を確認します。
   - □ もしフレームの送信元 MAC アドレスが MAC-VLAN エントリの MAC アドレスに一致している場合、ポートはフレームの VLAN ID がエントリの VLAN に一致するか確認します。
     - □ もし 2 つの VLAN ID が一致している場合、ポートは VLAN に加入し、フレームを転送します。
     - □ もし 2 つの VLAN ID が一致していない場合、ポートはフレームを廃棄します。
   - □ もしフレームの送信元 MAC アドレスが MAC-VLAN エントリの MAC アドレスに一致していない場合、ポートはフレームの VLAN ID が PVID かどうか確認します。
     - □ もしフレームの VLAN ID がポートの PVID である場合、ポートは PVID を許可するか確認します。ポートは PVID でフレームを転送します。もし PVID が許可されていない場合、ポートはフレームを廃棄します。
     - □ フレームの VLAN ID がポートの PVID でない場合、ポートはフレームの VLAN ID が、IP サブネット、プロトコルなどの他の基準に一致するか確認します。もし VLAN が有効でない場合、ポートはフレームを廃棄します。

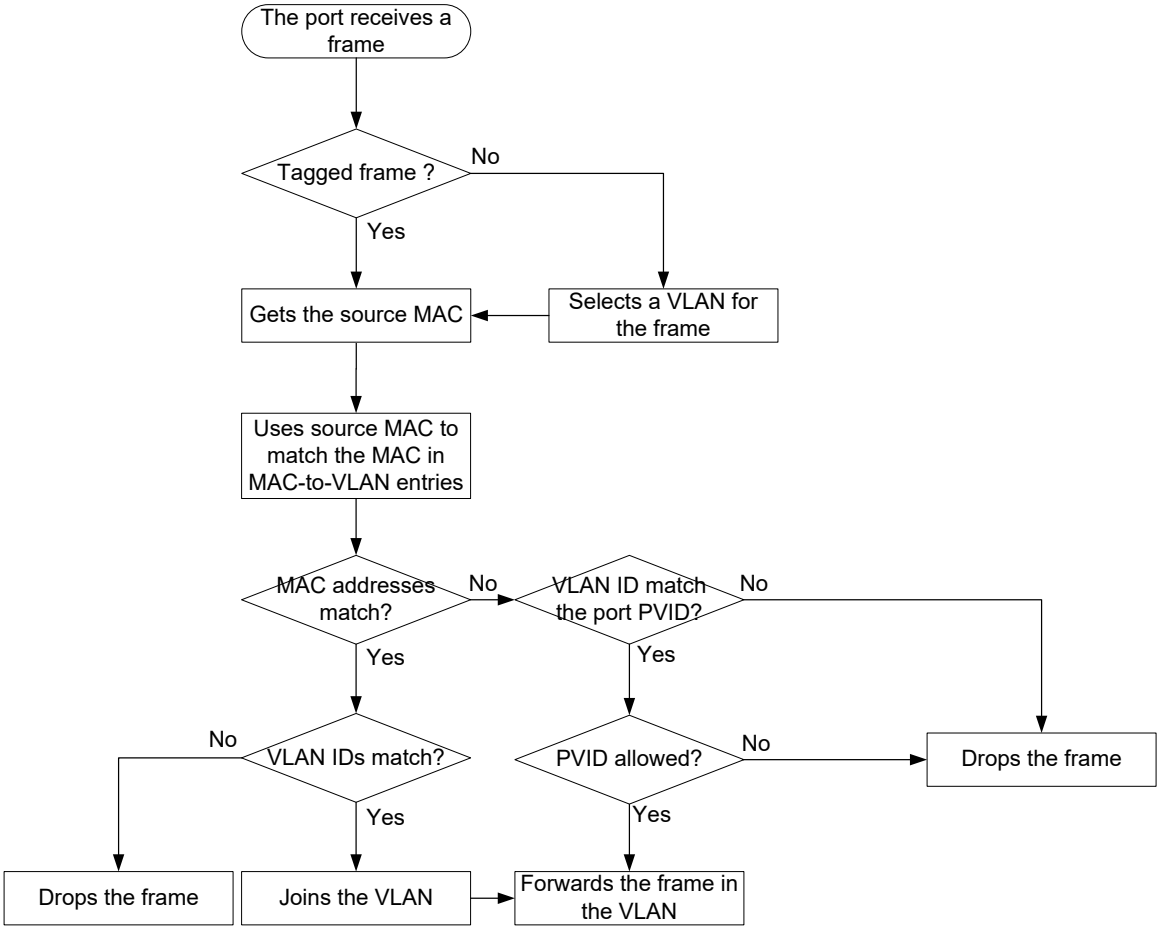


図 10-3 ダイナミック MAC ベース VLAN 割り当てでのフレーム処理のフローチャート

ダイナミック MAC ベース VLAN 割り当てを設定するとき、以下のガイドラインに従ってください。

- ポートを MAC-VLAN エントリの VLAN に加入するとき、ポートの設定に依存して以下のイベントの 1 つが発生します。
  - □ ポートが VLAN からのパケットを通過するように設定していない場合、ポートはタグなしメンバとして MAC-VLAN エントリの VLAN に加入します。
  - □ ポートが VLAN からのパケットを通過するように設定している場合、ポートの設定は変更されません。
- ポートでスタティック MAC ベース VLAN とダイナミック MAC ベース VLAN の両方が設定された場合、ダイナミック MAC ベース VLAN が適用されます。
- パケットが MAC-VLAN エントリに一致するとき、装置は、MAC-VLAN エントリの VLAN の 802.1p 優先度に従い、パケットを転送します。

III. サーバ割り当て MAC ベース VLAN

端末が安全で柔軟にアクセスできるように MAC ベース 802.1X 認証のようなアクセス認証を使用して、サーバによる MAC ベース VLAN を使用します。

1) アクセス装置にアクセスするため、装置で、サーバに割り当てられる MAC ベース VLAN を設定します。

2)　アクセス認証サーバでユーザ名－VLAN エントリを設定します。

ユーザがアクセス認証サーバの認証にパスしたとき、サーバは装置にユーザの VLAN ID を送信します。装置は以下の作業を行います。

3)　ユーザパケットの送信元 MAC アドレスと受信した VLAN ID を使用して MAC-VLAN エントリを作成します。許可 VLAN は MAC ベース VLAN です。

作成された MAC－VLAN エントリは既存のスタティック MAC-VLAN エントリと競合することができません。競合する場合、ダイナミック MAC-VLAN エントリは生成されません。

4)　MAC ベース VLAN にユーザに接続するポートを割り当てます。

ユーザがオフラインのとき、装置は自動的に MAC-VLAN エントリを削除し、MAC ベース VLAN からポートを削除します。802.1X、MAC アドレス認証の詳細は、オペレーションマニュアルのセクション 9 *セキュリティ*“*802.1X*”、“*MAC アドレス認証*”を参照してください。

10.5.2 設定の一般的な制限とガイドライン

MAC ベース VLAN を設定するとき、以下の制限とガイドラインに従ってください。

- MAC ベース VLAN 機能は主にユーザアクセスデバイスの下流ポートで設定されます。リンクアグリゲーションで、MAC ベース VLAN 機能を有効にしないでください。

10.5.3 スタティック MAC ベース VLAN の設定

操作	コマンド	補足
1.　system view に移行する	**system-view**	－
2.　MAC-VLAN エントリを作成する	**mac-vlan mac-address** *mac-address* [**mask** *mac-mask*] **vlan** *vlan-id* [**dot1q** *priority*]	デフォルト：設定なし
3.　interface view に移行する	**interface** *interface-type interface-number*	－
4.　リンクタイプをハイブリッドに設定する	**port link-type hybrid**	デフォルト：アクセス
5.　MAC ベース VLAN でパケットを転送するためハイブリッドポートで許可する VLAN を設定する	**port hybrid vlan** *vlan-id-list* { **tagged** | **untagged** }	デフォルト：ポートのリンクタイプがアクセスであるときに所属している VLAN のタグなしメンバです。
6.　MAC ベース VLAN を有効にする	**mac-vlan enable**	デフォルト：無効
7.　(オプション設定項目) VLAN マッチングの優先順位を設定する	**vlan precedence mac-vlan**	デフォルト：**mac-vlan**

10.5.4 ダイナミック MAC ベース VLAN の設定

I. 設定の制限とガイドライン

MAC ベース VLAN を設定するとき、以下の制限とガイドラインに従ってください。

- 802.1X や MAC アドレス認証を正しく動作させるため、802.1X 認証や MAC アドレス認証とダイナミック MAC ベース VLAN の割り当てを同時に設定しないでください。
- ダイナミック MAC ベース VLAN 割り当てがポートで有効であるとき、MAC 学習を制限する、あるいは MAC 学習を無効にする設定は適用されません。
- ダイナミック MAC ベース VLAN の割り当てを行うため、MAC－VLAN エントリを作成するときスタティック VLAN を使用してください。
- MSTP とダイナミック MAC ベース VLAN の割り当てを同時に設定しないことを推奨します。MSTP が有効になっており、対応する VLAN のインスタンスがブロックされている場合、装置が学習していない送信元 MAC アドレスのパケットは、CPU に送信されません。そのため、対応する VLAN をダイナミックに割り当てられることができません。
- PVST とダイナミック MAC ベース VLAN の割り当てを同時に設定しないことを推奨します。PVST が有効になっており、対応する VLAN がポートで許可されていない場合、ポートはブロック状態になります。受信パケットは CPU に送信されず、廃棄されます。そのため、対応する VLAN をダイナミックに割り当てられることができません。
- ダイナミック MAC ベース VLAN と自動 Voice VLAN の割り当てを同時に設定しないことを推奨します。ポートでダイナミック MAC ベース VLAN と自動 Voice VLAN の割り当ての両方を設定する場合、最初にダイナミック MAC ベース VLAN を設定してください。最初に自動 Voice VLAN の割り当てを設定した場合、衝突が発生します。設定の 1 つを削除するとき、もう一方の動作に影響します。

II. 設定手順

以下にダイナミック MAC ベース VLAN の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	－
2. MAC-VLAN エントリを作成する	**mac-vlan mac-address** *mac-address* [**mask** *mac-mask*] **vlan** *vlan-id* [**dot1q** *priority*]	デフォルト：設定なし
3. interface view に移行する	**interface** *interface-type interface-number*	－
4. リンクタイプをハイブリッドに設定する	**port link-type hybrid**	デフォルト：アクセス
5. MAC ベース VLAN を有効にする	**mac-vlan enable**	デフォルト：無効
6. ダイナミック MAC ベース VLAN を有効にする	**mac-vlan trigger enable**	デフォルト：無効 ポートのVLAN割り当ては受信したパケットのMACアドレスがMAC-VLANエントリのMACアドレスと完全に一致したときのみ発生します。
7. (オプション設定項目) VLAN マッチングの優先順位を設定する	**vlan precedence mac-vlan**	デフォルト：**mac-vlan**

操作	コマンド	補足
8.　（オプション設定項目）PVID で MAC アドレスに一致しないパケットの転送を無効する	**port pvid forbidden**	デフォルト : 受信したパケットの送信元MACアドレスが一致しないとき、PVIDに転送します。

10.5.5 サーバ割り当て MAC ベース VLAN

操作	コマンド	補足
1.　system view に移行する	**system-view**	―
2.　interface view に移行する	**interface** *interface-type interface-number*	―
3.　リンクタイプをハイブリッドに設定する	**port link-type hybrid**	デフォルト：アクセス
4.　MAC ベース VLAN でパケットを転送するためハイブリッドポートで許可する VLAN を設定する	**port hybrid vlan** *vlan-id-list* { **tagged** | **untagged** }	デフォルト : ポートのリンクタイプがアクセスであるときに所属しているVLANのタグなしメンバです。
5.　MAC ベース VLAN を有効にする	**mac-vlan enable**	デフォルト：無効
6.　802.1X あるいは MAC アドレス認証を設定する	コマンドマニュアルのセクション9 *セキュリティ*“*802.1X*”、“*MACアドレス認証*”を参照してください。	―

🕮 **メモ：**

Radius サーバに Tunnel-Private-Group-ID 属性を設定して VLAN アサインする場合は、string で属性値を設定してください。integer で設定した属性値では VLAN のアサインはできません。

10.6 IPサブネットベースVLANの設定

I. 制限とガイドライン

この機能はハイブリッドポートでのみ有効で、タグなしパケットのみ処理します。

II. 設定手順

操作	コマンド	補足
1.　system view に移行する	**system-view**	―
2.　VLAN view に移行する	**vlan** *vlan-id*	―

操作	コマンド	補足
3. VLAN に IP サブネットあるいは IP アドレスを割り当てる	**ip-subnet-vlan** [*ip-subnet-index*] **ip** *ip-address* [*mask*]	デフォルト：VLANはIPサブネットあるいはIPアドレスが割り当てられていません。マルチキャストサブネットあるいはマルチキャストアドレスはVLANに関連づけることができません。
4. system view に戻る	**quit**	―
5. interface view に移行する	● Layer 2 Ethernet interface view に移行する: **interface** *interface-type interface-number* ● Layer 2 aggregate interface viewに移行する: **interface bridge-aggregation** *interface-number*	―
6. リンクタイプをハイブリッドに設定する	**port link-type hybrid**	デフォルト：アクセス
7. IP サブネットベース VLAN にハイブリッドポートを割り当てる	**port hybrid vlan** *vlan-id-list* { **tagged** | **untagged** }	デフォルト：ポートのリンクタイプがアクセスであるときに所属しているVLANのタグなしメンバです。
8. IP サブネットベース VLAN にハイブリッドポートを割り当てる	**port hybrid ip-subnet-vlan vlan** *vlan-id*	デフォルト：設定なし

10.7 プロトコルベースVLAN

10.7.1 概要

プロトコルベース VLAN はプロトコルタイプとカプセル化フォーマットにもとづいて、異なる VLAN に入力パケットを割り当てます。VLAN で有効なプロトコルは IP、IPX、AT があります。カプセル化フォーマットは Ethernet II、802.3 raw、802.2 LLC、802.2 SNAP があります。

この機能は、ハイブリッドポートにのみ有効で、タグなしパケットのみ処理できます。有効なネットワークサービスタイプを VLAN に関連づけます。ネットワーク管理と維持を容易にします。

プロトコルベース VLAN は 1 つ以上のプロトコルテンプレートがあります。プロトコルテンプレートは、入力パケットに一致させる一致条件として、プロトコルタイプとカプセル化フォーマットを定義します。各プロトコルテンプレートはプロトコルベース VLAN で固有のインデックスを持ちます。プロトコルベース VLAN のすべてのプロトコルテンプレートは同一の VLAN ID を持ちます。

ポートで、入力パケットをプロトコルベース VLAN に割り当てるため、以下の作業が必要です。

- プロトコルベース VLAN にポートを割り当てます。
- プロトコルベース VLAN のプロトコルテンプレートにポートを関連づけます。

ポートにタグなしパケットが到達したとき、ポートは以下の処理を行います。

- パケットのプロトコルタイプとカプセル化フォーマットがプロトコルテンプレートに一致した場合、ポートはプロトコルテンプレートに特定な VLAN タグをパケットにタグづけします。
- パケットのプロトコルタイプとカプセル化フォーマットがプロトコルテンプレートに一致しない場合、ポートはパケットに PVID をタグづけします。

自動モードの voice VLAN は、タグあり voice 通信のみを処理します。プロトコルベース VLAN と voice VLAN の両方を VLAN に設定しないでください。

以下にプロトコル VLAN の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. VLAN view に移行する	**vlan** *vlan-id*	―
3. VLAN のプロトコルテンプレートを作成する	**protocol-vlan** [*protocol-index*] { **at** | **ipv4** | **ipv6** | **ipx** { **ethernetii** | **llc** | **snap** } | **mode** { **ethernetii etype** *etype-id* | **llc** { **dsap** *dsap-id* [**ssap** *ssap-id*] | **ssap** *ssap-id* } | **snap etype** *etype-id* } }	デフォルト：設定なし
4. VLAN view から戻る	**quit**	―
5. interface view に移行する	● interface view に移行する：**interface** *interface-type interface-number* ● aggregate interface view に移行する：**interface bridge-aggregation** *interface-number*	―
6. リンクタイプをハイブリッドに設定する	**port link-type hybrid**	デフォルト：アクセス
7. プロトコルベース VLAN にハイブリッドポートを割り当てる	**port hybrid vlan** *vlan-id-list* { **tagged** | **untagged** }	デフォルト：ポートのリンクタイプがアクセスであるときに所属しているVLANのタグなしメンバです。
8. ハイブリッドポートとプロトコルベース VLAN を関連づける	**port hybrid protocol-vlan vlan** *vlan-id* { *protocol-index* [**to** *protocol-end*] | **all** }	デフォルト：設定なし

10.8 VLANの表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
VLANインタフェース情報を表示する	**display interface vlan-interface** [*interface-number*] [**brief** [**description** | **down**]]
指定したポートに関連したIPサブネットベースVLANを表示する	**display ip-subnet-vlan interface** { *interface-type interface-number1* [**to** *interface-type interface-number2*] | **all** }
IPサブネットベースVLANの情報を表示する	**display ip-subnet-vlan vlan** { *vlan-id1* [**to** *vlan-id2*] | **all** }

操作	コマンド
指定したポートに関連したプロトコルベースVLANを表示する	**display protocol-vlan interface** { *interface-type interface-number1* [**to** *interface-type interface-number2*]	**all** }
プロトコルベースVLANの情報を表示する	**display protocol-vlan vlan** { *vlan-id1* [**to** *vlan-id2*]	**all** }
VLAN情報を表示する	**display vlan** [*vlan-id1* [**to** *vlan-id2*]	**all**	**dynamic**	**reserved**	**static**]
VLANの概要情報を表示する	**display vlan brief**
装置のハイブリッドあるいはトランクポートを表示する	**display port** { **hybrid**	**trunk** }
VLANインタフェースの統計情報を削除する	**reset counters interface vlan-interface** [*interface-number*]

10.9 VLAN設定例

10.9.1 ポートベース VLAN 設定例

I. ネットワーク要件

図 10-4に示すように設定します。

- Host A と Host C は Department A に属し、異なる装置を経由して企業ネットワークにアクセスします。VLAN100 は Department A に割り当てられます。
- Host B と Host D は Department D に属し、異なる装置を経由して企業ネットワークにアクセスします。VLAN200 は Department B に割り当てられます。

Host A が Host C と通信し、Host B が Host D に通信できるように、同一 VLAN のホストのみが互いに通信できることを確認します。

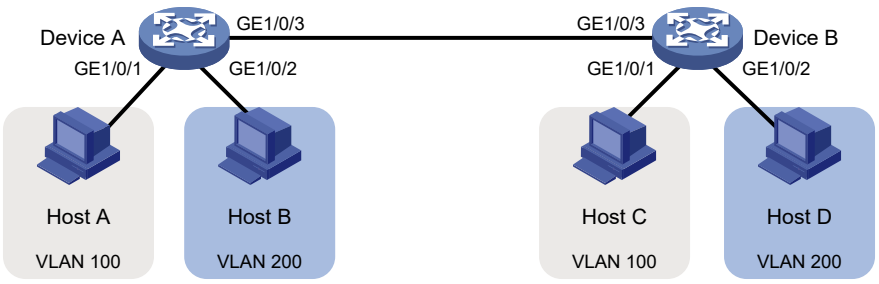


図 10-4 ネットワーク図

II. 設定手順

1)　Device A を設定します。

VLAN 100 を作成し、GigabitEthernet 1/0/1 に割り当てます。

```
<DeviceA> system-view
[DeviceA] vlan 100
```

```
[DeviceA-vlan100] port gigabitethernet 1/0/1
[DeviceA-vlan100] quit
```

VLAN 200 を作成し、GigabitEthernet 1/0/2 に割り当てます。

```
[DeviceA] vlan 200
[DeviceA-vlan200] port gigabitethernet 1/0/2
[DeviceA-vlan200] quit
```

GigabitEthernet 1/0/3 をトランクポートとして VLAN 100、VLAN 200 からのパケットを Device B に転送するよう設定します。

```
[DeviceA] interface gigabitethernet 1/0/3
[DeviceA-GigabitEthernet1/0/3] port link-type trunk
[DeviceA-GigabitEthernet1/0/3] port trunk permit vlan 100 200
Please wait... Done.
```

2) Device A と同様に Device B の設定を行います。
3) host を設定します。
   - □ Host A と Host C を同じ IP サブネットに設定します。たとえば 192.168.100.0/24 です。
   - □ Host B と Host D を同じ IP サブネットに設定します。たとえば 192.168.200.0/24 です。

III. 設定の確認

Host A と Host C がお互いに **ping** ができることを確認し、Host B に **ping** が失敗することを確認します。（詳細は省略します。）

Host B と Host D がお互いに **ping** ができることを確認し、Host A に **ping** が失敗することを確認します。（詳細は省略します。）

VLAN100 と VLAN200 が Device A で正しく設定されていることを確認します。

```
[DeviceA-GigabitEthernet1/0/3] display vlan 100
VLAN ID: 100
VLAN type: Static
Route interface: Not configured
Description: VLAN 0100
Name: VLAN 0100
Tagged ports:
   GigabitEthernet1/0/3
Untagged ports:
   GigabitEthernet1/0/1
[DeviceA-GigabitEthernet1/0/3] display vlan 200
VLAN ID: 200
VLAN type: Static
Route interface: Not configured
Description: VLAN 0200
Name: VLAN 0200
Tagged ports:
   GigabitEthernet1/0/3
Untagged ports:
   GigabitEthernet1/0/2
```

10.9.2 MAC ベース VLAN 設定例

I. ネットワーク要件

図 10-5に示すように設定します。

- Device A と Device C の GigabitEthernet 1/0/1 はミーティングルームに接続されています。Laptop 1、Laptop 2 は 2 つのミーティングルームのどちらかで使用されます。
- Laptop 1、Laptop 2 は異なる部門で使用されます。2 つの部門は VLAN 100、VLAN 200 を使用します。

それぞれの Laptop がミーティングルームで使用されても所属する各部門のみアクセスできるように、MAC ベース VLAN を設定します。

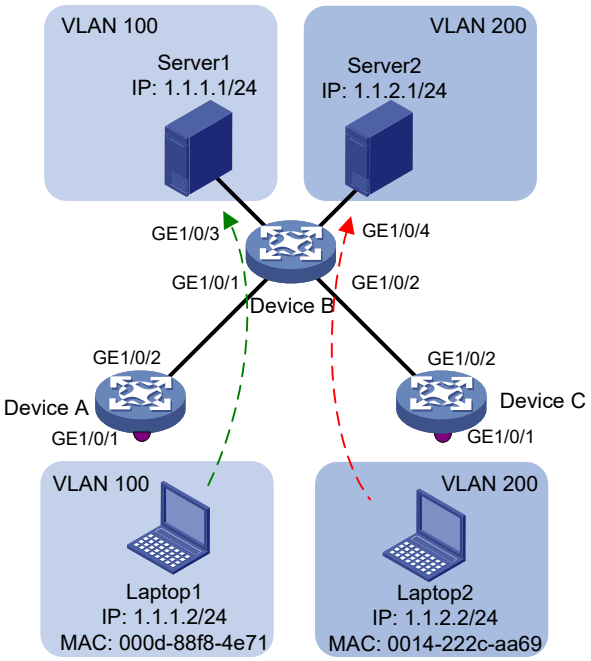


図 10-5 ネットワーク図

II. 設定手順

1)　Device A を設定します。

VLAN100、VLAN200 を作成します。

```
<DeviceA> system-view
[DeviceA] vlan 100
[DeviceA-vlan100] quit
[DeviceA] vlan 200
[DeviceA-vlan200] quit
```

Laptop1 と Laptop2 の MAC アドレスをそれぞれ VLAN 100、VLAN 200 に関連づけます。

```
[DeviceA] mac-vlan mac-address 000d-88f8-4e71 vlan 100
```

```
[DeviceA] mac-vlan mac-address 0014-222c-aa69 vlan 200
```

VLAN100 と VLAN200 からのパケットを VLAN タグなしで転送するため、GigabitEthernet 1/0/1 をハイブリッドポートとして設定します。

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-type hybrid
[DeviceA-GigabitEthernet1/0/1] port hybrid vlan 100 200 untagged
```

GigabitEthernet 1/0/1 で MAC ベース VLAN を有効にします。

```
[DeviceA-GigabitEthernet1/0/1] mac-vlan enable
[DeviceA-GigabitEthernet1/0/1] quit
```

アップリンクポート GigabitEthernet 1/0/2 をトランクポートとして設定し、VLAN 100、VLAN 200 を割り当てます。

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port link-type trunk
[DeviceA-GigabitEthernet1/0/2] port trunk permit vlan 100 200
[DeviceA-GigabitEthernet1/0/2] quit
```

2) Device B を設定します。

VLAN 100 を作成し、GigabitEthernet 1/0/13 を VLAN100 に割り当てます。

```
<DeviceB> system-view
[DeviceB] vlan 100
[DeviceB-vlan100] port gigabitethernet 1/0/3
[DeviceB-vlan100] quit
```

VLAN 200 を作成し、GigabitEthernet 1/0/14 を VLAN 200 に割り当てます。

```
[DeviceB] vlan 200
[DeviceB-vlan200] port gigabitethernet 1/0/4
[DeviceB-vlan200] quit
```

GigabitEthernet 1/0/3 をトランクポートとして設定し、VLAN 100、VLAN 200 を割り当てます。

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port link-type trunk
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[DeviceB-GigabitEthernet1/0/1] quit
```

GigabitEthernet 1/0/4 をトランクポートとして設定し、VLAN 100、VLAN 200 を割り当てます。

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] port link-type trunk
```

```
[DeviceB-GigabitEthernet1/0/2] port trunk permit vlan 100 200
[DeviceB-GigabitEthernet1/0/2] quit
```

3) Device A の設定と同様に、Device C を設定します。（詳細は省略します）

III. 設定の確認

Laptop1 が Server 1 のみアクセスでき、Laptop2 が Server 2 のみアクセスできることを確認します。（詳細は省略します）

Device A と Device C の MAC-VLAN エントリを確認します。たとえば、Device A を確認します。

```
[DeviceA] display mac-vlan all
  The following MAC VLAN addresses exist:
  S:Static  D:Dynamic
  MAC address      Mask             VLAN ID  Priority    State
  000d-88f8-4e71   ffff-ffff-ffff   100       0          S
  0014-222c-aa69   ffff-ffff-ffff   200       0          S

  Total MAC VLAN address count: 2
```

10.9.3 IP サブネットベース VLAN 設定例

I. ネットワーク要件

図 10-6に示すように、Office の Host は異なる IP サブネットに所属します。

それぞれ VLAN 100、VLAN 200 の 192.168.5.0/24、192.168.50.0/24 からパケットを転送するため、Device C を設定します。

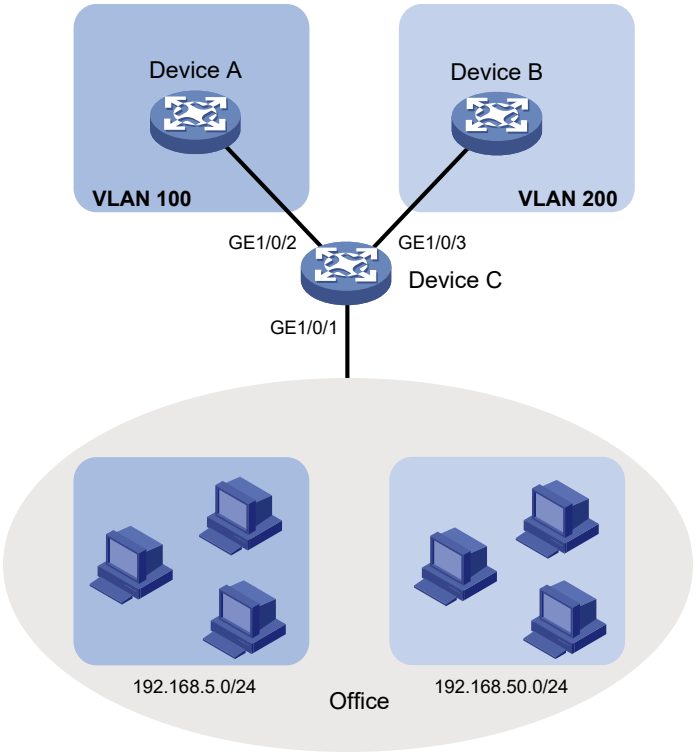


図 10-6 ネットワーク図

II. 設定手順

1)　Device C を設定します。

IP サブネット 192.168.5.0/24 を VLAN 100 に関連づけます。

```
<DeviceC> system-view
[DeviceC] vlan 100
[DeviceC-vlan100] ip-subnet-vlan ip 192.168.5.0 255.255.255.0
[DeviceC-vlan100] quit
```

IP サブネット 192.168.50.0/24 を VLAN 200 に関連づけます。

```
[DeviceC] vlan 200
[DeviceC-vlan200] ip-subnet-vlan ip 192.168.50.0 255.255.255.0
[DeviceC-vlan200] quit
```

ハイブリッドポートとして、GigabitEthernet 1/0/2 を設定し、タグづけ VLAN メンバとして VLAN 100 に割り当てます。

```
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] port link-type hybrid
[DeviceC-GigabitEthernet1/0/2] port hybrid vlan 100 tagged
[DeviceC-GigabitEthernet1/0/2] quit
```

ハイブリッドポートとして、GigabitEthernet 1/0/3 を設定し、タグづけ VLAN メンバとして VLAN 200 に割り当てます。

```
[DeviceC] interface gigabitethernet 1/0/3
[DeviceC-GigabitEthernet1/0/3] port link-type hybrid
[DeviceC-GigabitEthernet1/0/3] port hybrid vlan 200 tagged
[DeviceC-GigabitEthernet1/0/3] quit
```

ハイブリッドポートとして、GigabitEthernet 1/0/1 を設定し、タグなし VLAN メンバとして VLAN 100、VLAN 200 に割り当てます。

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] port link-type hybrid
[DeviceC-GigabitEthernet1/0/1] port hybrid vlan 100 200 untagged
```

GigabitEthernet 1/0/1 を IP サブネットベース VLAN100、VLAN200 に関連づけます。

```
[DeviceC-GigabitEthernet1/0/1] port hybrid ip-subnet-vlan vlan 100
[DeviceC-GigabitEthernet1/0/1] port hybrid ip-subnet-vlan vlan 200
[DeviceC-GigabitEthernet1/0/1] quit
```

2) それぞれ VLAN100、VLAN200 からパケットを転送するため、Device A と Device B を設定します。（詳細は省略します）

III. 設定の確認

Device C の IP サブネットベースの VLAN 設定を確認します。

```
[DeviceC] display ip-subnet-vlan vlan all
 VLAN ID: 100
  Subnet index       IP address      Subnet mask
  0                  192.168.5.0     255.255.255.0

 VLAN ID: 200
  Subnet index       IP address      Subnet mask
  0                  192.168.50.0    255.255.255.0
```

Device C の GigabitEthernet 1/0/1 で IP サブネットベースの VLAN 設定を確認します。

```
[DeviceC] display ip-subnet-vlan interface gigabitethernet 1/0/1
 Interface: GigabitEthernet1/0/1
  VLAN ID   Subnet index    IP address       Subnet mask       Status
  100       0               192.168.5.0      255.255.255.0     Active
  200       0               192.168.50.0     255.255.255.0     Active
```

10.9.4 プロトコルベース VLAN 設定例

I. ネットワーク要件

図 10-7に示すように設定します。

- 実験室の Host の大多数は IPv4 プロトコルで動作します。
- 他の Host は教育目的で IPv6 プロトコルが動作します。

レイヤ 2 で IPv4 トラフィックと IPv6 トラフィックを隔離するため、IPv4 と ARP プロトコルを VLAN 100 に関連づけ、IPv6 プロトコルを VLAN 200 に関連づけるように、プロトコルベース VLAN を設定します。

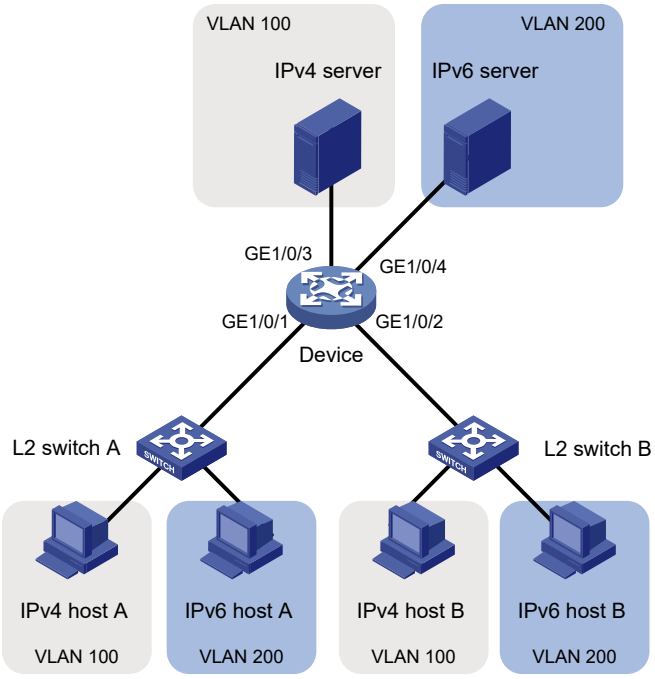


図 10-7 ネットワーク図

II. 設定手順

この例では L2 Switch と L2 Switch は工場出荷状態で使用します。

1)　Device を設定します。

VLAN 100 を作成し、IPv4 のプロトコル VLAN として VLAN 100 の説明を設定します。

```
<Device> system-view
[Device] vlan 100
[Device-vlan100] description protocol VLAN for IPv4
```

GigabitEthernet 1/0/3 に VLAN 100 を割り当てます。

```
[Device-vlan100] port gigabitethernet 1/0/3
[Device-vlan100] quit
```

VLAN200 を作成し、IPv6 のプロトコル VLAN として VLAN 200 の説明を設定します。

```
[Device] vlan 200
[Device-vlan200] description protocol VLAN for IPv6
```

GigabitEthernet 1/0/4 に VLAN 200 を割り当てます。

```
[Device-vlan200] port gigabitethernet 1/0/4
```

プロトコルベース VLAN として VLAN 200 を設定し、VLAN 200 用にインデックスが 1 の IPv6 プロトコルテンプレートを作成します。

```
[Device-vlan200] protocol-vlan 1 ipv6
```

```
[Device-vlan200] quit
```

プロトコルベース VLAN として VLAN 100 を設定し、VLAN 100 用にインデックスが 1 の IPv4 プロトコルテンプレートを作成します。VLAN 100 のインデックスが 2 の ARP プロトコルテンプレートを作成します。（カプセル化は Ethernet II で、ARP のプロトコルタイプが 16 進数で 0x0806 です。）

```
[Device] vlan 100
[Device-vlan100] protocol-vlan 1 ipv4
[Device-vlan100] protocol-vlan 2 mode ethernetii etype 0806
[Device-vlan100] quit
```

#ハイブリッドポートとして GigabitEthernet 1/0/1 を設定し、タグなし VLAN メンバとして VLAN 100、VLAN 200 に割り当てます。

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] port link-type hybrid
[Device-GigabitEthernet1/0/1] port hybrid vlan 100 200 untagged
```

GigabitEthernet 1/0/1 に VLAN 100 の IPv4、ARP プロトコルテンプレートを関連づけ、VLAN 200 の IPv6 プロトコルテンプレートを関連づけます。

```
[Device-GigabitEthernet1/0/1] port hybrid protocol-vlan vlan 100 1 to 2
[Device-GigabitEthernet1/0/1] port hybrid protocol-vlan vlan 200 1
[Device-GigabitEthernet1/0/1] quit
```

#ハイブリッドポートとして GigabitEthernet 1/0/2 を設定し、タグなし VLAN メンバとして VLAN 100、VLAN 200 に割り当てます。

```
[Device] interface gigabitethernet 1/0/2
[Device-GigabitEthernet1/0/2] port link-type hybrid
[Device-GigabitEthernet1/0/2] port hybrid vlan 100 200 untagged
```

GigabitEthernet 1/0/2 に VLAN 100 の IPv4、ARP プロトコルテンプレートを関連づけ、VLAN 200 の IPv6 プロトコルテンプレートを関連づけます。

```
[Device-GigabitEthernet1/0/2] port hybrid protocol-vlan vlan 100 1 to 2
[Device-GigabitEthernet1/0/2] port hybrid protocol-vlan vlan 200 1
[Device-GigabitEthernet1/0/2] quit
```

2) Host と Server を設定します。

a) IPv4 Host A、IPv4 Host B、IPv4 serverを同一ネットワークセグメント上に設定します。（たとえば、192.168.100.0/24です。）（詳細は省略します。）

b) IPv6 Host A、IPv6 Host B、IPv6 serverを同一ネットワークセグメント上に設定します。（たとえば、2001::1/64です。）（詳細は省略します。）

III. 設定の確認

1) 以下を確認します。

- □ VLAN 100 の Host と Server が互いに ping できることを確認します。（詳細は省略します。）
- □ VLAN 200 の Host と Server が互いに ping できることを確認します。（詳細は省略します）
- □ VLAN 100 の Host あるいは Server が、VLAN 200 の Host あるいは Server に ping できないことを確認します。（詳細は省略します）

2) プロトコルベース VLAN の設定を確認します。

Device のプロトコルベース VLAN を表示します。

```
[Device] display protocol-vlan vlan all
 VLAN ID: 100
  Protocol index  Protocol type
  1               IPv4
  2               Ethernet II Etype 0x0806

 VLAN ID: 200
  Protocol index  Protocol type
  1               IPv6
```

Device のポートでプロトコルベース VLAN を表示します。

```
[Device] display protocol-vlan interface all
 Interface: GigabitEthernet1/0/1
  VLAN ID  Protocol index  Protocol type             Status
  100      1              IPv4                     Active
  100      2              Ethernet II Etype 0x0806 Active
  200      1              IPv6                     Active

 Interface: GigabitEthernet 1/0/2
  VLAN ID  Protocol index  Protocol type             Status
  100      1              IPv4                     Active
  100      2              Ethernet II Etype 0x0806 Active
  200      1              IPv6                     Active
```

目次

このセクションのページは **3-x-x** です。

11 章 Private VLAN 11-1
11.1 概要 11-1
11.2 制限とガイドライン 11-2
11.3 Private VLAN 設定作業リスト 11-2
11.4 プライマリ VLAN の作成 11-2
11.5 セカンダリ VLAN の作成 11-3
11.6 プライマリ VLAN とセカンダリ VLAN の関連付け 11-3
11.7 アップリンクポートの設定 11-3
11.7.1 アップリンクポートについて 11-3
11.7.2 設定手順 11-3
11.8 ダウンリンクポートの設定 11-4
11.8.1 ダウンリンクポートについて 11-4
11.8.2 設定手順 11-4
11.9 セカンダリ VLAN 間のレイヤ 3 通信の設定 11-5
11.10 Private VLAN の表示と維持 11-5
11.11 Private VLAN 設定例 11-5
11.11.1 プロミスカスポートの設定例 11-5
11.11.2 トランクプロミスカスポートの設定例 11-8
11.11.3 トランクプロミスカスとトランクセカンダリの設定例 11-12
11.11.4 セカンダリ VLAN でのレイヤ 3 通信の 設定例 11-16

11章 Private VLAN

11.1 概要

VLAN 機能はカスタマからトラフィックを分離するための方法を提供します。ネットワークのアクセスレイヤでは、セキュリティ確保等の目的でカスタマトラフィックを分離する必要があります。VLAN がユーザ単位に割り当てられている場合、多数の VLAN が必要になります。

Private VLAN 機能は VLAN を 2 層構成にすることで VLAN のリソースを抑えることができます。

- **プライマリ VLAN**：アップリンクに接続するために使用します。プライマリ VLAN は複数のセカンダリ VLAN を関連付けできアップリンクの装置はプライマリ VLAN が指定されています。
- **セカンダリ VLANs**：ユーザ側に接続するために使用します。セカンダリ VLAN はレイヤ 2 で分離されます。プライマリ VLAN と関連付けたセカンダリ VLAN の間でレイヤ 3 通信を実現するためには、アップリンク装置ではローカルプロキシ ARP を有効にしてください。

図 11-1のように、Private VLAN 機能は L2 Device B で有効にします。VLAN10 はプライマリ VLAN、VLAN2、5、8 は VLAN10 のセカンダリ VLAN に関連付けられます。L3 Device A は VLAN10 のみ認識します。

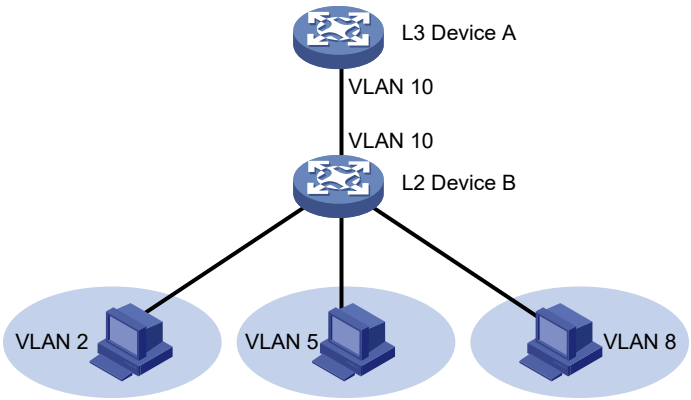


図 11-1 Private VLAN 例

Private VLAN 機能をレイヤ 3 装置上で設定する場合、レイヤ 3 通信を有効にするために以下の方法のいずれかを使用してください。レイヤ 3 通信は同じプライマリ VLAN に関連付けられたセカンダリ VLAN 間や他のネットワークの間で必要となる場合があります。

I. 方法 1:

- セカンダリ VLAN に VLAN インタフェースを作成します。
- セカンダリ VLAN インタフェースに IP アドレスを作成します。

II. 方法 2:

- プライマリ VLAN と関連付けられたセカンダリ VLAN 間でレイヤ 3 通信を有効にします。
- プライマリ VLAN の VLAN インタフェースを作成して、IP アドレスを作成します。（この方法を使用する場合は、セカンダリ VLAN インタフェースを作成しないでください。）
- プライマリ VLAN インタフェースでローカルプロキシ ARP を有効にします。

11.2 制限とガイドライン

- 以下の要件が満たされていることを確認してください。
  - プロミスカスポートの場合
    - プライマリ VLAN はそのポートの PVID であること。
    - そのポートがプライマリ VLAN とセカンダリ VLAN の untagged メンバであること。
  - ホストポートの場合
    - そのポートの PVID はセカンダリ VLAN であること。
    - そのポートはプライマリ VLAN とセカンダリ VLAN の untagged メンバであること。
  - トランクプロミスカスまたはトランクセカンダリポートはプライマリ VLAN とセカンダリ VLAN の tagged メンバであること。
- VLAN1（システムデフォルト VLAN）は Private VLAN 設定をサポートしていません。

11.3 Private VLAN設定作業リスト

作業リスト
（必須設定項目）プライマリVLANの作成
（必須設定項目）セカンダリVLANの作成
（必須設定項目）プライマリVLANとセカンダリVLANの関連付け
（必須設定項目）アップリンクポートの設定
（必須設定項目）ダウンリンクポートの設定
（オプション設定項目）セカンダリVLAN間のレイヤ3通信の設定

11.4 プライマリVLANの作成

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. VLAN を作成し、view へ移行する	**vlan** *vlan-id*	―
3. プライマリ VLAN を作成する	**private-vlan primary**	デフォルト： VLAN はプライマリ VLAN ではありません。

11.5 セカンダリVLANの作成

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. VLAN を作成し、view へ移行する	**vlan** { *vlan-id-list* | **all** }	―

11.6 プライマリVLANとセカンダリVLANの関連付け

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. VLAN を作成し、プライマリ VLAN の view へ移行する	**vlan** *vlan-id*	―
3. プライマリ VLAN にセカンダリ VLAN を関連付ける	**private-vlan secondary** *vlan-id-list*	デフォルト：設定なし

11.7 アップリンクポートの設定

11.7.1 アップリンクポートについて

アップリンクポートを以下に従い設定します。

- 1つだけプライマリ VLAN を許可する場合は、ポートをプライマリ VLAN のプロミスカスポートとして設定します。プロミスカスポートはプライマリ VLAN と関連付けられたセカンダリポートに自動的に割り当てられます。
- 複数のプライマリポートを許可する場合は、ポートをプライマリ VLAN のトランクプロミスカスポートとして設定します。トランクプロミスカスポートはプライマリ VLAN と関連付けられたセカンダリポートに自動的に割り当てられます。

11.7.2 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. アップリンクポートの interface view に移行する	**interface** *interface-type interface-number*	―
3. アップリンクポートを指定した VLAN のプロミスカスポートまたはトランクプロミスカスポートに設定する	• プロミスカスポートを設定する場合： **port private-vlan** *vlan-id* **promiscuous** • トランクプロミスカスポートを設定する場合： **port private-vlan** *vlan-id-list* **trunk promiscuous**	デフォルト：設定なし

11.8 ダウンリンクポートの設定

11.8.1 ダウンリンクポートについて

ダウンリンクポートを以下に従い設定します。

- ダウンリンクポートを 1 つのセカンダリ VLAN のみを許可する場合、そのポートはホストポートとして設定してください。そのホストポートはセカンダリ VLAN と関連付けたプライマリ VLAN が自動的に設定されます。
- ダウンリンクポートを複数のセカンダリ VLAN で許可する場合、そのポートはトランクセカンダリポートとして設定してください。そのトランクセカンダリポートはセカンダリ VLAN と関連付けたプライマリ VLAN が自動的に設定されます。

11.8.2 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. アップリンクポートの interface view に移行する	**interface** *interface-type interface-number*	―
3. ダウンリンクポートをセカンダリ VLAN に設定する	1. リンクタイプを設定する： **port link-type** { **access** | **hybrid** | **trunk** } 2. アクセス VLAN を設定する： **port access vlan** *vlan-id* 3. トランクポートで許可する VLAN を設定する： **port trunk permit vlan** { *vlan-id-list* | **all** } 4. ハイブリッドポートの VLAN を設定する： **port hybrid vlan** *vlan-id-list* { **tagged** | **untagged** } 2、3、4はリンクタイプの設定に依存します。	デフォルト：設定なし
4. ダウンリンクポートをホストポートまたはトランクセカンダリポートに設定する	1. ホストポートに設定する： **port private-vlan host** 2. トランクセカンダリポートに設定する： **port private-vlan** *vlan-id-list* **trunk secondary**	デフォルト：設定なし
5. System view に戻る	**quit**	―
6. セカンダリ VLAN の VLAN view へ移行する	**vlan** *vlan-id*	―
7. 同じセカンダリ VLAN のポート間でレイヤ 2 通信を有効にする	**undo private-vlan isolated**	(オプション設定項目) デフォルト：レイヤ2通信が可能

11.9 セカンダリVLAN間のレイヤ3通信の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. プライマリ VLAN の VLAN interface view へ移行する	**interface vlan-interface** *interface-number*	―
3. プライマリ VLAN と関連付けたセカンダリ VLAN 間のレイヤ 3 通信を有効にする	**private-vlan secondary** *vlan-id-list*	デフォルト：無効
4. プライマリ VLAN インタフェースに IP アドレスを設定する	**ip address** *ip-address* { *mask-length* | *mask* } [**sub**]	デフォルト：設定なし
5. ローカルプロキシ ARP を設定する	**local-proxy-arp enable**	デフォルト：無効

11.10 Private VLANの表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
プライマリVLANとセカンダリVLANの関連付け情報を表示する	**display private-vlan** [*primary-vlan-id*]

11.11 Private VLAN設定例

11.11.1 プロミスカスポートの設定例

I. ネットワーク要件

図 11-2に示すように設定します。

- Device B は、VLAN5 をプライマリ VLAN としてセカンダリ VLAN に VLAN2 と 3 を関連付けます。GigabitEthernet 1/0/5は VLAN 5、GigabitEthernet 1/0/2は VLAN 2、GigabitEthernet 1/0/3 は VLAN 3 を割り当てます。
- Device C は、VLAN6 をプライマリ VLAN としてセカンダリ VLAN に VLAN3 と 4 を関連付けます。GigabitEthernet 1/0/5は VLAN 6、GigabitEthernet 1/0/3は VLAN 3、GigabitEthernet 1/0/4は VLAN 4 を割り当てます。
- Device A は Device B の VLAN 5、Device C の VLAN 6 に接続します。

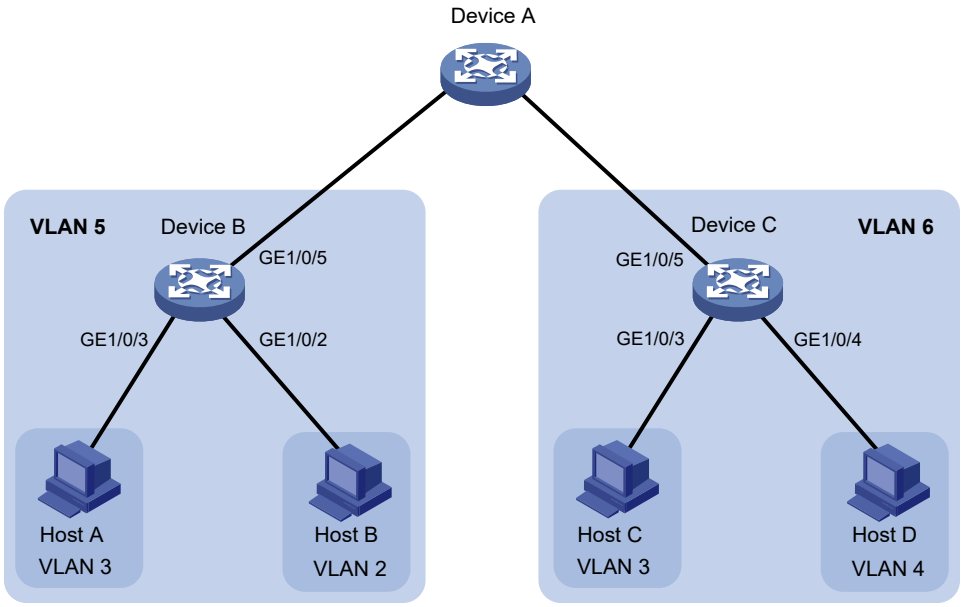


図 11-2 ネットワーク図

II. 設定手順

1)　Device B を設定します。

VLAN5 をプライマリ VLAN に設定します。

```
<DeviceB> system-view
[DeviceB] vlan 5
[DeviceB-vlan5] private-vlan primary
[DeviceB-vlan5] quit
```

VLAN2 と 3 を作成します。

```
[DeviceB] vlan 2 to 3
```

VLAN2 と 3 をプライマリ VLAN5 のセカンダリ VLAN に設定します。

```
[DeviceB] vlan 5
[DeviceB-vlan5] private-vlan secondary 2 to 3
[DeviceB-vlan5] quit
```

GigabitEthernet 1/0/5を VLAN5 のプロミスカスポートに設定します。

```
[DeviceB] interface gigabitethernet 1/0/5
[DeviceB-GigabitEthernet1/0/5] port private-vlan 5 promiscuous
[DeviceB-GigabitEthernet1/0/5] quit
```

GigabitEthernet 1/0/2を VLAN2 に割り当てホストポートに設定します。

```
[DeviceB] interface gigabitethernet 1/0/2
```

```
[DeviceB-GigabitEthernet1/0/2] port access vlan 2
[DeviceB-GigabitEthernet1/0/2] port private-vlan host
[DeviceB-GigabitEthernet1/0/2] quit
```

GigabitEthernet 1/0/3 を VLAN 3 に割り当てホストポートに設定します。

```
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] port access vlan 3
[DeviceB-GigabitEthernet1/0/3] port private-vlan host
[DeviceB-GigabitEthernet1/0/3] quit
```

2) Device C を設定します。

VLAN6 をプライマリ VLAN に設定します。

```
<DeviceC> system-view
[DeviceC] vlan 6
[DeviceC-vlan6] private-vlan primary
[DeviceC-vlan6] quit
```

VLAN3 と 4 を作成します。

```
[DeviceC] vlan 3 to 4
```

VLAN3 と 4 をプライマリ VLAN6 のセカンダリ VLAN に設定します。

```
[DeviceC] vlan 6
[DeviceC-vlan6] private-vlan secondary 3 to 4
[DeviceC-vlan6] quit
```

GigabitEthernet 1/0/5を VLAN6 のプロミスカスポートに設定します。

```
[DeviceC] interface gigabitethernet 1/0/5
[DeviceC-GigabitEthernet1/0/5] port private-vlan 6 promiscuous
[DeviceC-GigabitEthernet1/0/5] quit
```

GigabitEthernet 1/0/3を VLAN 3 に割り当てホストポートに設定します。

```
[DeviceC] interface gigabitethernet 1/0/3
[DeviceC-GigabitEthernet1/0/3] port access vlan 3
[DeviceC-GigabitEthernet1/0/3] port private-vlan host
[DeviceC-GigabitEthernet1/0/3] quit
```

GigabitEthernet 1/0/4を VLAN 4 に割り当て、ホストポートに設定します。

```
[DeviceC] interface gigabitethernet 1/0/4
[DeviceC-GigabitEthernet1/0/4] port access vlan 4
[DeviceC-GigabitEthernet1/0/4] port private-vlan host
[DeviceC-GigabitEthernet1/0/4] quit
```

III. 設定の確認

Private VLAN が装置に設定されていることを確認します（Device B を例とします）。

```
[DeviceB] display private-vlan
 Primary VLAN ID: 5
 Secondary VLAN ID: 2-3

 VLAN ID: 5
 VLAN type: Static
 Private VLAN type: Primary
 Route interface: Not configured
 Description: VLAN 0005
 Name: VLAN 0005
 Tagged ports:   None
 Untagged ports:
    GigabitEthernet1/0/2
    GigabitEthernet1/0/3
    GigabitEthernet1/0/5

 VLAN ID: 2
 VLAN type: Static
 Private VLAN type: Secondary
 Route interface: Not configured
 Description: VLAN 0002
 Name: VLAN 0002
 Tagged ports:   None
 Untagged ports:
    GigabitEthernet1/0/2
    GigabitEthernet1/0/5

 VLAN ID: 3
 VLAN type: Static
 Private VLAN type: Secondary
 Route interface: Not configured
 Description: VLAN 0003
 Name: VLAN 0003
 Tagged Ports:   None
 Untagged Ports:
    GigabitEthernet1/0/3
    GigabitEthernet1/0/5
```

出力は以下を示します。

- プロミスカスポート(GigabitEthernet 1/0/5) はプライマリ VLAN5 とセカンダリ VLAN2 と 3 の untagged メンバです。
- ホストポート(GigabitEthernet 1/0/2)はプライマリ VLAN5 とセカンダリ VLAN2 の untagged メンバです。
- ホストポート(GigabitEthernet 1/0/3)はプライマリ VLAN5 is an untagged member of primary VLAN 5 and secondary VLAN 3.

11.11.2 トランクプロミスカスポートの設定例

I. ネットワーク要件

図 11-3に示すように設定します。

- VLAN5 と VLAN10 を Device B のプライマリ VLAN とします。Device B のアップリンクポート(GigabitEthernet 1/0/1) は VLAN5 と VLAN10 から VLAN タグ付きパケットの転送を許可します。

- Device B は、ダウンリンクポート(GigabitEthernet 1/0/2)でセカンダリ VLAN2 を許可します。ダウンリンクポート(GigabitEthernet 1/0/3)でセカンダリ VLAN3 を許可します。セカンダリ VLAN2 と 3 はプライマリ VLAN5 に関連付けられています。
- Device B は、ダウンリンクポート(GigabitEthernet 1/0/4)でセカンダリ VLAN6 を許可します。ダウンリンクポート(GigabitEthernet 1/0/5)でセカンダリ VLAN8 を許可します。セカンダリ VLAN6 と 8 はプライマリ VLAN10 に関連付けられています。
- Device A は Device B の VLAN5 と 10 に接続します。

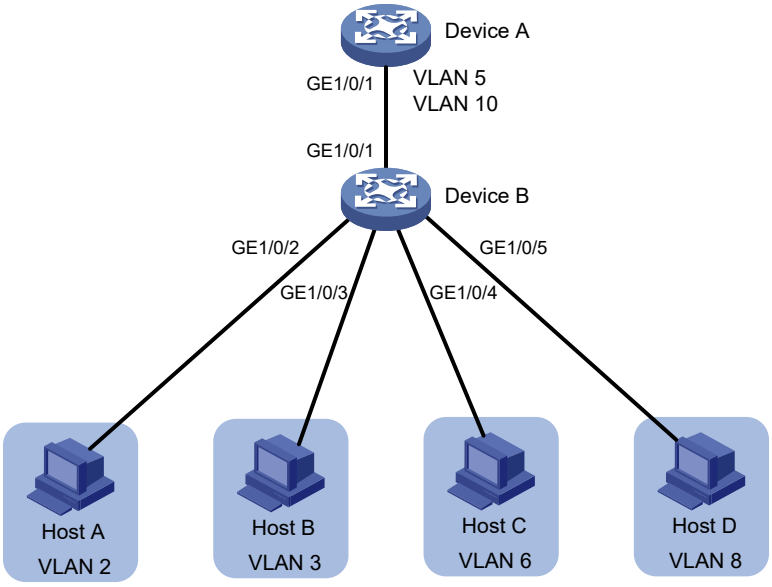


図 11-3 ネットワーク図

II. 設定手順

1)　Device B を設定します。

VLAN5 と 10 をプライマリ VLAN に設定します。

```
<DeviceB> system-view
[DeviceB] vlan 5
[DeviceB-vlan5] private-vlan primary
[DeviceB-vlan5] quit
[DeviceB] vlan 10
[DeviceB-vlan10] private-vlan primary
[DeviceB-vlan10] quit
```

VLAN2、3、6、8 を作成します。

```
[DeviceB] vlan 2 to 3
[DeviceB] vlan 6
[DeviceB-vlan6] quit
[DeviceB] vlan 8
```

```
[DeviceB-vlan8] quit
```

セカンダリ VLAN2 と 3 をプライマリ VLAN5 に関連付けます。

```
[DeviceB] vlan 5
[DeviceB-vlan5] private-vlan secondary 2 to 3
[DeviceB-vlan5] quit
```

セカンダリ VLAN6 と 8 をプライマリ VLAN10 に関連付けます。

```
[DeviceB] vlan 10
[DeviceB-vlan10] private-vlan secondary 6 8
[DeviceB-vlan10] quit
```

GigabitEthernet 1/0/1 を VLAN5 と 10 のトランクプロミスカスポートに設定します。

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port private-vlan 5 10 trunk promiscuous
[DeviceB-GigabitEthernet1/0/1] quit
```

GigabitEthernet 1/0/2 を VLAN2 に割り当て、ホストポートに設定します。

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] port access vlan 2
[DeviceB-GigabitEthernet1/0/2] port private-vlan host
[DeviceB-GigabitEthernet1/0/2] quit
```

GigabitEthernet 1/0/3 を VLAN 3 に割り当て、ホストポートに設定します。

```
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] port access vlan 3
[DeviceB-GigabitEthernet1/0/3] port private-vlan host
[DeviceB-GigabitEthernet1/0/3] quit
```

GigabitEthernet 1/0/4 を VLAN 6 に割り当て、ホストポートに設定します。

```
[DeviceB] interface gigabitethernet 1/0/4
[DeviceB-GigabitEthernet1/0/4] port access vlan 6
[DeviceB-GigabitEthernet1/0/4] port private-vlan host
[DeviceB-GigabitEthernet1/0/4] quit
```

GigabitEthernet 1/0/5 を VLAN 8 に割り当て、ホストポートに設定します。

```
[DeviceB] interface gigabitethernet 1/0/5
[DeviceB-GigabitEthernet1/0/5] port access vlan 8
[DeviceB-GigabitEthernet1/0/5] port private-vlan host
[DeviceB-GigabitEthernet1/0/5] quit
```

2) Device A を設定します。

VLAN5 と 10 を作成します。

```
[DeviceA] vlan 5
[DeviceA-vlan5] quit
[DeviceA] vlan 10
[DeviceA-vlan10] quit
```

GigabitEthernet 1/0/1 をハイブリッドポートに設定して、VLAN5 と 10 を tagged メンバとして割り当てます。

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-type hybrid
[DeviceA-GigabitEthernet1/0/1] port hybrid vlan 5 10 tagged
[DeviceA-GigabitEthernet1/0/1] quit
```

III. 設定の確認

Device B のプライマリ VLAN 情報を確認します（プライマリ VLAN5 を例とします）。

```
[DeviceB] display private-vlan 5
Primary VLAN ID: 5
Secondary VLAN ID: 2-3

VLAN ID: 5
VLAN type: Static
Private VLAN type: Primary
Route interface: Not configured
Description: VLAN 0005
Name: VLAN 0005
Tagged ports:
   GigabitEthernet1/0/1
Untagged ports:
   GigabitEthernet1/0/2
   GigabitEthernet1/0/3

VLAN ID: 2
VLAN type: Static
Private VLAN type: Secondary
Route interface: Not configured
Description: VLAN 0002
Name: VLAN 0002
Tagged ports:
   GigabitEthernet1/0/1
Untagged ports:
   GigabitEthernet1/0/2

VLAN ID: 3
VLAN type: Static
Private VLAN type: Secondary
Route interface: Not configured
Description: VLAN 0003
Name: VLAN 0003
Tagged ports:
   GigabitEthernet1/0/1
Untagged ports:
   GigabitEthernet1/0/3
```

出力は以下を示します。

- トランク プロミスカスポート(GigabitEthernet 1/0/1)はプライマリ VLAN5 とセカンダリ VLAN2 と 3 の tagged メンバです。
- ホストポート(GigabitEthernet 1/0/2)はプライマリ VLAN5 とセカンダリ VLAN2 の untagged ポートです。
- ホストポート(GigabitEthernet 1/0/3)はプライマリ VLAN5 とセカンダリ VLAN3 の untagged ポートです。

11.11.3 トランクプロミスカスとトランクセカンダリの設定例

I. ネットワーク要件

図 11-4に示すように設定します。

- VLAN10 と 20 は Device A のプライマリ VLAN です。Device A のアップリンクポート(GigabitEthernet 1/0/5)は VLAN10 と 20 からの VLAN タグ付きパケットの転送を許可します。
- VLAN11、12、21、22 は Device A のセカンダリ VLAN です。
  - ダウンリンクポート(GigabitEthernet 1/0/2)はセカンダリ VLAN11 と 21 からの VLAN タグ付きパケットの転送を許可します。
  - ダウンリンクポート(GigabitEthernet 1/0/1)はセカンダリ VLAN22 を許可します。
  - ダウンリンクポート(GigabitEthernet 1/0/3)はセカンダリ VLAN12 を許可します。
- セカンダリ VLAN11 と 12 はプライマリ VLAN10 と関連付けます。
- セカンダリ VLAN21 と 22 はプライマリ VLAN20 と関連付けます。

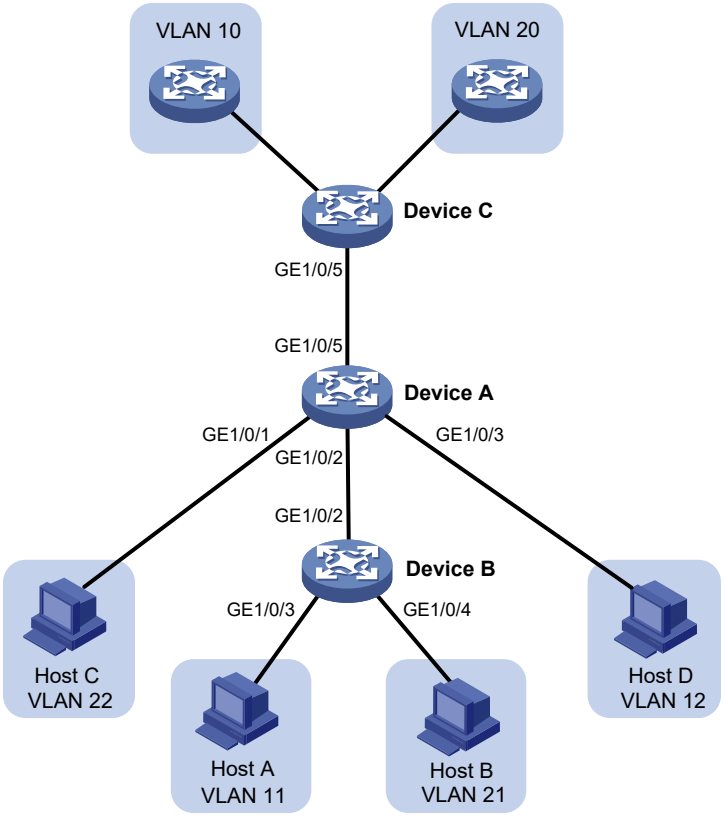


図 11-4 ネットワーク図

II. 設定手順

1)　Device A を設定します。

VLAN10 と 20 はプライマリ VLAN に設定します。

```
<DeviceA> system-view
[DeviceA] vlan 10
[DeviceA-vlan10] private-vlan primary
[DeviceA-vlan10] quit
[DeviceA] vlan 20
[DeviceA-vlan20] private-vlan primary
[DeviceA-vlan20] quit
```

VLAN11、12、21、22 を作成します。

```
[DeviceA] vlan 11 to 12
[DeviceA] vlan 21 to 22
```

セカンダリ VLAN11 と 12 をプライマリ VLAN10 に関連付けます。

```
[DeviceA] vlan 10
```

```
[DeviceA-vlan10] private-vlan secondary 11 12
[DeviceA-vlan10] quit
```

セカンダリ VLAN21 と 22 をプライマリ VLAN20 に関連付けます。

```
[DeviceA] vlan 20
[DeviceA-vlan20] private-vlan secondary 21 22
[DeviceA-vlan20] quit
```

GigabitEthernet 1/0/5 を VLAN10 と 20 のトランクプロミスカスポートに設定します。

```
[DeviceA] interface gigabitethernet 1/0/5
[DeviceA-GigabitEthernet1/0/5] port private-vlan 10 20 trunk promiscuous
[DeviceA-GigabitEthernet1/0/5] quit
```

GigabitEthernet 1/0/1 を VLAN 22 に割り当て、ホストポートに設定します。

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port access vlan 22
[DeviceA-GigabitEthernet1/0/1] port private-vlan host
[DeviceA-GigabitEthernet1/0/1] quit
```

GigabitEthernet 1/0/3 を VLAN 12 に割り当て、ホストポートに設定します。

```
[DeviceA] interface gigabitethernet 1/0/3
[DeviceA-GigabitEthernet1/0/3] port access vlan 12
[DeviceA-GigabitEthernet1/0/3] port private-vlan host
[DeviceA-GigabitEthernet1/0/3] quit
```

GigabitEthernet 1/0/2 を VLAN11 と 21 のトランクセカンダリに設定します。

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port private-vlan 11 21 trunk secondary
[DeviceA-GigabitEthernet1/0/2] quit
```

2) Device B を設定します。

VLAN11 と 21 を作成します。

```
<DeviceB> system-view
[DeviceB] vlan 11
[DeviceB-vlan11] quit
[DeviceB] vlan 21
[DeviceB-vlan21] quit
```

GigabitEthernet 1/0/2をハイブリッドポートに設定して、VLAN11 と 21 を tagged メンバとして割り当てます。

```
[DeviceB] interface gigabitethernet 1/0/2
```

```
[DeviceB-GigabitEthernet1/0/2] port link-type hybrid
[DeviceB-GigabitEthernet1/0/2] port hybrid vlan 11 21 tagged
[DeviceB-GigabitEthernet1/0/2] quit
```

GigabitEthernet 1/0/3 に VLAN 11 を割り当てます。

```
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] port access vlan 11
[DeviceB-GigabitEthernet1/0/3] quit
```

GigabitEthernet 1/0/4 に VLAN 21 を割り当てます。

```
[DeviceB] interface gigabitethernet 1/0/4
[DeviceB-GigabitEthernet1/0/4] port access vlan 21
[DeviceB-GigabitEthernet1/0/4] quit
```

3) Device C を設定します。

VLAN10 と 20 を作成します。

```
<DeviceC> system-view
[DeviceC] vlan 10
[DeviceC-vlan10] quit
[DeviceC] vlan 20
[DeviceC-vlan20] quit
```

GigabitEthernet 1/0/5 をハイブリッドポートに設定して、VLAN10 と 20 を tagged メンバとして割り当てます。

```
[DeviceC] interface gigabitethernet 1/0/5
[DeviceC-GigabitEthernet1/0/5] port link-type hybrid
[DeviceC-GigabitEthernet1/0/5] port hybrid vlan 10 20 tagged
[DeviceC-GigabitEthernet1/0/5] quit
```

III. 設定の確認

Device A のプライマリ VLAN 情報を確認します（プライマリ VLAN10 を例とします）。

```
[DeviceA] display private-vlan 10
 Primary VLAN ID: 10
 Secondary VLAN ID: 11-12

 VLAN ID: 10
 VLAN type: Static
 Private-vlan type: Primary
 Route interface: Not configured
 Description: VLAN 0010
 Name: VLAN 0010
 Tagged ports:
    GigabitEthernet1/0/2
    GigabitEthernet1/0/5
 Untagged ports:
    GigabitEthernet1/0/3
```

```
VLAN ID: 11
VLAN type: Static
Private-vlan type: Secondary
Route interface: Not configured
Description: VLAN 0011
Name: VLAN 0011
Tagged ports:
   GigabitEthernet1/0/2
   GigabitEthernet1/0/5
Untagged ports: None

VLAN ID: 12
VLAN type: Static
Private-vlan type: Secondary
Route interface: Not configured
Description: VLAN 0012
Name: VLAN 0012
Tagged ports:
   GigabitEthernet1/0/5
Untagged ports:
   GigabitEthernet1/0/3
```

出力は以下を示します。

- トランクプロミスカスポート(GigabitEthernet 1/0/5)はプライマリ VLAN10 とセカンダリ VLAN11 と 12 の tagged メンバです。
- トランクセカンダリポート(GigabitEthernet 1/0/2)はプライマリ VLAN10 とセカンダリ VLAN11 の tagged メンバです。
- ホストポート (GigabitEthernet 1/0/3)はプライマリ VLAN10 とセカンダリ VLAN12 の untagged メンバです。

11.11.4 セカンダリ VLAN でのレイヤ 3 通信の設定例

I. ネットワーク要件

図 11-5に示すように設定します。

- Device A のプライマリ VLAN10 はセカンダリ VLAN2 と 3 に関連付けます。VLAN インタフェース 10 の IP アドレスは 192.168.1.1/24 です。
- GigabitEthernet 1/0/1 は VLAN 10 に所属し、GigabitEthernet 1/0/2 と GigabitEthernet 1/0/3はそれぞれ VLAN 2 と VLAN 3 に所属します。
- セカンダリ VLAN はレイヤ 2 で隔離していますが、レイヤ 3 では相互通信します。

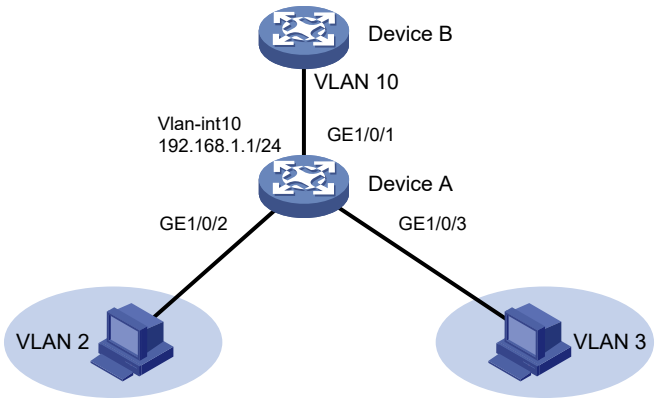


図 11-5 ネットワーク図

II. 設定手順

VLAN10 を作成して、プライマリ VLAN に設定します。

```
<DeviceA> system-view
[DeviceA] vlan 10
[DeviceA-vlan10] private-vlan primary
[DeviceA-vlan10] quit
```

VLAN2 と 3 を作成します。

```
<DeviceA> system-view
[DeviceA] vlan 2 to 3
```

プライマリ VLAN10 をセカンダリ VLAN2 と 3 と関連付けます。

```
[DeviceA] vlan 10
[DeviceA-vlan10] private-vlan secondary 2 3
[DeviceA-vlan10] quit
```

GigabitEthernet 1/0/1 を VLAN10 のプロミスカスポートに設定します。

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port private-vlan 10 promiscuous
[DeviceA-GigabitEthernet1/0/1] quit
```

GigabitEthernet 1/0/2 を VLAN 2 に割り当て、ホストポートに設定します。

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port access vlan 2
[DeviceA-GigabitEthernet1/0/2] port private-vlan host
[DeviceA-GigabitEthernet1/0/2] quit
```

GigabitEthernet 1/0/3 を VLAN 3 に割り当て、ホストポートに設定します。

```
[DeviceA] interface gigabitethernet 1/0/3
[DeviceA-GigabitEthernet1/0/3] port access vlan 3
[DeviceA-GigabitEthernet1/0/3] port private-vlan host
[DeviceA-GigabitEthernet1/0/3] quit
```

プライマリ VLAN10 に関連付けたセカンダリ VLAN2 と 3 間でレイヤ 3 通信を有効にします。

```
[DeviceA] interface vlan-interface 10
[DeviceA-Vlan-interface10] private-vlan secondary 2 3
```

VLAN インタフェース 10 に IP アドレス(192.168.1.1/24)を設定します。

```
[DeviceA-Vlan-interface10] ip address 192.168.1.1 255.255.255.0
```

ローカルプロキシ ARP を VLAN インタフェース 10 で有効にします。

```
[DeviceA-Vlan-interface10] local-proxy-arp enable
[DeviceA-Vlan-interface10] quit
```

III. 設定の確認

プライマリ VLAN10 の設定を確認します。

```
[DeviceA] display private-vlan 10
 Primary VLAN ID: 10
 Secondary VLAN ID: 2-3

 VLAN ID: 10
 VLAN type: Static
 Private VLAN type: Primary
 Route interface: Configured
 IPv4 address: 192.168.1.1
 IPv4 subnet mask: 255.255.255.0
 Description: VLAN 0010
 Name: VLAN 0010
 Tagged ports:   None
 Untagged ports:
    GigabitEthernet1/0/1
    GigabitEthernet1/0/2
    GigabitEthernet1/0/3

 VLAN ID: 2
 VLAN type: Static
 Private VLAN type: Secondary
 Route interface: Configured
 IPv4 address: 192.168.1.1
 IPv4 subnet mask: 255.255.255.0
 Description: VLAN 0002
 Name: VLAN 0002
 Tagged ports:   None
 Untagged ports:
    GigabitEthernet1/0/1
    GigabitEthernet1/0/2

 VLAN ID: 3
 VLAN type: Static
 Private VLAN type: Secondary
 Route interface: Configured
 IPv4 address: 192.168.1.1
 IPv4 subnet mask: 255.255.255.0
```

```
Description: VLAN 0003
Name: VLAN 0003
Tagged ports:   None
Untagged ports:
   GigabitEthernet1/0/1
   GigabitEthernet1/0/3
```

Route interface 情報が **Configured** と表示され、セカンダリ VLAN2 と 3 がレイヤ 3 で相互通信可能であることを示します。

目次

このセクションのページは**3-x-x** です。

12 章 Voice VLAN 12-1
12.1 概要 12-1
12.2 IP 電話の識別方法 12-1
12.2.1 OUI アドレスを使用した IP 電話の識別方法 12-1
12.3 IP 電話への Voice VLAN の配信 12-2
12.4 IP 電話のアクセス方式 12-2
12.4.1 ホストと IP 電話の直列接続 12-2
12.4.2 IP 電話の装置への接続 12-3
12.5 Voice VLAN のアサインモードの設定 12-3
12.5.1 自動モード 12-3
12.5.2 手動モード 12-4
12.5.3 Voice VLAN のアサインモードと IP 電話の協力 12-4
12.6 Voice VLAN のセキュリティモードとノーマルモード 12-5
12.7 Voice VLAN 設定作業リスト 12-6
12.8 音声トラフィックの QoS プライオリティの設定 12-6
12.9 自動 Voice VLAN アサインモードの設定 12-7
12.9.1 設定の制限とガイドライン 12-7
12.9.2 設定手順 12-7
12.10 手動 Voice VLAN アサインモードの設定 12-8
12.10.1 設定の制限とガイドライン 12-8
12.10.2 設定手順 12-9
12.11 Voice VLAN を配信する LLDP の設定 12-10
12.12 Voice VLAN を配信する CDP の設定 12-10
12.13 Voice VLAN の表示と維持 12-11
12.14 Voice VLAN の設定例 12-12
12.14.1 自動 Voice VLAN アサインモードの設定例 12-12
12.14.2 手動 Voice VLAN アサインモードの設定例 12-14

12章 Voice VLAN

12.1 概要

Voice VLAN は音声トラフィックのために特別に設定されます。音声装置が接続されるポートを Voice VLAN に設定すると、音声トラフィックのために QoS（Quality Of Service）パラメータを設定し、転送プライオリティを改善することで音声品質を確保します。

音声装置とは、IP 電話 IAD（統合アクセスデバイス）がありますが、本章では IP 電話（IP Phone）を用いて説明します。

音声通信を転送するためには、装置は以下の操作をします。

- ネットワーク中の IP 電話を識別し、その MAC アドレスを取得します。
- IP 電話に VLAN 情報を通知します。

VLAN 情報を受け取ると、IP 電話は自動設定を実行し、IP 電話の音声パケットを Voice VLAN に送信します。

12.2 IP電話の識別方法

装置は、IP 電話を識別するために OUI アドレスを使用します。

12.2.1 OUI アドレスを使用した IP 電話の識別方法

装置は受信パケットの送信元 MAC アドレスを確認することで音声パケットかどうかを判断します。送信元 MAC アドレスが音声装置の OUI（Organizationally Unique Identifier）アドレスに対応するパケットは、音声トラフィックと見なされ、Voice VLAN にアサインされます。

Voice VLAN には、事前に設定した OUI アドレスか、デフォルトで設定されている OUI アドレスを使用することができます。手動でデフォルト OUI アドレスを削除することも、新しく OUI アドレスを追加することもできます。

表 12-1のリストは、装置にデフォルトで設定されている各ベンダの OUI アドレスです。

表 12-1 デフォルトで設定されている OUI アドレス

番号	OUI アドレス	ベンダ
1	0001-e300-0000	Siemens phone
2	0003-6b00-0000	Cisco phone
3	0004-0d00-0000	Avaya phone
4	00d0-1e00-0000	Pingtel phone
5	0060-b900-0000	Philips/NEC phone
6	00e0-7500-0000	Polycom phone
7	00e0-bb00-0000	3Com phone

通常、OUI アドレスは、バイナリフォーマットで MAC アドレスの最初の 24 ビットにアサインされ、IEEE が各ベンダに割り当てるグローバルに固有な識別子です。しかし、本マニュアルの OUI アドレスは、システムが受信パケットを音声パケットどうか判断するために使用されます。これらは、MAC アドレスと **voice vlan mac-address** コマンドで設定された OUI マスクの 2 つの AND 演算の結果で求められます。

12.3 IP電話へのVoice VLANの配信

図 12-1に、IP 電話に Voice VLAN 情報を配信するフローを示します。

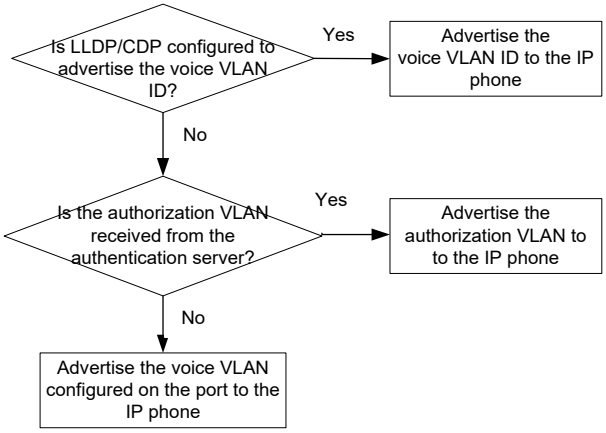


図 12-1 IP 電話への Voice VLAN の配信フロー

12.4 IP電話のアクセス方式

12.4.1 ホストと IP 電話の直列接続

図 12-2に示すように、ホストは IP 電話に接続され、IP 電話は装置に接続されています。この場合、以下の要件が満たされていなければなりません。

- ホストと IP 電話は異なる VLAN を使用します。
- 装置がホストと IP 電話のトラフィックを区別できるように、IP 電話は、タグ付けした VLAN パケットを送ることができます。
- IP 電話に接続したポートは Voice VLAN と PVID からのパケットを転送します。

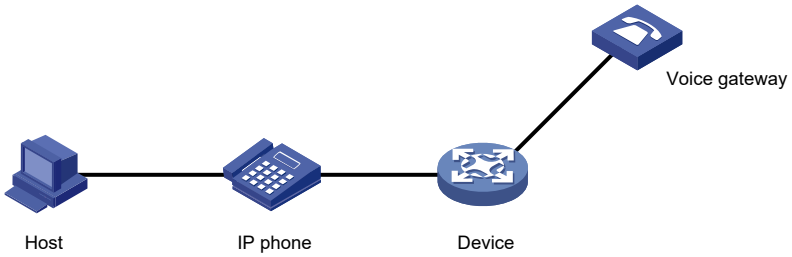


図 12-2 ホストと IP 電話が直列接続されたネットワーク

12.4.2 IP 電話の装置への接続

図 12-3に示すように、IP 電話はホストを使用せずに装置に接続されています。IP 電話がタグの無い音声パケットを送信する場合、この接続方法を使用してください。この場合、ポートの PVID として Voice VLAN を設定し、PVID からパケットを転送するためにポート設定をしなければなりません。

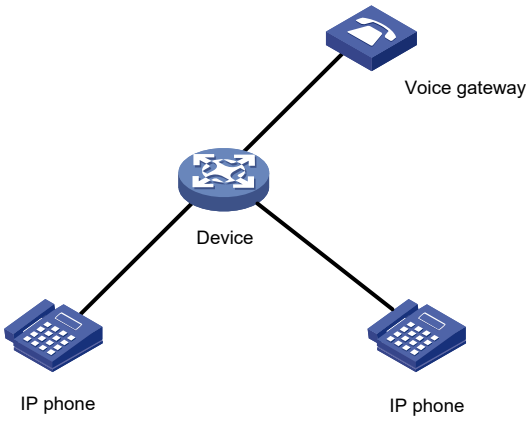


図 12-3 IP 電話が装置に接続されたネットワーク

12.5 Voice VLANのアサインモードの設定

ポートは、自動あるいは手動で Voice VLAN を割り当てることができます。

12.5.1 自動モード

図 12-2に示すように、PC と IP 電話が直列に接続されて装置を介してネットワークにアクセスする場合、自動モードを使用してください。装置のポートは、音声とデータのトラフィックの両方を送信します。

IP 電話は起動すると、プロトコルパケットを送信します。プロトコルパケットを受信した後、システムは装置の OUI アドレスとプロトコルパケットの送信元 MAC アドレスを照合します。照合が一致すれば、システムは以下の操作をします。

- 装置はプロトコルパケットの受信ポートに Voice VLAN を割り当てます。
- パケット優先順位を設定するために ACL ルールを適用します。
- Voice VLAN のエージングタイムを開始します。

エージングタイムが超過するまでにポートでパケットを受信しない場合、装置は Voice VLAN からポートを削除します。エージングタイムは設定可能です。

IP 電話が再起動した場合、ポートは正常に既存の音声装置に接続するため、再度 Voice VLAN に割り当てられます。音声トラフィックの開始は、Voice VLAN が正しく動作する限り必要ありません。

12.5.2 手動モード

図 12-3に示すように、装置を介して IP 電話だけがネットワークに接続している場合、手動モードを使用してください。このモードでは、Voice VLAN に割り当てられたポートは音声トラフィックのみが送信されます。そうすることでデータトラフィックが音声トラフィックの送信に与える影響を防止します。

手動で Voice VLAN に装置の受信ポートを割り当ててください。装置は装置の OUI アドレスとパケット内の送信元 MAC アドレスを照合します。照合が一致すれば、パケット優先順位を設定するために ACL ルールを適用します。

Voice VLAN からポートを削除する場合、手動で削除してください。

12.5.3 Voice VLAN のアサインモードと IP 電話の協力

IP 電話は VLAN タグつきパケットを送信するものと、タグなしパケットのみを送信するものがあります。正しくパケット処理をするために、さまざまなリンクタイプのポートは違う Voice VLAN アサインモードの中で特定の設定要件を満たさなければなりません。

表 12-2 IP 電話のタグ付き音声トラフィックの送信

ポートリンクタイプ	Voice VLAN アサインモード	設定要件
Trunk	自動モード	ポートのデフォルトVLANはVoice VLANにできません。
	手動モード	ポートのデフォルトVLANはVoice VLANにできません。Voice VLANのパケットを転送できるように設定する必要があります。
Hybrid	自動モード	ポートのデフォルトVLANはVoice VLANにできません。
	手動モード	ポートのデフォルトVLANはVoice VLANにできません。Voice VLANのタグ付きパケットを転送できるように設定する必要があります。

IP 電話がタグなしパケットを送信する場合、手動で Voice VLAN を割り当てる必要があります。

表 12-3 IP 電話のタグなし音声トラフィックの送信

ポートリンクタイプ	設定要件
Access	Voice VLANはポートのPVIDを設定する必要があります。
Trunk	Voice VLANはポートのPVIDを設定する必要があります。 ポートはVoice VLANのパケットを転送する必要があります。
Hybrid	Voice VLANはポートのPVIDを設定する必要があります。 ポートはVoice VLANのタグなしパケットを転送する必要があります。

IP 電話が VLAN タグ付きの音声トラフィックを送信し、アクセスポートに 802.1X 認証、Guest VLAN、または Auth-Fail VLAN が設定されている場合、VLAN ID を以下と異なるように割り当てる必要があります。

- Voice VLAN
- アクセスポートの PVID
- 802.1X Guest VLAN、Auth-Fail VLAN

IP 電話がタグなしの音声トラフィックを送信する場合、アクセスポートの PVID は Voice VLAN にする必要があります。このため、802.1X 認証はサポートしません。

12.6 Voice VLANのセキュリティモードとノーマルモード

Voice VLAN が有効なポートは入力パケットのフィルタリングメカニズムにもとづいて、以下の 1 つのモードで運用することができます。

- **ノーマルモード**– ポートは Voice VLAN でタグ付けされたパケットを受信し、MAC アドレスを確認せずに Voice VLAN に転送します。ポートの PVID が Voice VLAN でポートが手動の VLAN アサインモードで動作する場合、ポートは Voice VLAN のすべての受信したタグなしパケットを転送します。

  このモードでは Voice VLAN は通信攻撃に対して脆弱です。悪意のあるユーザは、音声帯域を消費させ音声通信に影響するように大量のタグ付きあるいはタグなしの偽のパケットを送信する可能性があります。
- **セキュリティモード**– ポートは送信元MACアドレスが装置のOUIアドレスと一致する音声パケットのみを受信します。ほかのすべてのパケットは廃棄します。

安全なネットワークでは、Voice VLAN を通常モードで動作するように設定できます。送信元 MAC アドレスのチェックを行うリソースの消費を削減することができます。

装置は OUI アドレスに一致する送信元 MAC アドレスの Voice VLAN パケットの転送プライオリティのみを変更することができます。

Voice VLAN で音声パケットと非音声パケットの両方を転送することは推奨しません。転送する必要がある場合は、Voice VLAN のセキュリティモードが無効であることを確認してください。

表 12-4 Voice VLAN 有効ポートのパケット処理方法

動作モード	パケットタイプ	パケット処理
ノーマルモード	• タグなしパケット • Voice VLANタグのパケット	MACアドレスをチェックしないため、音声トラフィックと非音声トラフィックの両方をVoice VLANで通過することができます。

動作モード	パケットタイプ	パケット処理
	ほかのVLANタグのパケット	ポートが、そのVLANのパケットが通過するのを許可するか許可しないかにより、パケットを通過させるか、廃棄させます。
セキュリティモード	• タグなしパケット • Voice VLANタグのパケット	• パケットの送信元MACアドレスが装置に設定されているOUIアドレスと一致する場合は、Voice VLANで通過します。 • パケットの送信元MACアドレスが装置に設定されているOUIアドレスと一致しない場合、パケットを廃棄します。
	ほかのVLANタグのパケット	ポートが、そのVLANのパケットが通過するのを許可するか許可しないかにより、パケットを通過させるか、廃棄させます。

12.7 Voice VLAN設定作業リスト

作業リスト
（必須設定項目）音声トラフィックのQoSプライオリティの設定
（必須設定項目）以下のどちらか1つを設定します。 • 自動Voice VLANアサインモードの設定 • 手動Voice VLANアサインモードの設定
（オプション設定項目）Voice VLANを配信するLLDPの設定

12.8 音声トラフィックのQoSプライオリティの設定

QoS プライオリティ設定には、CoS と DSCP を含みます。音声トラフィックは QoS プライオリティ設定にしたがって処理され、設定は変更することが可能です。

Voice VLAN が有効なポートでは QoS プライオリティを設定することができません。ポートに音声トラフィックの QoS プライオリティを設定する前に、Voice VLAN 機能が無効になっていることを確認してください。

以下に Voice VLAN トラフィックのプライオリティの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． interface view に移行する	• Ethernet interface viewに移行する： **interface** *interface-type interface-number* • aggregate interface viewに移行する： **interface bridge-aggregation** *interface-number*	—

操作	コマンド	補足
3． 受信 Voice VLAN パケットの QoS プライオリティを設定する	• QoSプライオリティの設定を信用し、プライオリティとして使用する： **voice-vlan qos trust** • パケットのCoS、DSCPをポートで変更する： **voice vlan qos** *cos-value dscp-value*	デフォルト：CoSは6、DSCPは46です。 受信Voice VLANパケットのQoSプライオリティの設定を信用し、プライオリティとして使用する場合、ポートでCoS、DSCPを変更することができません。

12.9 自動Voice VLANアサインモードの設定

12.9.1 設定の制限とガイドライン

ポートに自動 Voice VLAN アサインモードを設定する場合、以下の制限とガイドラインに従ってください。

- Voice VLAN とプロトコルベース VLAN を同時に設定しないでください。
  - ハイブリッドポートの自動モードの Voice VLAN はタグ付けされた受信音声トラフィックのみ処理します。
  - ハイブリッドポートのプロトコルベース VLAN はタグなしの受信パケットのみ処理します。プロトコルベースの VLAN については、オペレーションマニュアルのセクション 3 *アクセス”VLAN”の”プロトコルベース VLAN”*を参照してください。
- 自動 Voice VLAN アサインモードと MSTP は同時に使用しないことを推奨します。MSTP モードでは、ポートがターゲット Voice VLAN の MSTI でブロックされている場合、ポートは受信パケットを CPU に送信せず廃棄します。結果として、受信ポートは Voice VLAN に動的に割り当てられません。
- 自動 Voice VLAN アサインモードと PVST は同時に使用しないことを推奨します。PVST モードでは、ポートでターゲット Voice VLAN の MSTI を許可されていない場合、ポートはブロック状態になり、受信パケットを CPU に送信せず廃棄します。結果として、受信ポートは Voice VLAN に動的に割り当てられません。
- ポートにダイナミック MAC ベース VLAN と自動 Voice VLAN アサインモードの両方を設定しないことを推奨します。ポートでダイナミック MAC ベース VLAN と自動 Voice VLAN の割り当ての両方を設定する場合、最初にダイナミック MAC ベース VLAN を設定してください。最初に自動 Voice VLAN の割り当てを設定した場合、衝突が発生します。設定の 1 つを削除するとき、もう一方の動作に影響します。

12.9.2 設定手順

以下にポートに自動 Voice VLAN アサインモードの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	-

操作	コマンド	補足
2.　（オプション設定項目）Voice VLAN のエージングタイムを設定する	**voice vlan aging** *minutes*	デフォルト：1440分 Voice VLANエージングタイムの設定は、自動Voice VLANアサインモードのポートでのみ適用されます。
3.　（オプション設定項目）Voice VLAN セキュリティモードを有効にする	**voice vlan security enable**	デフォルト：有効
4.　（オプション設定項目）登録 OUI アドレスを追加する	**voice vlan mac-address** *oui* **mask** *oui-mask* [**description** *text*]	デフォルト：表 12-1に示すアドレスが登録されています。
5.　interface view に移行する	● Ethernet interface viewに移行する： **interface** *interface-type interface-number* ● aggregate interface viewに移行する： **interface bridge-aggregation** *interface-number*	—
6.　ポートのリンクタイプを設定する	● **port link-type trunk** ● **port link-type hybrid**	—
7.　（オプション設定項目）自動 Voice VLAN アサインモードで動作するように設定する	**voice vlan mode auto**	デフォルト：有効
8.　Voice VLAN を有効にする	**voice vlan** *vlan-id* **enable**	デフォルト：無効 VLANがすでに作成されていることを確認してください。

12.10 手動Voice VLANアサインモードの設定

12.10.1 設定の制限とガイドライン

ポートに自動 Voice VLAN アサインモードを設定する場合、以下の制限とガイドラインに従ってください。

- 同一装置の異なるポートに、同時に異なる Voice VLAN を設定することができます。以下の要件に従う必要があります。
  - □ 1 つのポートは 1 つの Voice VLAN のみ設定することができます。
  - □ Voice VLAN は装置で、すでにスタティック VLAN として設定されている必要があります。
- リンクアグリゲーショングループのメンバポートで Voice VLAN を有効にしないでください。リンクアグリゲーショングループの詳細は、オペレーションマニュアルのセクション 3 *アクセス”リンクアグリゲーション”*を参照してください。
- ポートで Voice VLAN を実行するには、Voice VLAN を有効にして、手動 Voice VLAN アサインモードを設定し、Voice VALN を手動でポートに割り当てる必要があります。

12.10.2 設定手順

以下にポートに手動 Voice VLAN アサインモードの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． （オプション設定項目）Voice VLAN セキュリティモードを有効にする	**voice vlan security enable**	デフォルト：有効
3． （オプション設定項目）登録 OUI アドレスを追加する	**voice vlan mac-address** *oui* **mask** *oui-mask* [**description** *text*]	デフォルト：表 12-1に示すアドレスが登録されています。
4． interface view に移行する	● Ethernet interface viewに移行する： **interface** *interface-type interface-number* ● aggregate interface viewに移行する： **interface bridge-aggregation** *interface-number*	―
5． （必須設定項目）手動 Voice VLAN アサインモードで動作するように設定する	**undo voice vlan mode auto**	デフォルト：無効
6． 手動モードで Voice VLAN をポートにアサインする	アクセスポートに設定する場合、オペレーションマニュアルのセクション3 *アクセス”VLAN”の”アクセスポートVLANの設定”*を参照してください。 トランクポートに設定する場合、オペレーションマニュアルのセクション3 *アクセス”VLAN”の”トランクポートVLANの設定”*を参照してください。 ハイブリッドポートに設定する場合、オペレーションマニュアルのセクション3 *アクセス”VLAN”の”ハイブリッドポートVLANの設定”*を参照してください。	3つから1つを選択します。 Voice VLANにAccess port をアサインすると、自動的にポートのPVIDになります。
7． （オプション設定項目）ポートのデフォルト VLAN として Voice VLAN を設定する	トランクポートに設定する場合、オペレーションマニュアルのセクション3 *アクセス”VLAN”の”トランクポートVLANの設定”*を参照してください。 ハイブリッドポートに設定する場合、オペレーションマニュアルのセクション3 *アクセス”VLAN”の”アクセスポートVLANの設定”*を参照してください。	この設定は受信音声トラフィックがタグなしの場合に必要です。タグ付きの場合は設定することができません。
8． Voice VLAN を有効にする	**voice vlan** *vlan-id* **enable**	デフォルト：無効 VLANがすでに作成されていることを確認してください。

12.11 Voice VLANを配信するLLDPの設定

IP 電話が LLDP をサポートしている場合、装置は LLDP-MED TLV を用いて IP 電話に Voice VLAN 情報を配信します。

この機能を設定する前に、グローバルとアクセスポートの両方で LLDP を有効にしてください。

以下に Voice VLAN を配信する LLDP の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． interface view に移行する	**interface** *interface-type interface-number*	—
3． LLDP を設定する	**lldp tlv-enable med-tlv network-policy** *vlan-id*	デフォルト：設定なし 詳細はコマンドマニュアルのセクション3 *アクセス”LLDP”* を参照してください。
4． （オプション設定項目）LLDP によって配信されあれた Voice VLAN を表示する	**display lldp local-information**	詳細はコマンドマニュアルのセクション3 *アクセス”LLDP”* を参照してください。

12.12 Voice VLANを配信するCDPの設定

IP 電話が CDP をサポートしていても LLDP をサポートしていない場合、CDP パケットをデバイスに送信して Voice VLAN ID を要求します。IP 電話が一定期間内に Voice VLAN ID を受信しない場合、タグなしパケットを送信します。デバイスは、タグなし音声パケットを他のタイプのパケットと区別できません。

デバイスで CDP 互換性を設定して、次の操作を実行できるようにすることができます。

- IP 電話から CDP パケットを受信して識別します。
- IP 電話に CDP パケットを送信します。Voice VLAN 情報は CDP パケットで伝送されます。

アドバタイズされた VLAN 情報を受信すると、IP 電話は自動 Voice VLAN 設定を実行します。IP 電話からのパケットは専用 Voice VLAN で送信されます。

デバイスから送信される LLDP パケットは、優先度情報を伝送します。デバイスから送信される CDP パケットは、優先度情報を伝送しません。

この機能を設定する前に、グローバルとアクセスポートの両方で LLDP を有効にしてください。

この機能を設定する際には、アクセスポートで Voice VLAN を有効にしてください。

cdp voice-vlan が有効で、Voice VLAN が無効の場合であっても、cdp voice-vlan で設定した Voice VLAN ID が CDP パケットで伝送されますが、Voice VLAN が有効になっていないため、デバイスは音声トラフィックとして扱わず、L2 トラフィックとして扱います。

また、cdp voice-vlan が無効で、Voice VLAN が有効の場合は、voice-vlan enable で設定した Voice VLAN ID が CDP パケットで伝送されます。

以下に CDP パケットで伝送される Voice VLAN ID を示します。

Voice VLAN	cdp voice-vlan	CDP パケットで伝送される Voice VLAN ID
有効	有効	cdp voice-vlan で設定した Voice VLAN ID
有効	無効	voice-vlan enable で設定した Voice VLAN ID
無効	有効	cdp voice-vlan で設定した Voice VLAN ID
無効	無効	Voice VLAN ID がない CDP パケットが伝送される

以下に Voice VLAN を配信する CDP の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． グローバルで CDP 互換モードを有効にする	**lldp compliance cdp**	デフォルト：無効
3． interface view に移行する	**interface** *interface-type interface-number*	—
4． Voice VLAN を有効にする	**voice vlan** *vlan-id* **enable**	デフォルト：無効 VLANがすでに作成されていることを確認してください。
5． CDP 互換 LLDP モードの動作モードを TxRx モードにする	**lldp compliance admin-status cdp txrx**	デフォルト：無効
6． アドバタイズされた Voice VLAN ID を設定する	**cdp voice-vlan vlan-id**	デフォルト:CDPフレームで伝送されるVoice VLAN IDが設定されていない。 詳細はコマンドマニュアルのセクション3 *アクセス”LLDP”* を参照してください。

12.13 Voice VLANの表示と維持

すべての view で **display** コマンドを実行し、user view で **reset** コマンドを実行できます。

操作	コマンド
Voice VLANの状態を表示する	**display voice vlan state**
装置でサポートされているOUIアドレスを表示する	**display voice-vlan mac-address**

12.14 Voice VLANの設定例

12.14.1 自動 Voice VLAN アサインモードの設定例

I. ネットワーク要件

図 12-4に示すように、Device A は IP 電話とホストからの通信トラフィックを転送します。

正しく音声トラフィックを転送するには、以下の操作を行ってください。

- IP 電話 A と IP 電話 B からの音声パケットを転送するように、それぞれ Voice VLAN 2 と Voice VLAN 3 を設定します。
- 自動 Voice VLAN アサインモードを動作させるために、GigabitEthernet 1/0/1 と GigabitEthernet 1/0/2 に設定をします。
- 音声パケットの認証のために IP 電話 A と IP 電話 B の MAC アドレスを追加します。2 つの MAC アドレスのマスクは FFFF-FF00-0000 です。

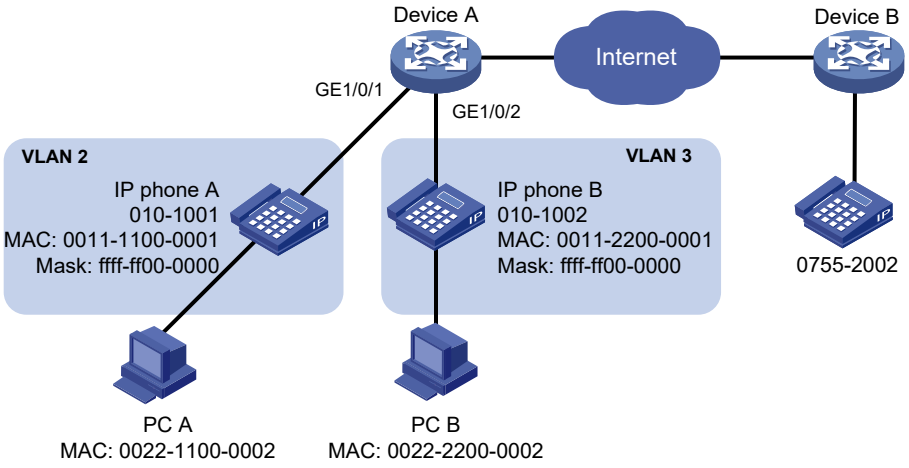


図 12-4 ネットワーク図

II. 設定手順

1) VLAN を設定します

VLAN 2 と VLAN 3 を作成します。

```
<DeviceA> system-view
[DeviceA] vlan 2 to 3
```

Voice VLAN のエージングタイムを 30 分に設定します。

```
[DeviceA] voice-vlan aging 30
```

Voice VLAN が音声パケットのみ転送するようにセキュリティモードでの動作を設定します。

```
[DeviceA] voice-vlan security enable
```

IP 電話 A と IP 電話 B にマスク値 FFFF-FF00-0000 と MAC アドレスを追加します。

```
[DeviceA] voice-vlan mac-address 0011-1100-0001 mask ffff-ff00-0000 description IP phone A
[DeviceA] voice-vlan mac-address 0011-2200-0001 mask ffff-ff00-0000 description IP phone B
```

2)　GigabitEthernet 1/0/1 ポートを設定します。

GigabitEthernet 1/0/1 をハイブリッドポートに設定します。

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-type hybrid
```

GigabitEthernet 1/0/1 を自動 Voice VLAN アサインモードとして動作するように設定します。

```
[DeviceA-GigabitEthernet1/0/1] voice-vlan mode auto
```

GigabitEthernet 1/0/1 の Voice VLAN として VLAN 2 を設定します。

```
[DeviceA-GigabitEthernet1/0/1] voice-vlan 2 enable
[DeviceA-GigabitEthernet1/0/1] quit
```

3)　GigabitEthernet 1/0/2 ポートを設定します。

GigabitEthernet 1/0/2 をハイブリッドポートに設定します。

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port link-type hybrid
```

GigabitEthernet 1/0/2 を自動 Voice VLAN アサインモードとして動作するように設定します。

```
[DeviceA-GigabitEthernet1/0/2] voice-vlan mode auto
```

GigabitEthernet 1/0/2 の Voice VLAN として VLAN 3 を設定します。

```
[DeviceA-GigabitEthernet1/0/2] voice-vlan 3 enable
[DeviceA-GigabitEthernet1/0/2] quit
```

III. 設定の確認

Device A でサポートされている OUI アドレスを表示します。

```
[DeviceA] display voice-vlan mac-address
OUI Address      Mask            Description
0001-e300-0000   ffff-ff00-0000  Siemens phone
0003-6b00-0000   ffff-ff00-0000  Cisco phone
0004-0d00-0000   ffff-ff00-0000  Avaya phone
000f-e200-0000   ffff-ff00-0000  H3C Aolynk phone
0011-1100-0000   ffff-ff00-0000  IP phone A
0011-2200-0000   ffff-ff00-0000  IP phone B
0060-b900-0000   ffff-ff00-0000  Philips/NEC phone
00d0-1e00-0000   ffff-ff00-0000  Pingtel phone
00e0-7500-0000   ffff-ff00-0000  Polycom phone
```

```
00e0-bb00-0000  ffff-ff00-0000  3Com phone
```

現在の Voice VLAN の状態を表示します。

```
[DeviceA] display voice-vlan state
 Current voice VLANs: 2
 Voice VLAN security mode: Security
 Voice VLAN aging time: 30 minutes
 Voice VLAN enabled ports and their modes:
 Port                      VLAN        Mode        CoS         DSCP
 GE1/0/1                   2           Auto        6           46
 GE1/0/2                   3           Auto        6           46
```

12.14.2 手動 Voice VLAN アサインモードの設定例

I. ネットワーク要件

図 12-5に示すように設定します。

GigabitEthernet 1/0/1 で音声トラフィックのみ転送するため、以下の設定を行います。

- VLAN 2 を作成します。VLAN 2 は Voice VLAN として使用します。
- 手動 Voice VLAN アサインモードを動作させるために、GigabitEthernet 1/0/1 を設定します。VLAN 2 に追加します。
- Device A の OUI リストに IP 電話 A の OUI アドレスを追加します。

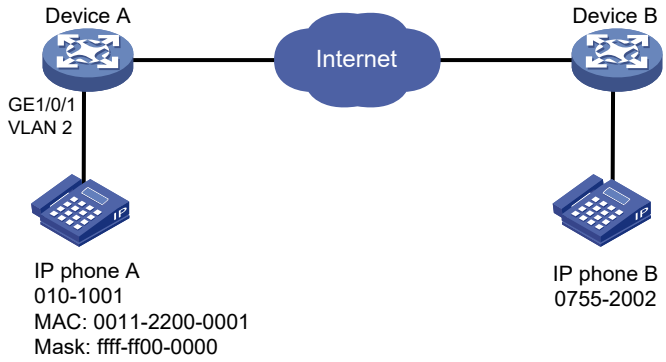


図 12-5 ネットワーク図

II. 設定手順

Voice VLAN がセキュリティモードで動作するように設定します。

```
<DeviceA> system-view
[DeviceA] voice-vlan security enable
```

マスク FFFF-FF00-0000 で MAC アドレス 0011-2200-0001 を追加します。

```
[DeviceA] voice-vlan mac-address 0011-2200-0001 mask ffff-ff00-0000 description test
```

VLAN 2 を作成します。

```
[DeviceA] vlan 2
```

```
[DeviceA-vlan2] quit
```

GigabitEthernet 1/0/1 を手動 Voice VLAN アサインモードで動作するように設定します。

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] undo voice-vlan mode auto
```

GigabitEthernet 1/0/1 をハイブリッドポートに設定します。

```
[DeviceA-GigabitEthernet1/0/1] port link-type hybrid
```

GigabitEthernet 1/0/1 の PVID を VLAN 2 に設定します。

```
[DeviceA-GigabitEthernet1/0/1] port hybrid pvid vlan 2
```

#タグなし VLAN メンバとして GigabitEthernet 1/0/1 を VLAN 2 に割り当てます。

```
[DeviceA-GigabitEthernet1/0/1] port hybrid vlan 2 untagged
```

Voice VLAN を有効にし、GigabitEthernet 1/0/1 の Voice VLAN として VLAN 2 を設定します。

```
[DeviceA-GigabitEthernet1/0/1] voice-vlan 2 enable
[DeviceA-GigabitEthernet1/0/1] quit
```

III. 設定の確認

Device A でサポートされている OUI アドレスを表示します。

```
[DeviceA] display voice-vlan mac-address
OUI Address      Mask            Description
0001-e300-0000   ffff-ff00-0000  Siemens phone
0003-6b00-0000   ffff-ff00-0000  Cisco phone
0004-0d00-0000   ffff-ff00-0000  Avaya phone
000f-e200-0000   ffff-ff00-0000  H3C Aolynk phone
0011-2200-0000   ffff-ff00-0000  test
0060-b900-0000   ffff-ff00-0000  Philips/NEC phone
00d0-1e00-0000   ffff-ff00-0000  Pingtel phone
00e0-7500-0000   ffff-ff00-0000  Polycom phone
00e0-bb00-0000   ffff-ff00-0000  3Com phone
```

現在の Voice VLAN の状態を表示します。

```
[DeviceA] display voice-vlan state
 Current voice VLANs: 1
 Voice VLAN security mode: Security
 Voice VLAN aging time: 1440 minutes
 Voice VLAN enabled ports and their modes:
 Port                        VLAN        Mode        CoS         DSCP
 GE1/0/1                     2           Manual      6           46
```

目次

このセクションのページは **3-x-x** です。

13 章 QinQ.....13-1
13.1 概要.....13-1
13.1.1 QinQ の動作.....13-1
13.1.2 QinQ の実装.....13-3
13.1.3 プロトコルと標準.....13-3
13.2 制限とガイドライン.....13-3
13.3 QinQ の有効化.....13-4
13.4 VLAN トランスペアレントトランスミッションの設定.....13-4
13.5 VLAN タグの TPID の設定.....13-5
13.5.1 TPID.....13-5
13.5.2 制限とガイドライン.....13-5
13.5.3 CVLAN タグの TPID の設定.....13-6
13.5.4 SVLAN タグの TPID の設定.....13-6
13.6 QinQ の表示と維持.....13-6
13.7 QinQ 設定例.....13-6
13.7.1 Basic QinQ 設定例.....13-6
13.7.2 VLAN トランスペアレントトランスミッション設定例.....13-9

13章 QinQ

この章では以下の用語を使用します。

- **CVLAN** – カスタマネットワーク VLAN（CVLAN [内部 VLAN]）は、顧客のプライベートネットワーク上で使う VLAN を示します。
- **SVLAN** – サービスプロバイダネットワーク VLAN（SVLAN[外部 VLAN]）は、サービスプロバイダが顧客の VLAN タグ付けされたトラフィックを転送する VLAN を示します。

13.1 概要

QinQ（802.1Q-in-802.1Q）機能は、802.1Q がタグ付けされたカスタマトラフィックに 802.1Q タグを追加します。カスタマサイト間で Ethernet ネットワークを越えてレイヤ 2 通信を行うことができるようにサービスプロバイダで有効にします。

QinQ は以下の利点があります。

- サービスプロバイダは 1 つの SVLAN を使用することで、カスタマ用に複数の CVLAN を転送することができます。
- カスタマが SVLAN のとの重複を気にせずに、CVLAN を設定できるようにします。
- サービスプロバイダが VLAN 割り当て方式を変更するとき、カスタマに割り当てた方式を変更しないで、保持することができます。
- カスタマが重複する CVLAN ID を使用することができます。サービスプロバイダネットワーク内の装置は CVLAN ID の代わりに SVLAN ID をもとにして転送を行います。

13.1.1 QinQ の動作

図 13-1に示すように、QinQ フレームはサービスプロバイダネットワークを経由して以下のタグを運びます。

- **CVLAN tag** – CVLAN タグはカスタマネットワークで転送されるとき、QinQ フレームが属している VLAN を識別します。
- **SVLAN tag** – サービスプロバイダは、このタグをカスタマに割り当てます。SVLAN タグはサービスプロバイダネットワークで転送されるとき、QinQ フレームが属している VLAN を識別します。

サービスプロバイダネットワークの装置は SVLAN タグのみに従ってタグが付いたフレームを転送します。CVLAN タグはフレームのペイロードの一部として転送されます。

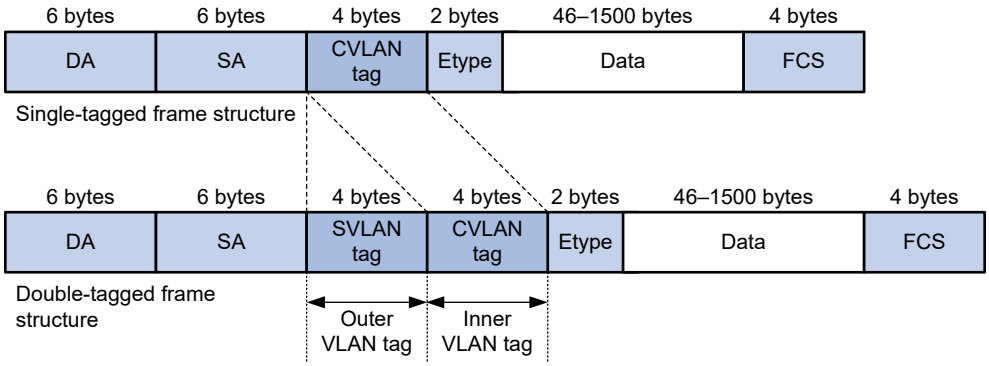


図 13-1 シングルタグ付きのイーサネットフレームヘッダと 2 重タグ付きのイーサネットフレームヘッダ

図 13-2に示すように、カスタマネットワーク A はリモート側の CE1、CE4 があります。カスタマネットワーク B はリモート側の CE2、CE3 があります。2 つのカスタマの CVLAN は重複します。サービスプロバイダはカスタマネットワーク A に SVLAN 3 を割り当て、カスタマネットワーク B に SVLAN 4 を割り当てます。

カスタマネットワーク A からタグが付いた Ethernet フレームが到着したとき、PE1 はフレームに SVLAN 3 のタグをつけます。2 重のタグが付いた Ethernet フレームは、サービスプロバイダを越えて転送し、PE2 に到着します。PE2 はフレームの SVLAN タグを取り外します。そして CE4 にフレームを送信します

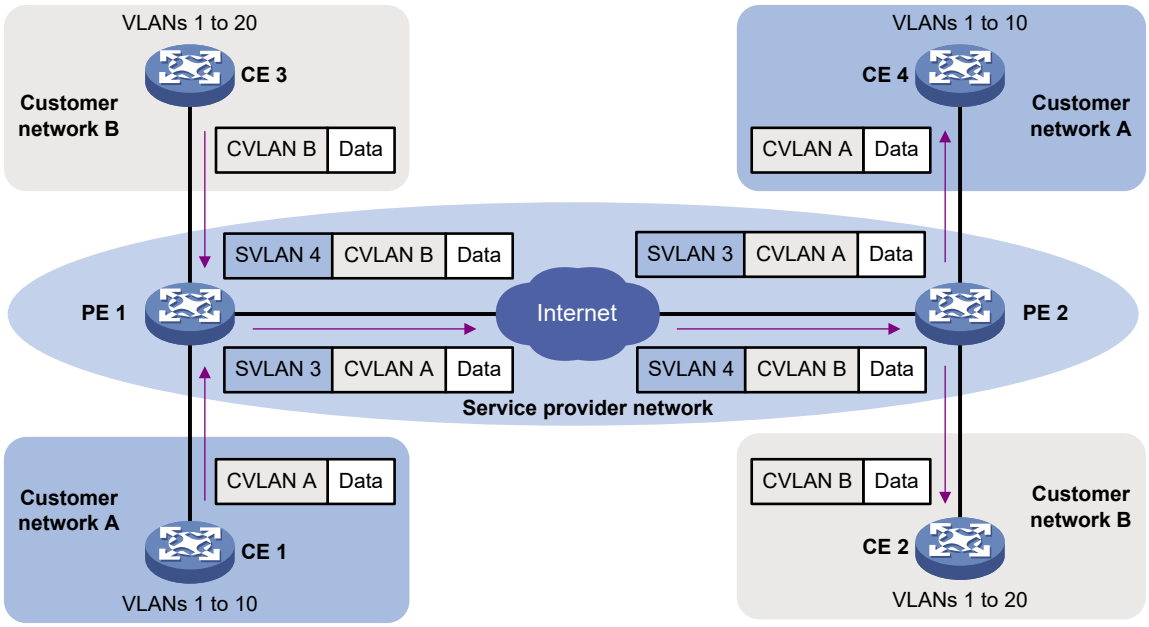


図 13-2 一般的な QinQ アプリケーションシナリオ

13.1.2 QinQ の実装

QinQ はポートベースで設定できます。QinQ が有効になったポートのリンクタイプにはアクセス、ハイブリッド、トランクが使用できます。QinQ のタグ付けはポートのタイプと同一です。

QinQ が有効なポートはすべての入力フレーム（タグありあるいはタグなし）に PVID タグをつけます。

- もし入力フレームが 1 つのタグを持っている場合、2 重タグフレームになります。
- もしフレームに 802.1Q タグがない場合、PVID のタグがつけられます。

QinQ はすべての入力フレーム（タグありあるいはタグなし）に PVID タグをタグ付けするために、最も基本的な VLAN の処理方式を提供します。拡張 VLAN 処理方式を実行するには、VLAN マッピングあるいは QoS ポリシーを使用します。

- 異なる CVLAN タグ用に異なる SVLAN を使用するため、one-to-two VLAN マッピングを使用します。
- SVLAN にタグをつける際、パケットに一致させるため CVLAN ID 以外の条件を使用する場合、QoS をネスト（入れ子）にするアクションを使用します。QoS をネストにするアクションは、同じトラフィック動作におけるほかのアクションでも使用されます。

VLAN マッピングの詳細は、オペレーションマニュアルのセクション 3 *アクセス* "*VLAN マッピング*"を参照してください。QoS ポリシーの詳細は、オペレーションマニュアルのセクション 8 *ACL and QoS* "*QoS ポリシー*"を参照してください。

13.1.3 プロトコルと標準

- IEEE 802.1Q, *IEEE Standard for Local and Metropolitan Area Networks-Virtual Bridged Local Area Networks*
- IEEE 802.1ad, *IEEE Standard for Local and Metropolitan Area Networks-Virtual Bridged Local Area Networks-Amendment 4: Provider Bridges*

13.2 制限とガイドライン

QinQ を設定する場合、以下の制限とガイドラインに従ってください。

- QinQ フレームの内部 802.1Q タグはペイロードの一部となります。QinQ フレームを正しく転送するため、QinQ フレームの転送パスの各ポートの最小 MTU を 1504 バイトに設定することを推奨します。この値はデフォルトの Ethernet インタフェースの MTU（1500 バイト）と VLAN タグ（4 バイト）の合計です。
- VLAN タグの処理を行うため、ポートで VLAN マッピング、QoS ポリシー、QinQ を設定することができます。設定が重複した場合、以下の降順で設定が優先されます。
  - □ VLAN マッピング
  - □ QoS ポリシー
  - □ QinQ

13.3 QinQの有効化

PE のカスタマ側のポートで QinQ を有効にします。QinQ が有効なポートは入力フレームに PVID をタグ付けします。

ポートで QinQ を設定する前に、VLAN マッピングの設定を削除してください。

以下に QinQ の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. Ethernet interface view あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	—
3. QinQ を有効にする	**qinq enable**	デフォルト：無効

13.4 VLANトランスペアレントトランスミッションの設定

カスタマ側のポートで QinQ のタグづけを行う際、VLAN（たとえばマネジメント VLAN）のトラフィックを除外することができます。この VLAN はトランスペアレント VLAN と呼ばれます。

トランスペアレント VLAN の転送を正しく行うために、以下の設定のガイドラインに従ってください。

- ポートにトランクあるいはハイブリッドのリンクタイプを設定し、トランスペアレント VLAN にポートを割り当ててください。
- ポートでトランスペアレント VLAN を処理するため、別の設定を行わないでください。
- 転送経路上にあるすべてのポートで VLAN を通過できることを確認してください。
- トランスペアレント VLAN と VLAN マッピングの両方を使用する場合、トランスペアレント VLAN は one-to-one VLAN マッピングと one-to-two VLAN マッピングのもとの VLAN あるいは変換される VLAN にすることはできません。

以下にトランスペアレントトランスミッションの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. Ethernet interface view あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	—
3. リンクタイプを設定する	**port link-type** { **hybrid** | **trunk** }	デフォルト：アクセス
4. ポートで PVID のパケットを許可し、通過できるようにトランスペアレント VLAN を設定する	• ハイブリッドポート：**port hybrid vlan** *vlan-id-list* { **tagged** | **untagged** } • トランクポート：**port trunk permit vlan** { *vlan-id-list* | **all** }	デフォルト： トランクポートはVLAN1のみ許可し、ハイブリッドポートはVLAN1のuntaggedメンバのみ許可します。
5. トランスペアレント VLAN を指定する	**qinq transparent-vlan** *vlan-id-list*	デフォルト：設定なし

13.5 VLANタグのTPIDの設定

13.5.1 TPID

TPID はフレームを 802.1Q のタグ付きフレームとして識別します。この値はベンダによって変わります。802.1Q が有効なポートで 802.1Q タグが付いた TPID はデフォルトで 0x8100 です。IEEE802.1Q に準拠しています。複数のベンダがあるネットワークでは、802.1Q のタグ付きフレームが正しく識別できるように、TPID の設定はすべての装置で同一にする必要があります。

TPID の設定は、CVLAN TPID と SVLAN TPID を含みます。

QinQ が有効なポートは、入力するタグ付けフレームにマッチさせるため、CVLAN TPID を使用します。もし TPID が CVLAN TPID と異なる場合、入力フレームはタグなしフレームとして扱われます。

SVLAN TPID はポート毎に設定できます。サービスプロバイダ側のポートは出力するフレームの SVLAN タグの TPID を置き換えるため、そして入力するタグ付けフレームにマッチさせるため、SVLAN TPID を使用します。もし外部 VLAN タグの TPID が SVLAN TPID と異なる場合、入力フレームはタグなしフレームとして扱われます。

たとえば、PE 装置は TPID 0x8200 を使用するカスタマデバイスと、TPID 0x9100 を使用するプロバイダデバイスに接続されています。正しいパケットの処理を行うため、PE で CVLAN TPID を 0x8200、SVLAN TPID を 0x9100 として設定する必要があります。

TPID フィールドはタグなし Ethernet フレームの EtherType フィールドと同じ位置づけとなります。パケットタイプを正しく識別するため、TPID は表 13-1に示す予約済み EtherType 値を設定することができません。

表 13-1 予約済み EtherType 値

プロトコルタイプ	値
ARP	0x0806
PUP	0x0200
RARP	0x8035
IP	0x0800
IPv6	0x86dd
PPPoE	0x8863/0x8864
MPLS	0x8847/0x8848
IPX/SPX	0x8137
IS-IS	0x8000
LACP	0x8809
LLDP	0x88cc
802.1X	0x888e
802.1ag	0x8902
Cluster	0x88a7
Reserved	0xfffd/0xfffe/0xffff

13.5.2 制限とガイドライン

CVLAN タグの TPID 値は通常、PE で設定します。 通常、SVLAN タグの TPID 値は、PE のサービスプロバイダ側のポートで設定されます。

13.5.3 CVLAN タグの TPID の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. CVLAN タグの TPID を設定する	**qinq ethernet-type customer-tag** *hex-value*	デフォルト：0x8100

13.5.4 SVLAN タグの TPID の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. Ethernet interface view あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	ー
3. SVLAN TPID を設定する	**qinq ethernet-type service-tag** *hex-value*	デフォルト：0x8100

13.6 QinQの表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
QinQが有効なインタフェースを表示する	**display qinq** [**interface** *interface-type interface-number*]

13.7 QinQ設定例

13.7.1 Basic QinQ 設定例

I. ネットワーク要件

図 13-3に示すように設定します。

- サービスプロバイダは、VLAN 100 を Company A の VLAN 10～VLAN 70 に割り当てます。
- サービスプロバイダは、VLAN 200 を Company B の VLAN 30～VLAN 90 に割り当てます。

Company A と Company B の VLAN 100 と VLAN 200 でトラフィックを転送するため、PE1 と PE2 の QinQ を設定します。

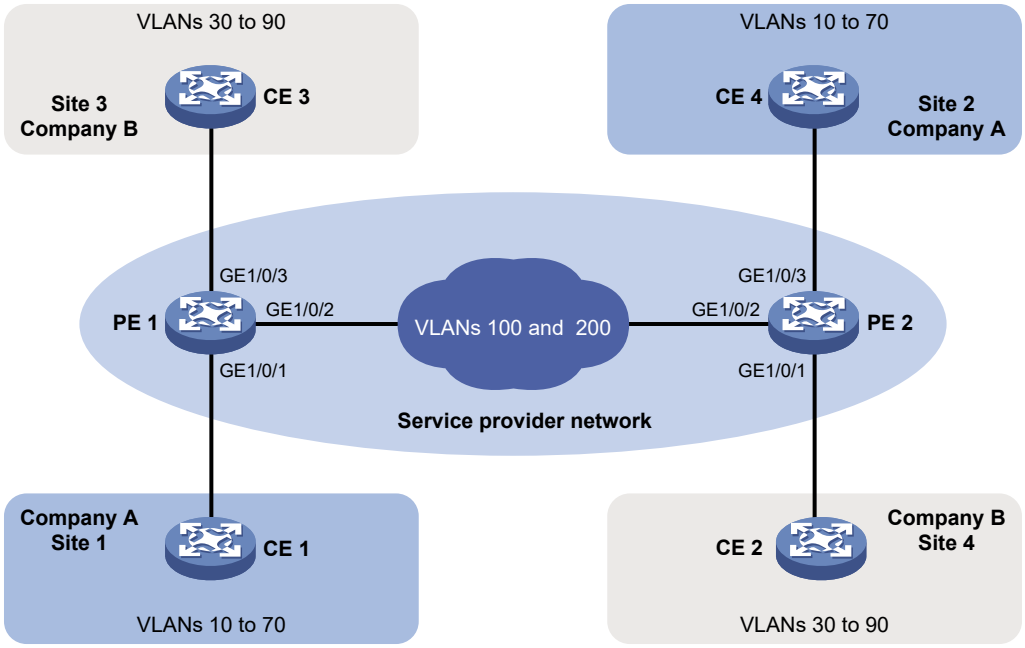


図 13-3 ネットワーク図

II. 設定手順

1)　PE 1 を設定します。

トランクポートとして GigabitEthernet 1/0/1 を設定し、VLAN 100 を割り当てます。

```
<PE1> system-view
[PE1] interface gigabitethernet 1/0/1
[PE1-GigabitEthernet1/0/1] port link-type trunk
[PE1-GigabitEthernet1/0/1] port trunk permit vlan 100
```

GigabitEthernet 1/0/1 の PVID として VLAN 100 を設定します。

```
[PE1-GigabitEthernet1/0/1] port trunk pvid vlan 100
```

GigabitEthernet 1/0/1 で QinQ を有効にします。

```
[PE1-GigabitEthernet1/0/1] qinq enable
[PE1-GigabitEthernet1/0/1] quit
```

トランクポートとして GigabitEthernet 1/0/2 を設定し、VLAN 100、VLAN 200 を割り当てます。

```
[PE1] interface gigabitethernet 1/0/2
[PE1-GigabitEthernet1/0/2] port link-type trunk
[PE1-GigabitEthernet1/0/2] port trunk permit vlan 100 200
```

GigabitEthernet 1/0/2 で、SVLAN タグの TPID 値を 0 x 8200 に設定します。

```
[PE1-GigabitEthernet1/0/2] qinq ethernet-type service-tag 8200
```

```
[PE1-GigabitEthernet1/0/2] quit
```

トランクポートとして GigabitEthernet 1/0/3 を設定し、VLAN 200 を割り当てます。

```
[PE1] interface gigabitethernet 1/0/3
[PE1-GigabitEthernet1/0/3] port link-type trunk
[PE1-GigabitEthernet1/0/3] port trunk permit vlan 200
```

GigabitEthernet 1/0/3 の PVID として VLAN 200 を設定します。

```
[PE1-GigabitEthernet1/0/3] port trunk pvid vlan 200
```

GigabitEthernet 1/0/3 で QinQ を有効にします。

```
[PE1-GigabitEthernet1/0/3] qinq enable
[PE1-GigabitEthernet1/0/3] quit
```

1)　PE 2 を設定します。

トランクポートとして GigabitEthernet 1/0/1 を設定し、VLAN 200 を割り当てます。

```
<PE2> system-view
[PE2] interface gigabitethernet 1/0/1
[PE2-GigabitEthernet1/0/1] port link-type trunk
[PE2-GigabitEthernet1/0/1] port trunk permit vlan 200
```

GigabitEthernet 1/0/1 の PVID として VLAN 200 を設定します。

```
[PE2-GigabitEthernet1/0/1] port trunk pvid vlan 200
```

GigabitEthernet 1/0/1 で QinQ を有効にします。

```
[PE2-GigabitEthernet1/0/1] qinq enable
[PE2-GigabitEthernet1/0/1] quit
```

トランクポートとして GigabitEthernet 1/0/2 を設定し、VLAN 100、VLAN 200 を割り当てます。

```
[PE2] interface gigabitethernet 1/0/2
[PE2-GigabitEthernet1/0/2] port link-type trunk
[PE2-GigabitEthernet1/0/2] port trunk permit vlan 100 200
```

GigabitEthernet 1/0/2 で、SVLAN タグの TPID 値を 0 x 8200 に設定します。

```
[PE2-GigabitEthernet1/0/2] qinq ethernet-type service-tag 8200
[PE2-GigabitEthernet1/0/2] quit
```

トランクポートとして GigabitEthernet 1/0/3 を設定し、VLAN 100 を割り当てます。

```
[PE2] interface gigabitethernet 1/0/3
[PE2-GigabitEthernet1/0/3] port link-type trunk
[PE2-GigabitEthernet1/0/3] port trunk permit vlan 100
```

GigabitEthernet 1/0/3 の PVID として VLAN 100 を設定します。

```
[PE2-GigabitEthernet1/0/3] port trunk pvid vlan 100
```

GigabitEthernet 1/0/3 で QinQ を有効にします。

```
[PE2-GigabitEthernet1/0/3] qinq enable
[PE2-GigabitEthernet1/0/3] quit
```

2)　PE1 と PE2 間のデバイスを設定します。

QinQ フレームのパスにある各ポートの MTU を 1504 バイト以上に設定します。（詳細は省略します。）

VLAN タグを取り外すことなく VLAN 100 と VLAN 200 からのすべてのフレームを許可するように転送パスのすべてのポートを設定します。（詳細は省略します。）

13.7.2 VLAN トランスペアレントトランスミッション設定例

I. ネットワーク要件

図 13-4に示すように設定します。

- サービスプロバイダは VLAN 100 を company の VLAN10～VLAN 50 に割り当てます。
- サービスプロバイダネットワークの company の専用 VLAN として VLAN 3000 を設定します。

サービスプロバイダネットワークを越えて CVLAN10～CVLAN 50 のレイヤ 2 接続を提供するため、PE1 と PE2 の QinQ を設定します。

SVLAN を使用しないで VLAN 3000 内のホストが通信できるように、PE1 と PE2 の VLAN 3000 の VLAN トランスペアレントトランスミッションを設定します。

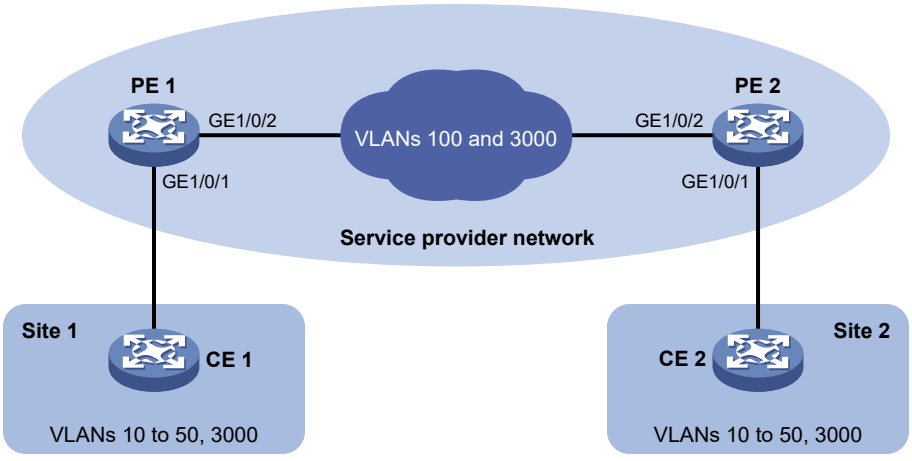


図 13-4 ネットワーク図

II. 設定手順

1)　PE 1 を設定します。

トランクポートとして GigabitEthernet 1/0/1 を設定し、VLAN 100、VLAN 3000 を割り当てます。

```
<PE1> system-view
[PE1] interface gigabitethernet 1/0/1
[PE1-GigabitEthernet1/0/1] port link-type trunk
[PE1-GigabitEthernet1/0/1] port trunk permit vlan 100 3000
```

GigabitEthernet 1/0/1 の PVID として VLAN 100 を設定します。

```
[PE1-GigabitEthernet1/0/1] port trunk pvid vlan 100
```

GigabitEthernet 1/0/1 で QinQ を有効にします。

```
[PE1-GigabitEthernet1/0/1] qinq enable
```

VLAN 3000 からトランスペアレントにフレームを転送するため、GigabitEthernet 1/0/1 を設定します。

```
[PE1-GigabitEthernet1/0/1] qinq transparent-vlan 3000
[PE1-GigabitEthernet1/0/1] quit
```

トランクポートとして GigabitEthernet 1/0/2 を設定し、VLAN 100、VLAN 3000 を割り当てます。

```
[PE1] interface gigabitethernet 1/0/2
[PE1-GigabitEthernet1/0/2] port link-type trunk
[PE1-GigabitEthernet1/0/2] port trunk permit vlan 100 3000
[PE1-GigabitEthernet1/0/2] quit
```

2) PE 2 を設定します。

トランクポートとして GigabitEthernet 1/0/1 を設定し、VLAN 100、VLAN 3000 を割り当てます。

```
<PE2> system-view
[PE2] interface gigabitethernet 1/0/1
[PE2-GigabitEthernet1/0/1] port link-type trunk
[PE2-GigabitEthernet1/0/1] port trunk permit vlan 100 3000
```

GigabitEthernet 1/0/1 の PVID として VLAN 100 を設定します。

```
[PE1-GigabitEthernet1/0/1] port trunk pvid vlan 100
```

GigabitEthernet 1/0/1 で QinQ を有効にします。

```
[PE2-GigabitEthernet1/0/1] qinq enable
```

VLAN 3000 からトランスペアレントにフレームを転送するため、GigabitEthernet 1/0/1 を設定します。

```
[PE2-GigabitEthernet1/0/1] qinq transparent-vlan 3000
[PE2-GigabitEthernet1/0/1] quit
```

トランクポートとして GigabitEthernet 1/0/2 を設定し、VLAN 100、VLAN 3000 を割り当てます。

```
[PE2] interface gigabitethernet 1/0/2
[PE2-GigabitEthernet1/0/2] port link-type trunk
[PE2-GigabitEthernet1/0/2] port trunk permit vlan 100 3000
```

3) PE1 と PE2 間のデバイスを設定します。

QinQ フレームのパスにある各ポートの MTU を 1504 バイト以上に設定します。（詳細は省略します。）

#VLAN タグを取り外すことなく VLAN 100 と VLAN3000 からのすべてのフレームを許可するように転送パスのすべてのポートを設定します。（詳細は省略します。）

目次

このセクションのページは**3-x-x** です。

14章 VLANマッピング 14-1
14.1 概要 14-1
14.1.1 VLANマッピングのアプリケーションシナリオ 14-1
14.1.2 VLANマッピングの実装 14-3
14.2 VLANマッピング設定作業リスト 14-5
14.3 one-to-one VLANマッピングの設定 14-6
14.4 one-to-two VLANマッピングの設定 14-6
14.5 VLANマッピングの表示と維持 14-7
14.6 VLANマッピングの設定例 14-8
14.6.1 One-to-one VLANマッピングの設定例 14-8
14.6.2 One-to-two VLANマッピングの設定例 14-11

14章 VLAN マッピング

重要：

QX-S5100G シリーズは、下記インタフェースでの VLAN マッピングをサポートしておりません。

- リンクアグリゲーションインタフェース
- ハイブリッドポートの untagged VLAN
- トランクポートの untagged VLAN
- アクセスポート

DHCP スヌーピングとの併用はできません。

14.1 概要

VLAN マッピングはタグ付けされたトラフィックを新しい VLAN ID で再マッピングします。NEC は以下のタイプを提供します。

- **One-to-One VLAN マッピング** — 1 つの VLAN タグを別の VLAN タグに置き換えます。
- **One-to-two VLAN マッピング** – シングルタグ付けされたパケットに外部 VLAN タグをタグ付けします。

14.1.1 VLAN マッピングのアプリケーションシナリオ

I. one-to-one VLAN マッピング

図 14-1に one-to-one VLAN マッピングの一般的なシナリオを示します。シナリオは通信用にブロードバンドインタネットアクセスを実装しています。

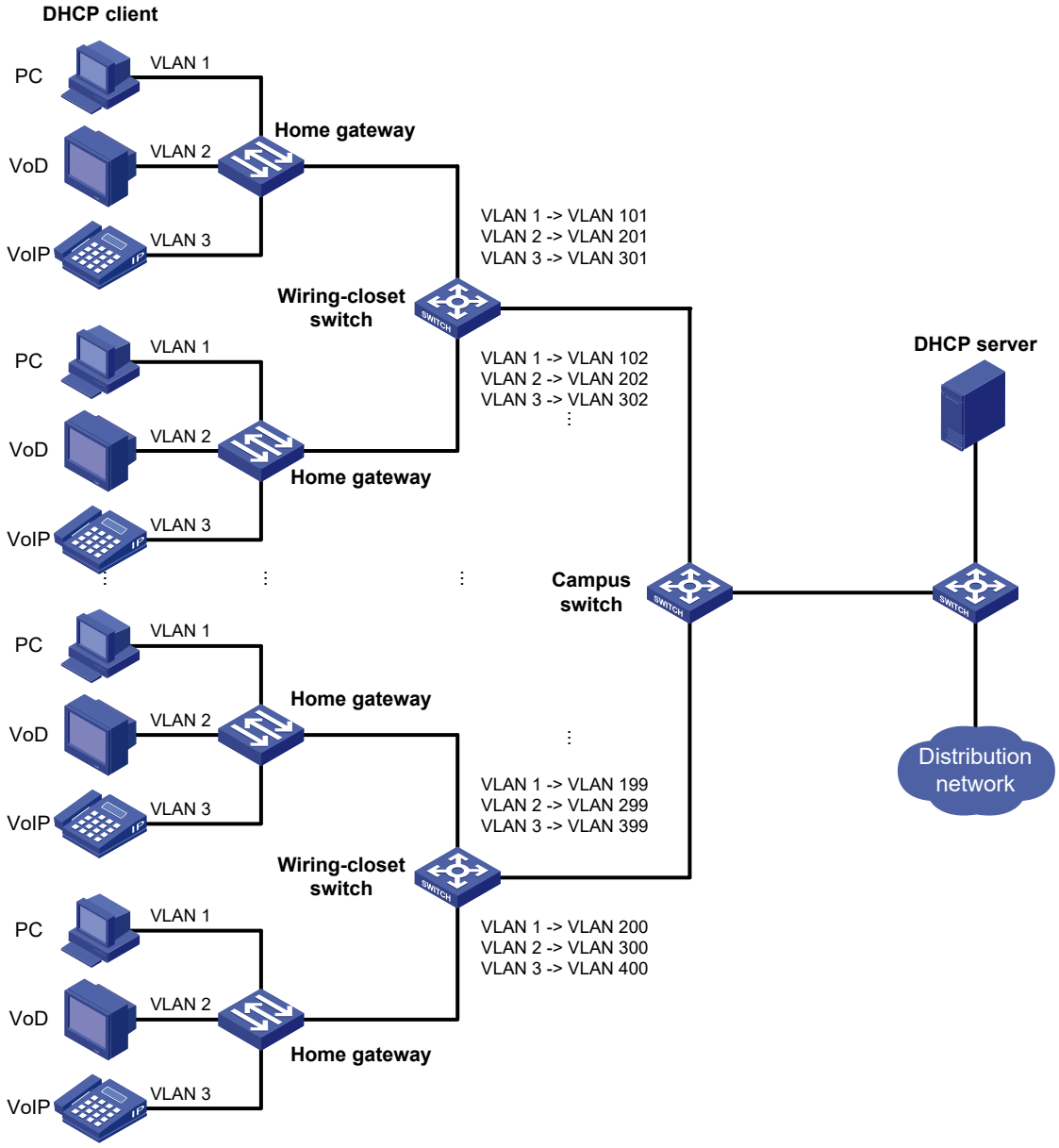


図 14-1 one-to-one VLAN マッピングの一般的なシナリオ

図 14-1における、ネットワークの概要を以下に示します。

- 各ホームゲートウェイは、PC、VoD、VoIP サービスを転送するため、異なる VLAN を使用します。
- カスタマ毎に詳細にトラフィックの各タイプを分類させるため、ワイヤリングクローゼットのスイッチで one-to-one VLAN を設定します。この機能は分類した VLAN を各カスタマからのトラフィックタイプ毎に割り当てます。必要とされる VLAN のトータル数は非常に多くなります。

II. one-to-two VLAN マッピングのシナリオ

図 14-2に one-to-two VLAN マッピングの一般的なシナリオを示します。2 つのリモートサイトの VLAN 10、VLAN 20 はパブリックネットワークを超えて通信する必要があります。

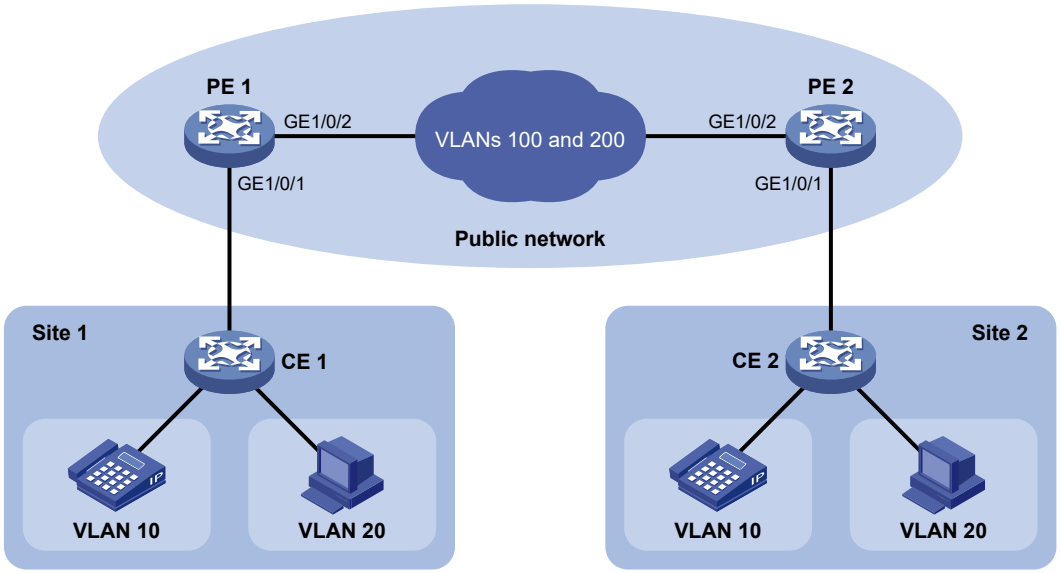


図 14-2 one-to-two VLAN マッピングの一般的なシナリオ

パブリックネットワークは SVLAN 100 を VLAN 10 に、SVLAN 200 を VLAN 20 に割り当てます。Site1 からのパケットは PE1 に到着します。PE1 は one-to-two VLAN マッピングを使用して、SVLAN 100 あるいは SVLAN 200 のパケットをタグ付けします。

One-to-two VLAN マッピングは以下の利点があります。

- SVLAN に重複することなく CVLAN の割り当てを計画するようにカスタマネットワークを設定することができます。
- タグ付けされたパケットに VLAN タグを追加し、4094 × 4094 に VLAN の数を拡張します。
- SVLAN のリソースを減少させます。つまりマッピングプロセスが初期化するまえに、パブリックネットワークに 4094 の VLAN が存在します。

14.1.2 VLAN マッピングの実装

図 14-3は VLAN マッピングが動作するときの、コンセプトと用語を説明するために、簡単なネットワークで示したものです。

基本的な VLAN マッピングの関係を以下に示します。

- **Uplink traffic** – カスタマネットワークからサービスプロバイダネットワークに転送されるトラフィック
- **Downlink traffic** – サービスプロバイダネットワークからカスタマネットワークに転送されるトラフィック
- **Network-side port** – サービスプロバイダに接続されたポート、あるいはサービスプロバイダに近いポート

- **Customer-side port** – カスタマネットワークに接続されたポート、あるいはカスタマネットワークに近いポート

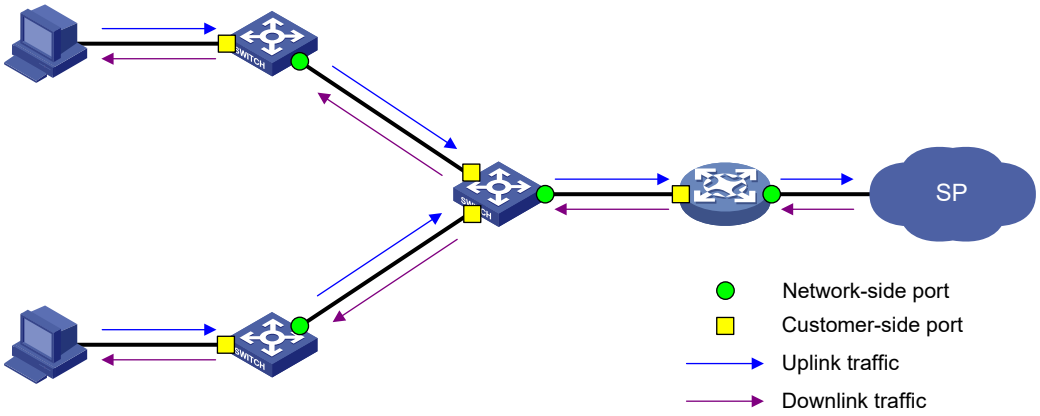


図 14-3 基本的な VLAN マッピングの関係

I. One-to-one VLAN マッピング

図 14-4に示すように、one-to-one VLAN マッピングはカスタマ側ポートで実装され、VLAN タグを以下のように置き換えます。

- アップリンクトラフィック用に CVLAN を SVLAN に置き換えます。
- ダウンリンクトラフィック用に SVLAN を CVLAN に置き換えます。

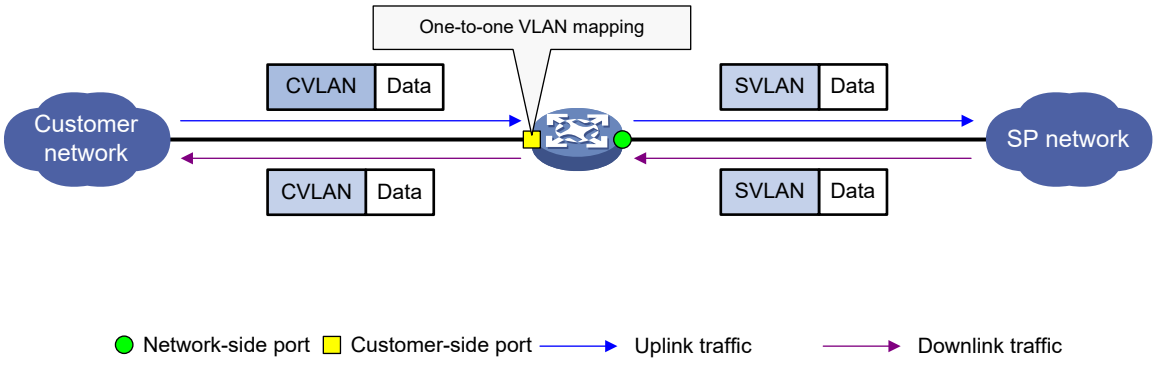


図 14-4 One-to-one VLAN マッピングの実装

II. One-to-two VLAN マッピング

図 14-5に示すように、one-to-two VLAN マッピングはアップリンクトラフィック用に SVLAN タグを追加するため、カスタマ側ポートで実装されます。

ダウンリンクトラフィック用にカスタマネットワークに正しく送信するため、転送するまえにカスタマ側ポートの SVLAN タグを取り外すことを確認してください。以下の方法の 1 つを使用してダウンリンクトラフィックの SVLAN タグを取り外してください。

- ハイブリッドポートとしてカスタマ側ポートを設定し、タグ付けメンバとして SVLAN にポートを割り当てます。

- トランクポートとしてカスタマ側ポートを設定し、PVID として SVLAN を設定します。

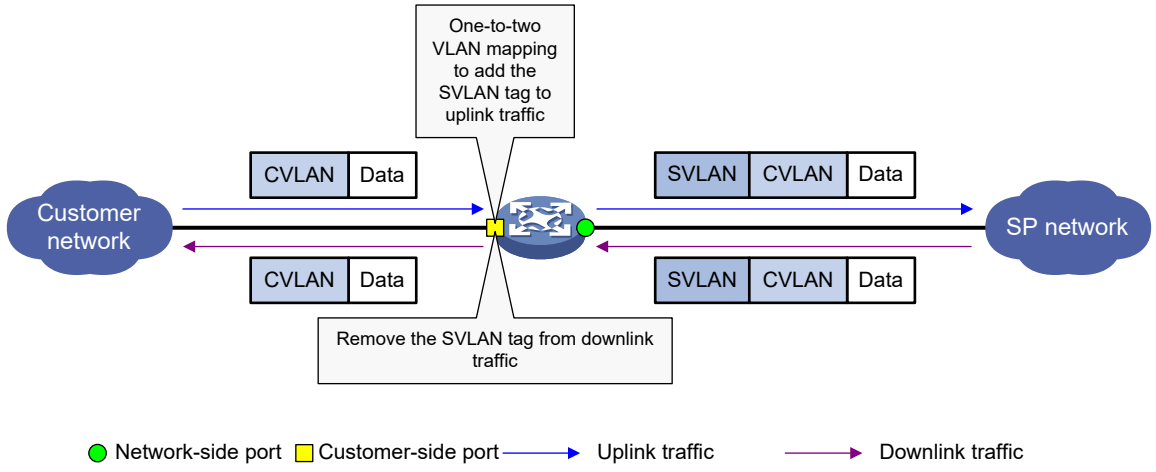


図 14-5 One-to-two VLAN マッピングの実装

14.2 VLANマッピング設定作業リスト

VLAN マッピングを設定するとき、以下の制限とガイドラインに従ってください。

- パケットに VLAN タグをつけることで QinQ が有効なポートで VLAN マッピングと QinQ の両方を設定することができます。設定の重複がある場合、VLAN マッピングが適用されます。QinQ の詳細は、オペレーションマニュアルのセクション 3 *アクセス "QinQ"*を参照してください。
- パケットの VLAN タグを追加あるいは置き換える場合、VLAN マッピングと QoS ポリシーの両方を設定することができます。設定の重複がある場合、VLAN マッピングが適用されます。QoS ポリシーの詳細は、オペレーションマニュアルのセクション 8 *ACL and QoS "QoS ポリシー"*を参照してください。
- VLAN マッピングを適用したインタフェースを経由し、かつ VLAN マッピング対象の VLAN インタフェースを経由する L3 通信は未サポートです。
- VLAN マッピング対象の VLAN に VLAN インタフェースを作成および IP アドレスを設定する場合は、L3 通信の経路（送受信インタフェース）には VLAN マッピングを適用しないでください。

重要：
ネットワークのデバイスで適切な VLAN マッピング方法を使用してください。

以下に VLAN マッピングの作業リストを示します。

作業リスト	補足
one-to-one VLANマッピングの設定	図 14-1に示すワイヤリングクローゼットのスイッチでone-to-one VLANマッピングを設定します。

作業リスト	補足
one-to-two VLANマッピングの設定	図 14-2に示すように、カスタマネットワークからサービスプロバイダにトラフィックが通過するPE1、PE2でone-to-two VLANマッピングを設定します。

14.3 one-to-one VLANマッピングの設定

異なるホームから同じサービスタイプのトラフィックを隔離するため、ワイヤリングクローゼット（図 14-1を参照してください）のカスタマ側ポートで one-to-one VLAN マッピングを設定します。

one-to-one VLAN マッピングを設定するまえに、VLAN、変換される VLAN を作成してください。

以下に one-to-one VLAN マッピングの設定を示します。

操作	コマンド	補足
1． system view.に移行する	**system-view**	—
2． Layer 2 Ethernet interface view に移行する	**interface** *interface-type interface-number*	—
3． ポートのリンクタイプを設定する	● トランクポートとしてポートを設定する：**port link-type trunk** ● ハイブリッドポートとしてポートを設定する：**port link-type hybrid**	デフォルト：アクセス
4． ポートにもとの VLAN と変換される VLAN を割り当てる	● トランクポート：**port trunk permit vlan** *vlan-id-list* ● ハイブリッドポート：**port hybrid vlan** *vlan-id-list* **tagged**	—
5． one-to-one VLAN マッピングを設定する	**vlan mapping** *vlan-id* **translated-vlan** *vlan-id*	デフォルト：設定なし

14.4 one-to-two VLANマッピングの設定

図 14-2に示すように、カスタマトラフィックが PE1、PE2 の SP ネットワークに入るエッジデバイスの one-to-two VLAN を実行します。たとえば、one-to-two VLAN マッピングは SVLAN タグを各入力パケットに追加するエッジデバイスを有効にします。

one-to-two VLAN マッピングを設定するまえに、CVLAN、SVLAN を作成してください。

インタフェースの MTU はデフォルトで 1500byte です。VLAN タグがパケットに追加されると 4byte のパケット長が追加されます。one-to-two VLAN マッピングを設定するとき、サービスプロバイダネットワークの転送パスのポートの MTU を少なくとも 1504byte にすることを推奨します。

以下に one-to-two VLAN マッピングの設定を示します。

操作	コマンド	補足
1． system view.に移行する	**system-view**	―
2． Layer 2 Ethernet interface view に移行する	**interface** *interface-type interface-number*	―
3． ポートのリンクタイプを設定する	• トランクポートとしてポートを設定する：**port link-type trunk** • ハイブリッドポートとしてポートを設定する：**port link-type hybrid**	デフォルト：アクセス
4． ポートに CVLAN を割り当てる	• トランクポート：**port trunk permit vlan** *vlan-id-list* • ハイブリッドポート：**port hybrid vlan** *vlan-id-list* **tagged**	―
5． タグつきメンバとして変換された SVLAN にポートを割り当てる	• トランクポート： 1． トランクポートの PVID として SVLAN を設定する：**port trunk pvid vlan** *vlan-id* 2． SVLAN にトランクポートを割り当てる：**port trunk permit vlan** { *vlan-id-list* | **all** } • ハイブリッドポート：**port hybrid vlan** *vlan-id-list* **tagged**	―
6． one-to-two VLAN マッピングを設定する	**vlan mapping nest** { **range** *vlan-range-list* | **single** *vlan-id-list* } **nested-vlan** *vlan-id*	デフォルト：設定なし 1つのSVLANタグのみを同一のCVLANからのパケットに追加することができます。異なるSVLANタグを異なるCVLANパケットに追加する場合、ポートのリンクタイプをハイブリッドに設定し、**vlan mapping nest**コマンドを繰り返してください。

14.5 VLANマッピングの表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
VLANマッピング情報を表示する	**display vlan mapping** [**interface** *interface-type interface-number*]

14.6 VLANマッピングの設定例

14.6.1 One-to-one VLAN マッピングの設定例

I. ネットワーク要件

図 14-6に示すように設定します。

- 各家庭は、DHCP を通して IP アドレスを取得し、PC、VoD、VoIP サービスを提供します。
- ホームゲートウェイで、PC トラフィック用に VLAN1、VoD トラフィック用に VLAN2、VoIP サービス用に VLAN3 を割り当てます。

異なる家庭から同じサービスタイプのトラフィックを隔離するため、ワイヤリングクローゼットスイッチで one-to-one VLAN マッピングを設定します。この機能は各ホームからのトラフィックの各タイプを 1 つの VLAN に割り当てます。

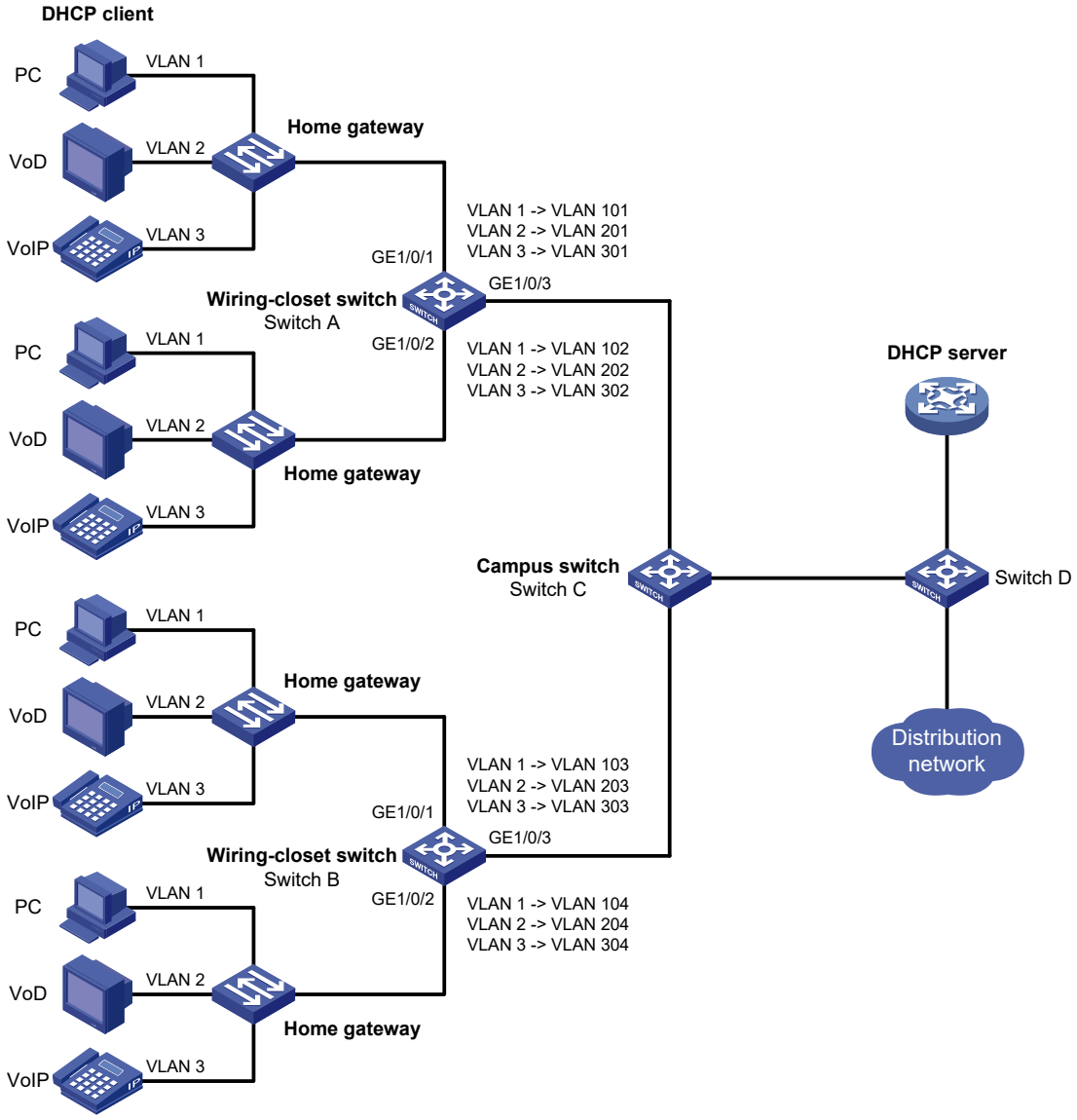


図 14-6 ネットワーク図

II. 設定手順

1)　Switch A を設定します。

もとの VLAN を作成します。

```
<SwitchA> system-view
[SwitchA] vlan 2 to 3
```

変換される VLAN を作成します。

```
[SwitchA] vlan 101 to 102
[SwitchA] vlan 201 to 202
[SwitchA] vlan 301 to 302
```

トランクポートとしてカスタマ側ポート GigabitEthernet 1/0/1 を設定します。

```
<SwitchA> system-view
[SwitchA] interface gigabitethernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] port link-type trunk
```

もとの VLAN と変換される VLAN を GigabitEthernet 1/0/1 に割り当てます。

```
[SwitchA-GigabitEthernet1/0/1] port trunk permit vlan 1 2 3 101 201 301
```

それぞれ VLAN1、VLAN 2、VLAN 3 に VLAN101、VLAN 201、VLAN 301 をマッピングするように GigabitEthernet 1/0/1 で one-to-one VLAN マッピングを設定します。

```
[SwitchA-GigabitEthernet1/0/1] vlan mapping 1 translated-vlan 101
[SwitchA-GigabitEthernet1/0/1] vlan mapping 2 translated-vlan 201
[SwitchA-GigabitEthernet1/0/1] vlan mapping 3 translated-vlan 301
[SwitchA-GigabitEthernet1/0/1] quit
```

トランクポートとしてカスタマ側ポート GigabitEthernet 1/0/2 を設定します。

```
[SwitchA] interface gigabitethernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] port link-type trunk
```

もとの VLAN と変換される VLAN を GigabitEthernet 1/0/2 に割り当てます。

```
[SwitchA-GigabitEthernet1/0/2] port trunk permit vlan 1 2 3 102 202 302
```

それぞれ VLAN1、VLAN 2、VLAN 3 に VLAN102、VLAN 202、VLAN 302 をマッピングするように GigabitEthernet 1/0/2 で one-to-one VLAN マッピングを設定します。

```
[SwitchA-GigabitEthernet1/0/2] vlan mapping 1 translated-vlan 102
[SwitchA-GigabitEthernet1/0/2] vlan mapping 2 translated-vlan 202
[SwitchA-GigabitEthernet1/0/2] vlan mapping 3 translated-vlan 302
[SwitchA-GigabitEthernet1/0/2] quit
```

トランクポートとしてネットワーク側ポート GigabitEthernet 1/0/3 を設定します。

```
[SwitchA] interface gigabitethernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] port link-type trunk
```

変換される VLAN を GigabitEthernet 1/0/3 に割り当てます。

```
[SwitchA-GigabitEthernet1/0/3] port trunk permit vlan 101 201 301 102 202 302
[SwitchA-GigabitEthernet1/0/3] quit
```

2)　Switch A の設定と同様に Switch B を設定します。（詳細は省略します）

III. 設定の確認

たとえば Switch A のワイヤリングクローゼットスイッチの VLAN マッピング情報を表示します。

```
[SwitchA] display vlan mapping
Interface GigabitEthernet1/0/1:
  Outer VLAN    Inner VLAN    Translated Outer VLAN    Translated Inner VLAN
  1             N/A           101                      N/A
  2             N/A           201                      N/A
  3             N/A           301                      N/A
Interface GigabitEthernet1/0/2:
  Outer VLAN    Inner VLAN    Translated Outer VLAN    Translated Inner VLAN
  1             N/A           102                      N/A
  2             N/A           202                      N/A
  3             N/A           302                      N/A
```

14.6.2 One-to-two VLAN マッピングの設定例

I. ネットワーク要件

図 14-7に示すように、ネットワーク要件を記載します。

- 会社の 2 つの部門の Site1 と Site2 は、異なるサービスのトラフィックを転送するため、VLAN 10、VLAN 20 を使用します。
- サービスプロバイダは SVLAN 100 に VLAN 10、SVLAN 200 に VLAN 20 を割り当てます。

パブリックネットワークを通して通信を行うため、2 つの部門で one-to-two VLAN マッピングを設定します。

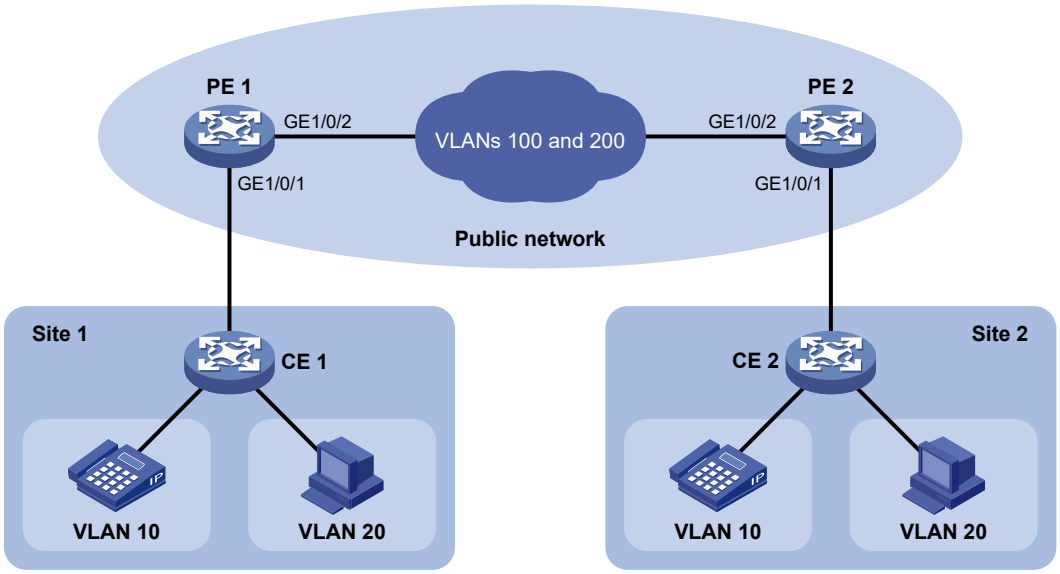


図 14-7 ネットワーク図

II. 設定手順

1)　PE 1 を設定します。

VLAN 10、VLAN 20、VLAN 100、VLAN 200 を作成します。

```
<PE1> system-view
```

```
[PE1] vlan 10
[PE1-vlan10] quit
[PE1] vlan 20
[PE1-vlan20] quit
[PE1] vlan 100
[PE1-vlan100] quit
[PE1] vlan 200
[PE1-vlan200] quit
```

カスタマ側の GigabitEthernet 1/0/1 に one-to-two VLAN を設定し、SVLAN タグ 100 を VLAN 10 からのパケットに追加し、SVLAN タグ 200 を VLAN 20 からのパケットに追加します。

```
[PE1] interface gigabitethernet 1/0/1
[PE1-GigabitEthernet1/0/1] vlan mapping nest single 10 nested-vlan 100
[PE1-GigabitEthernet1/0/1] vlan mapping nest single 20 nested-vlan 200
```

GigabitEthernet 1/0/1 をハイブリッドポートに設定します。

```
[PE1-GigabitEthernet1/0/1] port link-type hybrid
```

タグ付けメンバとして VLAN 10、VLAN 20、VLAN 100、VLAN 200 に GigabitEthernet 1/0/1 を割り当てます。

```
[PE1-GigabitEthernet1/0/1] port hybrid vlan 10 20 100 200 tagged
[PE1-GigabitEthernet1/0/1] quit
```

ネットワーク側の GigabitEthernet 1/0/2 をトランクポートに設定します。

```
[PE1] interface gigabitethernet 1/0/2
[PE1-GigabitEthernet1/0/2] port link-type trunk
```

VLAN 100、VLAN 200 に GigabitEthernet 1/0/2 を割り当てます。

```
[PE1-GigabitEthernet1/0/2] port trunk permit vlan 100 200
[PE1-GigabitEthernet1/0/2] quit
```

2)　PE1 の設定と同様に PE2 を設定します。（詳細は省略します。）

III. 設定の確認

PE1 で VLAN マッピングの情報を確認します。

```
[PE1] display vlan mapping
Interface GigabitEthernet1/0/1:
  Outer VLAN    Inner VLAN    Translated Outer VLAN    Translated Inner VLAN
  10             N/A           100                      10
  20             N/A           200                      20
```

PE2 で VLAN マッピングの情報を確認します。

[PE2] display vlan mapping

```
Interface GigabitEthernet1/0/2:
  Outer VLAN    Inner VLAN    Translated Outer VLAN    Translated Inner VLAN
  10             N/A           100                      10
  20             N/A           200                      20
```

目次

このセクションのページは**3-x-x** です。

15 章 LLDP.....15-1
15.1 概要.....15-1
15.1.1 基本コンセプト.....15-1
15.1.2 動作メカニズム.....15-7
15.1.3 プロトコルと標準.....15-8
15.2 LLDP 設定作業リスト.....15-8
15.3 LLDP の基本設定.....15-9
15.3.1 LLDP の有効化.....15-9
15.3.2 LLDP 動作モードの設定.....15-9
15.3.3 再初期化遅延時間の設定.....15-9
15.3.4 LLDP ポーリングの有効化.....15-10
15.3.5 アドバタイズ可能な TLV の設定.....15-10
15.3.6 管理アドレスの設定とカプセル化フォーマットの設定.....15-11
15.3.7 LLDP に関する他のパラメータの設定.....15-12
15.3.8 LLDP フレームのカプセル化フォーマットの設定.....15-12
15.4 LLDP PVID 不一致チェックの無効化.....15-13
15.5 CDP 互換モードの設定.....15-13
15.6 LLDP トラップの設定.....15-15
15.7 LLDP の表示と維持.....15-16
15.8 LLDP の設定例.....15-16
15.8.1 LLDP の基本的な設定例.....15-16
15.8.2 CDP 互換モードの設定例.....15-20

15章 LLDP

15.1 概要

異なるベンダが存在するネットワークのとき、標準の設定情報を交換するプラットフォームは、異なるベンダからの異なるタイプのネットワーク装置を相互に検出します。これにより設定を交換できることを保証します。

LLDP（Link Layer Discovery Protocol）は、IEEE802.1AB で規定されています。データリンクレイヤで直接装置に接続された装置間の装置情報を交換するプロトコルです。LLDP では、装置は LLDPDU（LLDP データユニット）にある TLV と呼ばれるタイプ（Type）長さ（Length）値（Value）の形式を利用して、ローカル装置情報を直接接続された装置に送信します。ローカル装置情報はシステム機能、管理 IP アドレス、装置 ID、ポート ID を含みます。装置は LLDP 隣接装置から受信した LLDPDU の装置情報を標準 MIB に格納します。MIB についての詳細は、オペレーションマニュアルのセクション 11 *システム管理*”*SNMP*”を参照してください。LLDP はレイヤ 2 のネットワークトポロジの変化をただちに検出し、識別するためにネットワーク管理システムを有効にします。

15.1.1 基本コンセプト

I. LLDP エージェント

LLDP が動作するところで LLDP エージェントはエンティティをマッピングします。複数の LLDP エージェントは同時にインタフェースで動作することができます。

LLDP エージェントは以下のタイプに分類されます。

- Nearest bridge エージェント
- Nearest customer bridge エージェント
- Nearest non-TPMR bridge エージェント

Two-port MAC Relay （TPMR）は 2 つの外部アクセスブリッジポートのブリッジタイプで、MAC ブリッジの機能をサポートします。TPMR は以下を除いて、すべてのフレームベースのメディアに独立したプロトコルに透過的です。

- 独立したプロトコル行き
- TPMR のリレー機能が転送しないように予約された MAC アドレス行き

LLDP は隣接エージェント間でパケットを交換し、隣接情報を作成、維持します。図 15-1 に LLDP エージェントの隣接関係を示します。LLDP はカスタマブリッジ（CB）とサービスブリッジ（SB）の 2 つのブリッジモードをもちます。

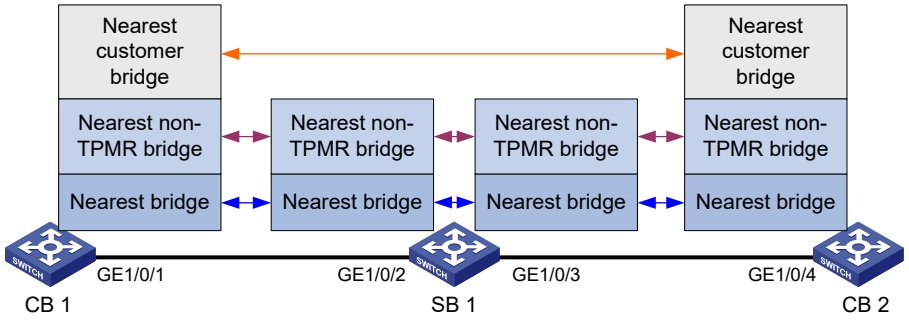


図 15-1 LLDP 隣接関係

II. LLDP フレームフォーマット

LLDP は LLDP フレームの装置情報を送信します。LLDP フレームは Ethernet II あるいは SNAP フレームでカプセル化されています。

- Ethernet II にカプセル化した LLDP フレーム

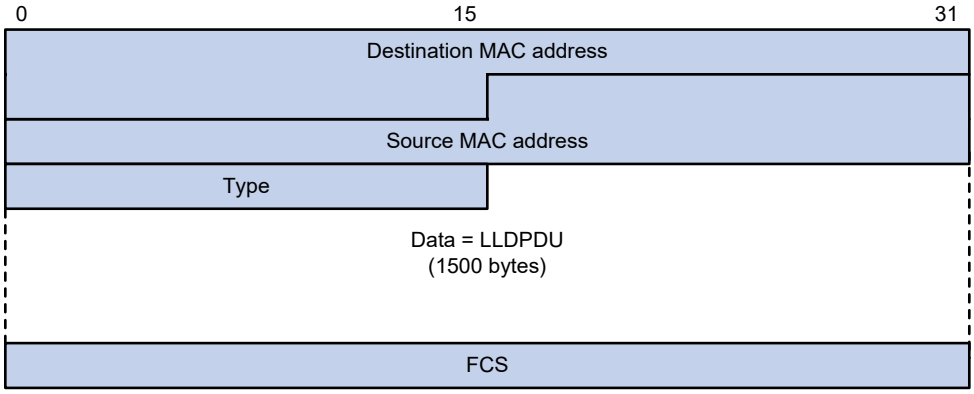


図 15-2 Ethernet II にカプセル化した LLDP フレーム

表 15-1 Ethernet II にカプセル化した LLDP フレームフィールド

フィールド	説明
Destination MAC address	LLDPフレームがアドバタイズしたMACアドレスです。 LLDPは異なるエージェントタイプ向けのLLDPフレームの宛先MACアドレスとして異なるマルチキャストアドレスを指定します。同一インタフェース上で異なるエージェントタイプで送受信したLLDPフレームを区別します。 • LLDPフレーム0x0180-C200-000Eはnearest bridge向けです。 • LLDPフレーム0x0180-C200-000はnearest customer bridge向けです。 • LLDPフレーム0x0180-C200-0003はnearest TPMR bridge向けです。
Source MAC address	送信ポートのMACアドレスです。
Type	上位レイヤプロトコルのEthernetタイプです。LLDPは0x88CCです。

フィールド	説明
Data	LLDPDUです。
FCS	フレームチェックシーケンスで、32ビットCRCの値が受信したEthernetフレームを確認するために使われます。

- SNAP にカプセル化した LLDP フレーム

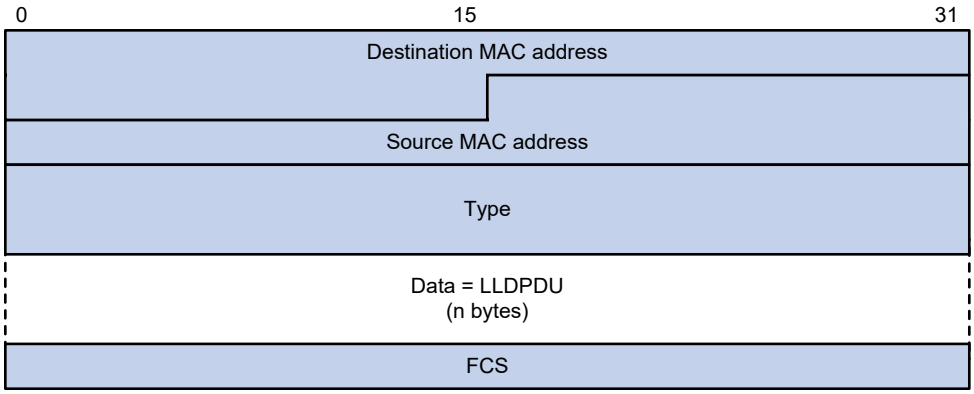


図 15-3 SNAP にカプセル化したフレーム

表 15-2 SNAP にカプセル化したフレームフィールド

フィールド	説明
Destination MAC address	LLDPフレームがアドバタイズしたマルチキャストのMACアドレスです。Ethernet2でカプセル化したLLDPフレームのMACアドレスと同一です。
Source MAC address	送信ポートのMACアドレスです。
Type	上位レイヤプロトコルのSNAPタイプです。LLDPは0xAAAA-0300-0000-88CCです。
Data	LLDPDUです。
FCS	フレームチェックシーケンスで、32ビットCRCの値が受信したEthernetフレームを確認するために使われます。

III. LLDPDU

LLDP は情報を交換するために LLDPDU を使用します。LLDPDU は複数の TLV（タイプ, 長さ,値）から構成されています。図 15-4で示すように、装置上の各 TLV をアドバタイズします。

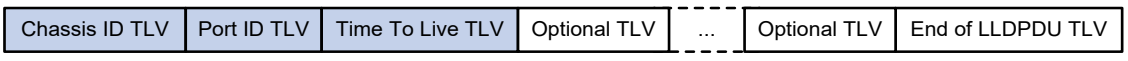


図 15-4 LLDPDU カプセルフォーマット

LLDPDU は、最大で 32 種類の TLV をもつことができます。ます。必須の TLV は、Chassis ID TLV、Port ID TLV、Time to Live TLV です。他の TLV はオプションです。

IV. TLV

TLV はタイプ、長さ、値のフィールドが含まれる情報の要素です。

LLDPDU TLV は以下のカテゴリに分類されます。

- 基本的な管理 TLV
- 組織規定された TLV （IEEE 802.1、IEEE 802.3）
- LLDP-MED（media endpoint discovery）関連の TLV

基本的な TLV は装置を管理するのに必要不可欠なカテゴリです。組織規定された TLV と LLDP-MED 関連の TLV は拡張された装置管理のために使用されます。標準あるいは他の組織によって定義され、LLDPDU のオプションです。

- 基本的な管理 TLV

表 15-3に基本的な管理 TLV タイプを示します。基本的な管理 TLV のいくつかは、各 LLDPDU に必須です。

表 15-3 基本的な管理 TLV

タイプ	説明	補足
Chassis ID	送信する装置のBridge MACアドレスを指定します。	必須
Port ID	送信ポートのIDを指定します。 ● LLDPDUがLLDP-MEDを含んでいる場合、Port ID TLVは送信ポートのMACアドレスです。 ● LLDPDUがLLDP-MEDを含んでいない場合、Port ID TLVはポート名です。	
Time to Live	受信する装置のTTLを指定します。	
End of LLDPDU	LLDPDUのTLVシーケンスの終端をマーキングします。	オプション
Port Description	送信するポートの説明を指定します。	
System Name	送信する装置の装置名を指定します。	
System Description	送信する装置の説明を指定します。	
System Capabilities	送信する装置の主な機能や有効な機能を識別します。	
Management Address	以下の要素を指定します。 ● ローカル装置の管理アドレスです。 ● インタフェース番号、アドレスに関連したOIDです。	

- IEEE 802.1 組織指定 TLV

表 15-4 IEEE 802.1 組織指定 TLV

タイプ	説明
Port VLAN ID	ポートのVLAN識別子（PVID） を指定します。
Port And Protocol VLAN ID	装置がプロトコルVLANをサポートしているかどうかを示します。サポートしている場合、プロトコルのVLAN IDです。
VLAN Name	ポートが属しているVLANの名前を示します。
Protocol Identity	ポートでサポートされるプロトコルを示します。
DCBX	Data center bridging exchangeプロトコルです。 🕮 **メモ：** QX-S5100GシリーズはDCBX TLVをサポートしていません。

タイプ	説明
EVB module	Edge Virtual Bridgingモジュールです。EVB TLV、CDCP TLVが含まれます。 🕮 メモ： QX-S5100GシリーズはEVB TLVをサポートしていません。
Link Aggregation	リンクアグリゲーションをサポートするポートかどうかを示します。もしサポートしている場合、リンクアグリゲーションが有効です。
Management VID	Management VLAN IDです。
VID Usage Digest	VLAN ID usage digestです。
ETS Configuration	Enhanced Transmission Selection configurationです。
ETS Recommendation	ETS recommendationです。
PFC	Priority-based Flow Controlです。
APP	Application protocolです。
QCN	Quantized Congestion Notificationです。 🕮 メモ： QX-S5100GシリーズはQCN TLVをサポートしていません。

🕮 メモ：

QX-S5100G シリーズは Protocol identity TLV と VLAN ID usage digest TLV を受信することができますが、TLV を送信することはできません。

- IEEE 802.3 組織指定 TLV

表 15-5 IEEE 802.3 組織指定 TLV

タイプ	説明
MAC/PHY Configuration/Status	送信するポートの通信速度、通信モード、オートネゴシエーションのサポート状況、オートネゴシエーションの状態、現在の通信速度、現在の通信モードの状態を示します。
Power Via MDI	ポートの電源供給状態を示します。 • PoEタイプ（PSEあるいはPD） • PoEモード • PSE電源供給のサポート状況 • PSE電源供給の有効/無効状態 • PoEモードの管理可能/不可状態 • 電力供給タイプ • 電力ソース • 電力優先度 • PDが要求した電力 • PSEが割り当てた電力
Maximum Frame Size	ポートでサポートされる最大フレームサイズ（MTU）を示します。

タイプ	説明
Power Stateful Control	送信ポートで管理される電源状態制御を示します。 ● PSE/PDの電源 ● PSE/PDの優先度 ● PSE/PDの電力
Energy-Efficient Ethernet	EEE（Energy Efficient Ethernet）を示します。

🕮 **メモ：**

Power Stateful Control TLV は IEEE802.3at Draft1.0 で定義されています。最近のバージョンでは Power Stateful Control TLV をサポートしていません。QX シリーズは Power Stateful Control TLV を受信したときのみ送信を行います。

LLDP-MED TLV は複数のアプリケーションを VoIP（voice over IP）の拡張されたアプリケーションに提供します。たとえば基本設定、ネットワークポリシー設定、アドレス、ディレクトリ管理などのアプリケーションです。LLDP-MED TLV は Ethernet で音声装置の費用効果、使用しやすさのソリューションを提供します。表 15-6に LLDP-MED TLV を示します。

表 15-6 LLDP-MED TLV

タイプ	説明
LLDP-MED Capabilities	LLDP-MED LEDをサポートするネットワークの装置がLLDP-MED LEDをアドバタイズすることを可能にします。
Network Policy	ポートのVLAN ID、VLANタイプ、指定アプリケーションのレイヤ2/レイヤ3の優先度を、ネットワーク装置あるいは端末装置がアドバタイズすることを可能にします。
Extended Power-via-MDI	ネットワーク装置あるいは端末装置が電源供給能力をアドバタイズすることを可能にします。TLVはPower Via MDI TLVの拡張です。
Hardware Revision	端末装置がハードウェアバージョンをアドバタイズすることを可能にします。
Firmware Revision	端末装置がファームウェアバージョンをアドバタイズすることを可能にします。
Software Revision	端末装置がソフトウェアバージョンをアドバタイズすることを可能にします。
Serial Number	端末装置がシリアル番号をアドバタイズすることを可能にします。
Manufacturer Name	端末装置がベンダ名をアドバタイズすることを可能にします。
Model Name	端末装置がモデル名をアドバタイズすることを可能にします。
Asset ID	端末装置がasset IDをアドバタイズすることを可能にします。一般的な使用方法として、ディレクトリ管理、価値のトラッキングを補助するためのエンドポイント用に指定されます。
Location Identification	位置をもとにしたアプリケーションの内容を使用するため、ネットワーク装置が端末装置の位置識別情報をアドバタイズすることを可能にします。

🕮 **メモ：**

- MAC/PHY configuration/status TLV がアドバタイズされない場合、LLDP-MED TLV をアドバタイズ可能でも LLDP-MED TLV はアドバタイズされません。
- LLDP-MED Capabilities TLV がアドバタイズできない場合、他の LLDP-MED TLV がアドバタイズ可能でもアドバタイズされません。

V. 管理アドレス

装置の管理アドレスは、ネットワークマネジメントシステムで使われ、トポロジ維持やネットワーク管理で装置を認識するために使われます。管理アドレスは、management address TLV にカプセル化されています。

15.1.2 動作メカニズム

I. LLDP 動作モード

LLDP エージェントは以下のモードを動作させることができます。

- **TxRx モード** – このモードの LLDP エージェントは LLDP フレームの送信、受信を行うことができます。
- **Tx モード** – このモードの LLDP エージェントは LLDP フレームの送信のみを行うことができます。
- **Rx モード** – このモードの LLDP エージェントは LLDP フレームの受信のみを行うことができます。
- **Disable モード** – このモードの LLDP エージェントは LLDP フレームの送信も受信も行うことができません。

LLDP エージェントの動作モードが別の動作モードに変更されるたびに LLDP は初期化されます。LLDP エージェントの動作モードが別の動作モードへ変更したとき、設定可能な再初期化遅延時間を設定することで LLDP が頻繁に初期化されるのを防ぐことができます。再初期化遅延時間を設定する場合、LLDP は LLDP 動作モードが変更したのち、指定された期間が終了するまで、再初期化を行いません。

II. LLDP フレームの送信

TxRx モードあるいは Tx モードで動作する LLDP エージェントは、定期的およびローカルの設定が変更されるときに、直接接続されている装置へ LLDP フレームを送信します。LLDP フレームがローカルの装置情報を頻繁に変更する際、ネットワークを占有してしまうことを防止するため、LLDP は LLDP フレームを制限するためトークバケットメカニズムを使用します。トークンバケットメカニズムの詳細は、オペレーションマニュアルのセクション 8 *ACL and QoS*”*トラフィックポリシング*、*GTS*、*ラインレート*”を参照してください。

LLDP は自動的に以下のいずれかのケースを用いて早急に LLDP フレームを送信することができます。

- 新しい LLDP フレームが受信され、ローカル装置に新しい装置情報をアドバタイズします。

- LLDP エージェントの LLDP 動作モードが Disable あるいは Rx から、TxRx あるいは Tx に変更したときに早急に LLDP フレームを送信します。

早急に LLDP フレームを送信するメカニズムでは、LLDP 隣接装置がローカル装置を発見できるように、指定した数の LLDP フレームが、設定可能なできるだけ早い送信間隔で連続して送信されます。装置は指定した数の LLDPDU を送信した後、送信間隔を通常に戻します。

III. LLDP フレームの受信

TxRx モードまたは Rx モードで動作している LLDP エージェントは、受信した LLDP フレームを受信するたびに TLV の有効性を確認します。TLV が有効である場合、LLDP エージェントは情報を保存し、エージングタイマを開始します。エージングタイマのデフォルトは LLDP フレームによってアドバタイズされる Time To Live TLV の TTL と同じ値です。LLDP エージェントが新しい LLDP フレームを受信したとき、エージングタイマは再スタートします。LLDP フレームでアドバタイズされた Time To Live TLV の TTL が 0 になったとき、保存されているすべての情報はエージアウトします。

15.1.3 プロトコルと標準

- IEEE 802.1AB-2005, *Station and Media Access Control Connectivity Discovery*
- IEEE 802.1AB-2009, *Station and Media Access Control Connectivity Discovery*
- ANSI/TIA-1057, *Link Layer Discovery Protocol for Media Endpoint Devices*
- IEEE Std 802.1Qaz-2011, *Media Access Control (MAC) Bridges and Virtual Bridged Local Area Networks-Amendment 18: Enhanced Transmission Selection for Bandwidth Sharing Between Traffic Classes*

15.2 LLDP設定作業リスト

作業リスト
LLDPの基本設定： • （必須設定項目） LLDPの有効化 • （オプション設定項目） LLDP動作モードの設定 • （オプション設定項目） 再初期化遅延時間の設定 • （オプション設定項目） LLDPポーリングの有効化 • （オプション設定項目） アドバタイズ可能なTLVの設定 • （オプション設定項目） 管理アドレスの設定とカプセル化フォーマットの設定 • （オプション設定項目） LLDPに関する他のパラメータの設定 • （オプション設定項目） LLDPフレームのカプセル化フォーマットの設定
（オプション設定項目） LLDP PVID不一致チェックの無効化
（オプション設定項目） CDP互換モードの設定
（オプション設定項目） LLDPトラップ、LLDP-MEDトラップの設定

15.3 LLDPの基本設定

15.3.1 LLDP の有効化

LLDP はポートで LLDP を有効にするには、ポートとグローバルの両方で有効にする必要があります。

以下に LLDP を有効化する設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． グローバルで LLDP を有効化する	**lldp global enable**	デフォルト：無効
3． Layer 2 Ethernet interface view あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	―
4． （オプション設定項目）LLDP を有効化する	**lldp enable**	デフォルト：有効

15.3.2 LLDP 動作モードの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． Layer 2 Ethernet interface view あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	―
3． 動作モードを設定する	● Layer 2 Ethernet interface view での設定：**lldp** [**agent nearest-customer**] **admin-status** { **disable** | **rx** | **tx** | **txrx** } ● aggregate interface viewでの設定：**lldp agent nearest-customer admin-status** { **disable** | **rx** | **tx** | **txrx** }	デフォルト：nearest bridgeエージェント：txrxモードです。nearest customer bridgeエージェント：disableです。Ethernet interface viewでエージェントタイプが指定されていない場合、nearest bridgeエージェントで動作モードを設定します。aggregate interface viewではnearest customer bridgeエージェントの動作モードのみを設定できます。

15.3.3 再初期化遅延時間の設定

ポートの LLDP 動作モードを変更した場合、ポートは遅延時間の経過後、プロトコル状態を初期化します。再初期化遅延時間を設定することで、ポートの LLDP 動作モードが頻繁に変更することを防ぐことができます。

以下に再初期化遅延時間の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． 再初期化遅延時間を設定する	**lldp timer reinit-delay** *delay*	デフォルト：2秒

15.3.4 LLDP ポーリングの有効化

LLDP ポーリングを有効にした装置はローカルの設定の変更を定期的に確認します。設定の変更を検出すると、装置は隣接装置へ変更を知らせるために LLDP フレームを送信します。

以下に LLDP ポーリングの有効化の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． Layer 2 Ethernet interface view あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	―
3． LLDP ポーリングの有効化を設定する	● Layer 2 Ethernet interface view での設定： **lldp** [**agent nearest-customer**] **check-change-interval** *interval* ● aggregate interface viewでの設定： **lldp agent nearest-customer check-change-interval** *interval*	デフォルト：無効

15.3.5 アドバタイズ可能な TLV の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． Layer 2 Ethernet interface view あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	―

操作	コマンド	補足
3． LLDPDU TLV を設定する（Layer 2 Ethernet interface view）	● **lldp tlv-enable** { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [*ip-address*] } | **dot1-tlv** { **all** | **port-vlan-id** | **link-aggregation** | **protocol-vlan-id** [*vlan-id*] | **vlan-name** [*vlan-id*] | **management-vid** [*mvlan-id*] } | **dot3-tlv** { **all** | **mac-physic** | **max-frame-size** | **power** } | **med-tlv** { **all** | **capability** | **inventory** | **network-policy** [*vlan-id*] | **power-over-ethernet** | **location-id** { **civic-address** *device-type country-code* { *ca-type ca-value* }&<1-10> | **elin-address** *tel-number* } } } ● **lldp agent nearest-customer tlv-enable** { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [*ip-address*] } | **dot1-tlv** { **all** | **port-vlan-id** | **link-aggregation** } }	デフォルト： ● Nearest bridgeエージェントはlocation identification TLV, port VLAN ID TLV、protocol VLAN ID TLV、VLAN name TLV、management VLAN ID TLVを除いてすべてのLLDP TLVタイプを送信します。 ● Nearest customer bridge エージェントはbasic TLV、IEEE 802.1 organizationally specific TLVを送信します。
4． LLDPDU TLV を設定する（aggregate interface view）	● **lldp agent nearest-customer tlv-enable** { **basic-tlv** { **all** | **management-address-tlv** [*ip-address*] | **port-description** | **system-capability** | **system-description** | **system-name** } | **dot1-tlv** { **all** | **port-vlan-id** } } ● **lldp tlv-enable dot1-tlv** { **protocol-vlan-id** [*vlan-id*] | **vlan-name** [*vlan-id*] | **management-vid** [*mvlan-id*] }	デフォルト： ● Nearest customer bridgeエージェントはbasic TLV、IEEE802.1組織指定TLV（port VLAN ID TLV、protocol VLAN ID TLV、VLAN name TLV、management VLAN ID TLVのみ）を送信します ● Nearest bridgeはアグリゲートインタフェースでサポートしていません。

15.3.6 管理アドレスの設定とカプセル化フォーマットの設定

LLDP は管理アドレス TLV の数値形式または string 形式でカプセル化します。

デフォルトでは、管理アドレス TLV は数値形式でカプセル化されています。隣接装置が管理アドレス TLV を string 形式でカプセル化している場合、管理アドレス TLV を string 形式でカプセル化することができます。これにより隣接装置と正常に通信することができます。

以下に管理アドレスのカプセル化フォーマットの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	—

操作	コマンド	補足
2． Layer 2 Ethernet interface view あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	―
3． LLDPDU 内の管理アドレスの設定、管理アドレスの送信を設定する	● Layer 2 Ethernet interface viewでの設定： **lldp** [**agent nearest-customer**] **tlv-enable basic-tlv management-address-tlv** [*ip-address*] ● aggregate interface viewでの設定： **lldp agent nearest-customer** | **tlv-enable basic-tlv management-address-tlv** [*ip-address*]	デフォルト：nearest bridgeエージェントと nearest customer bridgeエージェントはLLDPDU の管理アドレスを送信します。
4． 管理アドレス TLV のカプセル化フォーマットを string 形式として設定する	● Layer 2 Ethernet interface viewでの設定： **lldp** [**agent nearest-customer**] **management-address-format string** ● aggregate interface viewでの設定： **lldp agent nearest-customer management-address-format string**	デフォルト：数値形式

15.3.7 LLDP に関する他のパラメータの設定

LLDPDU でアドバタイズされる Time To Live TLV は、LLDPDU の装置情報の有効時間を決めて、隣接装置で保存されます。

TTL の乗数を設定することにより、隣接装置に送信する LLDPDU の TTL の設定を行うことができます。隣接装置についての情報の TTL は以下の式によって定義されます。

TTL の乗数 × LLDP フレームの 送信間隔 ＋ 1

TTL は最大 65535 秒ということに注意してください。それより大きい場合、65535 秒に丸められます。

以下に LLDPDU に関するパラメータの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． TTL の乗数を設定する	**lldp hold-multiplier** *value*	デフォルト： 4
3． LLDP フレームの送信間隔を設定する	**lldp timer tx-interval** *interval*	デフォルト： 30秒
4． 新しい隣接装置を検出したときの LLDP フレームの送信回数を設定する	**lldp fast-count** *count*	デフォルト： 4

15.3.8 LLDP フレームのカプセル化フォーマットの設定

LLDPDU は Ethernet II または SNAP フレームにカプセル化されます。

- **Ethernet II**－カプセル化フォーマットを Ethernet II に設定した場合、LLDP ポートは Ethernet II フレームで LLDP フレームを送信します。
- **SNAP**－カプセル化フォーマットを SNAP に設定した場合、LLDP ポートは SNAP フレームで LLDP フレームを送信します。

LLDP フレームを処理する初期バージョンの LLDP は、両端で同じカプセル化フォーマットが必要です。初期バージョンの LLDP で動作する装置に隣接したローカル装置は、初期バージョンの LLDP で動作する装置と同じカプセル化フォーマットで設定してください。

以下に SNAP に LLDP フレームのカプセル化フォーマットの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． Layer 2 Ethernet interface view あるいは Layer 2 aggregate interface view に移行する	**interface** *interface-type interface-number*	―
3． SNAP に LLDPDU のカプセル化フォーマットを設定する	● Layer 2 Ethernet interface view での設定： **lldp** [**agent nearest-customer**] **encapsulation snap** ● aggregate interface viewでの設定： **lldp agent nearest-customer encapsulation snap**	デフォルト： Ethernet II

15.4 LLDP PVID不一致チェックの無効化

デフォルトでは、システムは LLDP パケットを受信すると、パケットに含まれる PVID 値を受信側インタフェースに設定されている PVID と比較します。2 つの PVID が一致しない場合は、ログメッセージが印刷されてユーザに通知されます。

リンクで異なる PVID が必要な場合は、PVID 不一致チェックを無効にできます。

I. 設定手順

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． LLDP PVID 不一致チェックを無効にする	**lldp ignore-pvid-inconsistency**	デフォルト：有効

15.5 CDP互換モードの設定

CDP のみをサポートしている Cisco 製品と装置が直接接続されている場合、情報を交換するため、CDP 互換モードを有効に設定することができます。

CDP 互換モードを有効にした場合、装置は、直接接続された装置から CDP パケットを受信し、隣接装置に CDP パケットを送信します。装置が隣接の CDP 装置に送信するパケットは、以下の情報があります。

- device ID
- 隣接装置に接続されているポートの ID
- ポートの IP アドレス
- TTL

ポートの IP アドレスは、VLAN インタフェースがアップ状態のプライマリ IP アドレスです。VLAN インタフェースの VLAN ID はポートで許可されている VLAN のなかでもっとも低い ID にする必要があります。もし許可された VLAN インタフェースに、IP アドレスが割り当てられていないあるいはすべてのインタフェースがダウンである場合、ポートの IP アドレスはアドバタイズされません。

display lldp neighbor-information コマンドの出力の CDP neighbor-information-related フィールドは、装置が認識できる CDP 隣接装置情報を示します。**display lldp neighbor-information** コマンドについての詳細は、コマンドマニュアルのセクション 3 *アクセス*”*LLDP*”を参照してください。

Cisco の IP 電話と情報を交換する場合、CDP 互換モードを有効にする必要があります。

LLDP が有効な装置が CDP パケットを認識できない場合、装置で設定された Voice VLAN ID の Cisco の IP 電話の要求に応答しません。その結果、Cisco の IP 電話の要求は、装置に VLAN タグなしで音声トラフィックを送信します。装置はトラフィックの他のタイプから音声トラフィックを区別することができません。

CDP の互換モードを有効にすると、Cisco の IP 電話からの CDP パケットを受信して認識します。Voice VLAN の設定で TLV をアドバタイズする CDP パケットに応答します。CDP パケット用に Voice VLAN が設定されていない場合、CDP パケットは、ポートの Voice VLAN あるいは RADIUS サーバによって割り当てられた Voice VLAN をアドバタイズします。割り当てられた Voice VLAN は高い優先度をもちます。Voice VLAN の設定の TLV に従い、IP 電話は自動で Voice VLAN を設定します。その結果、設定された Voice VLAN で音声トラフィックが制限され、他のタイプのトラフィックと区別されます。

Voice VLAN の詳細は、オペレーションマニュアルのセクション 3 *アクセス*”*Voice VLAN*”を参照してください。

装置が、データポートに所属しているホストをもつ Cisco の IP 電話に接続されている場合、ホストは Cisco の IP 電話を通してネットワークにアクセスする必要があります。データポートがダウンした場合、装置がユーザをログアウトさせるため、IP 電話は装置に CDP パケットを送信します。

CDP 互換モードは以下のモードのどちらかで動作します。

- **TxRx**– CDP パケットを送受信できます。
- **Rx**– CDP パケットを送信できますが受信できません。
- **Disable**– CDP パケットを送受信できません。

I. 制限とガイドライン

指定したポートで CDP 互換モードの設定を行うために、以下の手順を設定します。

1) グローバルで CDP 互換モードを有効にします。
2) TxRx モードで動作するように CDP 互換モードの設定を行います。

CDP で許可される最大 TTL は 255 秒です。Cisco の IP phone と一緒に運用するために、LLDP フレーム送信間隔の値は、CDP 互換モードの TTL 値の 1/3 以内にする必要があります。

II. 設定要件

CDP 互換モードの設定を行う前に、以下の設定を行ってください。

- グローバルで LLDP を有効にします。
- CDP をサポートする装置に接続するポートで LLDP を有効にします。
- ポートの LLDP の動作モードを TxRx モードに設定します。
- アドバタイズされた Voice VLAN ID を設定します。

III. 設定手順

以下に CDP 互換モードの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. グローバルで CDP 互換モードを有効にする	**lldp compliance cdp**	デフォルト：無効
3. Layer 2 Ethernet interface view に移行する	**interface** *interface-type interface-number*	―
4. CDP 互換モードの動作モードを TxRx モードに設定する	**lldp compliance admin-status cdp txrx**	デフォルト：無効
5. アドバタイズされた Voice VLAN ID を設定する	**cdp voice-vlan vlan-id**	デフォルト：CDPフレームで伝送されるVoice VLAN IDが設定されていない。 詳細はコマンドマニュアルのセクション3 *アクセス” LLDP*”を参照してください。

15.6 LLDPトラップの設定

LLDP トラップは、ネットワーク管理システムに新しい隣接装置の検知やリンクの故障などのイベントを知らせるために使用されます。

トポロジが不安定なとき、LLDP トラップの送信間隔の設定を変更することで、指定した時間内での過度な LLDP トラップの送信を防ぐことができます。

以下に LLDP トラップの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Layer 2 Ethernet interface view あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	―

操作	コマンド	補足
3． LLDP トラップの送信を有効にする	● Layer 2 Ethernet interface view での設定：**lldp** [**agent nearest-customer**] **notification remote-change enable** ● aggregate interface viewでの設定：**lldp agent nearest-customer notification remote-change enable**	デフォルト：無効
4． system view に戻る	**quit**	―
5． （オプション設定項目）LLDP トラップの送信間隔を設定する	**lldp timer notification-interval** *interval*	デフォルト：30秒

15.7 LLDPの表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
ローカルLLDP情報を表示する	**display lldp local-information** [**global** | **interface** *interface-type interface-number*]
隣接装置から受信したLLDP TLVの情報を表示する	**display lldp neighbor-information** [[[**interface** *interface-type interface-number*] [**verbose**]] | **list** [**system-name** *system-name*]]
LLDPの統計情報を表示する	**display lldp statistics** [**global** | [**interface** *interface-type interface-number*]]
ポートのLLDPのステータスを表示する	**display lldp status** [**interface** *interface-type interface-number*]
現在送信されているLLDP TLVのタイプを表示する	**display lldp tlv-config** [**interface** *interface-type interface-number*]

15.8 LLDPの設定例

15.8.1 LLDP の基本的な設定例

I. ネットワーク要件

図 15-5で示すように、NMS と Switch A は、同じイーサネットネットワークに接続されています。MED 装置と Switch B は、Switch A の GigabitEthernet 1/0/1 と GigabitEthernet 1/0/2 に接続しています。

Switch A と Switch B で以下の処理を実行するためグローバルで LLDP を有効にします。

- Switch A と Switch B のリンクをモニタします。
- Switch A と NMS の MED 装置のリンクをモニタします。

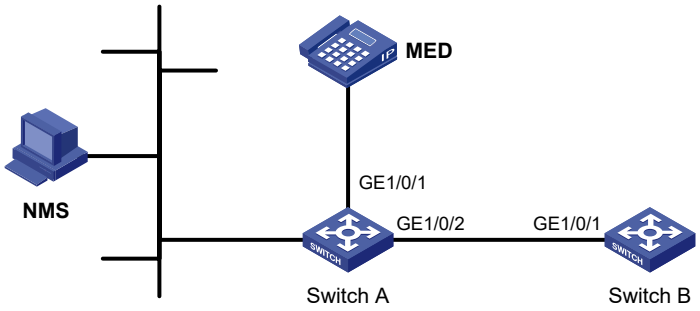


図 15-5 ネットワーク図

II. 設定手順

1)　Switch A を設定します。

グローバルで LLDP を有効にします。

```
<SwitchA> system-view
[SwitchA] lldp global enable
```

GigabitEthernet 1/0/1 で LLDP を有効にします。デフォルトではポートで LLDP が有効です。

```
[SwitchA] interface gigabitethernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] lldp enable
```

GigabitEthernet 1/0/1 で LLDP の動作モードを Rx に設定します。

```
[SwitchA-GigabitEthernet1/0/1] lldp admin-status rx
[SwitchA-GigabitEthernet1/0/1] quit
```

GigabitEthernet 1/0/2 で LLDP を有効にします。デフォルトではポートで LLDP が有効です。

```
[SwitchA] interface gigabitethernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] lldp enable
```

GigabitEthernet 1/0/2 で LLDP の動作モードを Rx に設定します。

```
[SwitchA-GigabitEthernet1/0/2] lldp admin-status rx
[SwitchA-GigabitEthernet1/0/2] quit
```

2)　Switch B を設定します。

グローバルで LLDP を有効にします。

```
<SwitchB> system-view
[SwitchB] lldp global enable
```

GigabitEthernet 1/0/1 で LLDP を有効にします。デフォルトではポートで LLDP が有効です。

```
[SwitchB] interface gigabitethernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] lldp enable
```

GigabitEthernet 1/0/1 で LLDP の動作モードを Tx に設定します。

```
[SwitchB-GigabitEthernet1/0/1] lldp admin-status tx
[SwitchB-GigabitEthernet1/0/1] quit
```

III. 設定の確認

以下のことを確認します。

- Switch A の GigabitEthernet 1/0/1 が MED 装置に接続しています。
- Switch A の GigabitEthernet 1/0/2 が非 MED 装置に接続しています。
- 両方のポートは Rx モードで動きます。つまり LLDP フレームの受信ができますが、LLDP フレームを送信できません。

```
[SwitchA] display lldp status
Global status of LLDP: Enable
Bridge mode of LLDP: customer-bridge
The current number of LLDP neighbors: 2
The current number of CDP neighbors: 0
LLDP neighbor information last changed time: 0 days, 0 hours, 4 minutes, 40 seconds
Transmit interval              : 30s
Fast transmit interval         : 1s
Transmit max credit            : 5
Hold multiplier                : 4
Reinit delay                   : 2s
Trap interval                  : 30s
Fast start times               : 4

LLDP status information of port 1 [GigabitEthernet1/0/1]:
LLDP agent nearest-bridge:
Port status of LLDP            : Enable
Admin status                   : Rx_Only
Trap flag                      : No
MED trap flag                  : No
Polling interval               : 0s
Number of LLDP neighbors       : 1
Number of MED neighbors        : 1
Number of CDP neighbors        : 0
Number of sent optional TLV    : 21
Number of received unknown TLV : 0

LLDP agent nearest-customer:
Port status of LLDP            : Enable
Admin status                   : Disable
Trap flag                      : No
MED trap flag                  : No
Polling interval               : 0s
Number of LLDP neighbors       : 0
Number of MED neighbors        : 0
Number of CDP neighbors        : 0
Number of sent optional TLV    : 16
Number of received unknown TLV : 0

LLDP status information of port 2 [GigabitEthernet1/0/2]:
LLDP agent nearest-bridge:
Port status of LLDP            : Enable
Admin status                   : Rx_Only
Trap flag                      : No
MED trap flag                  : No
Polling interval               : 0s
Number of LLDP neighbors       : 1
Number of MED neighbors        : 0
Number of CDP neighbors        : 0
Number of sent optional TLV    : 21
```

```
Number of received unknown TLV : 3

LLDP agent nearest-nontpmr:
Port status of LLDP             : Enable
Admin status                    : Disable
Trap flag                       : No
MED trap flag                   : No
Polling interval                : 0s
Number of LLDP neighbors        : 0
Number of MED neighbors         : 0
Number of CDP neighbors         : 0
Number of sent optional TLV     : 1
Number of received unknown TLV : 0

LLDP agent nearest-customer:
Port status of LLDP             : Enable
Admin status                    : Disable
Trap flag                       : No
MED trap flag                   : No
Polling interval                : 0s
Number of LLDP neighbors        : 0
Number of MED neighbors         : 0
Number of CDP neighbors         : 0
Number of sent optional TLV     : 16
Number of received unknown TLV : 0
```

Switch A と Switch B のリンクを切断します。

Switch A の GigabitEthernet 1/0/2 が隣接装置と接続していないことを確認します。

[SwitchA] display lldp status

```
Global status of LLDP: Enable
The current number of LLDP neighbors: 1
The current number of CDP neighbors: 0
LLDP neighbor information last changed time: 0 days, 0 hours, 5 minutes, 20 seconds
Transmit interval               : 30s
Fast transmit interval          : 1s
Transmit max credit             : 5
Hold multiplier                 : 4
Reinit delay                    : 2s
Trap interval                   : 30s
Fast start times                : 4

LLDP status information of port 1 [GigabitEthernet1/0/1]:
LLDP agent nearest-bridge:
Port status of LLDP             : Enable
Admin status                    : Rx_Only
Trap flag                       : No
MED trap flag                   : No
Polling interval                : 0s
Number of LLDP neighbors        : 1
Number of MED neighbors         : 1
Number of CDP neighbors         : 0
Number of sent optional TLV     : 0
Number of received unknown TLV : 5

LLDP agent nearest-nontpmr:
Port status of LLDP             : Enable
Admin status                    : Disable
Trap flag                       : No
MED trap flag                   : No
Polling interval                : 0s
Number of LLDP neighbors        : 0
Number of MED neighbors         : 0
Number of CDP neighbors         : 0
Number of sent optional TLV     : 1
Number of received unknown TLV : 0

LLDP status information of port 2 [GigabitEthernet1/0/2]:
```

```
LLDP agent nearest-bridge:
Port status of LLDP             : Enable
Admin status                    : Rx_Only
Trap flag                       : No
MED trap flag                   : No
Polling interval                : 0s
Number of LLDP neighbors        : 0
Number of MED neighbors         : 0
Number of CDP neighbors         : 0
Number of sent optional TLV     : 0
Number of received unknown TLV : 0

LLDP agent nearest-nontpmr:
Port status of LLDP             : Enable
Admin status                    : Disable
Trap flag                       : No
MED trap flag                   : No
Polling interval                : 0s
Number of LLDP neighbors        : 0
Number of MED neighbors         : 0
Number of CDP neighbors         : 0
Number of sent optional TLV     : 1
Number of received unknown TLV : 0

LLDP agent nearest-customer:
Port status of LLDP             : Enable
Admin status                    : Disable
Trap flag                       : No
MED trap flag                   : No
Polling interval                : 0s
Number of LLDP neighbors        : 0
Number of MED neighbors         : 0
Number of CDP neighbors         : 0
Number of sent optional TLV     : 16
Number of received unknown TLV : 0
```

15.8.2 CDP 互換モードの設定例

I. ネットワーク要件

図 15-6に示すように、Switch A の GigabitEthernet 1/0/1、GigabitEthernet 1/0/2 は VLAN タグがついた voice トラフィックを送信する Cisco の IP 電話に接続されています。

Switch A で Voice VLAN 2 を設定します。Cisco の IP 電話が Voice VLAN を自動で設定できるように Switch A で LLDP の CDP 互換モードを有効にします。Voice VLAN 機能は以下のアクションを実行します。

- Voice VLAN に voice トラフィックを制限します。
- 他のトラフィックタイプから voice トラフィックを隔離します。

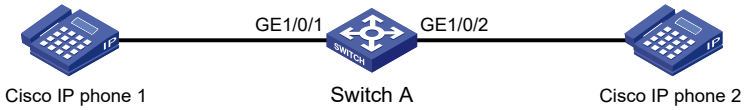


図 15-6 ネットワーク図

II. 設定手順

1)　Switch A で Voice VLAN を設定します。

VLAN 2 を作成します。

```
<SwitchA> system-view
[SwitchA] vlan 2
[SwitchA-vlan2] quit
```

GigabitEthernet 1/0/1 と GigabitEthernet 1/0/2 のリンクタイプを trunk に設定し、Voice VLAN を有効にします。

```
[SwitchA] interface gigabitethernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] port link-type trunk
[SwitchA-GigabitEthernet1/0/1] voice vlan 2 enable
[SwitchA-GigabitEthernet1/0/1] quit
[SwitchA] interface gigabitethernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] port link-type trunk
[SwitchA-GigabitEthernet1/0/2] voice vlan 2 enable
[SwitchA-GigabitEthernet1/0/2] quit
```

2)　Switch A で CDP 互換モードを設定します。

グローバルで LLDP を有効にします。グローバルで CDP 互換モードを有効にします。

```
[SwitchA] lldp global enable
[SwitchA] lldp compliance cdp
```

GigabitEthernet 1/0/1 で LLDP を有効にします。デフォルトではポートで LLDP が有効です。

```
[SwitchA] interface gigabitethernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] lldp enable
```

GigabitEthernet 1/0/1 で LLDP の動作モードを TxRx に設定します。

```
[SwitchA-GigabitEthernet1/0/1] lldp admin-status txrx
```

GigabitEthernet 1/0/1 で LLDP の TxRx の動作モードで動作させるため、CDP 互換モードを設定します。

```
[SwitchA-GigabitEthernet1/0/1] lldp compliance admin-status cdp txrx
[SwitchA-GigabitEthernet1/0/1] quit
```

GigabitEthernet 1/0/2 で LLDP を有効にします。デフォルトではポートで LLDP が有効です。

```
[SwitchA] interface gigabitethernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] lldp enable
```

GigabitEthernet 1/0/2 で LLDP の動作モードを TxRx に設定します。

```
[SwitchA-GigabitEthernet1/0/2] lldp admin-status txrx
```

GigabitEthernet 1/0/2 で LLDP の TxRx の動作モードで動作させるため、CDP 互換モードを設定します。

```
[SwitchA-GigabitEthernet1/0/2] lldp compliance admin-status cdp txrx
[SwitchA-GigabitEthernet1/0/2] quit
```

III. 設定の確認

Switch A が以下の作業が完了していることを確認します。

- GigabitEthernet 1/0/1 と GigabitEthernet 1/0/2 に接続されている IP 電話を検出します。
- IP 電話の情報を取得します。

```
[SwitchA] display lldp neighbor-information

CDP neighbor-information of port 1[GigabitEthernet1/0/1]:
 CDP neighbor index  : 1
 Chassis ID          : SEP00141CBCDBFE
 Port ID             : Port 1
 Software version    : P0030301MFG2
 Platform            : Cisco IP Phone 7960
 Duplex              : Full

CDP neighbor-information of port 2[GigabitEthernet1/0/2]:
 CDP neighbor index  : 2
 Chassis ID          : SEP00141CBCDBFF
 Port ID             : Port 1
 Software version    : P0030301MFG2
 Platform            : Cisco IP Phone 7960
 Duplex              : Full
```

目次

このセクションのページは**3-x-x** です。

16 章 L2PT 16-1
16.1 概要.....16-1
16.1.1 背景.....16-1
16.1.2 L2PT 動作メカニズム.....16-2
16.2 L2PT 設定作業リスト.....16-4
16.3 L2PT の有効化.....16-4
16.3.1 制限事項とガイドライン.....16-4
16.3.2 プロトコルでの L2PT の有効化.....16-4
16.3.3 トンネルパケットの宛先マルチキャスト MAC アドレスの設定.....16-5
16.4 L2PT の表示と維持.....16-5
16.5 L2PT の設定例.....16-6
16.5.1 STP での L2PT の設定.....16-6
16.5.2 LACP での L2PT の設定.....16-7

16章 L2PT

16.1 概要

L2PT（Layer 2 Protocol Tunneling）を使用すると、地理的に分散されているカスタマネットワークをサービスプロバイダネットワーク経由でレイヤ 2 プロトコルパケットを送信できます。

16.1.1 背景

特定ユーザ向けのレイヤ 2 ネットワークを構築するため、サービスプロバイダネットワークで専用線が使用されます。その結果、カスタマネットワークはサービスプロバイダネットワークの異なるサイドに存在します。

図 16-1に示すようにCustomer Aネットワークはサービスプロバイダによって接続されている network 1 と network 2 に分割されています。Customer A の 2 つネットワークでレイヤ 2 プロトコルの計算を行うため、レイヤ 2 プロトコルのパケットはサービスプロバイダネットワークを通過して転送される必要があります。

PE がレイヤ 2 プロトコルパケットを受信した場合、PE はカスタマネットワークから受信されたパケットなのかサービスプロバイダネットワークからのパケットなのか判断することができません。このプロセス処理を行うため、CPU にパケットを転送する必要があります。この場合、Customer A ネットワークのレイヤ 2 プロトコルの計算は、サービスプロバイダネットワークのレイヤ 2 プロトコルの計算と一緒に行われます。カスタマネットワークあるいはサービスプロバイダネットワークのどちらも、独立してレイヤ 2 プロトコルの計算を行うことができません。

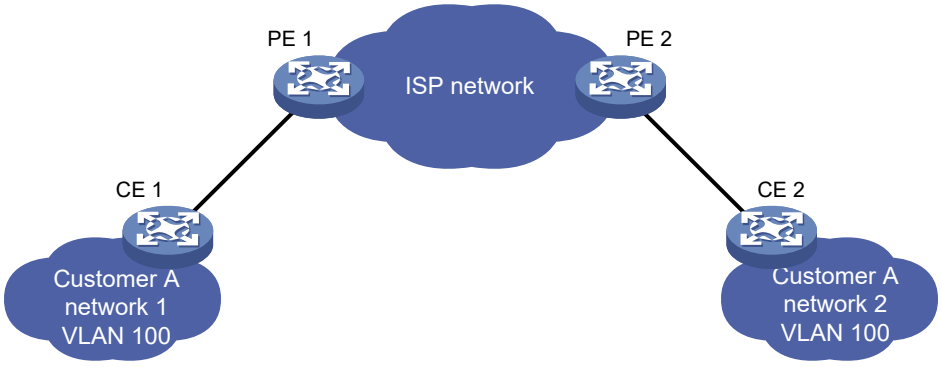


図 16-1 L2PT アプリケーションシナリオ

L2PT はこの問題を解決するために導入されました。L2PT は以下の機能を提供します。

- VLAN のカスタマネットワークからレイヤ 2 プロトコルパケットをマルチキャストします。分割されたカスタマネットワークは独立してレイヤ 2 プロトコルの計算を行うことができます。この計算はサービスプロバイダネットワークに対してトランスペアレントに行われます。
- 異なる VLAN を経由した異なるカスタマネットワークからのレイヤ 2 プロトコルパケットを隔離します。

装置は以下のプロトコルを行うため L2PT をサポートします。

- CDP
- DLDP
- EOAM
- GVRP
- LACP
- LLDP
- MVRP
- PAgP
- PVST
- STP（STP、RSTP、MSTP を含みます）
- UDLD
- VTP

16.1.2 L2PT 動作メカニズム

図 16-2に示すように L2PT は以下のように動作します。

- VLAN の PE1 のポートがカスタマネットワークからレイヤ 2 プロトコルパケットを受信したとき、以下の処理を行います。
  - 受信ポートを除く VLAN のすべてのカスタマ側のポートにパケットをマルチキャストします。
  - パケットの宛先マルチキャスト MAC アドレスを指定されたマルチキャスト MAC アドレスに変更し、VLAN のすべての ISP 側のポートにパケットをマルチキャストします。変更されたパケットはトンネルパケットと呼ばれます。
- VLAN の PE2 のポートがサービスプロバイダネットワークからトンネルパケットを受信したとき、以下の処理を行います。

- 受信ポートを除く VLAN のすべての ISP 側のポートにパケットをマルチキャストします。
- パケットの宛先マルチキャスト MAC アドレスをもとの MAC アドレスに変更し、VLAN のすべてのカスタマ側のポートにパケットをマルチキャストします。

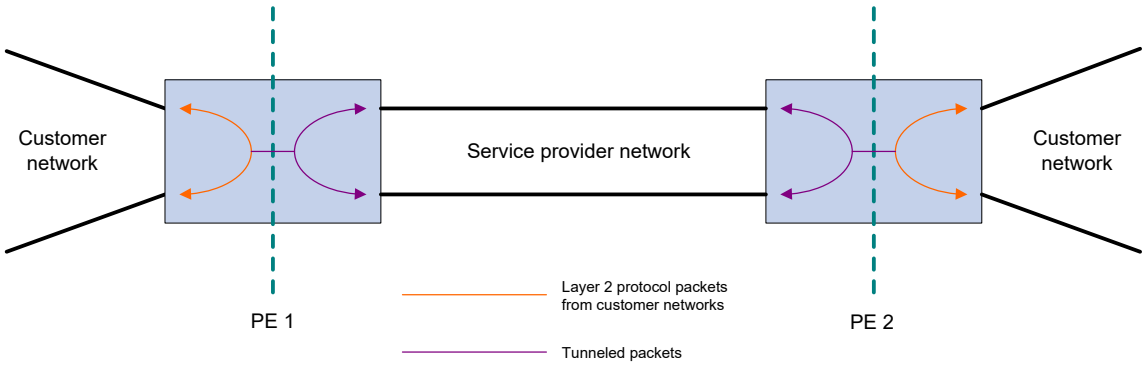


図 16-2 L2PT 動作メカニズム

たとえば、図 16-3に示すように PE1 はネットワーク 1 からネットワーク 2 への STP パケット（BPDU）を受信します。CE はカスタマネットワークの Edge 装置です。PE はサービスプロバイダネットワークの Edge 装置です。L2PT は以下のようにパケットを処理します。

1) PE1 は以下の処理を行います。

a) パケットの宛先MACアドレス0180-c200-0000を、BPDUの指定したマルチキャストMACアドレス（デフォルトは010f-e200-0003）に変更します。

b) パケットのVLANのすべてのISP側のポートにトンネルパケットを送信します。

2) トンネルパケットを受信すると、PE2 はパケットを復号化し、CE2 に BPDU を送信します。

L2PT を通して ISP ネットワークと Customer A ネットワークは独立したスパニングツリーの計算を行うことができます。

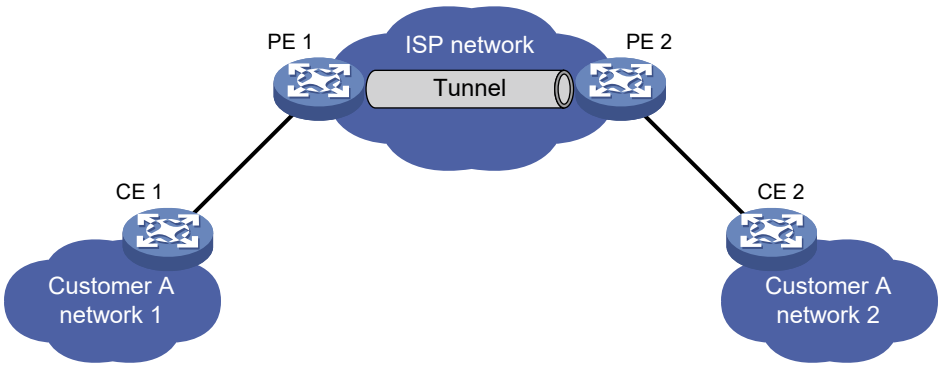


図 16-3 L2PT ネットワーク図

16.2 L2PT設定作業リスト

作業リスト
（必須設定項目）プロトコルでのL2PTの有効化
（オプション設定項目）トンネルパケットの宛先マルチキャストMACアドレスの設定

16.3 L2PTの有効化

16.3.1 制限事項とガイドライン

- ポートのレイヤ2 プロトコルでL2PT を有効にする前に以下の処理を行ってください。
  - 接続された CE のプロトコルを有効にし、ポートでプロトコルを無効にしてください。
  - 以下の条件において、CE 上のアグリゲーションインタフェースと接続している PE ポートでは STP などのプロトコルを無効にしてください。
    - プロトコルは CE 上のアグリゲーションインタフェースで動作しています。
    - CE 上のアグリゲーションインタフェースが PE 上の L2PT 対応のインタフェースに接続しています。
  - カスタマネットワークに接続された PE ポートで L2PT を有効にしてください。サービスプロバイダネットワークに接続されているポートで L2PT を有効にした場合、L2PT はポートがカスタマネットワークに接続されていると認識します。
  - トンネルパケットがサービスプロバイダネットワークを通して正常に転送できるようにするため、レイヤ 2 プロトコルパケットの VLAN タグが変更あるいは削除されていないことを確認してください。
- L2PT は nearest bridge エージェントのみからの LLDP パケットをサポートします。
- アグリゲーショングループのメンバポートで L2PT の設定を入力することができますが、設定は適用されません。

16.3.2 プロトコルでの L2PT の有効化

I. 制限事項とガイドライン

LACP と EOAM はポイントツーポイントの通信を必要としていますが、L2PT を LACP または EOAM のインタフェース上で使用する場合は、L2PT はカスタマ側のポートから LACP または EOAM をマルチキャストします。

2 つの CE 間の通信はポイントツーポイントではないため、LACP または EOAM パケットにポイントツーポイントの通信を保証するには別の機能を使用する必要があります。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	ー

操作	コマンド	補足
2． interface view に移行する	● Ethernet interface viewに移行する： **interface** *interface-type interface-number* ● aggregate interface viewに移行する： **interface bridge-aggregation** *interface-type interface-number*	―
3． プロトコルの L2PT を有効にする	● Ethernet interface view： **l2protocol** { **cdp** | **dldp** | **eoam** | **gvrp** | **lacp** | **lldp** | **mvrp** | **pagp** | **pvst** | **stp** | **udld** | **vtp** } **tunnel dot1q** ● aggregate interface view： **l2protocol** { **gvrp** | **mvrp** | **pvst** | **stp** | **vtp** | **cdp** | **lacp** | **lldp** | **pagp** | **udld** } **tunnel dot1q**	デフォルト：無効

16.3.3 トンネルパケットの宛先マルチキャスト MAC アドレスの設定

I. 宛先マルチキャスト MAC アドレスについて

使用可能なマルチキャスト MAC アドレスは 010f-e200-0003、0100-0ccd-cdd0、0100-0ccd-cdd1、0100-0ccd-cdd2 です。

II. 制限事項とガイドライン

- トンネルパケットを認識するため、同一カスタマネットワークに接続されている PE では同一の宛先マルチキャスト MAC アドレスを設定してください。
- 異なるカスタマネットワークに接続されている PE では異なる宛先マルチキャスト MAC アドレスを設定します。そのため L2PT は、カスタマネットワークのパケットから、別のカスタマネットワークにパケットを送信することを防止することができます。

III. 設定手順

以下にトンネルパケットの宛先マルチキャスト MAC アドレスの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． トンネルパケットの宛先マルチキャスト MAC アドレスを設定する	**l2protocol tunnel-dmac** *mac-address*	デフォルト：010f-e200-0003

16.4 L2PTの表示と維持

すべての view で **display** コマンドを実行し、user view で **reset** コマンドを実行できます。

操作	コマンド
L2PTの統計情報を表示する	**display l2protocol statistics** [**interface** *interface-type interface-number*]
L2PTの統計情報を削除する	**reset l2protocol statistics** [**interface** *interface-type interface-number*]

16.5 L2PTの設定例

16.5.1 STP での L2PT の設定

I. ネットワーク要件

図 16-4に示すように、CE1 の MAC アドレスは f474-8802-5800、CE2 の MAC アドレスは f474-8802-5802 です。Customer A ネットワークでは MSTP が使用されています。

PE で以下の処理を行います。

- CE に接続するポートをアクセスポートとして設定します。サービスプロバイダネットワークのポートをトランクポートとして設定します。サービスプロバイダネットワークのポートはすべての VLAN からのパケットを許可します。
- サービスプロバイダネットワークを通して、Customer A ネットワークで独立してスパニングツリーの計算を行うため、STP の L2PT を有効にします。
- トンネルパケットの宛先マルチキャスト MAC アドレスを 0100-0ccd-cdd0 に設定します。

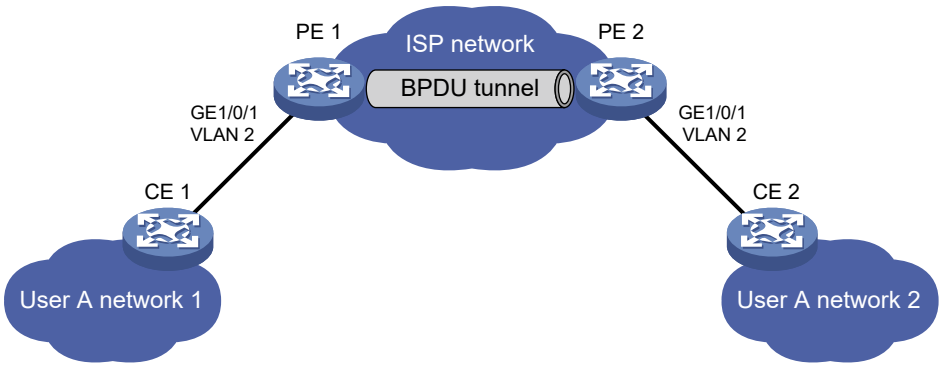


図 16-4 ネットワーク図

II. 設定手順

1)　PE1 を設定します。

トンネルパケットの宛先マルチキャストMACアドレスを0100-0ccd-cdd0に設定します。

```
<PE1> system-view
[PE1] l2protocol tunnel-dmac 0100-0ccd-cdd0
```

VLAN 2 を作成します。

```
[PE1] vlan 2
[PE1-vlan2] quit
```

GigabitEthernet 1/0/1 をアクセスポートとして設定し、VLAN 2 に割り当てます。

```
[PE1] interface gigabitethernet 1/0/1
[PE1-GigabitEthernet1/0/1] port access vlan 2
```

GigabitEthernet 1/0/1 で STP を無効にし、STP の L2PT を有効にします。

```
[PE1-GigabitEthernet1/0/1] undo stp enable
[PE1-GigabitEthernet1/0/1] l2protocol stp tunnel dot1q
[PE1-GigabitEthernet1/0/1] quit
```

サービスプロバイダに接続されている GigabitEthernet 1/0/2 をトランクポートとして設定し、すべての VLAN に割り当てます。

```
[PE1] interface gigabitethernet 1/0/2
[PE1-GigabitEthernet1/0/2] port link-type trunk
[PE1-GigabitEthernet1/0/2] port trunk permit vlan all
[PE1-GigabitEthernet1/0/2] quit
```

2) PE1 を PE1 の設定と同様に設定します。（詳細は省略します。）

III. 設定の確認

Customer A ネットワークのルートブリッジが CE1 であることを確認します。

```
<CE2> display stp root
 MST ID   Root Bridge ID        ExtPathCost IntPathCost Root Port
 0        32768. f474-8802-5800  0           0
```

サービスプロバイダネットワークのルートブリッジが CE1 でないことを確認します。

```
[PE1] display stp root
 MST ID   Root Bridge ID        ExtPathCost IntPathCost Root Port
 0        32768.0cda-41c5-ba50  0           0
```

16.5.2 LACP での L2PT の設定

I. ネットワーク要件

図 16-5に示すように、CE1 の MAC アドレスは 0001-0000-0000、CE2 の MAC アドレスは 0004-0000-0000 です。

以下の処理を行います。

- CE1、CE2 でリンクアグリゲーションを設定します。
- CE1 で GigabitEthernet 1/0/1 と GigabitEthernet 1/0/2 をアグリゲートインタフェースに設定し、CE2 で GigabitEthernet 1/0/1 と GigabitEthernet 1/0/2 をアグリゲートインタフェースに設定します。

- サービスプロバイダネットワークを通して、リンクアグリゲーションを行うため、CE1 と CE2 で LACP の L2PT を有効にします。

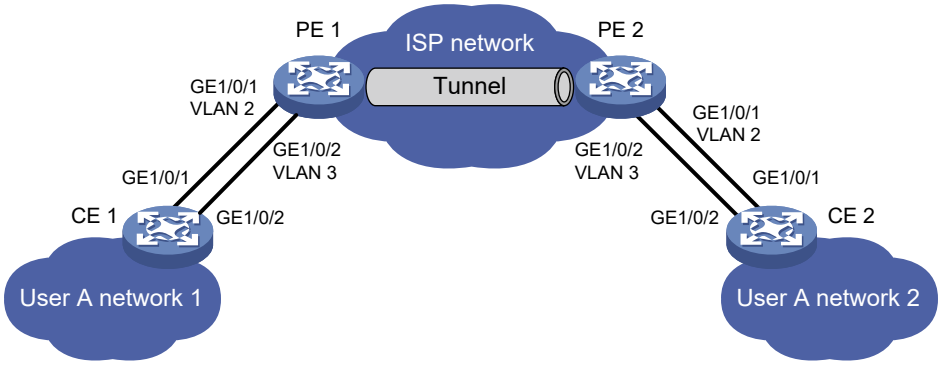


図 16-5 ネットワーク図

II. 要件の分析

ネットワーク要件に適合するため、以下の処理を行います。

- リンクアグリゲーションを正常に動作させるために、アグリゲーショングループの CE1 と CE2 間のポイントーポイントの転送を行うため PE で VLAN を設定してください。
  - GigabitEthernet 1/0/1 の PVID を VLAN 2 に設定してください。GigabitEthernet 1/0/2 の PVID を VLAN 3 に設定してください。
  - PE1 の設定と同様に PE2 を設定してください。
  - CE に接続されるポートをトランクポートに設定してください。
- カスタマネットワークの VLAN タグを保持するため PE1 と PE2 の両方の GigabitEthernet 1/0/1 と GigabitEthernet 1/0/2 で QinQ を有効にしてください。
- すべての VLAN からパケットを転送するため、サービスプロバイダネットワークのすべてのポートをトランクポートに設定してください。

III. 設定手順

1) CE1 を設定します。

ダイナミックアグリゲーションモードで動作させるため、アグリゲーショングループ Bridge-Aggregation 1 を設定します。

```
<CE1> system-view
[CE1] interface bridge-aggregation 1
[CE1-Bridge-Aggregation1] port link-type access
[CE1-Bridge-Aggregation1] link-aggregation mode dynamic
[CE1-Bridge-Aggregation1] quit
```

GigabitEthernet 1/0/1、GigabitEthernet 1/0/2 を Bridge-Aggregation 1 に割り当てます。

```
[CE1] interface gigabitethernet 1/0/1
```

```
[CE1-GigabitEthernet1/0/1] port link-aggregation group 1
[CE1-GigabitEthernet1/0/1] quit
[CE1] interface gigabitethernet 1/0/2
[CE1-GigabitEthernet1/0/2] port link-aggregation group 1
[CE1-GigabitEthernet1/0/2] quit
```

2) CE1 の設定と同様に CE2 を設定してください。（詳細は省略します。）
3) PE1 を設定します。

VLAN 2、VLAN 3 を作成します。

```
<PE1> system-view
[PE1] vlan 2
[PE1-vlan2] quit
[PE1] vlan 3
[PE1-vlan3] quit
```

GigabitEthernet 1/0/1 をトランクポートとして設定します。VLAN 2 に割り当て、PVID を VLAN 2 に設定します。

```
[PE1] interface gigabitethernet 1/0/1
[PE1-GigabitEthernet1/0/1] port link-type trunk
[PE1-GigabitEthernet1/0/1] port trunk permit vlan 2
[PE1-GigabitEthernet1/0/1] port trunk pvid vlan 2
```

GigabitEthernet 1/0/1 で QinQ を有効にします。

```
[PE1-GigabitEthernet1/0/1] qinq enable
```

GigabitEthernet 1/0/1 で LACP の L2PT を有効にします。

```
[PE1-GigabitEthernet1/0/1] l2protocol lacp tunnel dot1q
[PE1-GigabitEthernet1/0/1] quit
```

GigabitEthernet 1/0/2 をトランクポートとして設定します。VLAN 3 に割り当て、PVID を VLAN 3 に設定します。

```
[PE1] interface gigabitethernet 1/0/2
[PE1-GigabitEthernet1/0/2] port link-type trunk
[PE1-GigabitEthernet1/0/2] port trunk permit vlan 3
[PE1-GigabitEthernet1/0/2] port trunk pvid vlan 3
```

GigabitEthernet 1/0/2 で QinQ を有効にします。

```
[PE1-GigabitEthernet1/0/2] qinq enable
```

GigabitEthernet 1/0/2 で LACP の L2PT を有効にします。

```
[PE1-GigabitEthernet1/0/2] l2protocol lacp tunnel dot1q
[PE1-GigabitEthernet1/0/2] quit
```

4) PE1 の設定と同様に PE2 を設定してください。（詳細は省略します。）

IV. 設定の確認

CE1 と CE2 で正常にリンクアグリゲーションが設定されていることを確認します。

[CE1] display link-aggregation member-port

```
Flags: A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
       D -- Synchronization, E -- Collecting, F -- Distributing,
       G -- Defaulted, H -- Expired

GigabitEthernet1/0/1:
Aggregate Interface: Bridge-Aggregation1
Local:
    Port Number: 3
    Port Priority: 32768
    Oper-Key: 1
    Flag: {ACDEF}
Remote:
    System ID: 0x8000, 0004-0000-0000
    Port Number: 3
    Port Priority: 32768
    Oper-Key: 1
    Flag: {ACDEF}
Received LACP Packets: 23 packet(s)
Illegal: 0 packet(s)
Sent LACP Packets: 26 packet(s)

GigabitEthernet1/0/2:
Aggregate Interface: Bridge-Aggregation1
Local:
    Port Number: 4
    Port Priority: 32768
    Oper-Key: 1
    Flag: {ACDEF}
Remote:
    System ID: 0x8000, 0004-0000-0000
    Port Number: 4
    Port Priority: 32768
    Oper-Key: 1
    Flag: {ACDEF}
Received LACP Packets: 10 packet(s)
Illegal: 0 packet(s)
Sent LACP Packets: 13 packet(s)
```

[CE2] display link-aggregation member-port

```
Flags: A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
       D -- Synchronization, E -- Collecting, F -- Distributing,
       G -- Defaulted, H -- Expired

GigabitEthernet1/0/1:
Aggregate Interface: Bridge-Aggregation1
Local:
    Port Number: 3
    Port Priority: 32768
    Oper-Key: 1
    Flag: {ACDEF}
Remote:
    System ID: 0x8000, 0001-0000-0000
    Port Number: 3
    Port Priority: 32768
    Oper-Key: 1
    Flag: {ACDEF}
Received LACP Packets: 23 packet(s)
Illegal: 0 packet(s)
Sent LACP Packets: 26 packet(s)
```

```
GigabitEthernet1/0/2:
Aggregate Interface: Bridge-Aggregation1
Local:
    Port Number: 4
    Port Priority: 32768
    Oper-Key: 1
    Flag: {ACDEF}
Remote:
    System ID: 0x8000, 0001-0000-0000
    Port Number: 4
    Port Priority: 32768
    Oper-Key: 1
    Flag: {ACDEF}
Received LACP Packets: 10 packet(s)
Illegal: 0 packet(s)
Sent LACP Packets: 13 packet(s)
```

QX-S5100G シリーズ Ethernet スイッチ

オペレーションマニュアル

4. IP サービス

本マニュアルは以下に示す章で構成されています。

01-ARP

02-Gratuitous ARP

03-Proxy ARP

04-ARP スヌーピング

05-IP アドレス

06-DHCP の概要

07-DHCP サーバ

08-DHCP リレーエージェント

09-DHCP クライアント

10-DHCP スヌーピング

11-BOOTP クライアント

12-DNS

13-IP フォワーディングの基本

14-IP パフォーマンスの最適化

15-UDP ヘルパー

16-IPv6 の基本

17-DHCPv6 の概要

18-DHCPv6 リレーエージェント

19-DHCPv6 クライアント

20-HTTP リダイレクト

目次

このセクションのページは**4-x-x** です。

1章 ARP..... 1-1
1.1 概要..... 1-1
1.1.1 ARPメッセージフォーマット..... 1-1
1.1.2 ARP動作メカニズム..... 1-2
1.1.3 ARPテーブル..... 1-3
1.2 スタティックARPエントリの設定..... 1-4
1.2.1 マルチポートARPエントリの設定..... 1-4
1.3 ダイナミックARPエントリの設定..... 1-5
1.3.1 装置で学習できるダイナミックARPエントリの最大数の設定..... 1-5
1.3.2 インタフェースで学習できるARPエントリの最大数の設定..... 1-6
1.3.3 ダイナミックARPエントリのエージングタイマの設定..... 1-6
1.3.4 ARPエントリチェックの有効化..... 1-7
1.4 ARPロギング機能の有効化..... 1-7
1.5 インタフェースでのARPエントリとMACアドレスエントリの整合性のチェックの有効化1-7
1.6 ARPの表示と維持..... 1-8
1.7 ARPの設定例..... 1-8
1.7.1 ロングスタティックARPの設定例..... 1-8
1.7.2 ショートスタティックARPの設定例..... 1-10
1.7.3 マルチポートARPエントリの設定例..... 1-11

1章 ARP

1.1 概要

ARP（Address Resolution Protocol）は、IP アドレスを基に MAC アドレス（物理アドレス）を調べる仕組みのことです。

1.1.1 ARP メッセージフォーマット

ARP は ARP 要求/応答メッセージの 2 つのメッセージタイプがあります。図 1-1に ARP 要求/応答メッセージのフォーマットを示します。図の数字はフィールド長を示します。

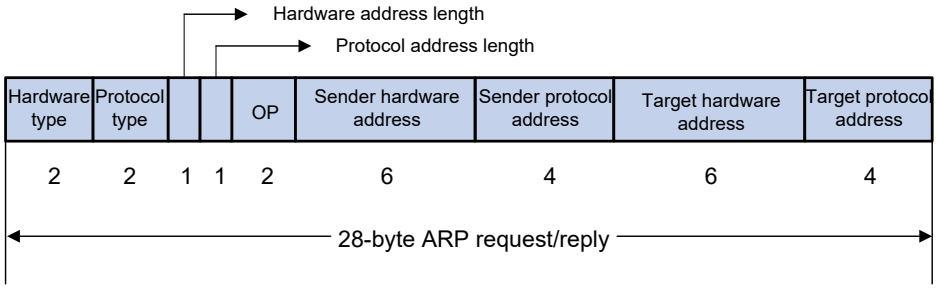


図 1-1 ARP メッセージフォーマット

- **Hardware type**– このフィールドはハードウェアアドレスタイプを指定します。1 は Ethernet を表します。
- **Protocol type**– このフィールドはマッピングされるプロトコルアドレスのタイプを指定します。16 進数で 0x0800 は IP を表します。
- **Hardware address length**、**protocol address length**– ハードウェアアドレスの長さと、プロトコルアドレスの長さをバイト単位で指定します。イーサネットアドレスに関して、Hardware address length の値は 6 です。IPv4 アドレスに関しては、protocol address length の値は 4 です。
- **OP**– このフィールド（Operation code）は ARP メッセージのタイプを指定します。1 は ARP 要求、2 は ARP 応答を表します。
- **Sender hardware address**– このフィールドはメッセージを送信する装置のハードウェアアドレスを指定します。
- **Sender protocol address**– このフィールドはメッセージを送信する装置のプロトコルアドレスを指定します。
- **Target hardware address**– このフィールドはメッセージが送られる装置のハードウェアアドレスを指定します。
- **Target protocol address**– このフィールドはメッセージが送られる装置のプロトコルアドレスを指定します。

1.1.2 ARP 動作メカニズム

図 1-2に示すように、Host A と Host B は同一サブネットにあります。Host A は Host B に以下のようにパケットを送信します。

1) Host A は Host B の ARP エントリが ARP テーブルにあるか検索します。もし ARP エントリがある場合、Host A は、ARP エントリの MAC アドレスを使用します。そしてデータリンクレイヤのフレームに IP パケットをカプセル化し、Host B にフレームを送信します。
2) もし Host B の ARP エントリがない場合、Host A はパケットをバッファし、ARP 要求をブロードキャストします。ARP リクエストのデータの内容は以下の情報が含まれます。
   - **送信元 IP アドレスと送信元 MAC アドレス** ― Host A の IP アドレスと MAC アドレス
   - **宛先 IP アドレス** ― Host B の IP アドレス
   - **宛先 MAC アドレス** ― 値がすべて 0 の MAC アドレス

   サブネットのすべてのホストはブロードキャストリクエストを受信することができますが、パケットを処理するホスト（Host B）のみが ARP 要求を処理します。
3) Host B は自身の IP アドレスと ARP リクエストの宛先 IP アドレスを比較し、同一の場合、以下の処理を行います。

   a) 送信元IPアドレスと送信元MACアドレスをARPテーブルに追加します。

   b) ARP応答に自身のMACアドレスを挿入します。

   c) Host AにARP応答をユニキャストで送信します。
4) ARP 応答を受信した後、Host A は以下の処理を行います。

   a) Host BのMACアドレスをARPテーブルに追加します。

   b) 以降、送信するパケットにHost BのMACアドレスを追加し、Host Bにパケットを送信します。

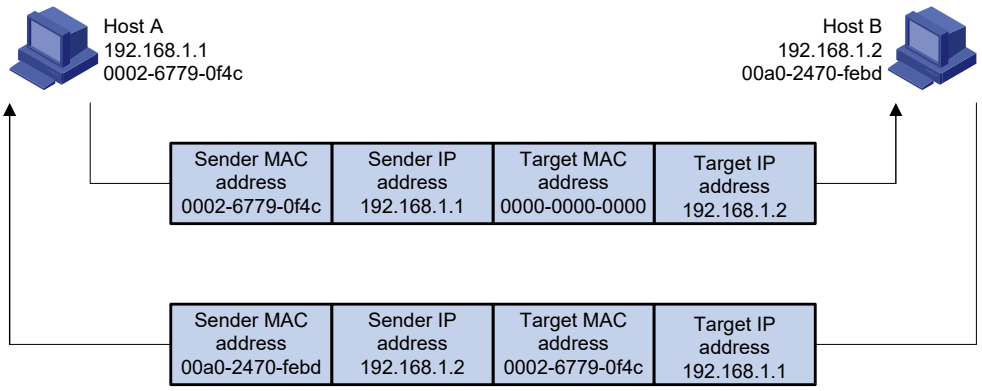


図 1-2 ARP アドレス解決プロセス

Host A と Host B が異なるサブネットにある場合、Host A は Host B に以下のようにパケットを送信します。

1) Host A は、宛先 IP アドレスをゲートウェイの IP アドレスにした ARP 要求をブロードキャストします。
2) ゲートウェイは、ARP 応答を行い、自身の MAC アドレスを Host A に送信します。

3) Host A はゲートウェイの MAC アドレスをパケットに挿入し、ゲートウェイにパケットを送信します。
4) ゲートウェイが Host B の ARP エントリがある場合、Host B にパケットを直接転送します。もし Host B の ARP エントリがない場合、宛先 IP アドレスを Host B の IP アドレスとして ARP 要求をブロードキャストします。
5) ゲートウェイが Host B の MAC アドレスを取得した後、Host B にパケットを送信します。

1.1.3 ARP テーブル

ARP テーブルはダイナミック、スタティックの ARP エントリがあります。

I. ダイナミック ARP エントリ

ダイナミックエントリは ARP によって自動的に作成、アップデートされます。エージングタイマが終了したとき、あるいは出力インタフェースがダウンしたとき、ダイナミックエントリは削除されます。ダイナミック ARP エントリはスタティック ARP エントリによって上書きされます。

II. スタティック ARP エントリ

スタティック ARP エントリは手動で設定され、維持します。スタティック ARP エントリはエージングせず、ダイナミック ARP エントリによって上書きされることもありません。

スタティック ARP エントリを使用することにより、通信のセキュリティを強化できます。スタティック ARP エントリで IP アドレスと MAC アドレスをマッピングすることにより、スタティック ARP エントリで指定された IP アドレスと MAC アドレスのマッピングが、攻撃パケットで変更されることはありません。

装置は以下のタイプのスタティック ARP エントリをサポートします。

- **ロングスタティック ARP エントリ**：IP アドレス、MAC アドレス、VLAN インタフェース、出力インタフェースから構成されます。パケットを転送するのに直接使用されます。
- **ショートスタティック ARP エントリ**：IP アドレス、MAC アドレスのみで構成されます。

  装置はターゲット IP アドレスがショートエントリの IP アドレスである ARP 要求を送信します。受信した ARP 応答の送信元 IP アドレスと MAC アドレスがショートスタティック ARP エントリと一致した場合、装置は以下の処理を行います。

  - ARP エントリを受信したインタフェースはショートスタティック ARP エントリを追加します。
  - IP パケットを転送するため、解決したショートスタティック ARP エントリを使用します。

固定の IP アドレス-MAC アドレスマッピングを使用してホストと通信する場合、装置は、ショートスタティック ARP エントリを設定します。固定の IP アドレス-MAC アドレスマッピングを使用して、指定した VLAN の指定したインタフェースを通してホストと通信する場合、装置はロングスタティック ARP エントリを設定します。

1.2 スタティックARPエントリの設定

スタティック ARP エントリは、装置が正常に動作するときに、適用されます。

解決済みのショートスタティック ARP エントリは、未解決となります。たとえば、解決した出力インタフェースがダウンあるいは対応する VLAN、VLAN インタフェースが削除したとき、解決済みのショートスタティック ARP エントリは、未解決となります。

未解決のロングスタティック ARP エントリはパケットの転送に使用することができません。ロングスタティック ARP エントリは以下の状態にある場合、未解決となります。

- 対応する VLAN インタフェースあるいは出力インタフェースがダウンしています。
- エントリの IP アドレスがローカル IP アドレスと衝突しています。
- インタフェースが同一サブネットの ARP エントリの IP アドレスを持っていません。

VLAN あるいは VLAN インタフェースが削除された場合、VLAN のロングスタティック ARP エントリは削除されます。

以下にスタティック ARP エントリの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． スタティック ARP エントリを設定する	● ロングスタティックARPエントリを設定する： **arp static** *ip-address mac-address* [*vlan-id interface-type interface-number*] [**vpn-instance** *vpn-instance-name*] ● ショートスタティックARPエントリを設定する： **arp static** *ip-address mac-address* [**vpn-instance** *vpn-instance-name*]	デフォルト：設定なし

1.2.1 マルチポート ARP エントリの設定

I. マルチポート ARP エントリ

マルチポート ARP エントリは IP アドレス、MAC アドレス、VLAN ID が含まれます。VLAN と出力インタフェースはマルチポートユニキャスト MAC アドレスエントリあるいはマルチキャスト MAC アドレスエントリによって指定されます。

マルチポート ARP エントリはダイナミック ARP エントリ、ショートスタティック ARP エントリ、あるいはロングスタティック ARP エントリに上書きすることができます。逆にショートスタティック ARP エントリ、あるいはロングスタティック ARP エントリはマルチポート ARP エントリに上書きすることができます。

II. 制限とガイドライン

パケット転送でマルチポート ARP エントリを適用させるためには、以下の対応を行う必要があります。

- マルチポートユニキャスト MAC アドレスエントリあるいはマルチキャスト MAC アドレスエントリが存在します。
- マルチポート ARP エントリの IP アドレスと VLAN インタフェースの IP アドレスは同一サブネット上に存在する必要があります。

III. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. マルチポートユニキャスト MAC アドレスエントリあるいはマルチキャスト MAC アドレスエントリを設定する	• マルチポートユニキャスト MACアドレスエントリを設定する: **mac-address multiport** *mac-address* **interface** *interface-list* **vlan** *vlan-id* • マルチキャストMACアドレスエントリを設定する: **mac-address multicast** *mac-address* **interface** *interface-list* **vlan** *vlan-id*	**mac-address**コマンドの詳細は、コマンドマニュアルのセクション3 *アクセス"MAC アドレステーブル"*を参照してください。 **mac-address multicast**コマンドの詳細は、コマンドマニュアルのセクション6 *マルチキャスト" IGMPスヌーピング"*を参照してください。
3. マルチポート ARP エントリを設定する	**arp multiport** *ip-address mac-address vlan-id* [**vpn-instance** *vpn-instance-name*]	マルチポートARPエントリは同一のMACアドレス、同一のVLAN IDにする必要があります。

1.3 ダイナミックARPエントリの設定

1.3.1 装置で学習できるダイナミック ARP エントリの最大数の設定

I. 装置で学習できるダイナミック ARP エントリの最大数

装置はダイナミックに ARP エントリを学習できます。多すぎる ARP エントリを保持しないように、装置が学習できるダイナミック ARP エントリの最大数を設定することができます。設定した最大数に到達すると、装置は ARP エントリの学習を停止します。

既存のダイナミック ARP エントリ数が設定した値よりも少ない場合、装置はエージアウトしない限り、既存のダイナミックエントリを削除しません。**reset arp dynamic** コマンドでダイナミック ARP エントリを削除することができます。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	ー

操作	コマンド	補足
2． ダイナミック ARP エントリの最大数を設定する	**arp max-learning-number** *max-number* **slot** *slot-number*	デフォルト：最大1024のダイナミックARPエントリを学習できます。 0～1024の範囲で設定してください。 0を設定した場合、ダイナミックARPエントリの学習を行いません。 1025以上の設定をした場合、安定動作ができない可能性があります。

1.3.2 インタフェースで学習できる ARP エントリの最大数の設定

インタフェースは動的に ARP エントリを学習します。多すぎる ARP エントリを保持しないように、インタフェースが学習できるダイナミック ARP エントリの最大数を設定することができます。設定した最大数に到達すると、インタフェースは ARP エントリの学習を停止します。

ダイナミック ARP エントリの最大数をレイヤ 2 インタフェースと VLAN インタフェースの両方で設定することができます。レイヤ 2 インタフェースはダイナミック ARP エントリが最大値に到達しないときのみ ARP エントリを学習します。

以下にインタフェースで学習できるダイナミック ARP エントリの最大数の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． interface view に移行する	**interface** *interface-type interface-number*	―
3． ダイナミック ARP エントリの最大数を設定する	**arp max-learning-num** *number*	デフォルト：1024 *number* 引数に0を設定した場合、ダイナミックARPエントリの学習を行いません。

1.3.3 ダイナミック ARP エントリのエージングタイマの設定

ARP テーブル上の各ダイナミック ARP エントリは有効期限があります。有効期限はエージングタイマと呼ばれ、有効期限内にダイナミック ARP エントリが使用される度に、エージングタイマはアップデートされます。有効期限切れになる前に更新されなかったダイナミック ARP エントリは、ARP テーブルから削除されます。

以下にダイナミック ARP エントリのエージングタイマの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． ダイナミック ARP エントリのエージングタイムを設定する	**arp timer aging** *aging-time*	デフォルト：20分

1.3.4 ARP エントリチェックの有効化

ダイナミック ARP エントリチェック機能は、装置でマルチキャスト MAC アドレスを含むダイナミック ARP エントリのサポートを無効にします。装置は送信元がマルチキャスト MAC アドレスであるダイナミック ARP エントリを学習できません。マルチキャスト MAC アドレスを含むスタティック ARP エントリを手動で学習させることもできません。

ARP エントリチェックを無効にした場合、装置はマルチキャスト MAC アドレスの ARP エントリを学習することができます。手動でマルチキャスト MAC アドレスを含むスタティック ARP エントリを追加することができます。

以下に ARP エントリチェック機能の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． ARP エントリチェック機能を有効にする	**arp check enable**	デフォルト：有効

1.4 ARPロギング機能の有効化

ARP が IP アドレスを正常に解決できないとき、装置で ARP イベントをロギングします。以下の ARP イベントをロギングできます。

- インタフェースで proxy ARP が無効な場合、受信した ARP パケットの宛先 IP アドレスは受信インタフェースの IP アドレスのいずれでもありません。
- 受信した ARP エントリの送信元 IP アドレスが受信インタフェースの IP アドレスの 1 つと重複しています。

装置は Information Center に ARP ログメッセージを送信します。Information Center のログ出力ルールを設定するため、**info-center source** コマンドを使用します。Information Center の詳細はオペレーションマニュアルのセクション 11 *システム管理* “*Information Center*”を参照してください。

以下に ARP ロギング機能の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． ARP ロギング機能を有効にする	**arp check log enable**	デフォルト：無効

1.5 インタフェースでのARPエントリとMACアドレスエントリの整合性のチェックの有効化

不安定なネットワークでは、ユーザからのパケットの受信側インタフェースが変更されることがあります。MAC アドレスエントリのインタフェースはすぐに更新できますが、ARP エントリのインタフェースは更新できません。この場合、ARP エントリに一致するパケットは、正しくないインタフェースから送信されます。この問題を解決するには、この機

能を使用して、エントリの ARP および MAC アドレスユーザのインタフェース整合性を定期的にチェックします。インタフェースが同じでない場合、ARP は ARP エントリの VLAN に ARP 要求を送信し、ARP 応答を受信したインタフェースでエントリを更新します。

以下にインタフェースで ARP エントリと MAC アドレスエントリの整合性のチェックを有効にする設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． インタフェースで ARP エントリと MAC アドレスエントリの整合性のチェックを有効にする	**arp mac-interface-consistency check enable**	デフォルト：有効

1.6 ARPの表示と維持

重要：
ARP テーブルから ARP エントリをクリアすると、通信障害を引き起こす恐れがあります。ARP エントリを削除した場合は、その後の通信に影響がないことを確認してください。

すべての view で **display** コマンドを実行でき、user view で **reset** コマンドが実行できます。

操作	コマンド
ARPエントリを表示する	**display arp** [[**all** | **dynamic** | **multiport** | **static**] [**slot** *slot-number*] | **vlan** *vlan-id* | **interface** *interface-type interface-number*] [**count** | **verbose**]
指定したIPアドレスのARPエントリを表示する	**display arp** *ip-address* [**slot** *slot-number*] [**verbose**]
ダイナミックARPエントリのエージングタイムを表示する	**display arp timer aging**
VPNインスタンスのARPエントリを表示する	**display arp vpn-instance** *vpn-instance-name* [**count**]
ARPテーブルからARPエントリを削除する	**reset arp** { **all** | **dynamic** | **interface** *interface-type interface-number* | **multiport** | **slot** *slot-number* | **static** }

1.7 ARPの設定例

1.7.1 ロングスタティック ARP の設定例

I. ネットワーク要件

図 1-3に示すように、Host は、Device B に接続されています。Device B は VLAN 10 の GigabitEthernet 1/0/1 によって Device A に接続されています。

Device A と Device B 間の通信を強化するため、Device B で Device A のロングスタティック ARP エントリの設定を行います。

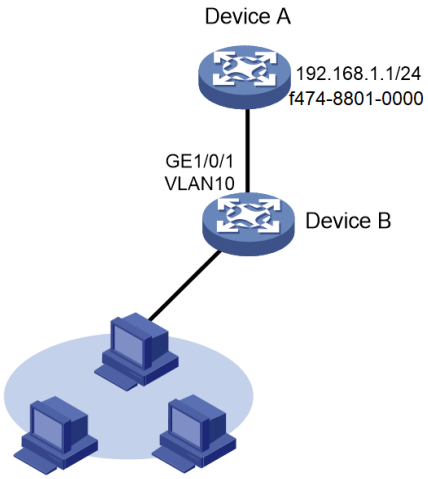


図 1-3 ネットワーク図

II. 設定手順

VLAN 10 を作成します。

```
<DeviceB> system-view
[DeviceB] vlan 10
[DeviceB-vlan10] quit
```

GigabitEthernet 1/0/1 に VLAN 10 を割り当てます。

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port access vlan 10
[DeviceB-GigabitEthernet1/0/1] quit
```

VLAN インタフェース 10 を作成し、IP アドレスを設定します。

```
[DeviceB] interface vlan-interface 10
[DeviceB-vlan-interface10] ip address 192.168.1.2 8
[DeviceB-vlan-interface10] quit
```

IP アドレス 192.168.1.1 と MAC アドレス f474-8801-0000 のスタティック ARP エントリを作成します。ロングスタティック ARP エントリに対応する出力インタフェースを VLAN 10 に所属する GigabitEthernet 1/0/1 とします。

```
[DeviceB] arp static 192.168.1.1 f474-8801-0000 10 gigabitethernet 1/0/1
```

III. 設定の確認

Device B で Device A のスタティック ARP エントリを表示します。

```
[DeviceB] display arp static
  Type: S-Static   D-Dynamic   O-Openflow   R-Rule   M-Multiport  I-Invalid
IP address       MAC address     VID     Interface/Link ID      Aging Type
192.168.1.1      f474-8801-0000  10      GE1/0/1                N/A   S
```

1.7.2 ショートスタティック ARP の設定例

I. ネットワーク要件

図 1-4に示すように、Host は、Device B に接続されています。Device B は VLAN 10 の GigabitEthernet 1/0/2 によって Device A に接続されています。

Device A と Device B 間の通信を強化するため、Device B で Device A のショートスタティック ARP エントリの設定を行います。

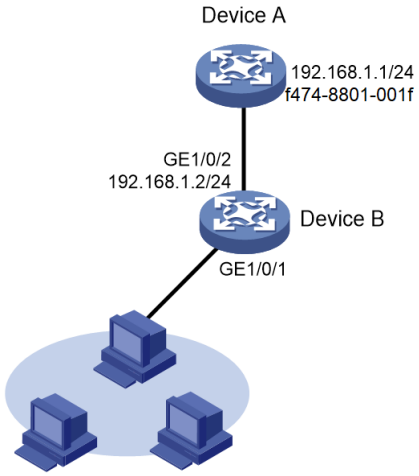


図 1-4 ネットワーク図

II. 設定手順

GigabitEthernet 1/0/2 の IP アドレスを設定します。

```
<DeviceB> system-view
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] ip address 192.168.1.2 24
[DeviceB-GigabitEthernet1/0/2] quit
```

IP アドレス 192.168.1.1 と MAC アドレス f474-8801-001f のショートスタティック ARP エントリを作成します。

```
[DeviceB] arp static 192.168.1.1 f474-8801-001f
```

III. 設定の確認

Device B で Device A のショートスタティック ARP エントリを表示します。

```
[DeviceB] display arp static
  Type: S-Static   D-Dynamic   O-Openflow   R-Rule   M-Multiport  I-Invalid
IP address       MAC address     VID     Interface/Link ID      Aging Type
192.168.1.1      f474-8801-001f  N/A     N/A                    N/A   S
```

1.7.3 マルチポート ARP エントリの設定例

I. ネットワーク要件

図 1-5に示すように Device は VLAN10 のインタフェース GigabitEthernet 1/0/1～GigabitEthernet 1/0/3 を通して 3 つのサーバに接続します。サーバは IP アドレス 192.168.1.1/24、MAC アドレス 4ce9-e401-0000 を共有します。

Device が 3 つのサーバに宛先 IP アドレス 192.168.1.1 に IP パケットを送信できるようにマルチポート ARP エントリを設定します。

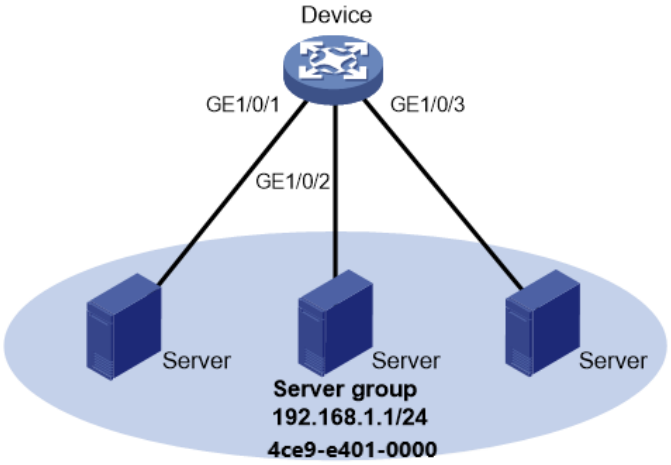


図 1-5 ネットワーク図

II. 設定手順

VLAN 10 を作成します。

```
<Device> system-view
[Device] vlan 10
[Device-vlan10] quit
```

VLAN 10 に GigabitEthernet 1/0/1～GigabitEthernet 1/0/3 を割り当てます。

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] port access vlan 10
```

```
[Device-GigabitEthernet1/0/1] quit
[Device] interface gigabitethernet 1/0/2
[Device-GigabitEthernet1/0/2] port access vlan 10
[Device-GigabitEthernet1/0/2] quit
[Device] interface gigabitethernet 1/0/3
[Device-GigabitEthernet1/0/3] port access vlan 10
[Device-GigabitEthernet1/0/3] quit
```

VLAN インタフェース 10 を作成し、IP アドレスを指定します。

```
[Device] interface vlan-interface 10
[Device-vlan-interface10] ip address 192.168.1.2 24
[Device-vlan-interface10] quit
```

MAC アドレスが 4ce9-e401-0000、出力インタフェースが VLAN10 の GigabitEthernet 1/0/1、GigabitEthernet 1/0/2、GigabitEthernet 1/0/3 のマルチポートユニキャスト MAC アドレスエントリを設定します。

```
[Device] mac-address multiport 4ce9-e401-0000 interface gigabitethernet 1/0/1 to gigabitethernet 1/0/3 vlan 10
```

IP アドレス 192.168.1.1、MAC アドレス 4ce9-e401-0000 のマルチポート ARP エントリを設定します。

```
[Device] arp multiport 192.168.1.1 4ce9-e401-0000 10
```

III. 設定の確認

Device が IP アドレス 192.168.1.1、MAC アドレス 4ce9-e401-0000 のマルチポート ARP エントリがあることを確認します。

```
[Device] display arp
  Type: S-Static   D-Dynamic   O-Openflow   R-Rule   M-Multiport  I-Invalid
IP address       MAC address     VLAN/VSI   Interface      Aging Type
192.168.1.1      4ce9-e401-0000  10         --                    --    M
```

目次

このセクションのページは**4-x-x** です。

2章 Gratuitous ARP 2-1
2.1 概要 2-1
2.1.1 Gratuitous ARPパケットの学習 2-1
2.1.2 Gratuitous ARPパケットの送信間隔の設定 2-1
2.2 設定手順 2-2
2.3 IP重複通知の有効化 2-2
2.4 デバイスのMACアドレス変更に対するgratuitous ARPパケット再送信の設定 2-3

2章 Gratuitous ARP

2.1 概要

GARP（Gratuitous ARP）は ARP パケットの 1 つであり、装置は以下の目的で Gratuitous ARP パケットを送信します。

- 他のネットワーク装置と、IP アドレスが重複していないかを確認できます。IP アドレスが既に使われていた場合、ARP 応答によって重複していることが通知されます。
- 他のネットワーク装置に MAC アドレス情報を通知して、ARP エントリを更新させます。

Gratuitous ARP パケットにおいて送信元 IP アドレスと宛先 IP アドレスは共に送信する装置の IP アドレスです。

2.1.1 Gratuitous ARP パケットの学習

Gratuitous ARP パケットの学習機能を有効にした場合、Gratuitous ARP パケットを受信すると、受信した Gratuitous ARP パケットの送信元 IP アドレスと MAC アドレスを使用して ARP エントリを作成あるいは更新します。

この機能を無効にした場合、ARP エントリの更新は行いますが、新しい ARP エントリは追加しません。ARP エントリは受信した Gratuitous ARP パケットをもとに ARP エントリを作成しないで、ARP テーブルを節約します。

2.1.2 Gratuitous ARP パケットの送信間隔の設定

定期的に Gratuitous ARP パケットを送信することにより、下流の装置の対応する ARP エントリあるいは MAC アドレスエントリを定期的に更新します。この機能は以下の機能を

- ゲートウェイスプーフィングの防御

攻撃者がネットワーク上のホストに捏造した Gratuitous ARP パケットを送信するためにゲートウェイアドレスを使用したとき、ゲートウェイスプーフィングが発生します。ホストからゲートウェイ宛のトラフィックは代わりに攻撃者に送信されます。その結果ホストは外部のネットワークにアクセスできません。

ゲートウェイスプーフィングの攻撃を防ぐため、ゲートウェイが Gratuitous ARP パケットを送信する間隔を設定することができます。Gratuitous ARP パケットは、ホストが正しいゲートウェイの情報を学習できるように、ゲートウェイのプライマリ IP アドレスと手動で設定されたセカンダリ IP アドレスが含まれます。

- ARP エントリのエージアウトの防止

ネットワークのトラフィックが非常に多い、あるいはホストの CPU の使用率が高い場合、受信した ARP パケットは廃棄、あるいはすぐに処理されません。そのため、受信ホストのダイナミック ARP エントリはエージアウトします。ホストと対応する装置間のトラフィックは、ホストが ARP エントリを再作成するまで中断されます。

この問題を防ぐため、定期的に Gratuitous ARP パケットを送信するゲートウェイを有効にします。受信ホストはすぐに ARP エントリをアップデートすることができます。

2.2 設定手順

以下に Gratuitous ARP の設定を行うため、制限とガイドラインに従ってください。

- 最大 1024 のインタフェースで Gratuitous ARP パケットの送信間隔を設定できます。
- Gratuitous ARP パケットの送信間隔の設定は、以下の状態の場合に適用されます。
  - インタフェースのリンク状態がアップです。
  - IP アドレスが割り当てられています。
- Gratuitous ARP パケットの送信間隔を変更する場合、設定は次の送信間隔から適用されます。
- Gratuitous ARP パケットの送信間隔は以下の状況によって、設定した値よりも長くなる可能性があります。
  - 複数のインタフェースで有効にされた場合
  - 各インタフェースで複数のセカンダリ IP アドレスが設定された場合
  - 複数のインタフェースで有効にされ、各インタフェースで複数のセカンダリ IP アドレスが設定された場合、Gratuitous ARP パケットの送信間隔は設定された送信間隔よりも短くなります。

以下に Gratuitous ARP の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Gratuitous ARP パケット学習機能を有効にする	**gratuitous-arp-learning enable**	デフォルト：無効
3. 他のネットワークセグメントから ARP 要求を受信した際、Gratuitous ARP パケットの送信を有効にする	**gratuitous-arp-sending enable**	デフォルト：無効
4. interface view に移行する	**interface** *interface-type interface-number*	―
5. Gratuitous ARP パケットの定期的な送信を有効化し、送信間隔を設定する	**arp send-gratuitous-arp** [**interval** *interval*]	デフォルト：無効

2.3 IP重複通知の有効化

デフォルトで、受信装置が Gratuitous ARP パケットの送信者の IP アドレスを使用する場合、受信装置は gratuitous ARP 要求を送信します。重複に関する ARP 応答を受信したのち、エラーメッセージを表示します。

このコマンドを使用することで、Gratuitous ARP 応答あるいは要求を送信することなく、装置でエラーメッセージを表示することができます。

以下に IP 重複通知の有効化の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． IP 重複通知を有効にする	**arp ip-conflict log prompt**	デフォルト：無効

2.4 デバイスのMACアドレス変更に対するgratuitous ARPパケット再送信の設定

I. 制限とガイドライン

装置は、MAC アドレスの変更を他のデバイスに通知するために、Gratuitous ARP パケットを送信します。ただし、装置はデフォルトで 1 回だけ Gratuitous ARP パケットを送信するため、他の装置はパケットの受信に失敗する可能性があります。Gratuitous ARP パケットの再送信機能を設定して、他の装置がパケットを受信できるようにします。

II. 設定手順

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． 装置の MAC アドレス変更のために、Gratuitous ARP パケットを再送信する時間と間隔を設定する。	**gratuitous-arp mac-change retransmit** *times* **interval** *seconds*	デフォルト：装置は1回だけMACアドレスの変更を通知するためにGratuitous ARPパケットを送信します。

目次

このセクションのページは **4-x-x** です。

3 章 Proxy ARP 3-1
3.1 一般的な Proxy ARP の有効化 3-1
3.2 ローカル Proxy ARP の有効化 3-1
3.3 Proxy ARP の表示と維持 3-1
3.4 一般的な Proxy ARP 設定例 3-2
3.4.1 ネットワーク要件 3-2
3.4.2 設定手順 3-2
3.4.3 設定の確認 3-3

3章 Proxy ARP

Proxy ARP が有効な装置で、別のネットワークの IP アドレスの ARP リクエストに応答します。Proxy ARP を有効にすることで、異なるブロードキャストドメインのホストが同一のブロードキャストドメインにいるように互いに通信できるようにします。

Proxy ARP は一般的な Proxy ARP とローカル Proxy ARP があります。

- **一般的な Proxy ARP**－異なるレイヤ 3 インタフェースに接続され、異なるブロードキャストドメインに存在するホスト間で通信することができます。
- **ローカル Proxy ARP**－同一のレイヤ 3 インタフェースに接続され、異なるブロードキャストドメインに存在するホスト間で通信することができます。

3.1 一般的なProxy ARPの有効化

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. VLAN interface view に移行する	**interface** *vlan-interface vlan-interface-id*	―
3. 一般的な Proxy ARP を有効にする	**proxy-arp enable**	デフォルト：無効

3.2 ローカルProxy ARPの有効化

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. VLAN interface view に移行する	**interface** *vlan-interface vlan-interface-id*	―
3. ローカル Proxy ARP を有効にする	**local-proxy-arp enable** [**ip-range** *startIP* **to** *endIP*]	デフォルト：無効

3.3 Proxy ARPの表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
一般的なProxy ARPの状態を表示する	**display proxy-arp** [**interface** *interface-type interface-number*]
ローカルProxy ARPの状態を表示する	**display local-proxy-arp** [**interface** *interface-type interface-number*]

3.4 一般的なProxy ARP設定例

3.4.1 ネットワーク要件

図 3-1に示すように、Host A と Host D は同一 IP アドレスとマスクを持ちますが、Switch によって異なるサブネットに分離されています。Host A は VLAN1、Host D は VLAN2 に所属しています。Host A と Host D のデフォルトゲートウェイは設定されていません。

2 つの Host 間で通信ができるように Switch で一般的な Proxy ARP を設定します。

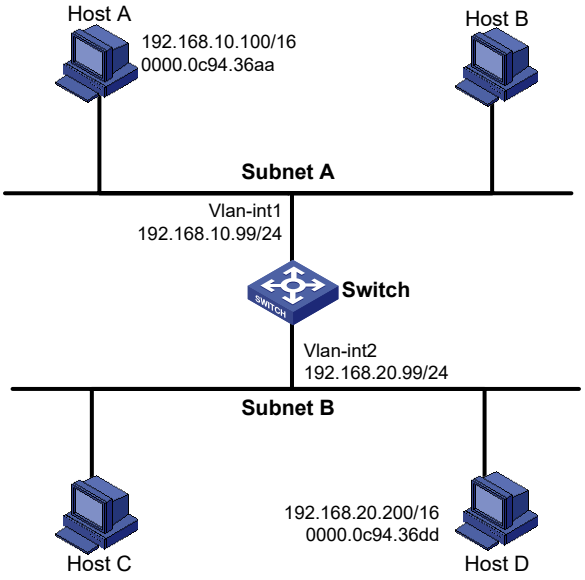


図 3-1 ネットワーク図

3.4.2 設定手順

VLAN 2 を作成します。

```
<Switch> system-view
[Switch] vlan 2
[Switch-vlan2] quit
```

VLAN インタフェース 1 の IP アドレスを設定します。

```
[Switch] interface vlan-interface 1
[Switch-Vlan-interface1] ip address 192.168.10.99 255.255.255.0
```

VLAN インタフェース 1 で一般的な Proxy ARP を有効にします。

```
[Switch-Vlan-interface1] proxy-arp enable
[Switch-Vlan-interface1] quit
```

VLAN インタフェース 2 の IP アドレスを設定します。

```
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ip address 192.168.20.99 255.255.255.0
```

VLAN インタフェース 2 で一般的な Proxy ARP を有効にします。

```
[Switch-Vlan-interface2] proxy-arp enable
```

3.4.3 設定の確認

Host A と Host D で互いに ping ができるかどうか確認してください。

目次

このセクションのページは **4-x-x** です。

4 章 ARP スヌーピング 4-1
4.1 設定手順 4-1
4.2 ARP snooping の表示と維持 4-1

4章 ARP スヌーピング

ARP snooping はレイヤ 2 ネットワークで使用されます。ARP パケットの情報を使用することで、ARP snooping エントリを作成します。

VLAN で ARP snooping を有効にした場合、VLAN 内のインタフェースで受信された ARP パケットは CPU にリダイレクトされます。CPU は ARP snooping エントリを作成するため、ARP パケットの送信元 IP アドレスと送信元 MAC アドレス、受信する VLAN、ポートを使用します。

ARP snooping エントリのエージタイマは 25 分で有効期限は 15 分です。ARP snooping エントリが 15 分以内にアップデートされない場合、ARP snooping エントリは無効になり、使用できなくなります。その後、送信元 IP アドレスと送信元 MAC アドレスがエントリと一致する ARP パケットを受信すると、エントリが有効になり、エージタイマが再スタートします。エントリがエージアウトすると削除されます。

有効な ARP エントリとして、同じ送信元 IP アドレスで異なる送信元 MAC アドレスの ARP パケットを受信すると、装置は攻撃者からのアタックが発生していると認識します。ARP エントリは無効になり、1 分後に削除されます。

🕮 **メモ：**

arp snooping enable コマンドを有効にした VLAN は、ARP パケットが **arp rate-limit** コマンドで指定したレートで転送されます。設定を追加する場合は、事前に設定する VLAN に流れる ARP の量を確認してください。

4.1 設定手順

以下に VLAN での ARP snooping の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. VLAN view に移行する	**vlan** *vlan-id*	ー
3. ARP snooping を有効にする	**arp snooping enable**	デフォルト：無効

4.2 ARP snoopingの表示と維持

すべての view で **display** コマンドが実行でき、user view で **reset** コマンドが実行できます。

操作	コマンド
ARP snoopingエントリを表示する	**display arp snooping** [**vlan** *vlan-id*] [**slot** *slot-number*] [**count**] **display arp snooping ip** *ip-address* [**slot** *slot-number*]

操作	コマンド
ARP snooping エントリを削除する	**reset arp snooping** [**ip** *ip-address* | **vlan** *vlan-id*]

目次

このセクションのページは **4-x-x** です。

5 章 IP アドレス 5-1
5.1 概要 5-1
5.1.1 IP アドレスクラス 5-1
5.1.2 特別な IP アドレス 5-2
5.1.3 サブネットとマスク 5-2
5.2 インタフェースへの IP アドレスの割り当て 5-3
5.3 IP アンナンバードの設定 5-3
5.4 IP アドレスの表示と維持 5-4
5.5 IP アドレスの設定例 5-5

5章 IP アドレス

この章の IP アドレスは、特に指定がない限り、IPv4 アドレスについて記載します。

5.1 概要

IP アドレスは、IPv4 ネットワークの各ホストを識別するため、32 ビットアドレスを使用します。たとえば、2 進数では 00001010000000010000000100000001 となります。IP アドレスをわかりやすくするために、32 ビットの整数値を 8 ビットずつ 4 つに分割し、ドット付きの 10 進数で IP アドレスを表します。先ほどの 32 ビットの 2 進数は、10.1.1.1 となります。

5.1.1 IP アドレスクラス

各 IP アドレスは以下のセクションに分類されます。

- **Net ID** – ネットワークを定義します。先頭の数ビットはネットワークを定義するアドレスです。クラスフィールドあるいはクラスビットで、IP アドレスのクラスを識別します。
- **Host ID** – ホストを定義します。

図 5-1に示すように、IP アドレスは 5 つのクラスに分類されます。IP アドレスがどのクラスに所属するのかは、下図の青い部分のアドレスによって決まります。最初の 3 つのクラスは一般的に使用されます。

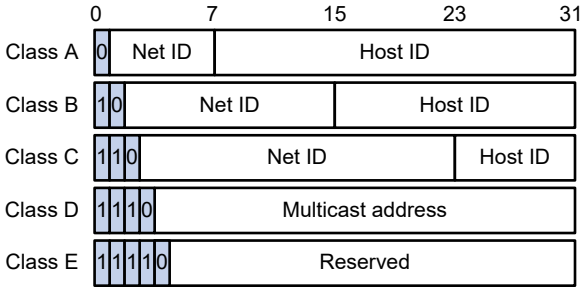


図 5-1 IP アドレスクラス

表 5-1 IP アドレスクラスと範囲

クラス	アドレス範囲	補足
A	0.0.0.0 ～ 127.255.255.255	0.0.0.0はブートストラップ時に一時的にホストが使用するため、有効な宛先アドレスにはなりません。127 からはじまるアドレスはループバックテストのために予約されているため、このアドレス宛てのパケットは、入力パケットとしてローカルで処理されます。

クラス	アドレス範囲	補足
B	128.0.0.0 ～ 191.255.255.255	ー
C	192.0.0.0 ～ 223.255.255.255	ー
D	224.0.0.0 ～ 239.255.255.255	マルチキャストアドレス
E	240.0.0.0 ～ 255.255.255.255	予約済みです。255.255.255.255はブロードキャストアドレスです。

5.1.2 特別な IP アドレス

以下の IP アドレスは特別な用途で使用されるため、ホストの IP アドレスに設定することができません。

- **Net ID がすべて 0 の IP アドレス** ー ローカルネットワークのホストを識別します。たとえば、IP アドレス 0.0.0.16 はローカルネットワークの Host ID が 16 のホストを示します
- **Host ID がすべて 0 の IP アドレス** ー ネットワークアドレスを示します。
- **Host ID がすべて 1 の IP アドレス** ー ディレクテッドブロードキャストを示します。たとえば、宛先アドレスが 192.168.1.255 のパケットは、ネットワーク 192.168.1.0 に属するすべてのホストにブロードキャストされます。

5.1.3 サブネットとマスク

サブネットは、Host ID のいくつかのビットを使用して Subnet ID を作成し、ネットワークをサブネットと呼ばれるより小さいネットワークに分割します。

Host ID と、Net ID と Subnet ID の組み合わせの境界を識別するために、サブネットマスクが使用されます。

各サブネットマスクは IP アドレス関連する 32 ビットで構成されています。サブネットマスクは 1 と 0 で構成されています。1 が連続している部分で Net ID と Subnet ID の組み合わせを識別し、0 が連続している部分で Host ID を識別します。

サブネットとなるまえに、クラス A、B、C ネットワークは、それぞれ 255.0.0.0、255.255.0.0、255.255.255.0 のデフォルトマスク（ナチュラルマスクと呼ばれます）を使用します。

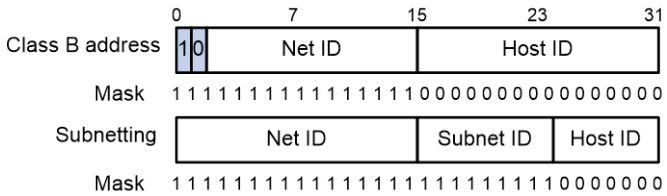


図 5-2 クラス B ネットワークのサブネット

サブネットは、ホストに割り当てることができないアドレスを増大させます。従って、サブネットを使用することは、ある程度少ないホストを適用することになります。

たとえばクラス B ネットワークでは、1022 のサブネットを持つネットワークよりも、512 のサブネットを持つネットワークのほうが、多くのホストを収容することができます。

- **サブネットがないネットワーク** － 65534 個（2^{16} － 2）のホストを収容できます。（Host ID がすべて 1 のブロードキャストアドレスと、Host ID すべて 0 のネットワークアドレスを差し引きます。）
- **サブネットネットワーク** － Host-ID の最初の 9 ビットをサブネットに割り当てると、512 個（2^9）のサブネットができます。Host-ID に使用できるのは残りの 7 ビットだけとなり、各サブネットに 126 個（2^7 － 2）のホストを収容できます。従って、全部で 64512 個（512 × 126）のホストを収容できます。

5.2 インタフェースへのIPアドレスの割り当て

インタフェースは他のホストと通信するために IP アドレスが必要です。手動でインタフェースに IP アドレスを割り当てるか、BOOTP あるいは DHCP によって IP アドレスを取得することができます。IP アドレスを取得する方法を変更した場合、新しい IP アドレスは古い IP アドレスに上書きします。

インタフェースは 1 つのプライマリアドレスと複数のセカンダリアドレスを持つことができます。

通常、インタフェースのプライマリアドレスを設定する必要があります。もしインタフェースが複数のサブネットに接続する場合、サブネットが、インタフェースを通して互いに通信できるようにインタフェースにプライマリとセカンダリ IP アドレスを設定します。

I. 制限とガイドライン

インタフェースに IP アドレスを割り当てるとき以下のガイドラインに従ってください。

- インタフェースは 1 つのプライマリ IP アドレスのみを設定することができます。新しく IP アドレスを設定した場合、古いアドレスが上書きされます。
- BOOTP または DHCP により IP アドレスを取得する設定をしているインタフェースでは、セカンダリ IP アドレスを設定することはできません。
- インタフェースに設定するプライマリとセカンダリ IP アドレスは同じネットワークセグメントに存在することができます。しかし、装置上の異なるインタフェースは異なるネットワークセグメントにしなければなりません。

II. 設定手順

以下にインタフェースに IP アドレスの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	－
2. interface view に移行する	**interface** *interface-type interface-number*	－
3. インタフェースに IP アドレスを設定する	**ip address** *ip-address* { *mask-length* | *mask* } [**sub**]	デフォルト：設定なし

5.3 IPアンナンバードの設定

他のインタフェースから IP アドレスを借用するようにインタフェースを設定できます。これを IP アンナンバードと呼び、IP アドレスを借用しているインタフェースを IP アンナンバードインタフェースと呼びます。

IP アンナンバードを使用すると、使用可能な IP アドレスが不十分な場合や、インタフェースがごくたまにしか使用されない場合に、IP アドレスを保存できます。

I. 制限とガイドライン

- ループバックインタフェースは他のインタフェースの IP アドレスを借用できませんが、他のインタフェースはループバックインタフェースの IP アドレスを借用できます。
- インタフェースは、アンナンバードインタフェースから IP アドレスを借りることはできません。
- 複数のインタフェースが同じアンナンバード IP アドレスを使用できます。
- インタフェースに手動で設定された IP アドレスが複数ある場合は、手動で設定されたプライマリ IP アドレスだけを借用できます。
- IP アンナンバードが設定されているインタフェースでは、ダイナミックルーティングプロトコルを有効にできません。インタフェースが他の装置と通信できるようにするには、インタフェース上のピア装置へのスタティックルートを設定します。

II. 前提条件

IP アドレスを借用するインタフェースに IP アドレスを割り当てます。また、BOOTP または DHCP を使用して取得するようにインタフェースを設定することもできます。

III. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. interface view に移行する	**interface** *interface-type interface-number*	—
3. 指定したインタフェースの IP アドレスを借用するインタフェースを指定する	**ip address unnumbered interface** *interface-type interface-number*	デフォルト：設定なし

5.4 IPアドレスの表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
指定した、またはすべてのレイヤ3インタフェースの設定と統計情報を表示する	**display ip interface** [*interface-type interface-number*]
指定した、またはすべてのレイヤ3インタフェースの概要情報を表示する	**display ip interface** [*interface-type* [*interface-number*]] **brief**

5.5 IPアドレスの設定例

I. ネットワーク要件

図 5-3に示すように、Switch の VLAN1 は、IP アドレス 172.16.1.0/24 と IP アドレス 172.16.2.0/24 の 2 つの LAN に接続されています。

Switch を経由して外部ネットワークに接続された 2つのサブネット上にある Host が互いに通信可能なように設定します。

- VLAN インタフェース 1 に、プライマリ IP アドレスとセカンダリ IP アドレスを割り当てます。
- Switch のプライマリ IP アドレスを、サブネット 172.16.1.0/24 の PC のゲートウェイアドレスに設定し、Switch のセカンダリ IP アドレスを、サブネット 172.16.2.0/24 の PC のゲートウェイアドレスに設定します。

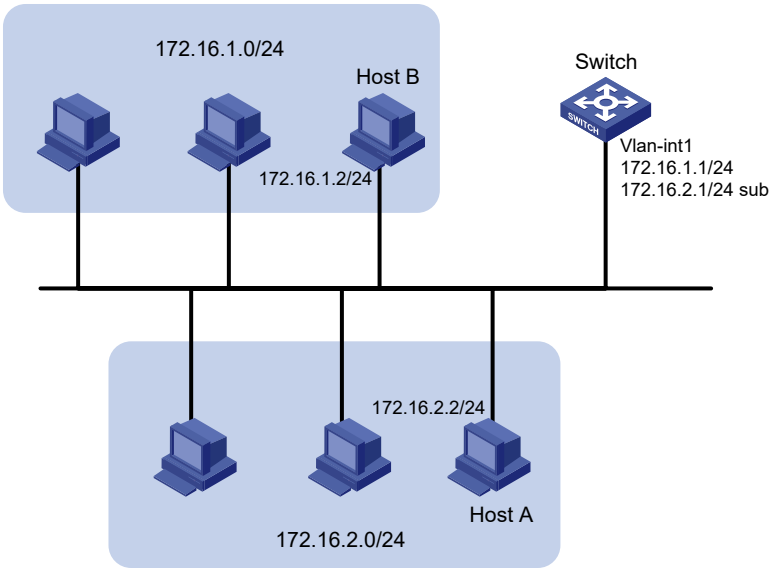


図 5-3 ネットワーク図

II. 設定手順

VLAN インタフェース 1にプライマリ IP アドレスとセカンダリ IP アドレスを割り当てます。

```
<Switch> system-view
[Switch] interface vlan-interface 1
[Switch-Vlan-interface1] ip address 172.16.1.1 255.255.255.0
[Switch-Vlan-interface1] ip address 172.16.2.1 255.255.255.0 sub
```

サブネット 172.16.1.0/24 に接続された PC にゲートウェイアドレス 172.16.1.1 を設定し、サブネット 172.16.2.0/24 に接続された PC にゲートウェイアドレス 172.16.2.1 を設定します。

III. 設定の確認

接続されているか確認するため、Switch からサブネット 172.16.1.0/24 の Host に ping を実施します。

```
<Switch> ping 172.16.1.2
Ping 172.16.1.2 (172.16.1.2): 56 data bytes, press CTRL_C to break
56 bytes from 172.16.1.2: icmp_seq=0 ttl=128 time=7.000 ms
56 bytes from 172.16.1.2: icmp_seq=1 ttl=128 time=2.000 ms
56 bytes from 172.16.1.2: icmp_seq=2 ttl=128 time=1.000 ms
56 bytes from 172.16.1.2: icmp_seq=3 ttl=128 time=1.000 ms
56 bytes from 172.16.1.2: icmp_seq=4 ttl=128 time=2.000 ms

--- Ping statistics for 172.16.1.2 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.000/2.600/7.000/2.245 ms
```

接続されているか確認するため、Switch からサブネット 172.16.2.0/24 の Host に ping を実施します。

```
<Switch> ping 172.16.2.2
Ping 172.16.2.2 (172.16.2.2): 56 data bytes, press CTRL_C to break
56 bytes from 172.16.2.2: icmp_seq=0 ttl=128 time=2.000 ms
56 bytes from 172.16.2.2: icmp_seq=1 ttl=128 time=7.000 ms
56 bytes from 172.16.2.2: icmp_seq=2 ttl=128 time=1.000 ms
56 bytes from 172.16.2.2: icmp_seq=3 ttl=128 time=2.000 ms
56 bytes from 172.16.2.2: icmp_seq=4 ttl=128 time=1.000 ms

--- Ping statistics for 172.16.2.2 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.000/2.600/7.000/2.245 ms
```

接続されたかどうか確認するため、サブネット 172.16.2.0/24 に接続された Host A からサブネット 172.16.1.0/24 に接続された Host B に ping を実施します。Host B は Host A から ping 応答を受信することができます。

目次

このセクションのページは **4-x-x** です。

6 章 DHCP の概要 6-1
6.1 DHCP アドレスの割り当て 6-1
6.1.1 割り当てメカニズム 6-1
6.1.2 IP アドレスの割り当てプロセス 6-2
6.1.3 IP アドレスのリース延長 6-3
6.2 DHCP メッセージフォーマット 6-3
6.3 DHCP オプション 6-4
6.3.1 一般的な DHCP オプション 6-4
6.3.2 自己定義 DHCP オプション 6-5
6.4 プロトコルと標準 6-8

6章 DHCP の概要

DHCP（Dynamic Host Configuration Protocol）は、ネットワークにおいて通信用の基本的な設定を自動的に行う機能を提供します。

図 6-1に示すように、一般的な DHCP の構成は、同一サブネットに DHCP サーバとクライアントがあります。

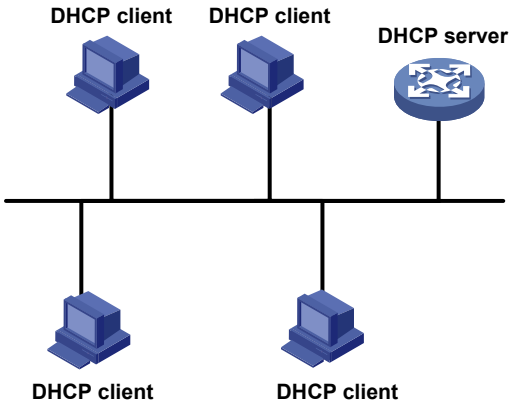


図 6-1 一般的な DHCP の構成

6.1 DHCPアドレスの割り当て

6.1.1 割り当てメカニズム

DHCP は以下の IP アドレスの割り当てメカニズムをサポートします。

- **手動割り当て** － ネットワーク管理者が WWW サーバなどのクライアントに IP アドレスを割り当てます。DHCP 割り当てられたアドレスをクライアントに伝送します。
- **自動割り当て** － DHCP がクライアントに永続的に使用可能な IP アドレスを割り当てます。
- **動的（ダイナミック）割り当て** － DHCP は、クライアントに一定期間（リース期間）使用可能な IP アドレスを割り当てます。ほとんどのクライアントがこの方法でアドレスを取得します。

6.1.2 IP アドレスの割り当てプロセス

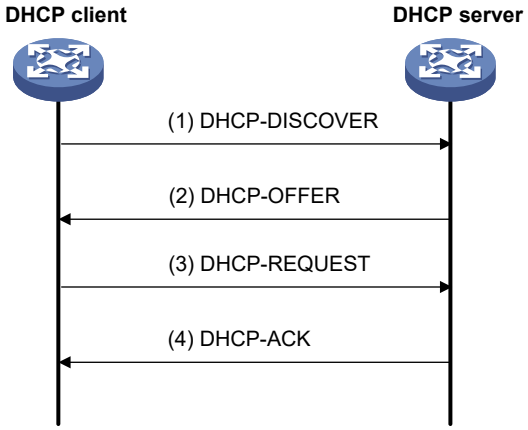


図 6-2 IP アドレスの割り当てプロセス

図 6-2に示すように DHCP サーバは以下の手順で DHCP クライアントに IP アドレスを割り当てます。

1) クライアントは DHCP-DISCOVER メッセージをブロードキャストし、DHCP サーバを特定します。
2) DHCP サーバは、DHCP-OFFER メッセージの中で IP アドレスなどの設定パラメータをクライアントに提供します。DHCP-OFFER の送信モードは DHCP-DISCOVER メッセージのフラグフィールドによって決定します。関連情報は、オペレーションマニュアルのセクション 4 *IP サービス* "*DHCP の概要*"の"*DHCP メッセージフォーマット*"を参照してください。
3) クライアントが複数の DHCP-OFFER を受信した場合、クライアントは最初に受け取った DHCP-OFFER を受け入れ、正式に IP アドレスを要求するために DHCP-REQUEST メッセージをブロードキャストで送信します。(他の DHCP サーバから提供された IP アドレスは他のクライアントに提供することができます。)
4) すべての DHCP サーバが DHCP-REQUEST メッセージを受信します。しかし、クライアントによって選択されたサーバのみ以下の動作を行います。
   - □ サーバは、クライアントに IP アドレスが割り当てられていることを確認して DHCP-ACK メッセージを返します。
   - □ IP アドレスの割り当てを拒否して DHCP-NAK ユニキャストメッセージを返します。

クライアントは DHCP-ACK メッセージを受信した後、クライアントは割り当てられた IP アドレスを使用する前に、詳細を確認します。

- 割り当てられた IP アドレスが使用中であるかどうかを確認します。Gratuitous ARP パケットをブロードキャストで送信することによって、サーバから割り当てられた IP アドレスが使用中かどうかを調べます。一定時間内に応答がなければ、クライアントはこの IP アドレスを使用することができます。
- 割り当てられた IP アドレスがクライアントで使用している IP アドレスと同一サブネットにないかどうかを確認します。

そうでない場合、クライアントは DHCP-DECLINE メッセージをサーバに送信し、再度 IP アドレスを要求します。

6.1.3 IP アドレスのリース延長

DHCP サーバがクライアントに動的に割り当てた IP アドレスには、リース期間があります。リース期間が経過すると、その IP アドレスは DHCP から返還を要求（回収）されます。クライアントが再び IP アドレスを使用する場合は、リース期間を延長する必要があります。

リース期間の半分が経過したところで、DHCP クライアントはリース期間を延長するために DHCP サーバに DHCP-REQUEST ユニキャストメッセージを送信します。IP アドレスの使用状況に依存して、DHCP サーバは以下のメッセージの 1 つを返します。

- クライアントのリース期間が延長されていることを確認する DHCP-ACK ユニキャストを返します。
- 要求を拒否する DHCP-NAK ユニキャストメッセージを返します。

クライアントが応答を受信しない場合、クライアントはリース期間が 7/8 経過したところで、リースを延長するために別の DHCP-REQUEST メッセージをブロードキャストします。IP アドレスの使用状況に応じて、DHCP サーバはリース期間を延長されたことを示す DHCP-ACK ユニキャストあるいは DHCP-NAK ユニキャストメッセージを返します。

6.2 DHCPメッセージフォーマット

図 6-3に DHCP メッセージフォーマットを示します。DHCP フィールドのいくつかを異なる方法で使用します。カッコ内の数字は、各フィールドのサイズをバイト数で示したものです。

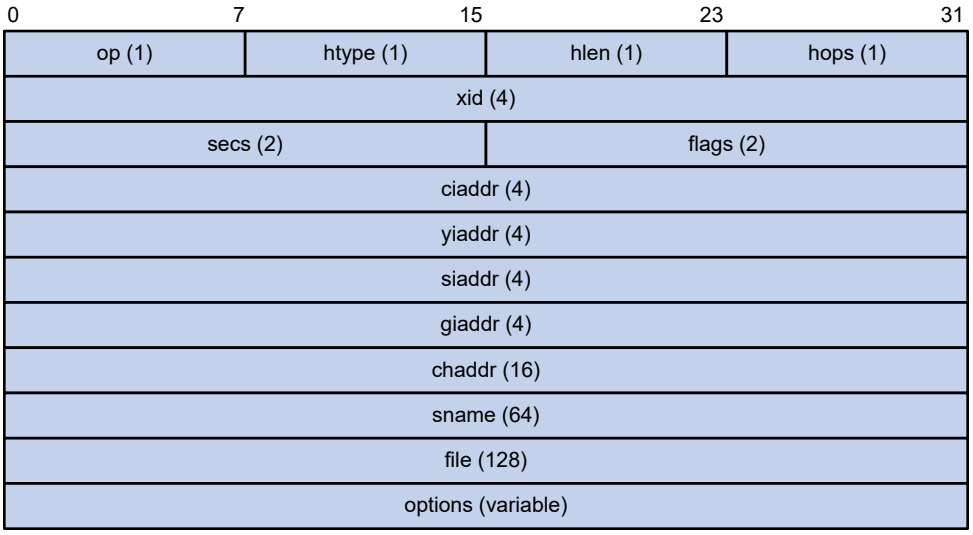


図 6-3 DHCP メッセージフォーマット

- **op**– オプションフィールドに定義されているメッセージタイプです。1 = REQUEST,2 = REPLY
- **htype, hlen**– DHCP クライアントのハードウェアアドレスのタイプと長さです。
- **hops**– 要求メッセージが伝送される（経由する）リレーエージェントの数です。

- **xid**– トランザクション ID で、IP アドレスの割り当てを特定するために、クライアントがランダムに選択した数です。
- **secs**– クライアントがアドレスを取得または更新プロセスを始めてから経過した秒数です。このフィールドは予約されており 0 に設定されています。
- **flags**– 1 ビット目は BROADCAST（B）フラグです。このフラグが 0 に設定されていると、DHCP サーバは応答をユニキャストで返します。このフラグの設定値が 1 のときは、DHCP サーバはブロードキャストで応答を返します。フラグフィールドの残りのビットは、今後の使用のために予約されています。
- **ciaddr**– 有効で使用可能なクライアントの IP アドレスです。そうでなければ 0 に設定されています。（クライアントは、このフィールドを特定の IP アドレスを要求するために使いません。）
- **yiaddr**– DHCP サーバが DHCP クライアントに割り当てる IP アドレスです。
- **siaddr**– サーバの IP アドレスです。クライアントはここから設定パラメータを取得します。
- **giaddr**– 要求メッセージが最初に伝送されたリレーエージェントのゲートウェイ IP アドレスです。
- **chaddr**– クライアントの MAC アドレスです。
- **sname**– サーバのホスト名です。クライアントはここから設定パラメータを取得します。
- **file**– サーバからクライアントに対して定義されたブートファイル名（システムソフトウェアイメージと呼ばれます）、パス情報です。
- **options**– オプションの可変長パラメータです。メッセージタイプ、リース期間、DNS サーバの IP アドレスおよび WINS サーバの IP アドレスなどが含まれます。

6.3 DHCPオプション

DHCP メッセージは、BOOTP（Bootstrap Protocol）と同じメッセージフォーマットを使用しますが、DHCP は動的な IP アドレス割り当て情報と追加の設定情報をクライアントに送信するため、option フィールドを使用します。

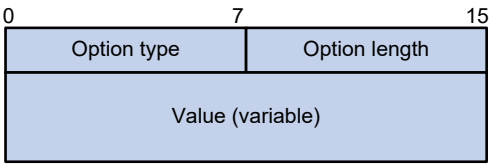


図 6-4 DHCPオプションフォーマット

6.3.1 一般的な DHCP オプション

以下に一般的な DHCP オプションを示します。

- **オプション 3** –　ルータのオプションです。ゲートウェイアドレスを指定します。
- **オプション 6** –　DNS サーバのオプションです。DNS サーバの IP アドレスを指定します。
- **オプション 33** –　スタティックルートオプションです。ルーティングテーブルに追加する必要のあるクラスフルスタティックルート（クラスフルスタティックルートの宛先アドレス）のリストを指定します。クライアントはルーティングテーブルに追加

します。オプション 33 とオプション 121 の両方が存在する場合、オプション 33 は無視されます。

- **オプション 51** – IP アドレスのリースオプションです。
- **オプション 53** – DHCP メッセージタイプのオプションです。DHCP メッセージのタイプを識別します。
- **オプション 55** – パラメータ要求リストのオプションです。DHCP クライアントが、指定の設定パラメータを要求するために使用します。このオプションには、クライアントが要求したパラメータに対応する値が含まれます。
- **オプション 60** – ベンダクラスの識別オプションです。DHCP クライアントがベンダを識別するために使用します。DHCP サーバが、DHCP クライアントを区別し、指定された IP アドレスを割り当てるために使用します。
- **オプション 66** – TFTP サーバ名のオプションです。クライアントに割り当てる TFTP サーバを指定します。
- **オプション 67** – ブートファイル名のオプションです。クライアントに割り当てるブートファイル名を指定します。
- **オプション 121** – クラスレスルートオプションです。クラスレススタティックルート（スタティックルートの宛先ネットワークアドレスがクラスレス）のリストを指定します。クライアントがルーティングテーブルに追加するために要求します。オプション 33 とオプション 121 の両方が存在する場合、オプション 33 は無視されます。
- **オプション 150** – TFTP サーバの IP アドレスのオプションです。クライアントに割り当てる TFTP サーバの IP アドレスを指定します。

DHCP オプションについての詳細は、RFC2132、RFC3442 を参照してください。

6.3.2 自己定義 DHCP オプション

オプション 43、オプション 82、オプション 184 のようなオプションは、RFC2132 で定義されていません。

I. ベンダ指定オプション（オプション 43）

DHCP サーバとクライアントは、ベンダ指定の設定情報を交換するため、オプション 43 を使用します。

DHCP クライアントはオプション 43 を以下の情報を通して取得します。

- ACS の URL、ユーザ名、パスワードを含んだ自動設定パラメータ（ACS パラメータ）です。
- CPE によって DHCP サーバから取得され、ベンダ固有の設定とパラメータを選択するために ACS に送信されるサービスプロバイダ識別子です。
- PXE（Preboot Execution Environment）サーバからブートファイルあるいは、他のコントロール情報を取得するために使用する PXE サーバアドレスです。

1) オプション 43 のフォーマット

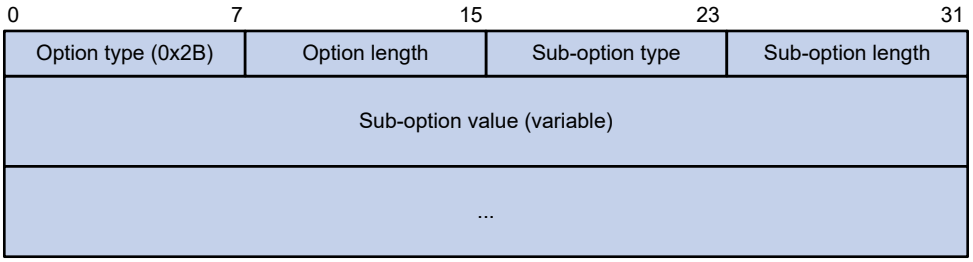


図 6-5 オプション 43 のフォーマット

図 6-5に示すように、ネットワーク設定パラメータは、異なるオプション 43 のサブオプションで送信されます。

- **サブオプションタイプ** ー サブオプションのタイプです。フィールド値は、0x01（ACS パラメータのサブオプション）、0x02（サービスプロバイダ識別子のサブオプション）または 0x80（PXE サーバアドレスのサブオプション）です。
- **サブオプション長** ー サブオプションタイプとサブオプション長フィールドを除くサブオプションの長さです。
- **サブオプション値** ー サブオプションによって値のフォーマットは変更します。

2)　サブオプションフィールドのフォーマット

- **ACS パラメータのサブオプションフィールド**– 図 6-6に示すように、ACS パラメータのサブオプションのフィールドは、ACS の URL、ユーザ名、パスワードです。それぞれの間はスペース（0x20）で分離されます。

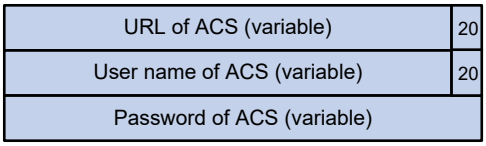


図 6-6 サブオプションフィールドのフォーマット

- **サービスプロバイダ識別子のサブオプションフィールド** ー サービスプロバイダ識別子のサブオプションフィールドは、サービスプロバイダ識別子を含みます。
- **PXE サーバアドレスのサブオプションフィールド** ー 図 6-7に示すように、PXE server type が 0 で、Server number がサブオプションに含まれる PXE サーバの数を示し、Server IP addresses が PXE サーバの IP アドレスを示します。

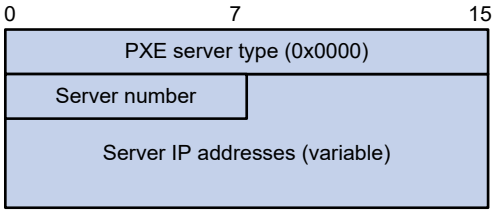


図 6-7 PXE サーバアドレスのサブオプションフィールド

II. リレーエージェントオプション（オプション 82）

オプション 82 は、オプションフィールドにおけるリレーエージェントのオプションです。DHCP クライアントの位置情報を記録します。DHCP リレーエージェントあるいは DHCP snooping がクライアントの要求を受信すると、要求メッセージにオプション 82 を追加してサーバに送信します。

管理者は DHCP クライアントの位置を特定して、セキュリティ管理とアカウンティングを実行することができます。DHCP サーバは、クライアントの個別の設定ポリシーを提供するためにオプション 82 を使用します。

オプション 82 には、最大 255 のサブオプションがあります。少なくとも 1 つのサブオプションを定義する必要があります。オプション 82 は、サブオプション 1（Circuit ID）とサブオプション 2（Remote ID）、サブオプション 5（Link Selection）の 3 つのサブオプションをサポートしています。オプション 82 は標準の定義がありません。ベンダによってパディングフォーマットは変わります。

- Circuit ID は以下に示すパディングフォーマットを持ちます。
  - **文字列パディングフォーマット** – ユーザが定義した文字列を含みます。
  - **標準（Normal）パディングフォーマット** – VLAN ID、クライアントの要求を受信したインタフェースのインタフェース番号を含みます。
  - **詳細（Verbose）パディングフォーマット** – ユーザ定義のアクセスノード識別子、VLAN ID、クライアントの要求を受信したインタフェースの番号、インタフェースのタイプを含みます。
- Remote ID は以下に示すパディングフォーマットを持ちます。
  - **文字列パディングフォーマット** – ユーザが定義した文字列を含みます。
  - **標準（Normal）パディングフォーマット** – DHCP リレーエージェントのインタフェースの MAC アドレスあるいはクライアントの要求を受信した DHCP snooping の MAC アドレスを含みます。
  - **システム名パディングフォーマット** – 装置のシステム名を含みます。装置のシステム名を設定する場合、system view で **sysname** コマンドを使用します。
- Link Selection は、**giaddr** フィールドの IP アドレスあるいは DHCP リレーインタフェースの IP アドレスを送信します。サブオプションはオプション 82 に含まれます。

III. オプション 184

オプション 184 は予約されているオプションです。パラメータを必要に応じて定義することができます。音声機能を持つ DHCP クライアントが DHCP サーバから音声パラメータを取得できるため、装置は音声関連パラメータを含むオプション 184 をサポートします。

オプション 184 は以下のサブオプションがあります。

- **サブオプション 1** – プライマリネットワークコーリングプロセッサの IP アドレスを指定します。プライマリネットワークコーリングプロセッサはネットワークコーリング制御ソースとして機能し、ダウンロード可能なプログラムを提供するサーバです。オプション 184 では、他のサブオプションを適用させるためには、サブオプション 1 を定義する必要があります。
- **サブオプション 2** – プライマリネットワークコーリングプロセッサが到達不可能な場合に、DHCP クライアントがコンタクトをとるバックアップのネットワークコーリングプロセッサの IP アドレスです。
- **サブオプション 3** – 音声 VLAN ID、および DHCP クライアントがこの ID を音声 VLAN として適用するかどうかの結果を示します。
- **サブオプション 4** – ターゲットユーザの IP アドレスと呼び出し番号を含むファイルオーバルートを指定します。プライマリとバックアップのコーリングプロセッサが両方とも到達不可能な場合、SIP VoIP ユーザは直接ターゲットの SIP ユーザに接続を確立するために使用する宛先 IP アドレスと呼び出し番号（SIP ユーザは IP アドレスとナンバを使用して相互に通信する）を指定します。

6.4 プロトコルと標準

- RFC 2131, *Dynamic Host Configuration Protocol*
- RFC 2132, *DHCP Options and BOOTP Vendor Extensions*
- RFC 1542, *Clarifications and Extensions for the Bootstrap Protocol*
- RFC 3046, *DHCP Relay Agent Information Option*
- RFC 3442, *The Classless Static Route Option for Dynamic Host Configuration Protocol (DHCP) version 4*

目次

このセクションのページは**4-x-x** です。

7 章 DHCP サーバ.....7-1
7.1 概要.....7-1
7.1.1 DHCP アドレスプール.....7-1
7.1.2 IP アドレス割り当て順序.....7-3
7.2 DHCP サーバ設定作業リスト.....7-3
7.3 DHCP サーバのアドレスプールの設定.....7-3
7.3.1 設定作業リスト.....7-3
7.3.2 DHCP アドレスプールの作成.....7-4
7.3.3 DHCP アドレスプールの IP アドレス範囲の設定.....7-4
7.3.4 DHCP クライアントのゲートウェイの設定.....7-6
7.3.5 クライアントへのドメイン名サフィックスの設定.....7-7
7.3.6 DHCP クライアントの DNS サーバの設定.....7-7
7.3.7 DHCP クライアントの WINS サーバと NetBIOS ノードタイプの設定.....7-7
7.3.8 DHCP クライアントの BIMS サーバ情報の設定.....7-8
7.3.9 DHCP クライアントのオートコンフィグレーションの設定ファイルの設定.....7-8
7.3.10 DHCP クライアントのサーバの設定.....7-9
7.3.11 DHCP クライアントのオプション 184 パラメータの設定.....7-9
7.3.12 DHCP ユーザクラスの設定.....7-10
7.3.13 カスタマイズ DHCP オプションの設定.....7-10
7.4 DHCP の有効化.....7-12
7.5 インタフェースでの DHCP サーバの有効化.....7-12
7.6 インタフェースでのアドレスプールの適用.....7-12
7.7 IP アドレス競合検出の設定.....7-13
7.8 オプション 82 の処理モードの有効化.....7-13
7.9 DHCP サーバが送信した DHCP パケットの DSCP 値の設定.....7-14
7.10 DHCP サーバの表示と維持.....7-14
7.11 DHCP サーバ設定例.....7-15
7.11.1 スタティック IP アドレスの割り当て設定例.....7-15
7.11.2 ダイナミック IP アドレスの割り当て設定例.....7-17
7.11.3 プライマリ、セカンダリサブネット設定例.....7-19
7.11.4 自己定義オプション設定例.....7-21
7.12 DHCP サーバ設定のトラブルシューティング.....7-22
7.12.1 症状.....7-22
7.12.2 分析.....7-22
7.12.3 解決策.....7-22

7章 DHCP サーバ

7.1 概要

DHCP(Dynamic Host Configuration Protocol)サーバ機能とは、IP アドレスなどのネットワーク利用に必要な設定情報を、各クライアントに自動的に割り当てる機能です。これにより、各クライアントでネットワークの詳細な設定を行わなくても、ネットワークに接続することができます。

DHCP サーバは以下のようなネットワークに適しています。

- 手動の設定や集中管理が難しいネットワーク
- 同時にアクセスできる IP アドレス数が制限されているネットワーク
- 多くのホストで、固定の IP アドレスが必要でないネットワーク

7.1.1 DHCP アドレスプール

各 DHCP アドレスプールは、割り当て可能な IP アドレス、ネットワーク設定パラメータのグループを持っています。DHCP サーバは、アドレスプールから IP アドレスとほかのパラメータを選択し、DHCP クライアントに割り当てます。

I. アドレス割り当てメカニズム

必要に応じて以下のようにアドレス割り当てメカニズムの設定を行います。

- **スタティックアドレス割り当て** － DHCP アドレスプールの IP アドレスをクライアントの MAC アドレスあるいは ID に手動で割り当てます。クライアントが IP アドレスを要求したとき、DHCP サーバは、スタティックバインディングの IP アドレスをクライアントに割り当てます。
- **ダイナミックアドレス割り当て** － DHCP アドレスプールの IP アドレス範囲を設定します。DHCP クライアントからの要求を受信したとき、DHCP サーバは、ダイナミックにアドレスプールの IP アドレス範囲から IP アドレスを選択します。

アドレスプールの IP アドレス範囲を設定する場合、アドレスプールの 1 つのプライマリサブネットと複数のセカンダリサブネットを設定します。

DHCP サーバは最初にプライマリサブネットから IP アドレスを選択します。もしプライマリサブネットに割り当て可能な IP アドレスがない場合、DHCP サーバは、設定された順番でセカンダリサブネットから IP アドレスを選択します。

II. アドレスプール選択の原則

DHCP サーバは以下の原則に従い、アドレスプールを選択してクライアントに IP アドレスを割り当てます。

1) IP アドレスがクライアントの MAC アドレスあるいは ID にスタティックで割り当てられているアドレスプールがある場合は、DHCP サーバが、このアドレスプールを選択し、スタティックに割り当てられている IP アドレスとほかのパラメータをクライアントに割り当てます。
2) 受信インタフェースがアドレスプールに割り当てられている場合、DHCP サーバは、このアドレスプールを選択し、IP アドレスとほかのパラメータをクライアントに割り当てます。
3) 手動で設定したアドレスプールがなく、受信インタフェースに適用されるアドレスプールがない場合、DHCP サーバはクライアントの位置に依存して以下の方法でアドレスプールを選択します。
   - **クライアントとサーバが同一サブネットにある場合**－DHCP サーバは受信インタフェースの IP アドレスをすべてのアドレスプールのプライマリサブネットにマッチさせます。
     - マッチしたプライマリサブネットが複数ある場合、最長一致（ロンゲストマッチ）のルールでアドレスプールを選択します。
     - マッチしたプライマリサブネットがない場合、DHCP サーバはすべてのアドレスプールのセカンダリサブネットにマッチさせます。DHCP サーバは最長一致（ロンゲストマッチ）のルールでアドレスプールを選択します。
   - **クライアントとサーバが異なるサブネットにある場合**－DHCP サーバは DHCP リクエストの **giaddr** フィールドにある IP アドレスをすべてのアドレスプールのプライマリサブネットにマッチさせます。（DHCP リレーエージェントはクライアントとサーバの間にあります）
     - マッチしたプライマリサブネットが複数ある場合、最長一致（ロンゲストマッチ）のルールでアドレスプールを選択します。
     - マッチしたプライマリサブネットがない場合、DHCP サーバはすべてのアドレスプールのセカンダリサブネットにマッチさせます。DHCP サーバは最長一致（ロンゲストマッチ）のルールでアドレスプールを選択します。

たとえば、1.1.1.0/24 と 1.1.1.0/25 の 2 つのアドレスプールが設定可能ですが、DHCP サーバのインタフェースに適用されていないとします。

- 受信したインタフェースの IP アドレスが 1.1.1.1/25 である場合、DHCP サーバはアドレスプール 1.1.1.0/25 を選択します。アドレスプールに割り当て可能な IP アドレスがない場合、DHCP サーバはほかのプールを選択できず、アドレス割り当ては失敗します。
- 受信したインタフェースの IP アドレスが 1.1.1.130/25 である場合、DHCP サーバはアドレスプール 1.1.1.0/24 からクライアントの IP アドレスを選択します。

正しくアドレスの割り当てを行うため、以下のサブネットの 1 つでダイナミック割り当て用の IP アドレスを保持しておいてください。

- **クライアントとサーバが同一サブネットにある場合**－DHCP サーバのインタフェースが接続されているサブネット
- **クライアントとサーバが異なるサブネットにある場合**－クライアント側に面し、最初の DHCP リレーのインタフェースが接続されているサブネット

🕮 **メモ：**

ネットワークで最低 1 つの一致したプライマリのサブネットを設定してください。そうでない場合、最初にセカンダリサブネットを選択します。セカンダリサブネットで割り当て可能な IP アドレス数より多くの DHCP クライアントが存在する場合、すべての DHCP クライアントに IP アドレスの割り当てを行うことができません。

7.1.2 IP アドレス割り当て順序

DHCP サーバはクライアントの IP アドレスを以下の順序で選択します。

1) クライアントの MAC アドレスあるいは ID に手動で割り当てされている IP アドレスです。
2) クライアントに割り当てられていた IP アドレスです。
3) DHCP-DISCOVER メッセージ内のオプション 50 フィールドに設定されている IP アドレスです。

   オプション 50 は、DHCP-DISCOVER メッセージの要求した IP アドレスフィールドです。クライアントが取得したい IP アドレスを設定するために、クライアントにより追加されます。追加される内容は、ユーザが定義します。
4) 適切な DHCP アドレスプールで検出された､最初に割り当て可能な IP アドレスです。
5) 競合していた IP アドレスか、リース期間を過ぎた IP アドレスです。割り当て可能な IP アドレスがない場合、サーバは応答しません。

🕮 **メモ：**

- クライアントが別のサブネットに移動した場合､DHCP サーバは一度クライアントに割り当てた IP アドレスの代わりに、新しいサブネットにマッチする IP アドレスを割り当てます。
- 競合した IP アドレスは 1 時間経過したのち、ほかの DHCP クライアントに割り当てることができます。

7.2 DHCPサーバ設定作業リスト

作業リスト
（必須設定項目） DHCPサーバのアドレスプールの設定
（必須設定項目） DHCPの有効化
（必須設定項目） インタフェースでのDHCPサーバの有効化
（オプション設定項目） インタフェースでのアドレスプールの適用
（オプション設定項目） IPアドレス競合検出の設定
（オプション設定項目） オプション82の処理モードの有効化
（オプション設定項目） DHCPサーバが送信したDHCPパケットのDHCP値の設定

7.3 DHCPサーバのアドレスプールの設定

7.3.1 設定作業リスト

作業リスト
（必須設定項目） DHCPアドレスプールの作成

作業リスト
少なくとも以下の作業の1つを実行します。 • DHCPアドレスプールのIPアドレス範囲の設定 • DHCPクライアントのゲートウェイの設定 • DHCPクライアントへのドメイン名サフィックスの設定 • DHCPクライアントのDNSサーバの設定 • DHCPクライアントのWINSサーバとNetBIOSノードタイプの設定 • DHCPクライアントのBIMSサーバ情報の設定 • DHCPクライアントのオートコンフィグレーションの設定ファイルの設定 • DHCPクライアントのサーバの設定 • クライアントのオプション184パラメータの設定 • DHCPユーザクラスの設定 • 自己定義DHCPオプションの設定

7.3.2 DHCP アドレスプールの作成

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. DHCP アドレスプールを作成し、その view に移行する	**dhcp server ip-pool** *pool-name*	デフォルト：設定なし

7.3.3 DHCP アドレスプールの IP アドレス範囲の設定

DHCP アドレスプールに、スタティックのアドレス割り当ておよびダイナミックアドレスの割り当ての両方を設定することができます。ダイナミックアドレスの割り当ては、1 つのプライマリサブネットに複数のセカンダリサブネットを設定することができます。

I. DHCP アドレスプールのプライマリサブネットと複数のセカンダリサブネットの設定

プライマリサブネットで割り当て可能な IP アドレスがないとき、DHCP サーバは、クライアントに要求するセカンダリサブネットの IP アドレスを割り当てることができます。

DHCP アドレスプールのプライマリサブネットとセカンダリサブネットを設定するとき、以下のガイドラインに従ってください。

- 各アドレスプールに 1 つのプライマリサブネットのみを設定することができます。**network** コマンドを使用して複数設定した場合、最後に行った設定が適用されます。
- 各アドレスプールで最大 32 のセカンダリサブネットを設定することができます。
- **forbidden-ip** コマンドで設定された IP アドレスは、現在のアドレスプールに割り当てすることができません。ほかのアドレスプールに割り当てすることができます。**dhcp server forbidden-ip** コマンドで設定した IP アドレスはアドレスプールに割り当てることができません。

以下に DHCP アドレスプールのプライマリサブネットとセカンダリサブネットを設定する方法を示します。

操作	コマンド	補足
3． system view に移行する	**system-view**	―
4． DHCP アドレスプールを作成し、その view に移行する	**dhcp server ip-pool** *pool-name*	デフォルト：設定なし
5． プライマリサブネットを設定する	**network** *network-address* [*mask-length* | **mask** *mask*]	デフォルト：設定なし
6． （オプション設定項目）セカンダリサブネットを設定する	**network** *network-address* [*mask-length* | **mask** *mask*] **secondary**	デフォルト：設定なし
7． （オプション設定項目）system view に戻る	**quit**	―
8． （オプション設定項目）アドレスのリース期間を設定する	**expired** { **day** *day* [**hour** *hour* [**minute** *minute* [**second** *second*]]] | **unlimited** }	デフォルト：1日
9． （オプション設定項目）ダイナミック割り当てから設定された IP アドレスを除外する	**forbidden-ip** *ip-address*&<1-8>	デフォルト：DHCPアドレスプールすべてのアドレスが割り当て可能です。 複数のアドレス範囲を除外する場合、このステップを繰り返します。
10．system view に戻る	**quit**	―
11．（オプション設定項目）グローバルにダイナミック割り当てから設定された IP アドレスを除外する	**dhcp server forbidden-ip** *start-ip-address* [*end-ip-address*]	デフォルト：DHCPサーバインタフェースのIPアドレスを除いて、DHCPアドレスプールすべてのアドレスが割り当て可能です。 複数のアドレス範囲を除外する場合、このステップを繰り返します。

II. DHCP アドレスプールのスタティック割り当ての設定

WWW サーバのような特定の DHCP クライアントは固定の IP アドレスが必要です。クライアントに固定の IP アドレスを提供する場合、MAC アドレスあるいはクライアントの ID を DHCP アドレスプールの IP アドレスにスタティックで割り当てることができます。

スタティック割り当てを設定するとき、以下のガイドラインに従ってください。

- 1 つの IP アドレスは 1 つの MAC アドレスあるいはクライアントの ID にのみ割り当てることができます。作成されたバインディングは変更することができません。DHCP クライアントのバインディングを変更する場合、最初に既存のバインディングを削除する必要があります。
- スタティックバインディングの IP アドレスは DHCP サーバインタフェースのアドレスにすることができません。そうでない場合、IP アドレスの競合が発生し、隣接のクライアントが正常に IP アドレスを取得することができません。
- 同一装置の複数インタフェースはスタティック IP アドレスを要求するため、DHCP を使用します。この場合、要求しているインタフェースを識別するため MAC アドレスよりもクライアントの ID を設定する必要があります。そうでない場合、IP アドレスの割り当てが失敗します。

以下にスタティックバインディングを設定する方法を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． DHCP アドレスプールを作成し、その view に移行する	**dhcp server ip-pool** *pool-name*	デフォルト：設定なし
3． スタティックバインディングを設定する	**static-bind ip-address** *ip-address* [*mask-length* | **mask** *mask*] { **client-identifier** *client-identifier* | **hardware-address** *hardware-address* [**ethernet** | **token-ring**] }	デフォルト：設定なし 複数のスタティックバインディングを設定する場合、このステップを繰り返します。
4． （オプション設定項目）アドレスのリース期間を設定する	**expired** { **day** *day* [**hour** *hour* [**minute** *minute* [**second** *second*]]] | **unlimited** }	デフォルト：1日

7.3.4 DHCP クライアントのゲートウェイの設定

DHCP クライアントはほかのネットワークへのパケットをゲートウェイに送信します。DHCP サーバは DHCP クライアントにゲートウェイアドレスを割り当てることができます。

DHCP サーバで各アドレスプールにゲートウェイアドレスを設定することができます。最大 64 つのゲートウェイを DHCP address pool view あるいは secondary subnet view で設定することができます。

DHCP サーバは以下の方法でセカンダリサブネットのクライアントにゲートウェイアドレスを割り当てます。

- address pool view と secondary subnet view の両方でゲートウェイアドレスを設定する場合、DHCP サーバは secondary subnet view で設定されたゲートウェイアドレスを設定します。
- ゲートウェイアドレスが address pool view で設定されているが、secondary subnet view にない場合、DHCP サーバは address pool view のゲートウェイアドレスを割り当てます。

以下に DHCP アドレスプールのゲートウェイを設定する方法を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． DHCP アドレスプールを作成し、その view に移行する	**dhcp server ip-pool** *pool-name*	デフォルト：設定なし
3． ゲートウェイを設定する	**gateway-list** *ip-address*&<1-64>	デフォルト：設定なし
4． （オプション設定項目）secondary subnet view に移行する	**network** *network-address* [*mask-length* | **mask** *mask*] **secondary**	―
5． （オプション設定項目）ゲートウェイを設定する	**gateway-list** *ip-address*&<1-64>	デフォルト：設定なし

7.3.5 クライアントへのドメイン名サフィックスの設定

DHCP サーバの DHCP アドレスプールにドメイン名サフィックス（DNS）を設定することができます。このサフィックスを設定することで、クライアントはドメイン名の入力部分のみ必要となります。システムは名前解決のため、ドメイン名サフィックスを追加します。DNS の詳細は、オペレーションマニュアルのセクション 4 *IP サービス* "*DNS*"を参照してください。

以下に DHCP アドレスプールのドメイン名サフィックスの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． DHCP アドレスプールを作成し、その view に移行する	**dhcp server ip-pool** *pool-name*	デフォルト：設定なし
3． ドメイン名サフィックスを設定する	**domain-name** *domain-name*	デフォルト：設定なし

7.3.6 DHCP クライアントの DNS サーバの設定

インターネット上のホストがドメイン名を使用してアクセスする場合、DHCP クライアントは名前を解決するため、DNS（Domain Name System）サーバにコンタクトをとる必要があります。DHCP アドレスプールで最大 8 つの DNS サーバを設定することができます。

以下に DHCP アドレスプールの DNS サーバの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． DHCP address pool view に移行する	**dhcp server ip-pool** *pool-name*	デフォルト：設定なし
3． DNS サーバを設定する	**dns-list** *ip-address*&<1-8>	デフォルト：設定なし

7.3.7 DHCP クライアントの WINS サーバと NetBIOS ノードタイプの設定

NetBIOS プロトコルを使用している Microsoft DHCP クライアントは、名前解決のために WINS（Windows Internet Naming Service）サーバにコンタクトする必要があります。DHCP アドレスプールのクライアントに最大 8 つの WINS サーバを設定することができます。

クライアントが名前解決できるように、DHCP アドレスプールに NetBIOS ノードタイプを設定する必要があります。NetBIOS ノードタイプには以下の 4 つがあります。

- **b（ブロードキャスト）-ノード** － b-ノードクライアントは、ブロードキャストメッセージで宛先名を送信します。宛先はメッセージを受信後、クライアントに IP アドレスを返します。
- **p（ピアツー-ピア）-ノード** － P-ノードクライアントは WINS サーバにユニキャストメッセージで宛先名を送信します。WINS サーバは宛先の IP アドレスを返します。
- **m（ミックス）-ノード** － m-ノードクライアントは、宛先名をブロードキャストし、応答がない場合は、WINS サーバに宛先名をユニキャストして宛先 IP アドレスを取得します。

- **h（ハイブリッド）-ノード** – h-ノードクライアントは宛先名を WINS サーバにユニキャストし、応答がない場合は、宛先名をブロードキャストして宛先 IP アドレスを取得します。

以下に DHCP アドレスプールの WINS サーバと NetBIOS ノードタイプの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． DHCP アドレスプールを作成し、その view に移行する	**dhcp server ip-pool** *pool-name*	デフォルト：設定なし
3． WINS サーバを設定する	**nbns-list** *ip-address*&<1-8>	b-ノードでは、オプション設定項目です。 デフォルト：設定なし
4． NetBIOS ノードタイプを設定する	**netbios-type** { **b-node** | **h-node** | **m-node** | **p-node** }	デフォルト：設定なし

7.3.8 DHCP クライアントの BIMS サーバ情報の設定

この設定は BIMS サーバの IP アドレス、ポート番号および共有キーをクライアントに提供します。DHCP クライアントは BIMS（branch intelligent management system）サーバから取得した設定ファイルを使用して、ソフトウェアの定期的なアップデートとバックアップを実行します。

以下に DHCP アドレスプールの BIMS サーバの IP アドレス、ポート番号、共有キーの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． DHCP アドレスプールを作成し、その view に移行する	**dhcp server ip-pool** *pool-name*	デフォルト：設定なし
3． BIMS サーバの IP アドレス、ポート番号、共有キーを設定する	**bims-server ip** *ip-address* [**port** *port-number*] **sharekey** { **cipher** | **simple** } *string*	デフォルト：設定なし

7.3.9 DHCP クライアントのオートコンフィグレーションの設定ファイルの設定

オートコンフィグレーションは装置がコンフィグレーションファイルなしで起動するとき、装置がサーバから自動でコンフィグレーションの設定を取得できることを有効にします。DHCP サーバ、DNS サーバ、TFTP サーバの協力が必要です。

コンフィグレーションファイルの取得を行うため DHCP サーバでパラメータを設定する際、以下のガイドラインに従ってください。

- コンフィグレーションファイルが TFTP サーバにある場合、TFTP サーバの IP アドレスアドレスあるいは名前、コンフィグレーションファイル名を設定してください。

DHCP クライアントはコンフィグレーションファイルを取得する TFTP サーバとコンタクトをとるため、取得したパラメータを使用します。

以下に DHCP アドレスプールのコンフィグレーションファイル名を設定する方法を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. DHCP アドレスプールを作成し、その view に移行する	**dhcp server ip-pool** *pool-name*	デフォルト：設定なし
3. TFTP サーバの IP アドレスあるいは名前を設定する	● TFTPサーバのIPアドレスを設定する： **tftp-server ip-address** *ip-address* ● TFTPサーバの名前を設定する： **tftp-server domain-name** *domain-name*	IPアドレスあるいはTFTPサーバの名前を設定することができます。 デフォルト：設定なし
4. ブートファイル名を設定する	**bootfile-name** *bootfile-name*	デフォルト：設定なし

7.3.10 DHCP クライアントのサーバの設定

特定の DHCP クライアントは TFTP サーバのようなサーバから設定情報を取得する必要があります。サーバの IP アドレスを設定することができます。DHCP サーバはサーバの IP アドレスを DHCP クライアントにほかの設定情報と共に送信します。

以下にサーバの IP アドレスの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. DHCP アドレスプールを作成し、その view に移行する	**dhcp server ip-pool** *pool-name*	デフォルト：設定なし
3. サーバの IP アドレスを設定する	**next-server** *ip-address*	デフォルト：設定なし

7.3.11 DHCP クライアントのオプション 184 パラメータの設定

音声サービスを備えた DHCP クライアントに音声サービスを割り当てるためには、DHCP サーバにオプション 184 を設定する必要があります。オプション 184 の詳細はオペレーションマニュアルのセクション 4 *IP サービス”DHCP の概要”*を参照してください。

以下に DHCP アドレスプールのオプション 184 パラメータの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. DHCP アドレスプールを作成し、その view に移行する	**dhcp server ip-pool** *pool-name*	デフォルト：設定なし

操作	コマンド	補足
3． プライマリネットワークコーリングプロセッサの IP アドレスを設定する	**voice-config ncp-ip** *ip-address*	デフォルト：設定なし このコマンドを設定した後、ほかのオプション184のパラメータが適用されます。
4． （オプション設定項目）バックアップサーバの IP アドレスを設定する	**voice-config as-ip** *ip-address*	デフォルト：設定なし
5． （オプション設定項目）音声 VLAN を設定する	**voice-config voice-vlan** *vlan-id* { **disable** | **enable** }	デフォルト：設定なし
6． （オプション設定項目）フェイルオーバーの IP アドレス､ダイヤル番号を設定する	**voice-config fail-over** *ip-address dialer-string*	デフォルト：設定なし

7.3.12 DHCP ユーザクラスの設定

DHCP サーバは、受信した DHCP 要求のハードウェアアドレス、オプション情報、または giaddr フィールドに従って、DHCP ユーザをさまざまなユーザクラスに分類します。サーバは、異なるユーザクラスの DHCP クライアントに IP アドレスと設定パラメータを割り当てます。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． DHCP ユーザクラスを作成し、その view に移行する	**dhcp class** *class-name*	―
3． DHCP ユーザクラスの一致ルールを設定します。	**if-match rule** *rule-number* **{ hardware-address** *hardware-address* **mask** *hardware-address-mask* **| option** *option-code* **[ascii** *ascii-string* **[offset** *offset* **| partial] | hex** *hex-string* **[mask** *mask* **| offset** *offset* **length** *length* **| partial]] | relay-agent** *gateway-address* **}**	デフォルト：設定なし

7.3.13 カスタマイズ DHCP オプションの設定

重要：
カスタマイズ DHCP オプションを設定するとき、DHCP の動作への影響を十分考慮して行ってください。

カスタマイズ DHCP オプションを設定すると、以下のことが可能になります。

- 新規に定義したオプションを追加します。
- オプション 43 のようなベンダ定義のオプションを追加します。

- CLI によって設定できない、専用の設定コマンドのオプションを追加します。たとえば **option 4 ip-address 1.1.1.1** コマンドで DHCP クライアントにタイムサーバアドレス 1.1.1.1 を定義することができます。
- 予約されたオプションの設定コマンドの制限を超過させる場合、すべてのオプションを追加します。たとえば、**dns-list** コマンドを使用して、8 つを超える DNS サーバアドレスを設定することはできません。8 つを超える DNS サーバを設定する場合、すべての DNS サーバで **option 6** コマンドを使用する必要があります。

表 7-1 一般的な DHCP オプション

オプション	オプション名	対応コマンド	コマンドパラメータ
3	Router Option	**gateway-list**	**ip-address**
6	Domain Name Server Option	**dns-list**	**ip-address**
15	Domain Name	**domain-name**	**ascii**
44	NetBIOS over TCP/IP Name Server Option	**nbns-list**	**ip-address**
46	NetBIOS over TCP/IP Node Type Option	**netbios-type**	**hex**
66	TFTP server name	**tftp-server**	**ascii**
67	Boot file name	**bootfile-name**	**ascii**
43	Vendor Specific Information	—	**hex**

I. DHCP アドレスプールでのカスタマイズ DHCP オプション設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. DHCP アドレスプールを作成し、その view に移行する	**dhcp server ip-pool** *pool-name*	デフォルト：設定なし
3. カスタマイズ DHCP オプションを設定する	**option** *code* { **ascii** *ascii-string* | **hex** *hex-string* | **ip-address** *ip-address*&<1-8> }	デフォルト：設定なし DHCPオプショングループで設定されたDHCPオプションはDHCPアドレスプールで設定されたDHCPオプションより優先されます。

II. DHCP オプショングループでのカスタマイズ DHCP オプション設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. DHCP オプショングループを作成し、その view に移行する	**dhcp option-group** *option-group-number*	—
3. カスタマイズ DHCP オプションを設定する	**option** *code* { **ascii** *ascii-string* | **hex** *hex-string* | **ip-address** *ip-address*&<1-8> }	デフォルト：設定なし DHCPオプショングループで設定されたDHCPオプションはDHCPアドレスプールで設定されたDHCPオプションより優先されます。
4. system view に移行する	**quit**	—

操作	コマンド	補足
5． DHCP アドレスプールを作成し、その view に移行する	**dhcp server ip-pool** *pool-name*	デフォルト：設定なし
6． DHCP ユーザクラスに DHCP オプショングループを指定する。	**class** *class-name* **option-group** *option-group-number*	デフォルト：設定なし DHCPユーザクラスは事前に作成しておく必要があります。

7.4 DHCPの有効化

ほかの DHCP 設定を有効にする前に DHCP を有効にする必要があります。

以下に DHCP の有効化の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． DHCP を有効にする	**dhcp enable**	デフォルト：無効

7.5 インタフェースでのDHCPサーバの有効化

インタフェースで DHCP サーバを有効にする場合、この設定を行います。インタフェースで DHCP 要求を受信すると、DHCP サーバは DHCP アドレスプールから DHCP クライアントに IP アドレスとほかの設定パラメータを割り当てます。

以下にインタフェースでの DHCP サーバの有効化の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． interface view に移行する	**interface** *interface-type interface-number*	―
3． インタフェースで DHCP サーバを有効にする	**dhcp select server**	デフォルト：有効

7.6 インタフェースでのアドレスプールの適用

インタフェースに DHCP アドレスプールを適用する場合、この設定を行います。

インタフェースから DHCP 要求を受信すると、DHCP サーバは以下の方法でアドレスを割り当てます。

- DHCP 要求にスタティックバインディングがある場合、DHCP サーバはスタティックバインディングが含まれるアドレスプールからスタティックバインディング IP アドレスと設定パラメータをクライアントに割り当てます。
- DHCP 要求にスタティックバインディングがない場合、DHCP サーバはアドレスプールと設定パラメータのために適用されたアドレスプールを選択します。

以下にインタフェースにアドレスプールを適用する設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． interface view に移行する	**interface** *interface-type interface-number*	―
3． インタフェースにアドレスプールを適用する	**dhcp server apply ip-pool** *pool-name*	デフォルト : 適用されていません。 アドレスプールがない場合、DHCPサーバはダイナミックアドレスの割り当てに失敗します。

7.7 IPアドレス競合検出の設定

IP アドレスを割り当てる前に、DHCP サーバは、ping パケットを送信して、割り当てるアドレスが使用中かどうかを調べます。

- DHCP サーバが設定した期間内に ping 応答を受信した場合、サーバは別の IP アドレスに ping を行います。
- 応答がない場合、指定数の ping パケットが送信されるまでサーバは IP アドレスに ping を行います。応答がない場合は、サーバは要求元のクライアントに IP アドレスを割り当てます。DHCP クライアントは gratuitous ARP パケットを送信して IP アドレスが競合しているかどうかを調べます。

以下に IP アドレス競合検出の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． （オプション設定項目）IP アドレス競合検出の ping パケットの最大数を設定する	**dhcp server ping packets** *number*	デフォルト：1 **0**に設定した場合、IPアドレスの競合検出を行いません。
3． （オプション設定項目）ping に対する応答の待機タイムアウトを設定する	**dhcp server ping timeout** *milliseconds*	デフォルト：500ms **0**に設定した場合、IPアドレスの競合検出を行いません。

7.8 オプション82の処理モードの有効化

DHCP サーバがオプション 82 を処理するように設定されている場合、オプション 82 のメッセージを受信すると、DHCP サーバは DHCP 応答メッセージにオプション 82 を追加します。

DHCP サーバがオプション 82 を無視するように設定されている場合、DHCP 応答メッセージにオプション 82 を追加しません。

オプション 82 のパラメータが正常に動作するために、DHCP サーバと DHCP リレーエージェントの両方でオプション 82 を処理するように有効にする必要があります。DHCP リレーエージェントでの有効にする設定については、オペレーションマニュアルのセクション 4 *IP サービス”DHCP リレーエージェント”*を参照してください。

以下に DHCP サーバでのオプション 82 の処理モードの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． オプション 82 の処理モードを有効にする	**dhcp server relay information enable**	デフォルト：有効

7.9 DHCPサーバが送信したDHCPパケットのDSCP値の設定

パケットの DSCP 値は、パケットの優先度レベルを設定し、パケットの優先度に影響します。

以下に DHCP サーバが送信した DHCP パケットの DSCP 値の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． DHCP サーバが送信した DHCP パケットの DSCP 値を設定する	**dhcp dscp** *dscp-value*	デフォルト：56

7.10 DHCPサーバの表示と維持

重要：

DHCP サーバの再起動あるいは、**reset dhcp server ip-in-use** コマンドが実行されると、すべてのリース情報を削除します。DHCP サーバは DHCP クライアントからのリース期間延長要求を拒否するので、クライアントは再度 IP アドレスを要求する必要があります。

すべての view で **display** コマンドを実行でき、user view で **reset** コマンドを実行できます。

操作	コマンド
IPアドレスの競合に関する情報を表示する	**display dhcp server conflict** [**ip** *ip-address*]
リース期限切れに関する情報を表示する	**display dhcp server expired** [**ip** *ip-address* | **pool** *pool-name*]
割り当て可能なIPアドレスに関する情報を表示する	**display dhcp server free-ip** [**pool** *pool-name*]
割り当てられたIPアドレス情報を表示する	**display dhcp server ip-in-use** [**ip** *ip-address* | **pool** *pool-name*]
DHCPサーバの統計情報を表示する	**display dhcp server statistics** [**pool** *pool-name*]
DHCPアドレスプールの情報を表示する	**display dhcp server pool** [*pool-name*]
IPアドレスの競合に関する情報を削除する	**reset dhcp server conflict** [**ip** *ip-address*]
リース期限切れに関する情報を削除する	**reset dhcp server expired** [**ip** *ip-address* | **pool** *pool-name*]

操作	コマンド
割り当てられたIPアドレス情報を削除する	**reset dhcp server ip-in-use** [**ip** *ip-address* | **pool** *pool-name*]
DHCPサーバの統計情報を削除する	**reset dhcp server statistics**

7.11 DHCPサーバ設定例

DHCP のネットワークの構築は以下のタイプがあります。

- 同一サブネット上の DHCP サーバと DHCP クライアントは、直接メッセージを交換できます。
- 異なるサブネット上の DHCP サーバと DHCP クライアントは、DHCP リレーエージェントを介して相互に通信します。

DHCP サーバの設定は、どちらのタイプでも同じです。

7.11.1 スタティック IP アドレスの割り当て設定例

I. ネットワーク要件

図 7-1に示すように、Switch B（DHCP クライアント）、Switch C（BOOTP クライアント）は Switch A（DHCP サーバ）からスタティック IP アドレス、DNS サーバアドレス、ゲートウェイアドレスを取得します。

Switch B の VLAN インタフェース 2 のクライアント ID は以下です。

0030-3030-662e-6532-3030-2e30-3030-322d-4574-6865-726e-6574

Switch C の VLAN インタフェース 2 の MAC アドレスは 000f-e200-01c0 です。

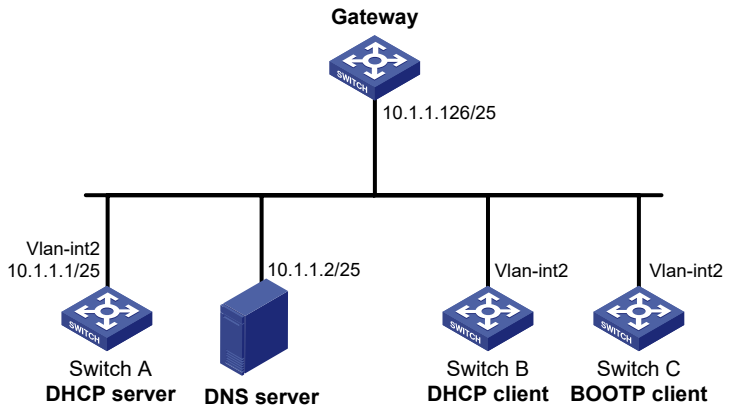


図 7-1 ネットワーク図

II. 設定手順

1)　Switch A の VLAN インタフェース 2 に IP アドレスを設定します。

```
<SwitchA> system-view
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ip address 10.1.1.1 25
[SwitchA-Vlan-interface2] quit
```

2)　DHCP サーバを設定します。

DHCP を有効にします。

```
[SwitchA] dhcp enable
```

VLAN インタフェース 2 で DHCP サーバを有効にします。

```
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] dhcp select server
[SwitchA-Vlan-interface2] quit
```

DHCP アドレスプール 0 を作成します。

```
[SwitchA] dhcp server ip-pool 0
```

Switch B のスタティックバインディングの設定をします。

```
[SwitchA-dhcp-pool-0] static-bind ip-address 10.1.1.5 25 client-identifier 0030-3030-662e-6532-3030-2e30-3030-322d-4574-6865-726e-6574
```

Switch C のスタティックバインディングの設定をします。

```
[SwitchA-dhcp-pool-0] static-bind ip-address 10.1.1.6 25 hardware-address 000f-e200-01c0
```

DNS サーバ、ゲートウェイを設定します。

```
[SwitchA-dhcp-pool-0] dns-list 10.1.1.2
[SwitchA-dhcp-pool-0] gateway-list 10.1.1.126
[SwitchA-dhcp-pool-0] quit
```

III. 設定の確認

Switch B は Switch A から IP アドレス 10.1.1.5 とほかのパラメータを取得します。（詳細は省略します。）

Switch C は Switch A から IP アドレス 10.1.1.6 とほかのパラメータを取得します。（詳細は省略します。）

DHCP サーバでクライアントに割り当てられた IP アドレスを表示します。

```
[SwitchA] display dhcp server ip-in-use
IP address       Client identifier/    Lease expiration      Type
                 Hardware address
10.1.1.5         0030-3030-662e-6532-  Jan 21 14:27:27 2014  Static(C)
                 3030-2e30-3030-322d-
```

```
                    4574-6865-726e-6574
10.1.1.6            000f-e200-01c0        Unlimited             Static(C)
```

7.11.2 ダイナミック IP アドレスの割り当て設定例

I. ネットワーク要件

図 7-2に示すように、DHCP サーバ（Switch A）はサブネット 10.1.1.0/24 のクライアントに IP アドレスを割り当てます。10.1.1.0/24 はさらに 10.1.1.0/25 と 10.1.1.128/25 にサブネット化されます。

Switch A の DHCP サーバで以下の割り当てを行います。

表 7-2 割り当て方法

DHCP クライアント	IP アドレス	リース期間	ほかの設定パラメータ
VLANインタフェース10に接続するクライアント	10.1.1.0/25	10日間と12時間	• ゲートウェイアドレス：10.1.1.126/25 • DNSサーバ：10.1.1.2/25 • ドメイン名：aabbcc.com • WINSサーバ：10.1.1.4/25
VLANインタフェース20に接続するクライアント	10.1.1.128/25	5日間	• ゲートウェイアドレス：10.1.1.254/25 • DNSサーバ：10.1.1.2/25 • ドメイン名：aabbcc.com

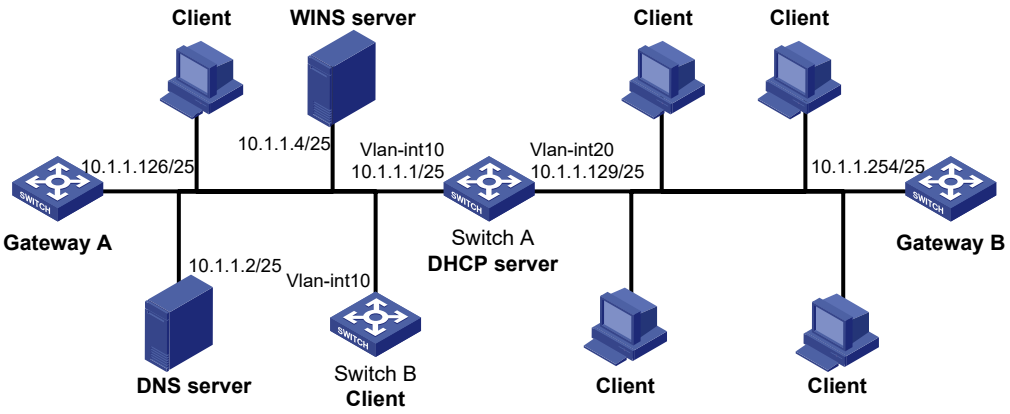


図 7-2 ネットワーク図

II. 設定手順

VLAN インタフェースに IP アドレスを設定します。（詳細は省略します。）

1)　DHCP サーバを設定します。

DHCP を有効にします。

```
<SwitchA> system-view
[SwitchA] dhcp enable
```

VLAN インタフェース 10、VLAN インタフェース 20 で DHCP サーバを有効にします。

```
[SwitchA] interface vlan-interface 10
[SwitchA-Vlan-interface10] dhcp select server
[SwitchA-Vlan-interface10] quit
[SwitchA] interface vlan-interface 20
[SwitchA-Vlan-interface20] dhcp select server
[SwitchA-Vlan-interface20] quit
```

ダイナミック割り当てから DNS サーバアドレス、WINS サーバアドレス、ゲートウェイアドレスを除外します。

```
[SwitchA] dhcp server forbidden-ip 10.1.1.2
[SwitchA] dhcp server forbidden-ip 10.1.1.4
[SwitchA] dhcp server forbidden-ip 10.1.1.126
[SwitchA] dhcp server forbidden-ip 10.1.1.254
```

サブネット 10.1.1.0/25 のクライアントに IP アドレス、ほかのパラメータを割り当てるように DHCP アドレスプール 1 を設定します。

```
[SwitchA] dhcp server ip-pool 1
[SwitchA-dhcp-pool-1] network 10.1.1.0 mask 255.255.255.128
[SwitchA-dhcp-pool-1] expired day 10 hour 12
[SwitchA-dhcp-pool-1] domain-name aabbcc.com
[SwitchA-dhcp-pool-1] dns-list 10.1.1.2
[SwitchA-dhcp-pool-1] gateway-list 10.1.1.126
[SwitchA-dhcp-pool-1] nbns-list 10.1.1.4
[SwitchA-dhcp-pool-1] quit
```

サブネット 10.1.128/25 のクライアントに IP アドレス、ほかのパラメータを割り当てるように DHCP アドレスプール 2 を設定します。

```
[SwitchA] dhcp server ip-pool 2
[SwitchA-dhcp-pool-2] network 10.1.1.128 mask 255.255.255.128
[SwitchA-dhcp-pool-2] expired day 5
[SwitchA-dhcp-pool-2] domain-name aabbcc.com
[SwitchA-dhcp-pool-2] dns-list 10.1.1.2
[SwitchA-dhcp-pool-2] gateway-list 10.1.1.254
[SwitchA-dhcp-pool-2] quit
```

III. 設定の確認

サブネット 10.1.1.0/25 と 10.1.1.128/25 のクライアントが Switch A から正しい IP アドレスとほかのパラメータを取得することを確認します。（詳細は省略します。）

DHCP サーバでクライアントに割り当てられた IP アドレスを表示します。

```
[SwitchA] display dhcp server ip-in-use
IP address       Client identifier/    Lease expiration      Type
                 Hardware address
10.1.1.3         0031-3865-392e-6262-  Jan 14 22:25:03 2015  Auto(C)
                 3363-2e30-3230-352d-
                 4745-302f-30
10.1.1.5         0031-fe65-4203-7e02-  Jan 14 22:25:03 2015  Auto(C)
                 3063-5b30-3230-4702-
                 620e-712f-5e
10.1.1.130       3030-3030-2e30-3030-  Jan 9 10:45:11 2015   Auto(C)
                 662e-3030-3033-2d45-
                 7568-6572-1e
10.1.1.131       3030-0020-fe02-3020-  Jan 9 10:45:11 2015   Auto(C)
                 7052-0201-2013-1e02
                 0201-9068-23
10.1.1.132       2020-1220-1102-3021-  Jan 9 10:45:11 2015   Auto(C)
                 7e52-0211-2025-3402
                 0201-9068-9a
10.1.1.133       2021-d012-0202-4221-  Jan 9 10:45:11 2015   Auto(C)
                 8852-0203-2022-55e0
                 3921-0104-31
```

7.11.3 プライマリ、セカンダリサブネット設定例

I. ネットワーク要件

図 7-3に示すように、DHCP サーバ（Switch A）は LAN 上のクライアントにダイナミックに IP アドレスを割り当てます。

DHCP サーバのアドレスプールにプライマリサブネット 10.1.1.0/24、セカンダリサブネット 10.1.2.0/24 を設定します。プライマリサブネットで割り当てるアドレスがないとき、DHCP サーバは、セカンダリサブネットの IP アドレスを選択します。

Switch A は以下のパラメータを割り当てます。

- サブネット 10.1.1.0/24 のクライアントにデフォルトゲートウェイ 10.1.1.254/24 を割り当てます。
- サブネット 10.1.2.0/24 のクライアントにデフォルトゲートウェイ 10.1.2.254/24 を割り当てます。

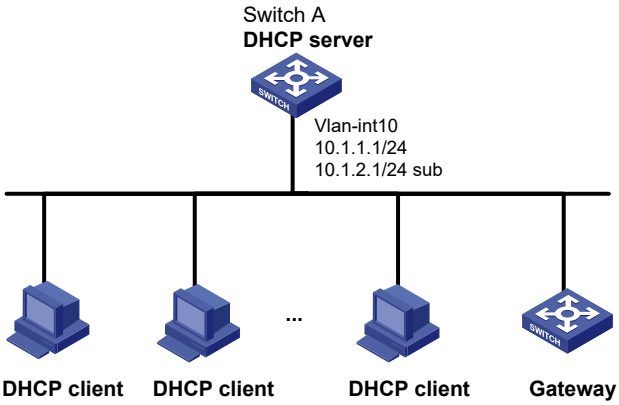


図 7-3 ネットワーク図

II. 設定手順

DHCP を有効にします。

```
<SwitchA> system-view
[SwitchA] dhcp enable
```

VLAN インタフェース 10 のプライマリ IP アドレス、セカンダリ IP アドレスを設定します。

```
[SwitchA] interface vlan-interface 10
[SwitchA-Vlan-interface10] ip address 10.1.1.1 24
[SwitchA-Vlan-interface10] ip address 10.1.2.1 24 sub
```

VLAN インタフェース 10 で DHCP サーバを有効にします。

```
[SwitchA-Vlan-interface10] dhcp select server
[SwitchA-Vlan-interface10] quit
```

DHCP アドレスプール aa を作成します。

```
[SwitchA] dhcp server ip-pool aa
```

ダイナミック割り当てのプライマリアドレス、ゲートウェイアドレスを設定します。

```
[SwitchA-dhcp-pool-aa] network 10.1.1.0 mask 255.255.255.0
[SwitchA-dhcp-pool-aa] gateway-list 10.1.1.254
```

ダイナミック割り当てのセカンダリサブネット、ゲートウェイアドレスを設定します。

```
[SwitchA-dhcp-pool-aa] network 10.1.2.0 mask 255.255.255.0 secondary
[SwitchA-dhcp-pool-aa-secondary] gateway-list 10.1.2.254
[SwitchA-dhcp-pool-aa-secondary] quit
[SwitchA-dhcp-pool-aa] quit
```

III. 設定の確認

プライマリサブネットで割り当て可能なアドレスがない場合、DHCP サーバはセカンダリサブネットから割り当てることを確認します。（詳細は省略します。）

DHCP サーバが割り当てたプライマリ、セカンダリサブネット IP アドレスを表示します。

```
[SwitchA] display dhcp server ip-in-use
IP address       Client identifier/    Lease expiration      Type
                 Hardware address
10.1.1.2         0031-3865-392e-6262-  Jan 14 22:25:03 2015  Auto(C)
                 3363-2e30-3230-352d-
                 4745-302f-30
10.1.2.2         3030-3030-2e30-3030-  Jan 14 22:25:03 2015  Auto(C)
                 662e-3030-3033-2d45-
                 7568-6572-1e
```

7.11.4 自己定義オプション設定例

I. ネットワーク要件

図 7-4に示すように、DHCP クライアント（Switch B）は DHCP サーバ（Switch A）から、IP アドレスと PXE サーバアドレスを取得します。IP アドレスはサブネット 10.1.1.0/24 に属しています。PXE サーバアドレスは、1.2.3.4 と 2.2.2.2 です。

DHCP サーバは、オプション 43（自己定義オプション）を通して、PXE サーバアドレスを DHCP クライアントに割り当てます。オプション 43 のフォーマットと PXE サーバアドレスのサブオプションはオペレーションマニュアルのセクション 4 *IP サービス* "*DHCP の概要*"を参照してください。この例では、DHCP サーバで設定されるオプション 43 の値は、80 0B 00 00 02 01 02 03 04 02 02 02 02 です。

- 番号 80 は、サブオプションタイプの値です。
- 番号 0B は、サブオプション長の値です。
- 番号 00 00 は、PXE サーバタイプの値です。
- 番号 02 は、サーバの数を示します。
- 番号 01 02 03 04 02 02 02 02 は、PXE サーバアドレスが 1.2.3.4 と 2.2.2.2 であることを示します。

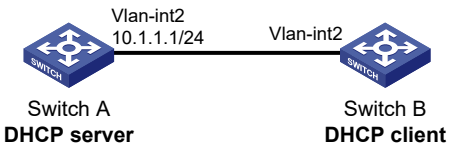


図 7-4 ネットワーク図

II. 設定手順

1)　インタフェースに IP アドレスを設定します。（詳細は省略します。）
2)　DHCP サーバを設定します。

DHCP を有効にします。

```
<SwitchA> system-view
[SwitchA] dhcp enable
```

VLAN インタフェース 2 で DHCP サーバを有効にします。

```
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] dhcp select server
[SwitchA-Vlan-interface2] quit
```

DHCP アドレスプール 0 を設定します。

```
[SwitchA] dhcp server ip-pool 0
```

ダイナミックアドレス割り当てのサブネットを設定します。

```
[SwitchA-dhcp-pool-0] network 10.1.1.0 mask 255.255.255.0
```

自己定義オプション 43 を設定します。

```
[SwitchA-dhcp-pool-0] option 43 hex 800B000002010203040202020202
```

III. 設定の確認

Switch B は Switch A から 10.1.1.0/24 の IP アドレスと PXE サーバアドレスを取得できることを確認します。（詳細は省略します。）

DHCP サーバでクライアントに割り当てられた IP アドレスを表示します。

```
[SwitchA] display dhcp server ip-in-use
IP address       Client identifier/    Lease expiration      Type
                 Hardware address
10.1.1.2         aabb-aabb-ab01        Jan 14 22:25:03 2015  Auto(C)
```

7.12 DHCPサーバ設定のトラブルシューティング

7.12.1 症状

DHCP サーバから取得したクライアントの IP アドレスが別の IP アドレスと競合しています。

7.12.2 分析

サブネットの別のホストが同一 IP アドレスを持っている可能性があります。

7.12.3 解決策

1) クライアントのネットワークアダプタを無効にする、もしくはネットワークケーブルの接続を切断します。別のホストにあるクライアントの IP アドレスに ping を行い、同じ IP アドレスを使用しているホストがあるかを調べます。

2) ping に対する応答があれば、そのホストには IP アドレスが手動で設定されています。DHCP サーバで **dhcp server forbidden-ip** コマンドを実行して、ダイナミックな割り当てからその IP アドレスを除外します。
3) クライアントのネットワークアダプタを有効にする、もしくはネットワークケーブルを接続します。クライアントの IP アドレスを解放し、IP アドレスを再取得します。Windows の DHCP クライアントの場合、以下のように行います。

a) DOS環境で**cmd**コマンドを実行し、コマンドプロンプトを起動します。

b) **ipconfig /release**を実行してIPアドレスを放棄します。

c) **ipconfig /renew**を実行し、IPアドレスの再取得を行います。

目次

このセクションのページは **4-x-x** です。

8 章 DHCP リレーエージェント 8-1
8.1 概要 8-1
8.1.1 動作 8-1
8.1.2 DHCP リレーエージェントのオプション 82 のサポート 8-2
8.2 DHCP リレーエージェント設定作業リスト 8-3
8.3 DHCP の有効化 8-3
8.4 インタフェースでの DHCP リレーエージェントの有効化 8-3
8.5 リレーエージェントの DHCP サーバの指定 8-4
8.6 DHCP リレーエージェントセキュリティ機能の設定 8-4
8.6.1 DHCP リレーエージェントのリレーエントリの記録の有効化 8-4
8.6.2 ダイナミックリレーエントリの定期的な更新の有効化 8-5
8.7 DHCP リレーエージェントでの IP アドレスのリリース設定 8-5
8.8 オプション 82 の設定 8-5
8.9 DHCP リレーエージェントが送信した DHCP パケットの DSCP の設定 8-6
8.10 giaddr フィールドに DHCP リレーエージェントアドレスを設定 8-7
8.11 DHCP リレーエージェントの表示と維持 8-7
8.12 DHCP リレーエージェント設定例 8-8
8.12.1 DHCP リレーエージェント設定例 8-8
8.12.2 オプション 82 設定例 8-9
8.12.3 DHCP サーバ選択の設定例 8-10
8.13 DHCP リレーエージェントのトラブルシューティング 8-11
8.13.1 症状 8-11
8.13.2 分析 8-11
8.13.3 解決策 8-12

8章 DHCP リレーエージェント

8.1 概要

DHCP リレーエージェントは、DHCP クライアントが別のサブネット上にある DHCP サーバから IP アドレスと設定パラメータを取得できるようにします。

図 8-1に DHCP リレーエージェントの一般的な図を示します。

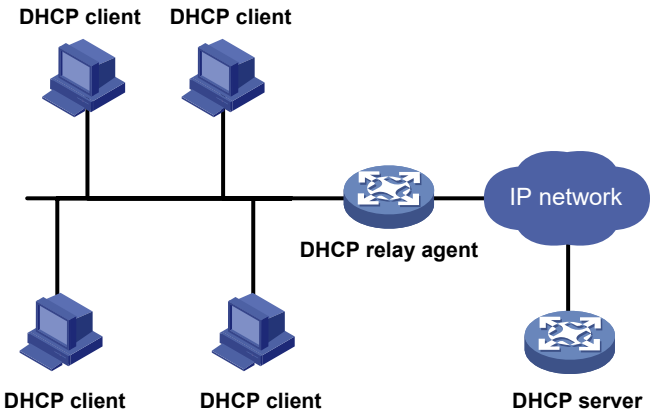


図 8-1 DHCP リレーエージェント構成

8.1.1 動作

DHCP サーバと DHCP クライアントは、DHCP リレーエージェントの有無に関わらず、同様の方法で互いに相互に通信します。相互接続の詳細は、オペレーションマニュアルのセクション 4 *IP サービス* "*DHCP の概要*"を参照してください。以下に、DHCP リレーエージェントに関連した手順を示します。

1) DHCP クライアントから DHCP-DISCOVER または DHCP-REQUEST ブロードキャストメッセージを受信すると、DHCP リレーエージェントはメッセージを以下のように処理します。
   a) メッセージの**giaddr**フィールドにIPアドレスを入力します。
   b) メッセージを指定したDHCPサーバにユニキャストで転送します。
2) **giaddr** フィールドにもとづいて、DHCP サーバは IP アドレスおよびその他の設定パラメータをリレーエージェントに返信します。
3) リレーエージェントはそれらの情報をクライアントへ転送します。

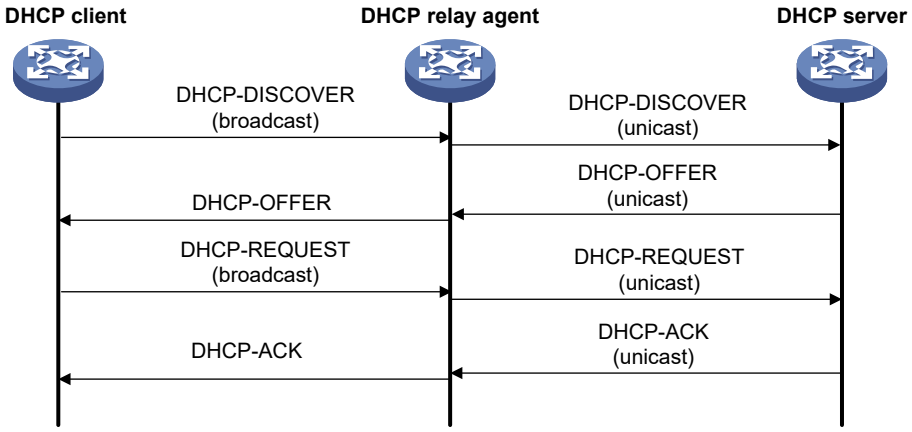


図 8-2 DHCP リレーエージェントの動作

8.1.2 DHCP リレーエージェントのオプション 82 のサポート

オプション 82 は DHCP クライアントの位置情報を記録します。オプション 82 は以下の作業を行います。

- セキュリティとアカウンティングのため、DHCP クライアントの位置を示します。
- DHCP クライアントに指定した範囲の IP アドレスを割り当てます。

詳細は、オペレーションマニュアルのセクション 4 *IP サービス* "*DHCP の概要*"を参照してください。

DHCP リレーエージェントがオプション 82 をサポートしている場合、表 8-1に示されている処理方法に従って、DHCP 要求を処理します。

DHCP サーバからの返答にオプション 82 が含まれている場合は、DHCP リレーエージェントがクライアントに応答を転送する前にオプション 82 を取り除きます。

表 8-1 DHCP リレーエージェントのオプション 82 の処理方法

クライアントの要求メッセージに含まれるオプション	処理方法	DHCP リレーエージェントの動作
Option 82	Drop	メッセージを廃棄します。
	Keep	オプション82を変更せずにメッセージを転送します。
	Replace	元のオプション82を設定されたパディング形式、パディングの内容、コードタイプに従って、新しいオプション82に置き換えてからメッセージを転送します。
No Option 82	–	設定されたパディング形式、パディングの内容、コードタイプに従って、元のオプション82に追加し、メッセージを転送します。

8.2 DHCPリレーエージェント設定作業リスト

作業リスト
（必須設定項目）DHCPの有効化
（必須設定項目）インタフェースでのDHCPリレーエージェントの有効化
（必須設定項目）リレーエージェントのDHCPサーバの指定
（オプション設定項目）DHCPリレーエージェントセキュリティ機能の設定
（オプション設定項目）DHCPリレーエージェントでのIPアドレスのリリース設定
（オプション設定項目）オプション82の設定
（オプション設定項目）DHCPリレーエージェントが送信したDHCPパケットのDHCP値の設定
（オプション設定項目）giaddrフィールドにDHCPリレーエージェントアドレスを設定

8.3 DHCPの有効化

ほかの DHCP リレーエージェントの設定を有効にするために、DHCP を有効にしてください。

以下に DHCP の有効化の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. DHCP を有効にする	**dhcp enable**	デフォルト：無効

8.4 インタフェースでのDHCPリレーエージェントの有効化

DHCP リレーエージェントが有効なとき、インタフェースは DHCP サーバに受信した DHCP 要求を転送します。

DHCP リレーエージェントのインタフェースの IP アドレスが含まれる IP アドレスプールは DHCP サーバに設定する必要があります。そうでない場合、DHCP リレーエージェントに接続される DHCP クライアントは IP アドレスを取得できません。

以下にインタフェースでの DHCP リレーエージェントの有効化の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. interface view に移行する	**interface** *interface-type interface-number*	―
3. DHCP リレーエージェントを有効にする	**dhcp select relay**	デフォルト：DHCPが有効にされたとき、インタフェースはDHCPサーバモードで動作します。

8.5 リレーエージェントのDHCPサーバの指定

可用性を向上するため、DHCP リレーエージェントでいくつかの DHCP サーバを指定することができます。インタフェースがクライアントから要求メッセージを受信したとき、リレーエージェントはすべての DHCP サーバに要求メッセージを転送します。

リレーエージェントで DHCP サーバアドレスを指定するとき、以下のガイドラインに従ってください。

- 指定された DHCP サーバアドレスは、リレーエージェントインタフェースの IP アドレスと異なるサブネットにする必要があります。そうでなければクライアントは IP アドレスの取得に失敗します。
- 最大 8 つの DHCP サーバを指定することができます。

以下にリレーエージェントに DHCP サーバアドレスの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. interface view に移行する	**interface** *interface-type interface-number*	―
3. リレーエージェントに DHCP サーバアドレスを指定する	**dhcp relay server-address** *ip-address*	デフォルト：指定なし

8.6 DHCPリレーエージェントセキュリティ機能の設定

8.6.1 DHCP リレーエージェントのリレーエントリの記録の有効化

DHCP から IP アドレスを取得した後、クライアントの IP アドレスと MAC アドレスバインディング情報（リレーエントリ）を自動的に記録することができます。

ARP アドレスチェック、IP ソースガードのようないくつかのセキュリティ機能は、入力パケットを確認するため、記録されたリレーエントリを使用し、エントリにマッチしないパケットをブロックします。ブロックすることで、不正なホストがリレーエージェントを通して外部ネットワークにアクセスできないようにします。たとえば、セキュリティ機能には ARP アドレスの確認、許可 ARP、IP ソースガードがあります。

以下に DHCP リレーエージェントのリレーエントリの記録を有効にする設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. DHCP リレーエージェントのリレーエントリの記録を有効にする	**dhcp relay client-information record**	デフォルト：無効

8.6.2 ダイナミックリレーエントリの定期的な更新の有効化

DHCP クライアントは DHCP サーバに IP アドレスをリリースするため、DHCP-RELEASE メッセージをユニキャストします。DHCP リレーエージェントは DHCP サーバにメッセージを送信し、クライアントの IP-MAC アドレスエントリを削除しません。

この機能で、DHCP リレーエージェントは DHCP サーバに DHCP-REQUEST メッセージを定期的に送信するため、以下の情報を使用します。

- リレーエントリの IP アドレス
- DHCP リレーインタフェースの MAC アドレス

DHCP リレーエージェントは DHCP サーバからの受信に従って、リレーエントリを保持します。

- サーバが DHCP-ACK メッセージを送信する、あるいは時間以内にメッセージを返信しない場合、DHCP リレーエージェントはリレーエントリを削除します。そして IP アドレスをリリースするため、DHCP サーバに DHCP-RELEASE メッセージを送信します。
- サーバが DHCP-NAK メッセージを返信する場合、リレーエージェントはエントリを保持します。

以下にダイナミックリレーエントリの定期的な更新の有効化の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. ダイナミックリレーエントリの定期的な更新を有効にする	**dhcp relay client-information refresh enable**	デフォルト：有効

8.7 DHCPリレーエージェントでのIPアドレスのリリース設定

クライアントの IP アドレスをリリースするためにリレーエージェントを設定します。リレーエージェントは DHCP-RELEASE メッセージをサーバに送信し、リレーエントリを削除します。DHCP-RELEASE メッセージを受信した DHCP サーバは IP アドレスをリリースします。

以下に IP アドレスをリリースするために DHCP リレーエージェントの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. IP アドレスをリリースするために DHCP リレーエージェントを設定する	**dhcp relay release ip** *client-ip*	このコマンドでは、DHCPリレーエージェントでリレーエントリが記録されたIPアドレスのみリリースすることができます。

8.8 オプション82の設定

オプション 82 を設定するとき、以下のガイドラインに従ってください。

- オプション 82 をサポートするため、関連する DHCP サーバと DHCP リレーエージェントの設定を実行してください。DHCP サーバのオプション 82 の設定については オペレーションマニュアルのセクション 4 *IP サービス "DHCP サーバ"*を参照してください。
- 要求メッセージの処理方法が replace である場合、オプション 82 のパディングモード、パディング形式を設定してください。要求メッセージの処理方法が keep あるいは drop である場合、オプション 82 のパディングモード、パディング形式を設定する必要はありません。
- オプション 82 のサブオプション 1 が設定されている場合、ノードの装置名（**sysname**）でパディングされている場合、装置名はスペースを含んではいけません。スペースが含まれている場合、DHCP リレーエージェントはオプション 82 の追加、更新に失敗します。

以下にオプション 82 の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. interface view に移行する	**interface** *interface-type interface-number*	―
3. オプション 82 を動作できるようにリレーエージェントで有効にする	**dhcp relay information enable**	デフォルト：無効
4. （オプション設定項目）オプション 82 が含まれる要求メッセージの処理方法を設定する	**dhcp relay information strategy** { **drop** | **keep** | **replace** }	デフォルト：**replace**
5. （オプション設定項目）サーキット ID サブオプションのパディング内容とコードタイプを設定する	**dhcp relay information circuit-id** { **string** *circuit-id* | { **normal** | **verbose** [**node-identifier** { **mac** | **sysname** | **user-defined** *node-identifier* }] } [**format** { **ascii** | **hex** }] }	デフォルト：サーキット ID サブオプションのパディング内容は**normal**で、コードタイプは**hex**です。
6. （オプション設定項目）リモート ID サブオプションのパディング内容とコードタイプを設定する	**dhcp relay information remote-id** { **normal** [**format** { **ascii** | **hex** }] | **string** *remote-id* | **sysname** }	デフォルト：リモート ID サブオプションのパディング内容は**normal**で、コードタイプは**hex**です。

8.9 DHCPリレーエージェントが送信したDHCPパケットのDSCPの設定

パケットの DSCP は、パケットの優先度レベルを指定し、パケットの優先度に影響します。

以下に DHCP リレーエージェントが送信した DHCP パケットの DSCP の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. DHCP リレーエージェントが送信した DHCP パケットの DSCP を設定する	**dhcp dscp** *dscp-value*	デフォルト：56

8.10 giaddrフィールドにDHCPリレーエージェントアドレスを設定

I. スマートリレー機能について

デフォルトでは、リレーエージェントは、すべての要求を DHCP サーバにリレーする前に、それらの要求の **giaddr** フィールドにプライマリ IP アドレスをカプセル化するだけです。次に、DHCP サーバは、**giaddr** フィールドのアドレスと同じサブネット上の IP アドレスを選択します。サブネット上に割り当て可能なアドレスがない場合、DHCP サーバは IP アドレスを割り当てません。DHCP スマートリレー機能は、DHCP サーバが DHCP-OFFER メッセージを返送しない場合に、DHCP リレーエージェントがセカンダリ IP アドレスをカプセル化できるようにするために導入されました。

リレーエージェントは、DHCP サーバに要求を転送する前に、最初にプライマリ IP アドレスを **giaddr** フィールドにカプセル化します。DHCP-OFFER を受信しない場合、リレーエージェントはクライアントがプライマリ IP アドレスを使用して DHCP サーバに最大 2 つの要求を送信できるようにします。2 回再試行しても DHCP-OFFER が返されない場合、リレーエージェントはセカンダリ IP アドレスに切り替えます。それでも DHCP サーバが応答しない場合は、次のセカンダリ IP アドレスが使用されます。セカンダリ IP アドレスがすべて試行され、DHCP サーバが応答しなくなると、リレーエージェントはプライマリ IP アドレスから開始してプロセスを繰り返します。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. スマートリレー機能を有効に設定する	**dhcp smart-relay enable**	デフォルト：無効

8.11 DHCPリレーエージェントの表示と維持

すべての view で **display** コマンドを実行でき、user view で **reset** コマンドを実行できます。

操作	コマンド
インタフェース上のDHCPリレーエージェントのDHCPサーバ情報を表示する	**display dhcp relay server-address** [**interface** *interface-type interface-number*]
DHCPリレーエージェントのオプション82の設定情報を表示する	**display dhcp relay information** [**interface** *interface-type interface-number*]
DHCPリレーエージェントのリレーエントリを表示する	**display dhcp relay client-information** [**interface** *interface-type interface-number* | **ip** *ip-address*]
DHCPリレーエージェントのパケット統計情報を表示する	**display dhcp relay statistics** [**interface** *interface-type interface-number*]

操作	コマンド
DHCPリレーエージェントのリレーエントリを削除する	**reset dhcp relay client-information** [**interface** *interface-type interface-number* | **ip** *ip-address*]
DHCPリレーエージェントのパケット統計情報を削除する	**reset dhcp relay statistics** [**interface** *interface-type interface-number*]

8.12 DHCPリレーエージェント設定例

8.12.1 DHCP リレーエージェント設定例

I. ネットワーク要件

図 8-3に示すように、DHCP クライアントが別のサブネット上にある DHCP サーバから IP アドレスと設定パラメータを取得するため、Switch A に DHCP リレーエージェントを設定します。

DHCP リレーエージェントとサーバは異なるサブネットにあり、互いに通信できるようにするため、スタティックあるいはダイナミックルーティングを設定します。

クライアントとサーバ間の通信を行うため、DHCP サーバで設定を行います。DHCP サーバの設定については、オペレーションマニュアルのセクション 4 *IP サービス* "*DHCP サーバ*"を参照してください。

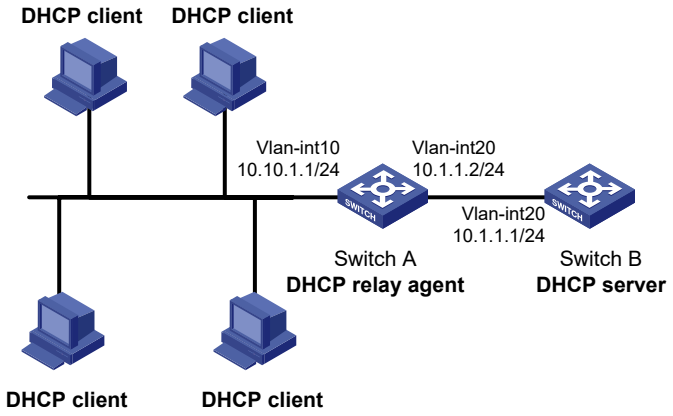


図 8-3 ネットワーク図

II. 設定手順

インタフェースの IP アドレスを指定します。（詳細は省略します。）

DHCP を有効にします。

```
<SwitchA> system-view
[SwitchA] dhcp enable
```

VLAN インタフェース 10 で DHCP リレーエージェントを有効にします。

```
[SwitchA] interface vlan-interface 10
[SwitchA-Vlan-interface10] dhcp select relay
```

リレーエージェントで DHCP サーバの IP アドレスを指定します。

```
[SwitchA-Vlan-interface10] dhcp relay server-address 10.1.1.1
```

III. 設定の確認

DHCP クライアントが DHCP リレーエージェントを通して DHCP サーバから IP アドレスとほかのネットワークパラメータを取得できることを確認します。（詳細は省略します。）

DHCP リレーエージェントによって転送された DHCP パケットの統計情報を表示します。

```
[SwitchA] display dhcp relay statistics
```

DHCP リレーエージェントの記録を有効にしている場合、リレーエントリを表示します。

```
[SwitchA] display dhcp relay client-information
```

8.12.2 オプション 82 設定例

I. ネットワーク要件

図 8-3に示すように、DHCP リレーエージェント（Switch A）は、DHCP サーバ（Switch B）に DHCP 要求を転送する前に、DHCP 要求のオプション 82 を置き換えます。

- サーキット ID サブオプションは **company001** です。
- リモート ID サブオプションは **device001** です。

オプション 82 を使用するため、オプション 82 を処理する DHCP サーバを有効にする必要があります。

II. 設定手順

インタフェースの IP アドレスを指定します。（詳細は省略します。）

DHCP を有効にします。

```
<SwitchA> system-view
[SwitchA] dhcp enable
```

VLAN インタフェース 10 で DHCP リレーエージェントを有効にします。

```
[SwitchA] interface vlan-interface 10
[SwitchA-Vlan-interface10] dhcp select relay
```

DHCP サーバの IP アドレスを指定します。

```
[SwitchA-Vlan-interface10] dhcp relay server-address 10.1.1.1
```

オプション 82 の処理方法とパディング内容を設定します。

```
[SwitchA-Vlan-interface10] dhcp relay information enable
[SwitchA-Vlan-interface10] dhcp relay information strategy replace
[SwitchA-Vlan-interface10] dhcp relay information circuit-id string company001
[SwitchA-Vlan-interface10] dhcp relay information remote-id string device001
```

8.12.3 DHCP サーバ選択の設定例

I. ネットワーク要件

図 8-4に示すように、DHCPクライアントと DHCPサーバは異なるサブネットにあります。

DHCP server 1、DHCP server 2 はサブネット 22.22.22.0/24 の IP アドレスが含まれる DHCP アドレスプールを持ちますが DHCP が無効です。DHCP クライアントが DHCP サーバからサブネット 22.22.22.0/24 の IP アドレス、ほかの設定パラメータを取得するため DHCP リレーエージェントを設定します。DHCP リレーエージェントは VLAN インタフェース 2 を通して DHCP クライアントに接続されています。DHCP リレーエージェントは VLAN インタフェース 3 を通して DHCP server 1 に接続されています。DHCP リレーエージェントは VLAN インタフェース 4 を通して DHCP server 2 に接続されています。

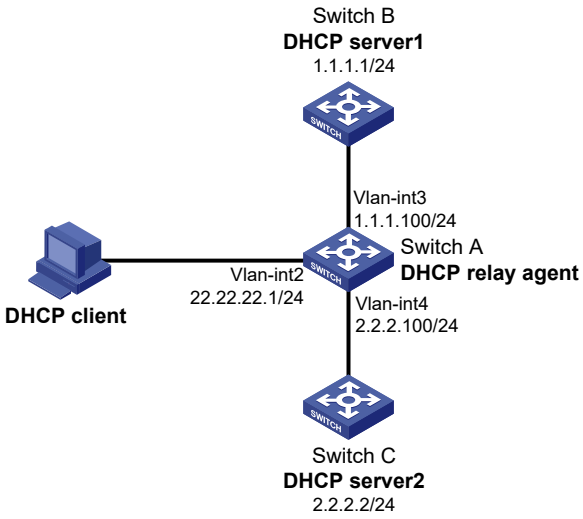


図 8-4 ネットワーク図

II. 設定手順

1) インタフェースの IP アドレスを指定します。（詳細は省略します。）
2) DHCP サーバとして Switch B、Switch C を設定します。（詳細は省略します。）
3) Switch A で DHCP リレーエージェントを設定します。

DHCP を有効にします。

```
<SwitchA> system-view
[SwitchA] dhcp enable
```

VLAN インタフェース 2 で DHCP リレーエージェントを有奥にします。

```
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] dhcp select relay
```

DHCP サーバの IP アドレスを指定します。

```
[SwitchA-Vlan-interface2] dhcp relay server-address 1.1.1.1
[SwitchA-Vlan-interface2] dhcp relay server-address 2.2.2.2
```

III. 設定の確認

DHCP クライアントが IP アドレスを取得し、30 秒の間に以下のログを出力することを確認します。

```
DHCPR/3/DHCPR_SERVERCHANGE: -MDC=1;
 Switched to the server at 2.2.2.2 because the current server did not respond.
```

DHCP サーバ 1.1.1.1 で DHCP を有効にします。（詳細は省略します。）

DHCP クライアントが IP アドレスを取得できず、3 分の間に以下のログを出力することを確認します。

```
DHCPR/3/DHCPR_SWITCHMASTER: -MDC=1;
 Switched to the master DHCP server at 1.1.1.1.
```

DHCP クライアントが IP アドレスを取得することを確認します。（詳細は省略します。）

8.13 DHCPリレーエージェントのトラブルシューティング

8.13.1 症状

DHCP クライアントが、DHCP リレーエージェントを通して設定パラメータを取得することができません。

8.13.2 分析

DHCP リレーエージェントあるいは DHCP サーバの設定に問題が発生している可能性があります。

8.13.3 解決策

問題を切り分けるため、デバッグを有効にし、DHCP リレーエージェントで **display** コマンドを実行します。デバッグ情報とインタフェース状態の情報を確認してください。

以下の項目を確認してください。

- DHCP サーバと DHCP リレーエージェントで DHCP が有効になっているかどうか確認してください。
- DHCP サーバが DHCP クライアントと同じサブネットでアドレスプールを持っているかどうか確認してください。
- DHCP サーバと DHCP リレーエージェントが互いに通信可能であることを確認してください。
- DHCP クライアントに接続される DHCP リレーエージェントのインタフェースで、DHCP サーバのアドレスが正しく設定されているかどうか確認してください。

目次

このセクションのページは **4-x-x** です。

9 章 DHCP クライアント 9-1
9.1 インタフェースでの DHCP クライアントの有効化 9-1
9.2 アドレス重複検出の有効化 9-1
9.3 DHCP クライアントが送信する DHCP パケットの DSCP の設定 9-2
9.4 DHCP クライアントの表示と維持 9-2
9.5 DHCP クライアント設定例 9-2
9.5.1 ネットワーク要件 9-2
9.5.2 設定手順 9-3
9.5.3 設定の確認 9-4

9章 DHCP クライアント

装置は DHCP クライアントが有効である場合、DHCP サーバから IP アドレスを含む設定パラメータを取得できます。

DHCP クライアントの設定は VLAN インタフェースでのみサポートします。

9.1 インタフェースでのDHCPクライアントの有効化

インタフェースで DHCP クライアントを有効にするため、以下のガイドラインに従ってください。

- IP アドレス要求の失敗数がシステムで定義した値に到達した場合、DHCP クライアントが有効なインタフェースはデフォルトの IP アドレスを使用します。
- インタフェースは何度も IP アドレスを取得することができますが、古い設定が新しい設定に上書きされ、新しい設定が適用されます。
- DHCP クライアントが有効になったインタフェースはセカンダリ IP アドレスを設定することができません。
- DHCP サーバから割り当てられた IP アドレスが装置上のほかのインタフェースの IP アドレスとネットワークセグメントを共有していた場合、インタフェースは割り当てられた IP アドレスを使用しません。その代わり、DHCP サーバから新しい IP アドレスを要求します。

以下にインタフェースでの DHCP クライアントの有効化の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. interface view に移行する	**interface** *interface-type interface-number*	―
3. インタフェースで DHCP クライアントを有効にする	**ip address dhcp-alloc**	デフォルト：無効

9.2 アドレス重複検出の有効化

DHCP クライアントは、ARP パケットを使用して IP アドレスの重複があるかどうかを検出します。攻撃者は、サーバが割り当てた IP アドレスを使用できなくさせるため、ARP 応答を送信し、IP アドレスのオーナーとして動作します。ARP 攻撃がネットワークに存在する場合、アドレス重複検出機能を無効にすることを推奨します。

以下にアドレス重複検出の有効化の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. アドレス重複検出を有効にする	**dhcp client dad enable**	デフォルト : インタフェースで有効

9.3 DHCPクライアントが送信するDHCPパケットのDSCPの設定

パケットの DSCP は、パケットの優先度レベルを指定し、パケットの優先度に影響します。

以下に DHCP クライアントが送信した DHCP パケットの DSCP の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. DHCP クライアントが送信する DHCP パケットの DSCP を設定する	**dhcp client dscp** *dscp-value*	デフォルト：56

9.4 DHCPクライアントの表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
DHCPクライアント情報を表示する	**display dhcp client** [**verbose**] [**interface** *interface-type interface-number*]

9.5 DHCPクライアント設定例

9.5.1 ネットワーク要件

図 9-2に示すように、LAN で Switch B は VLAN インタフェース 2 を通して DHCP サーバと接続し、IP アドレス、DNS サーバアドレス、スタティックルート情報を取得します。DHCP クライアントのアドレスはネットワーク 10.1.1.0/24 にあり、DNS サーバアドレスは 20.1.1.1、スタティックルートの 20.1.1.0/24 のネットワークのネクストホップアドレスは、10.1.1.2 です。

DHCP サーバは DHCP クライアントにスタティックルートの情報を割り当てるため、オプション 121 を使用します。図 9-1にオプション 121 のフォーマットを示します。Destination descriptor フィールドは、16 進数で記載されたサブネットマスク長、宛先ネットワークアドレスの情報が含まれます。この例では Destination descriptor は 18 14 01 01（10 進数でサブネットマスク長が 24、ネットワークアドレスが 20.1.1.0）です。ネクストホップアドレスは 0A 01 01 02（10 進数で 10.1.1.2）です。

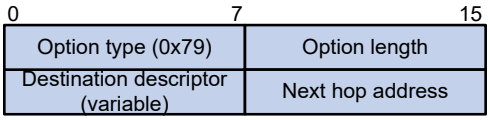


図 9-1 オプション 121 フォーマット

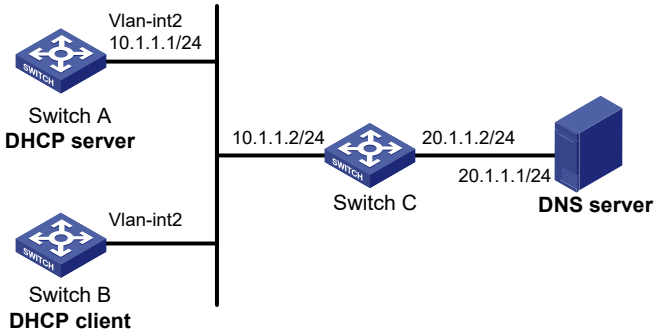


図 9-2 ネットワーク図

9.5.2 設定手順

1)　Switch A を設定します。

VLAN インタフェース 2 の IP アドレスを指定します。

```
<SwitchA> system-view
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ip address 10.1.1.1 24
[SwitchA-Vlan-interface2] quit
```

DHCP を有効にします。

```
[SwitchA] dhcp enable
```

自動割り当てから除外する IP アドレスを指定します。

```
[SwitchA] dhcp server forbidden-ip 10.1.1.2
```

DHCP アドレスプール 0 を設定します。サブネット、リース期間、DNS サーバアドレス、スタティックルートのサブネット 20.1.1.0/24 を指定します。

```
[SwitchA] dhcp server ip-pool 0
[SwitchA-dhcp-pool-0] network 10.1.1.0 mask 255.255.255.0
[SwitchA-dhcp-pool-0] expired day 10
[SwitchA-dhcp-pool-0] dns-list 20.1.1.1
[SwitchA-dhcp-pool-0] option 121 hex 18 14 01 01 0A 01 01 02
```

2)　Switch B を設定します。

IP アドレスを取得するため、VLAN インタフェース 2 で DHCP クライアントを有効にします。

```
<SwitchB> system-view
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] ip address dhcp-alloc
[SwitchB-Vlan-interface2] quit
```

9.5.3 設定の確認

Switch B に割り当てられた IP アドレス、他のネットワークパラメータを表示します。

```
[SwitchB-Vlan-interface2] display dhcp client verbose
Vlan-interface2 DHCP client information:
 Current state: BOUND
 Allocated IP: 10.1.1.3 255.255.255.0
 Allocated lease: 864000 seconds, T1: 331858 seconds, T2: 756000 seconds
 Lease from May 21 19:00:29 2012   to   May 31 19:00:29 2012
 DHCP server: 10.1.1.1
 Transaction ID: 0xcde72232
 Classless static routes:
   Destination: 20.1.1.0, Mask: 255.255.255.0, NextHop: 10.1.1.2
 DNS servers: 20.1.1.1
 Client ID type: acsii(type value=00)
 Client ID value: 000c.29d3.8659-Vlan2
 Client ID (with type) hex: 0030-3030-632e-3239-
                            6433-2e38-3635-392d-
                            4574-6830-2f30-2f32
 T1 will timeout in 3 days 19 hours 48 minutes 43 seconds
```

Switch B のルート情報を表示します。ルーティングテーブルにスタティックルートのネットワーク 20.1.1.0/24 が追加されています。

```
[SwitchB] display ip routing-table

Destinations : 11        Routes : 11

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
10.1.1.0/24         Direct 0    0            10.1.1.3        Vlan2
10.1.1.3/32         Direct 0    0            127.0.0.1       InLoop0
20.1.1.0/24         Static 70   0            10.1.1.2        Vlan2
10.1.1.255/32       Direct 0    0            10.1.1.3        Vlan2
127.0.0.0/8         Direct 0    0            127.0.0.1       InLoop0
127.0.0.0/32        Direct 0    0            127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0            127.0.0.1       InLoop0
127.255.255.255/32  Direct 0    0            127.0.0.1       InLoop0
224.0.0.0/4         Direct 0    0            0.0.0.0         NULL0
224.0.0.0/24        Direct 0    0            0.0.0.0         NULL0
255.255.255.255/32  Direct 0    0            127.0.0.1       InLoop0
```

目次

このセクションのページは**4-x-x** です。

10章 DHCPスヌーピング 10-1
10.1 概要 10-1
10.1.1 トラステッドポートと非トラステッドポートのアプリケーション 10-2
10.1.2 DHCP snoopingでのオプション82のサポート 10-3
10.2 DHCP snooping設定作業リスト 10-4
10.3 DHCP snoopingの基本機能の設定 10-4
10.4 オプション82の設定 10-5
10.5 DHCP snoopingの表示と維持 10-6
10.6 DHCP snooping設定例 10-6
10.6.1 DHCP snoopingの基本機能の設定例 10-6
10.6.2 オプション82設定例 10-8

10章 DHCP スヌーピング

⚠ **重要：**

VLAN マッピングとの併用はできません。

10.1 概要

DHCP スヌーピング（DHCP snooping）は、DHCP サーバと DHCP クライアント間でやりとりされる DHCP メッセージを監視して動的な IP ソースフィルタリングを行う機能です。本機能を利用することで、DHCP サーバを用いたネットワーク環境において、正当な DHCP クライアントにだけ IP 通信を許可することができる DHCP セキュリティ機能です。セキュリティの目的から DHCP クライアントの IP アドレスと MAC アドレスバインディング（DHCP snooping エントリと呼ばれます）を記録します。

DHCP snooping は DHCP サーバと DHCP リレーエージェント間では動作しません。

DHCP snooping は許可された DHCP サーバからのみ IP アドレスを取得することができるように、トラステッド（trusted）ポートと非トラステッド（untrusted）ポートを定義します。

- **トラステッド（Trusted）** – DHCP メッセージを正常に転送し、DHCP クライアントが承認された DHCP サーバから IP アドレスを取得できることを確実にします。
- **非トラステッド（Untrusted）** – 不正な DHCP サーバからの IP アドレスの割り当てを防ぐため、受信した DHCP-ACK パケットまたは DHCP-OFFER パケットを廃棄します。

DHCP snooping は DHCP snooping エントリを作成するため、トラステッドポートから受信した DHCP-ACK メッセージと、DHCP-REQUEST メッセージを読み込みます。DHCP snooping エントリはクライアントの MAC アドレスと IP アドレス、DHCP クライアントに接続するポート、VLAN 情報を含みます。

DHCP snooping エントリを使用するため、以下の機能が必要となります。

- **ARP detection** – 承認されたクライアントからの ARP パケットかどうか、DHCP Snooping エントリにもとづいて決定します。この機能は、不正なクライアントからの ARP 攻撃を防ぐことができます。詳細は、オペレーションマニュアルのセクション 9 *セキュリティ "ARP アタックプロテクション"*を参照してください。
- **IP ソースガード** – ポート毎に不正なパケットをフィルタするために使用します。詳細は、オペレーションマニュアルのセクション 9 *セキュリティ "IP ソースガード"* を参照してください。

10.1.1 トラステッドポートと非トラステッドポートのアプリケーション

DHCP サーバに接続されているポートをトラステッドポートとして設定し、他のポートを非トラステッドポートとして設定します。

図 10-1に示すように、DHCP サーバに接続している DHCP snooping 装置のポートをトラステッドポートとして設定します。トラステッドポートは DHCP サーバからクライアントに応答メッセージを転送します。許可されていない DHCP サーバに接続されている非トラステッドポートは入力した DHCP 応答メッセージを廃棄します。

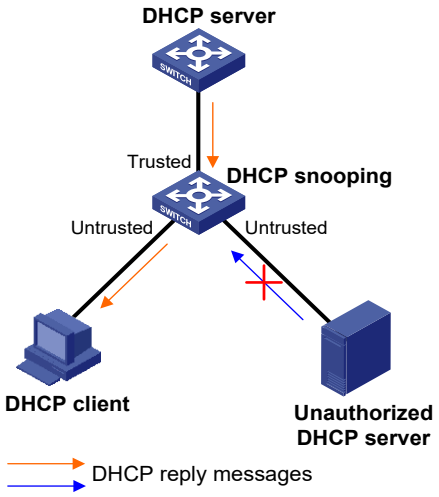


図 10-1 トラステッドポートと非トラステッドポート

図 10-2に示すようなカスケードネットワーク構成では、DHCP サーバに面しているポートはトラステッドポートとして設定する必要があります。システムリソースを節約するため、直接 DHCP クライアントに接続されている非トラステッドポートのみが、DHCP snooping エントリを記録することができます。

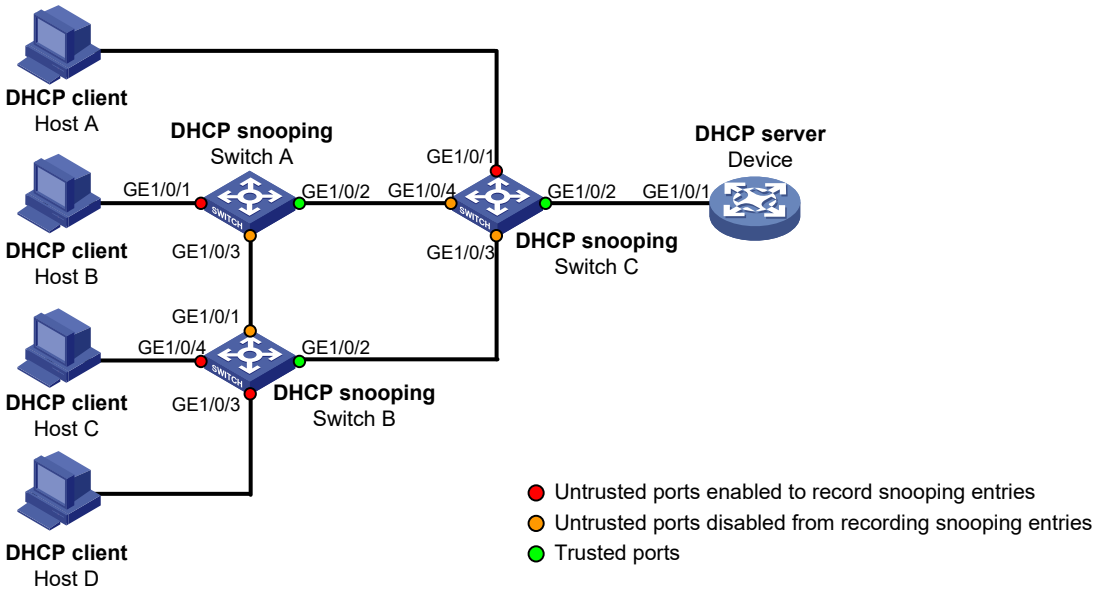


図 10-2 カスケードネットワーク構成のトラステッドポートと非トラステッドポート

10.1.2 DHCP snooping でのオプション 82 のサポート

オプション 82 は DHCP クライアントの位置情報を記録します。管理者はセキュリティとアカウンティングのため、DHCP クライアントを特定することができます。オプション 82 の詳細は、オペレーションマニュアルのセクション 4 *IP サービス* "*DHCP の概要*"を参照してください。

DHCP snooping は表 10-1に示すように、DHCP リクエストメッセージのオプション 82 を処理するため、DHCP リレーエージェントと同様の処理を行います。DHCP サーバからの応答にオプション 82 が含まれている場合は、クライアントに応答を転送する前に DHCP Snooping 装置がオプション 82 を取り除きます。応答にオプション 82 が含まれていない場合、そのまま転送します。

表 10-1 DHCP snooping の動作

クライアントの要求メッセージに含まれるオプション	処理方法	DHCP Snooping の動作
Option 82	Drop	メッセージを破棄します。
	Keep	オプション82を変更せずにメッセージを転送します。
	Replace	もとのオプション82を設定されたパディング形式、パディングの内容、コードタイプに従って、新しいオプション82に置き換えてからメッセージを転送します。
No Option 82	ー	設定されたパディング形式、パディングの内容、コードタイプに従って、もとのオプション82に追加し、メッセージを転送します。

10.2 DHCP snooping設定作業リスト

アグリゲーショングループに接続されているレイヤ 2 Ethernet インタフェースに DHCP snooping を設定する場合、アグリゲーショングループからインタフェースを削除するまで設定は適用されません。

作業リスト
（必須設定項目） DHCP snoopingの基本機能の設定
（オプション設定項目） オプション82の設定

10.3 DHCP snoopingの基本機能の設定

DHCP snooping の基本機能の設定を行うとき、以下のガイドラインに従ってください。

- 許可された DHCP サーバに接続されているポートをトラステッドポートとして指定し、DHCP クライアントが確実に有効な IP アドレスを取得できるようにします。トラステッドポートと、DHCP クライアントに接続されているポートは同じ VLAN 内になければなりません。
- レイヤ 2 Ethernet インタフェースとアグリゲートインタフェースは、トラステッドポートとして指定できます。アグリゲートインタフェースの詳細は、オペレーションマニュアルのセクション 3 *アクセス”リンクアグリゲーション”*を参照してください。
- アグリゲーショングループに追加された Ethernet インタフェースで DHCP snooping の設定を行う場合、アグリゲーショングループからインタフェースが削除されるまで設定内容は適用されません。
- QinQ で動作する DHCP snooping はクライアントから受信した DHCP パケットの VLAN タグを記録することができます。QinQ の詳細はオペレーションマニュアルのセクション 3 *アクセス”QinQ”*を参照してください。

以下に DHCP snooping の基本機能の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． DHCP snooping を有効にする	**dhcp snooping enable**	デフォルト：無効
3． interface view に移行する	**interface** *interface-type interface-number*	インタフェースはDHCPサーバに接続する必要があります。
4． トラステッドポートとしてポートを指定する	**dhcp snooping trust**	デフォルト：DHCP snoopingが有効になった後、すべてのポートは非トラステッドポートとなります。
5． system view に戻る	**quit**	ー
6． interface view に移行する	**interface** *interface-type interface-number*	インタフェースはDHCPクライアントに接続する必要があります。
7． （オプション設定項目）DHCP snooping エントリの記録を有効にする	**dhcp snooping binding record**	デフォルト：DHCP snoopingが有効になった後、DHCP snoopingエントリの記録は無効です。

10.4 オプション82の設定

オプション 82 を設定するとき、以下のガイドラインに従ってください。

- アグリゲーショングループに追加されたEthernetインタフェースでオプション82の設定を行う場合、アグリゲーショングループからインタフェースが削除されるまで設定内容は適用されません。
- オプション 82 をサポートする場合、DHCP サーバと DHCP snooping 装置の両方でオプション 82 を設定する必要があります。DHCP サーバのオプション 82 の設定の詳細はオペレーションマニュアルのセクション 4 *IP サービス "DHCP サーバ"*を参照してください。
- DHCP Snooping が有効になっている装置の処理方法が **replace** と設定されている場合、オプション 82 のパディングフォーマットを設定する必要があります。処理方法が **keep** または **drop** の場合は、パディングフォーマットを設定する必要はありません。
- オプション 82 がノードの装置名でパディングされる場合、装置名にスペースを含めることはできません。含まれている場合、DHCP Snooping が有効になっている装置はメッセージを破棄します。**sysname** コマンドを使用して装置名を指定することができます。コマンドの詳細は、コマンドマニュアルのセクション 1 *はじめに*”*装置管理*”を参照してください。
- 以下の状況のどちらかが存在している場合、verbose パディングフォーマットのオプション 82 のサブオプション 1 の VLAN ID フィールドを満たすため、“外部 VLAN タグ.内部 VLAN タグ”を使用します。
  - □ DHCP snooping と QinQ を同時に使用します。
  - □ DHCP パケットに 2 つの VLAN タグを含みます。

  たとえば、外部 VLAN タグが 10、内部 VLAN タグが 20 である場合、VLAN ID フィールドは 000a.0014 です。16 進数で表記される a は外部 VLAN タグ 10 を示し、16 進数で表記される 14 は内部 VLAN タグ 20 を示します。
- オプション 82 のサブオプション 1 がノードの装置名（**sysname**）でパディングされている場合、装置名はスペースを含んではいけません。スペースが含まれている場合、DHCP snooping はオプション 82 の追加、更新に失敗します。

以下にオプション 82 をサポートする DHCP snooping の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. interface view に移行する	**interface** *interface-type interface-number*	—
3. オプション 82 をサポートする DHCP snooping を有効にする	**dhcp snooping information enable**	デフォルト：無効
4. （オプション設定項目）オプション 82 が含まれている要求メッセージの処理方法を設定する	**dhcp snooping information strategy** { **drop** | **keep** | **replace** }	デフォルト：**replace**
5. （オプション設定項目）サーキット ID サブオプションのパディング内容とコードタイプを設定する	**dhcp snooping information circuit-id** { [**vlan** *vlan-id*] **string** *circuit-id* | { **normal** | **verbose** [**node-identifier** { **mac** | **sysname** | **user-defined** *node-identifier* }] } [**format** { **ascii** | **hex** }] }	デフォルト：パディング内容は**normal**、サーキットIDサブオプションは**hex**です。

操作	コマンド	補足
6.　（オプション設定項目）リモート ID サブオプションのパディング内容とコードタイプを設定する	**dhcp snooping information remote-id** { **normal** [**format** { **ascii** | **hex** }] | [**vlan** *vlan-id*] { **string** *remote-id* | **sysname** } }	デフォルト : パディング内容は**normal**、リモートIDサブオプションは**hex**です。

10.5 DHCP snoopingの表示と維持

すべての view で **display** コマンドを実行でき、user view で **reset** コマンドを実行できます。

操作	コマンド
DHCP snoopingエントリを表示する	**display dhcp snooping binding** [**ip** *ip-address* [**vlan** *vlan-id*]]
DHCP Snooping装置でオプション82の設定に関する情報を表示する	**display dhcp snooping information** { **all** | **interface** *interface-type interface-number* }
DHCP Snooping装置のDHCPパケット統計情報を表示する	**display dhcp snooping packet statistics** [**slot** *slot-number*]
トラステッドポートの情報を表示する	**display dhcp snooping trust**
DHCP snoopingエントリを削除する	**reset dhcp snooping binding** { **all** | **ip** *ip-address* [**vlan** *vlan-id*] }
DHCP Snooping装置のDHCPパケット統計情報を削除する	**reset dhcp snooping packet statistics** [**slot** *slot-number*]

10.6 DHCP snooping設定例

10.6.1 DHCP snooping の基本機能の設定例

I. ネットワーク要件

図 10-3に示すように設定します。GigabitEthernet 1/0/1 をトラステッドポートとして DHCP サーバに接続します。GigabitEthernet 1/0/3 は許可されていない DHCP サーバに接続します。GigabitEthernet 1/0/2 を通して DHCP クライアントに接続します。

DHCP サーバから応答を転送するため、許可されている DHCP サーバにのみ接続するように設定します。トラステッドポートから受信した DHCP-REQUEST メッセージと DHCP-ACK メッセージを確認することで、DHCP snooping がクライアントの IP-MAC バインディングを記録するようにします。

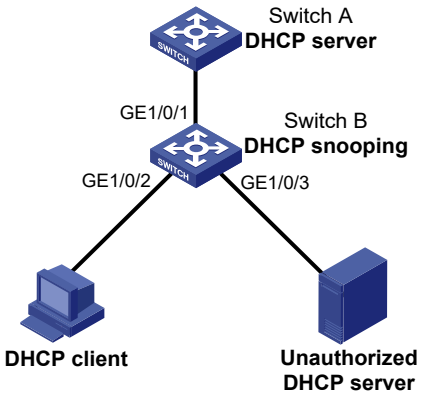


図 10-3 ネットワーク図

II. 設定手順

DHCP snooping を有効にします。

```
<SwitchB> system-view
[SwitchB] dhcp snooping enable
```

トラステッドポートとして GigabitEthernet 1/0/1 を設定します。

```
[SwitchB] interface gigabitethernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] dhcp snooping trust
[SwitchB-GigabitEthernet1/0/1] quit
```

GigabitEthernet 1/0/2 でクライアントの IP-MAC バインディングを記録することを有効にします。

```
[SwitchB] interface gigabitethernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] dhcp snooping binding record
[SwitchB-GigabitEthernet1/0/2] quit
```

III. 設定の確認

DHCP クライアントは許可された DHCP サーバからのみ IP アドレスと他の設定パラメータを取得できることを確認します。（詳細は省略します。）

クライアントの記録された DHCP snooping エントリを表示します。

```
[SwitchB] display dhcp snooping binding
```

10.6.2 オプション 82 設定例

I. ネットワーク要件

図 10-4に示すように、DHCP snooping を有効にし、以下のように Switch B のオプション 82 の設定を行います。

- オプション 82 が含まれる DHCP 要求の処理方法を **replace** に設定します。
- GigabitEthernet 1/0/2 のパディング内容のサーキット ID のサブオプションを **company001**、リモート ID サブオプションを **device001** に設定します。
- サーキット ID サブオプションの GigabitEthernet 1/0/3 のパディングフォーマットを **verbose**、アクセスノードの識別子を **sysname**、コードタイプを **ascii** に設定します。リモート ID サブオプションのパディングフォーマットを **device001** に設定します。

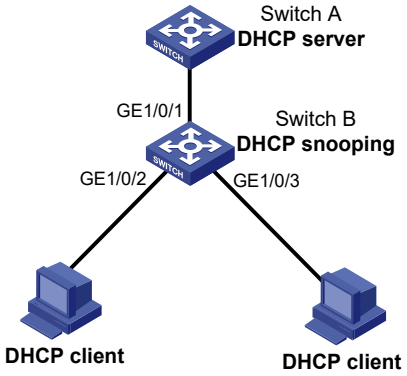


図 10-4 ネットワーク図

II. 設定手順

DHCP snooping を有効にします。

```
<SwitchB> system-view
[SwitchB] dhcp snooping enable
```

トラステッドポートとして GigabitEthernet 1/0/1 を設定します。

```
[SwitchB] interface gigabitethernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] dhcp snooping trust
[SwitchB-GigabitEthernet1/0/1] quit
```

GigabitEthernet 1/0/2 でオプション 82 を設定します。

```
[SwitchB] interface gigabitethernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] dhcp snooping information enable
[SwitchB-GigabitEthernet1/0/2] dhcp snooping information strategy replace
[SwitchB-GigabitEthernet1/0/2] dhcp snooping information circuit-id string company001
[SwitchB-GigabitEthernet1/0/2] dhcp snooping information remote-id string device001
```

```
[SwitchB-GigabitEthernet1/0/2] quit
```

GigabitEthernet 1/0/3 でオプション 82 を設定します。

```
[SwitchB] interface gigabitethernet 1/0/3
[SwitchB-GigabitEthernet1/0/3] dhcp snooping information enable
[SwitchB-GigabitEthernet1/0/3] dhcp snooping information strategy replace
[SwitchB-GigabitEthernet1/0/3] dhcp snooping information circuit-id verbose node-identifier sysname format ascii
[SwitchB-GigabitEthernet1/0/3] dhcp snooping information remote-id string device001
```

III. 設定の確認

DHCP snooping 装置の GigabitEthernet 1/0/2 と GigabitEthernet 1/0/3 のオプション 82 の設定情報を表示します。

```
[SwitchB] display dhcp snooping information
```

目次

このセクションのページは **4-x-x** です。

11 章 BOOTP クライアント 11-1
11.1 BOOTP アプリケーション 11-1
11.2 動的 IP アドレスの取得.....11-1
11.3 プロトコルと標準.....11-1
11.4 インタフェースでの BOOTP を使用した IP アドレスの取得の設定 11-2
11.5 BOOTP クライアントの表示と維持 11-2
11.6 BOOTP クライアントの設定例.....11-2
11.6.1 ネットワーク要件.....11-2
11.6.2 設定手順 11-3
11.6.3 設定の確認.....11-3

11章 BOOTP クライアント

BOOTP（ブートストラッププロトコル）は、コンピュータネットワークに接続されたクライアントが、IP アドレスやホスト名、サブネットマスク等を自動的に取得するためのプロトコルです。

BOOTP クライアントは VLAN インタフェースでのみサポートします。

11.1 BOOTPアプリケーション

BOOTP クライアントとして指定したインタフェースは BOOTP を使用して BOOTP サーバから情報（IP アドレスなど）を入手することができます。

BOOTP を使用するため、管理者は各 BOOTP クライアントに対し BOOTP パラメータファイルを BOOTP サーバ上に用意する必要があります。パラメータファイルには、BOOTP クライアントの IP アドレス、MAC アドレスなどの情報が含まれます。BOOTP クライアントが BOOTP サーバに要求を送信すると、BOOTP サーバは BOOTP パラメータファイルを検索し、対応する設定情報を返信します。

一般的に BOOTP は安定した環境で使用します。ネットワーク環境が頻繁に変わる場合、DHCP が適しています。

DHCP サーバは BOOTP クライアントと相互に対応しています。そのため、BOOTP クライアントの IP アドレスを変更する場合、BOOTP サーバを使用しないで DHCP サーバを使用することができます。

11.2 動的IPアドレスの取得

BOOTP クライアントは以下のように BOOTP サーバから動的に IP アドレスを取得します。

1) BOOTP クライアントは自身の MAC アドレスを含めた、BOOTP 要求をブロードキャストします。
2) BOOTP サーバは、BOOTP 要求を受信するとクライアントの MAC アドレスに対応する IP アドレスの情報を検索します。
3) BOOTP サーバは BOOTP クライアントに BOOTP 応答を返信します。
4) BOOTP クライアントは受信した応答から IP アドレスを取得します。

DHCP サーバは BOOTP サーバの代わりに動的に IP アドレスを取得することができます。

11.3 プロトコルと標準

- RFC 951, *Bootstrap Protocol (BOOTP)*
- RFC 2132, *DHCP Options and BOOTP Vendor Extensions*
- RFC 1542, *Clarifications and Extensions for the Bootstrap Protocol*

11.4 インタフェースでのBOOTPを使用したIPアドレスの取得の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. interface view に移行する	**interface** *interface-type interface-number*	―
3. インタフェースで BOOTP を使用した IP アドレスの取得を設定する	**ip address bootp-alloc**	デフォルト：設定なし

11.5 BOOTPクライアントの表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
BOOTPクライアント情報を表示する	**display bootp client** [**interface** *interface-type interface-number*]

11.6 BOOTPクライアントの設定例

11.6.1 ネットワーク要件

図 11-1に示すように、Switch B の VLAN10 に属しているポートは、LAN に接続しています。VLAN インタフェース 10 は BOOTP を使用して DHCP サーバから IP アドレスを取得します。

BOOTP クライアントが DHCP サーバから IP アドレスを取得するため、DHCP サーバの設定を行う必要があります。詳細はオペレーションマニュアルのセクション 4 *IP サービス”DHCP サーバ”*を参照してください。

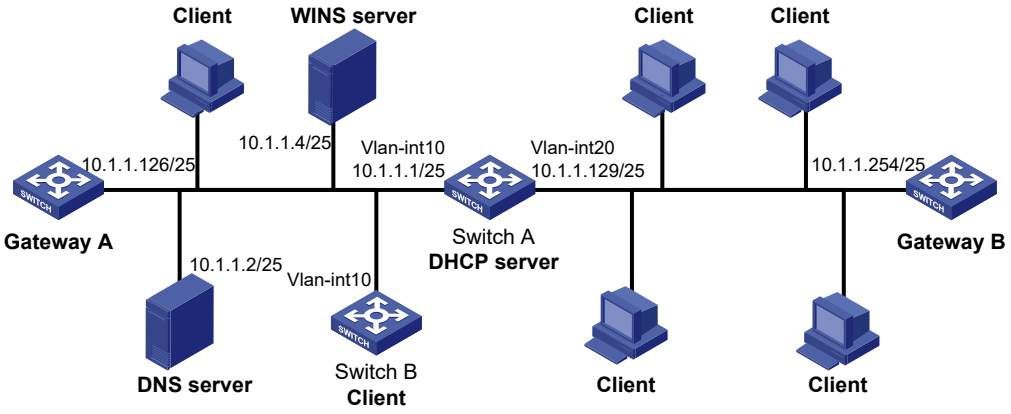


図 11-1 ネットワーク図

11.6.2 設定手順

以下の手順は、Switch B をクライアントとして動作させる設定です。

VLAN インタフェース 10 が DHCP サーバから動的に IP アドレスを取得できるように設定します。

```
<SwitchB> system-view
[SwitchB] interface vlan-interface 10
[SwitchB-Vlan-interface10] ip address bootp-alloc
```

11.6.3 設定の確認

BOOTP クライアントに割り当てられている IP アドレスを表示します。

```
[SwitchB] display bootp client
```

目次

このセクションのページは **4-x-x** です。

12 章 DNS 12-1
12.1 概要 12-1
12.1.1 スタティックドメイン名解決 12-1
12.1.2 ダイナミックドメイン名解決 12-1
12.1.3 DNS プロキシ 12-3
12.2 DNS 設定作業リスト 12-4
12.3 IPv4 DNS クライアントの設定 12-4
12.3.1 スタティックドメイン名解決の設定 12-4
12.3.2 ダイナミックドメイン名解決の設定 12-4
12.4 DNS プロキシの設定 12-5
12.5 送信される DNS パケットの DSCP 値の設定 12-5
12.6 IPv4 DNS の表示と維持 12-6
12.7 IPv4 DNS 設定例 12-6
12.7.1 スタティックドメイン名解決の設定例 12-6
12.7.2 ダイナミックドメイン名解決の設定例 12-7
12.7.3 DNS プロキシの設定例 12-10
12.8 IPv4 DNS 設定のトラブルシューティング 12-12
12.8.1 症状 12-12
12.8.2 解決策 12-12

12章 DNS

12.1 概要

DNS（Domain Name System）は、DNS サーバから DNS プロトコルを介してホスト名を IP アドレスにマッピングできる分散データベースです。各固有の IP アドレスには、ホスト名を関連付けることができます。

ドメイン名－IP アドレスのマッピングは DNS エントリと呼ばれます。

DNS サービスには、スタティックとダイナミックの 2 種類があります。ユーザが名前を指定したのち、装置はスタティックの名前解決のデータベースで IP アドレスを調べます。有効な IP アドレスがない場合、ダイナミック（動的）な名前を解決するために DNS サーバに問い合わせを行います。これは、スタティック（静的）な名前解決の場合よりも時間がかかります。そこで効率化のために、よく照会される名前と IP アドレスのマッピングがローカルのスタティックな名前解決のデータベーステーブルに保存されています。

12.1.1 スタティックドメイン名解決

スタティックドメイン名解決は、ドメイン名と IP アドレスの間にマッピングを手動でマッピングを作成します。たとえば、Telnet などのアプリケーションを使用する際に、装置のスタティックドメイン名解決のマッピングを作成することができます。

12.1.2 ダイナミックドメイン名解決

I. 解決手段

1) ユーザプログラムは、DNS クライアントの解決者にネームクエリを送信します。
2) DNS の解決者は、ローカルでドメイン名を適合させるためにキャッシュを調べます。適合するものがあれば、それに対応する IP アドレスを返送します。適合するものがなければ、DNS サーバにネームクエリを送信します。
3) DNS サーバはドメイン名を適合させるために名前解決のデータベースを調べます。適合するものがなければ、他のより高レベルの DNS サーバにネームクエリを送信します。このプロセスは、結果（成功、もしくは失敗）が返ってくるまで続けられます。
4) DNS サーバから応答を受信した後、DNS クライアントはユーザプログラムに解決結果を返信します。

図 12-1に、ユーザプログラム、DNS クライアントおよび DNS サーバ間の関係を示しています。

解決者（Resolver）とキャッシュ（Cache）は DNS クライアントによって構成されます。通常、ユーザプログラムと DNS クライアントは同じ装置あるいは異なる装置で動作しますが、DNS サーバと DNS クライアントが異なる装置間で動作します。

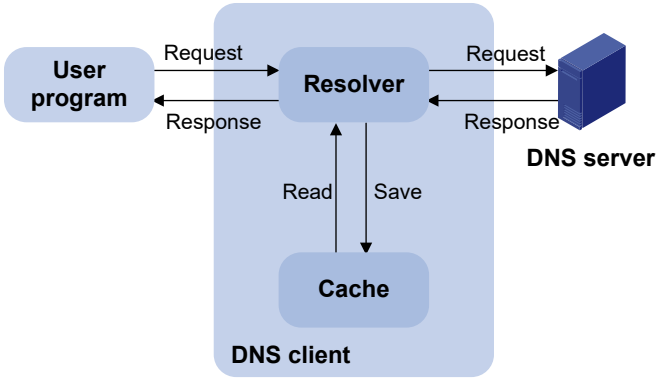


図 12-1 ダイナミックドメイン名解決

ダイナミックドメイン名解決は、DNS クライアントがダイナミックドメイン名のキャッシュに、DNS エントリを格納するようにします。有効期間内に度重なるクエリ用に DNS 要求を DNS サーバに送信する必要はありません。有効期間が満了したとき、DNS サーバからのエントリが最新であることを確認するため、DNS エントリを削除します。DNS サーバはマッピングの有効な期間を決定します。DNS クライアントは DNS 応答からエージング情報を取得します。

II. DNS サフィックス

DNS クライアントは、通常、ユーザによって定義することのできるサフィックスのリストを保持します。それは解決する名前が完全に一致しないときに使用します。解決者は不明な部分を提供することができます。

たとえば、ユーザは aabbcc.com のためのサフィックスとして com を設定することができます。これによって、ユーザは、aabbcc を入力するだけで aabbcc.com の IP アドレスを取得することができます。解決者は DNS サーバに名前を通過させる前に、サフィックスとデリミタ（区切り記号）を付加します。

名前解決は、ユーザが入力したドメインネームにもとづくクエリを処理します。

- ユーザがドット（.）なしでドメイン名を入力した場合（たとえば aabbcc）、解決者は、ホスト名と認識し、処理する前にホスト名に DNS サフィックスを追加します。すべての DNS の検索に失敗した場合、解決者は、IP アドレスのクエリのためにユーザが入力したドメイン名（たとえば aabbcc）を使用します。
- 文字の間にドメイン名にドット（.）がある場合（たとえば www.aabbcc）、解決者は、最初に DNS の検索を行うために、このドメイン名を直接使用します。DNS の検索に失敗した場合、解決者は、他の DNS を検索するために DNS サフィックスを追加します。
- ドメイン名の末尾にドット（.）がある場合（たとえば、aabbcc.com.）、解決者は、ドメイン名を FQDN（Fully Qualified Domain Name、完全修飾ドメイン名）と認識し、クエリが正常に処理されたかエラーが発生したか、結果が解決者から返信されます。このため、ドメイン名末尾のドット（.）は終端記号と認識されます。

装置は、スタティック DNS サービスおよびダイナミック DNS サービスをサポートしています。

DNS サーバでドメイン名にエイリアスが設定されている場合、そのエイリアスをホストの IP アドレスに変換できます。

12.1.3 DNS プロキシ

図 12-2に示すように、DNS プロキシは以下のように動作します。

- DNS クライアント（DNS client）は DNS プロキシ（DNS proxy）に DNS 要求を送信します。
- DNS プロキシから指定された DNS サーバ（DNS server）に転送されます。DNS サーバからの応答は DNS プロキシを通して DNS クライアントに送信されます。

DNS プロキシは、ネットワーク管理を容易にします。DNS サーバのアドレスが変更された場合、DNS プロキシの設定を変更するだけで、各 DNS クライアントの設定を変更する必要がなくなります。

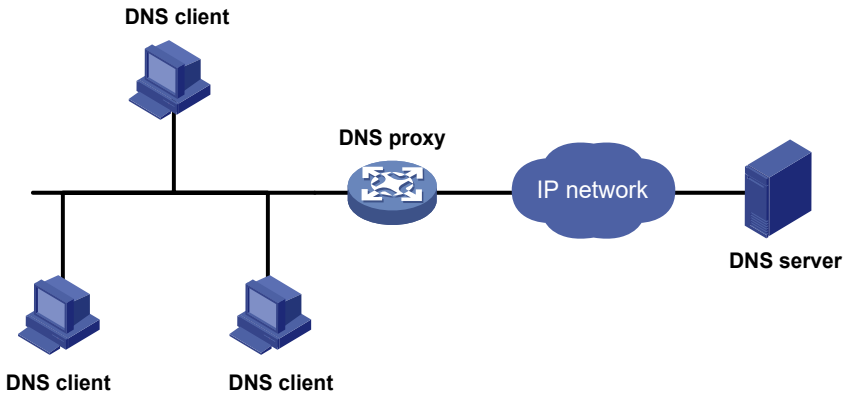


図 12-2 DNS プロキシアプリケーション

DNS プロキシは以下のように動作します。

1) DNS クライアントは DNS プロキシを DNS サーバと認識し、DNS プロキシに DNS 要求を送信します。つまり、要求の宛先アドレスは DNS プロキシの IP アドレスです。
2) DNS プロキシは、要求を受信すると、ローカルスタティックドメイン名解決テーブルおよびダイナミックドメイン名解決テーブルを検索します。要求された情報がテーブル内にあれば、DNS プロキシはクライアントに DNS 応答を返します。
3) 要求された情報が見つからない場合は、DNS プロキシから指定の DNS サーバに要求が送信され、ドメイン名の解決を行います。
4) DNS サーバから応答を受け取ると、DNS プロキシは IP アドレス－ドメイン名のマッピングを記録し、応答を DNS クライアントに転送します。

DNS サーバが存在しない、あるいは、指定された DNS サーバへのルートがない場合、DNS プロキシは DNS 要求を転送しません。

12.2 DNS設定作業リスト

作業リスト
IPv4 DNSクライアントの設定
（オプション設定項目） DNSプロキシの設定
（オプション設定項目） 送信されるDNSパケットのDSCP値の設定

12.3 IPv4 DNSクライアントの設定

12.3.1 スタティックドメイン名解決の設定

スタティックドメイン名解決は、IPv4 アドレスの代わりにホスト名を使用してホストに接続する Telnet のようなアプリケーションを提供します。

スタティックドメイン名解決の設定を行うとき、以下のガイドラインに従ってください。

- 各ホスト名は 1 つの IPv4 アドレスのみ割り当てられます。既にホスト名に割り当てられた IPv4 アドレスがある場合、最後に行われた設定が適用されます。
- IPv4 DNS エントリを最大 1024 まで設定することができます。

以下にスタティックドメイン名解決の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. スタティック名前解決テーブルでホスト名とIPv4アドレスの間のマッピングを設定する	**ip host** *host-name ip-address*	デフォルト：設定なし

12.3.2 ダイナミックドメイン名解決の設定

ダイナミックドメイン名解決を使用する場合、正しいサーバに DNS クエリを送信できるように DNS サーバを設定します。DNS サーバは DHCP を通して動的に取得した設定よりも、手動の設定が優先されます。複数設定を行った場合、最初に行った設定が優先されます。最初に最も高い優先度の DNS サーバにドメイン名解決リクエストを送信します。DNS サーバからの応答がない場合、順番に、2 番目の優先度のドメイン名解決リクエストが DNS サーバに送信されます。

加えて、取得したドメイン名を、システムが自動で追加するように DNS サフィックスを設定することができます。DNS サフィックスは DHCP を通して動的に取得した設定よりも、手動での設定が優先されます。複数設定を行った場合、最初に行った設定が優先されます。DNS 解決者は最初に最も高い優先度のサフィックスを使用します。名前解決に失敗した場合、順番に、2 番目の優先度のサフィックスを使用します。

I. 設定ガイドライン

ダイナミックドメイン名解決の設定を行うとき、以下のガイドラインに従ってください。

- DNS サーバは最大 6 台まで設定することができます。
- DNS サフィックスは最大 16 まで設定できます。

II. 設定手順

以下にダイナミックドメイン名解決の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. DNS サーバの IP アドレスを設定する	**dns server** *ip-address*	デフォルト：設定なし
3. （オプション設定項目）ドメイン名のサフィックスを設定する	**dns domain** *domain-name*	デフォルト：設定なし 定義済みのドメイン名のみ解決します。

12.4 DNSプロキシの設定

複数の DNS サーバを指定することができます。DNS プロキシは最も高い優先度の DNS サーバに要求を転送します。もし DNS サーバから応答がない場合、2 番目以降の優先度の DNS サーバに要求を転送します。

以下に DNS プロキシの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. DNS プロキシを有効にする	**dns proxy enable**	デフォルト：無効
3. DNS サーバの IP アドレスを指定する	**dns server** *ip-address*	デフォルト：指定なし

12.5 送信されるDNSパケットのDSCP値の設定

パケットの DSCP は、パケットの優先度レベルを指定し、パケットの優先度に影響します。DSCP が高いほど、優先度が高くなります。

以下に出力される DNS パケットの DSCP の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. 出力される DNS パケットの DSCP 値を設定する	● IPv4: **dns dscp** dscp-value ● IPv6: **ipv6 dns dscp** *dscp-value*	デフォルト：0 DNSクライアント、DNSプロキシの装置で有効です。

12.6 IPv4 DNSの表示と維持

すべての view で **display** コマンドを実行でき、user view で **reset** コマンドを実行できます。

操作	コマンド
ドメイン名解決テーブルを表示する	**display dns host** [**ip**]
IPv4 DNSサーバ情報を表示する	**display dns server** [**dynamic**]
DNSサフィックスを表示する	**display dns domain** [**dynamic**]
ダイナミックドメイン名キャッシュの情報を削除する	**reset dns host** [**ip**]

12.7 IPv4 DNS設定例

12.7.1 スタティックドメイン名解決の設定例

I. ネットワーク要件

図 12-3に示すように、Device は IP アドレスよりも、覚えやすいドメイン名を使用して、Host にアクセスします。

ドメイン名 host.com で IP アドレス 10.1.1.2 のホストにアクセスできるように、Device にスタティックドメイン名解決の設定を行います。

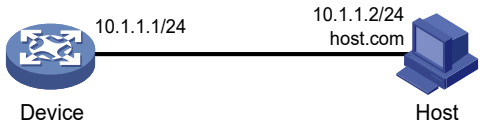


図 12-3 ネットワーク図

II. 設定手順

ホスト名 host.com と IP アドレス 10.1.1.2 のマッピングを設定します。

```
<Switch> system-view
[Switch] ip host host.com 10.1.1.2
```

ping host.com コマンドを使用します。Device がスタティックドメイン名解決により、host.com に対応する IP アドレスの 10.1.1.2 を取得できることを確認します。

```
[Switch] ping host.com
Ping host.com (10.1.1.2): 56 data bytes, press CTRL_C to break
56 bytes from 10.1.1.2: icmp_seq=0 ttl=255 time=1.000 ms
56 bytes from 10.1.1.2: icmp_seq=1 ttl=255 time=1.000 ms
56 bytes from 10.1.1.2: icmp_seq=2 ttl=255 time=1.000 ms
```

```
56 bytes from 10.1.1.2: icmp_seq=3 ttl=255 time=1.000 ms
56 bytes from 10.1.1.2: icmp_seq=4 ttl=255 time=2.000 ms

--- Ping statistics for host.com ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.000/1.200/2.000/0.400 ms
```

12.7.2 ダイナミックドメイン名解決の設定例

I. ネットワーク要件

図 12-4に示すように、Device を以下のように設定します。

- IP アドレスよりも、覚えやすいドメイン名を使用して Host にアクセスします。
- ダイナミック DNS を使用し、DNS Server に IP アドレスの要求を行います。

DNS Server の IP アドレスは 2.1.1.2/16 で、ドメインは com で、IP アドレス 3.1.1.1/16 とドメイン名 host のマッピングは com に保存されます。

DNS client として動作する Device でダイナミック DNS、DNS サフィックス com を設定します。Device は、Device がドメイン名 host.com と IP アドレス 3.1.1.1/16 で Host にアクセスできるように設定します。

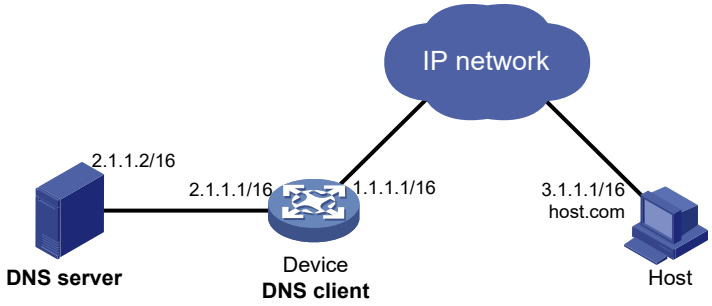


図 12-4 ネットワーク図

II. 設定手順

設定を行う前に、以下を確認してください。

- Device と Host が互いに通信可能できることを確認してください。
- インタフェースの IP アドレスが、図 12-4に示すように設定されていることを確認してください。

1) DNS server を設定します。

設定は DNS サーバによって異なります。以下の設定は、Windows 2008 R2 サーバで行われています。

a) “Start” > “Programs” > “Administrative Tools” > “DNS” を選択します。図 12-5 に示すようにDNS serverの設定ページが表示されます。

b) “Forward Lookup Zones” を右クリックし、“New zone” を選択します。指示に従って、新しいゾーンcomを作成します。

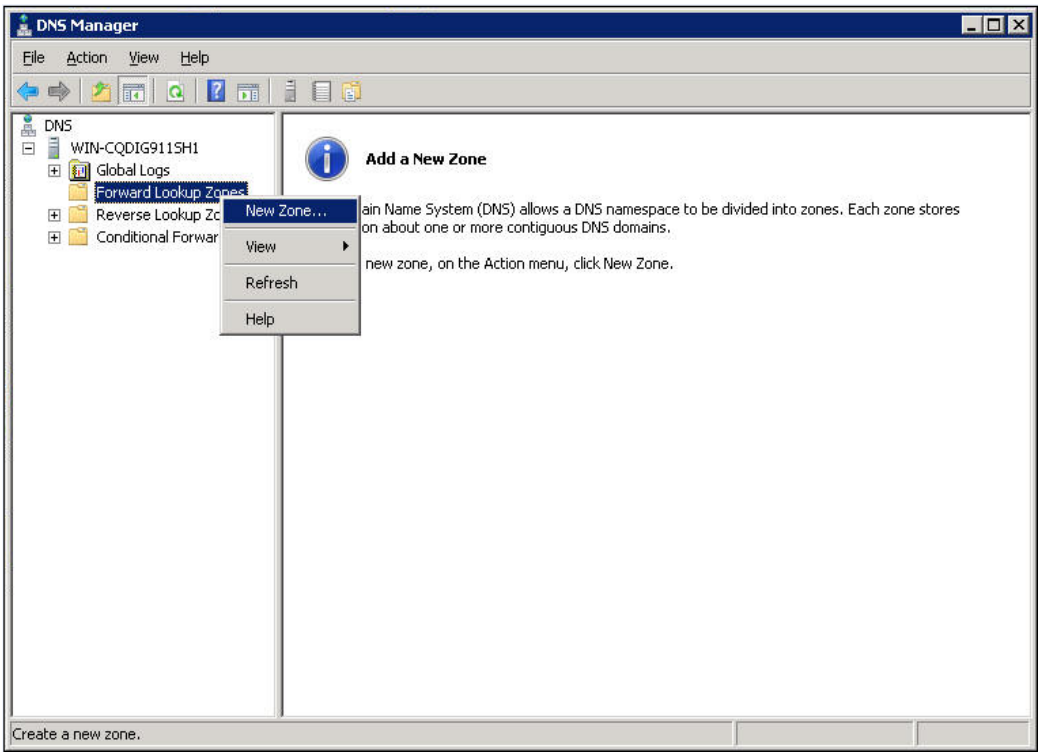


図 12-5 ゾーンの作成

c)　DNS server設定ページで、ゾーンcomを右クリックし、“New Host”を選択します。

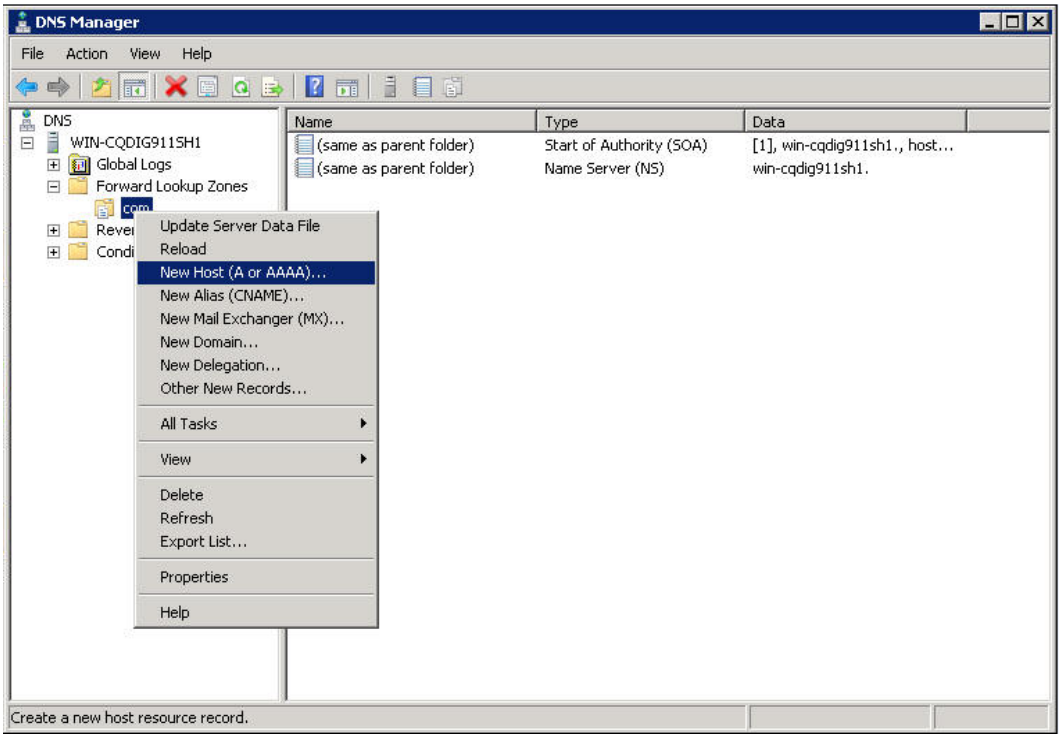


図 12-6 ホストの追加

d) ダイアログボックスで、ホスト名host、IPアドレス3.1.1.1を入力します。

e) “Add Host”をクリックします。IPアドレスとホスト名間のマッピングが作成されます。

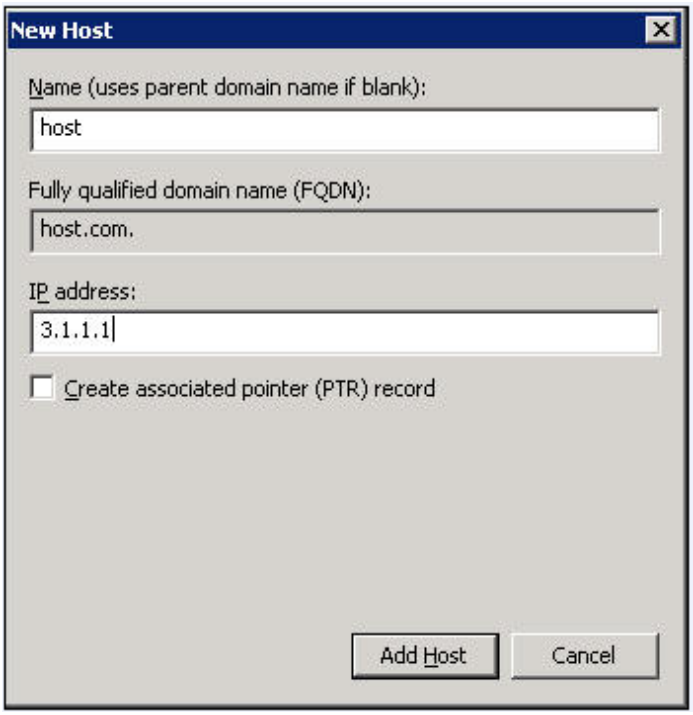


図 12-7 IP アドレスとホスト名間のマッピングの作成

2)　DNS client を設定します。

IP アドレスとして 2.1.1.2 を指定します。

```
<Switch> system-view
[Switch] dns server 2.1.1.2
```

#ドメイン名のサフィックスとして com を設定します。

```
[Switch] dns domain com
```

III. 設定の確認

Device で **ping** host コマンドを使用します。Device と host 間の通信が正常であり、ドメイン名 host.com に対応する宛先 IP アドレスが 3.1.1.1 であることを確認します。

12.7.3 DNS プロキシの設定例

I. ネットワーク要件

図 12-8に示すように Device B（DNS client）と DNS Server 間で DNS パケットを転送する DNS プロキシとして Device A を設定します。DNS Server の IP アドレスは 4.1.1.1 です。

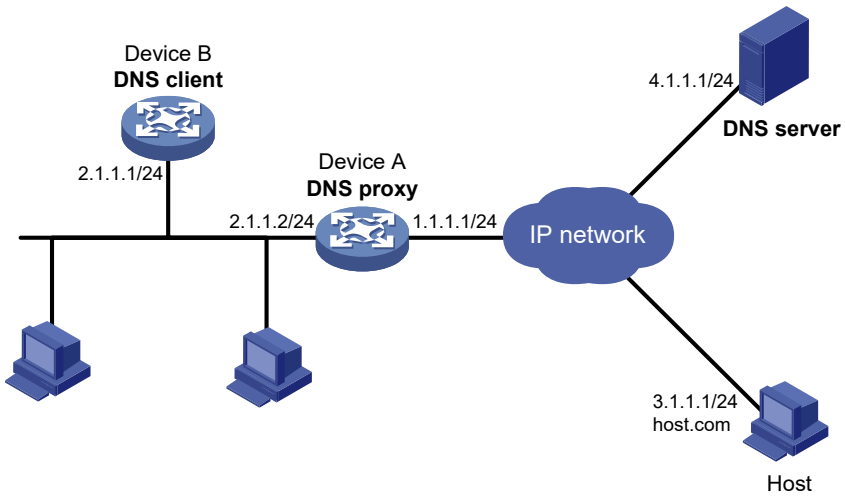


図 12-8 ネットワーク図

II. 設定手順

設定を行う前に、以下のことを確認してください。

- Device A と DNS Server、Host の間が互いに通信可能であることを確認してください
- インタフェースの IP アドレスが、図 12-8に示すように設定されていることを確認してください

1)　DNS サーバを設定します。

この設定は DNS サーバによって異なります。Windows 2008 R2 サーバを DNS サーバとして使用する場合、オペレーションマニュアルのセクション 4 *IP サービス*”*DNS*“の“*ダイナミックドメイン名解決の設定例*“を参照してください。

2)　DNS proxy を設定します。

DNS Server の IP アドレスとして、4.1.1.1 を指定します。

```
<DeviceA> system-view
[DeviceA] dns server 4.1.1.1
```

DNS プロキシを有効にします。

```
[DeviceA] dns proxy enable
```

3)　DNS client を設定します。

```
<DeviceB> system-view
```

DNS Server の IP アドレスとして、2.1.1.2 を指定します。

```
[DeviceB] dns server 2.1.1.2
```

III. 設定の確認

Device A で DNS プロキシが有効であることを確認します。

[DeviceB] ping host.com

```
Ping host.com (3.1.1.1): 56 data bytes, press CTRL_C to break
56 bytes from 3.1.1.1: icmp_seq=0 ttl=255 time=1.000 ms
56 bytes from 3.1.1.1: icmp_seq=1 ttl=255 time=1.000 ms
56 bytes from 3.1.1.1: icmp_seq=2 ttl=255 time=1.000 ms
56 bytes from 3.1.1.1: icmp_seq=3 ttl=255 time=1.000 ms
56 bytes from 3.1.1.1: icmp_seq=4 ttl=255 time=2.000 ms

--- Ping statistics for host.com ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.000/1.200/2.000/0.400 ms
```

12.8 IPv4 DNS設定のトラブルシューティング

12.8.1 症状

ダイナミックドメイン名解決を有効にした後、ユーザが正しい IP アドレスを取得することができません。

12.8.2 解決策

1) **display dns host ip** コマンドを使用して、指定されたドメイン名がキャッシュにあることを確認してください。
2) 定義済みのドメイン名がない場合、ダイナミックドメイン名解決を有効にし、DNS クライアントと DNS サーバ間の通信が可能なことを確認してください。
3) キャッシュに特定のドメイン名はあっても、IP アドレスが正しくない場合、DNS クライアントが DNS サーバの正しい IP アドレスであることを確認してください。
4) DNS サーバのドメイン名と IP アドレス間のマッピングが正しいことを確認してください。

目次

このセクションのページは **4-x-x** です。

13 章 IP フォワーディングの基本 13-1
13.1 FIB テーブル 13-1
13.2 FIB テーブルエントリの表示と維持.....13-2

13章 IP フォワーディングの基本

装置は、パケットを受信した際、FIB（forwarding information base）テーブルにマッチするかどうか検索するため、パケットの宛先 IP アドレスを使用します。マッチしたエントリを使用して、パケットを転送します。

13.1 FIBテーブル

装置はルーティングテーブルから最適なルートを選択し、FIB テーブルにルートを記載します。各 FIB エントリは、指定したサブネットあるいはホストにパケットを転送するため、ネクストホップの IP アドレスと出力インタフェースを指定しています。

ルーティングテーブルの詳細は、オペレーションマニュアルのセクション 5 *ルーティングプロトコル”IP ルーティングの基本*”を参照してください。

display fib コマンドを使用して FIB テーブルのエントリを表示します。以下に FIB テーブルの表示例を示します。

```
<Switch> display fib

Destination count: 4 FIB entry count: 4

Flag:
  U:Usable   G:Gateway   H:Host   B:Blackhole   D:Dynamic   S:Static
  R:Relay     F:FRR

Destination/Mask   Nexthop         Flag     OutInterface/Token       Label
10.2.0.0/16        10.2.1.1        U        GE1/0/1                  Null
10.2.1.1/32        127.0.0.1       UH       InLoop0                  Null
127.0.0.0/8        127.0.0.1       U        InLoop0                  Null
127.0.0.1/32       127.0.0.1       UH       InLoop0                  Null
```

FIB エントリは以下のアイテムが含まれます。

- **Destination** － 宛先 IP アドレスです。
- **Mask** － ネットワークマスクです。マスクと宛先アドレスは宛先ネットワークを識別します。宛先アドレスとネットワークマスク間の論理的 AND を行い、宛先ネットワークのアドレスを算出します。たとえば、宛先アドレスが 192.168.1.40、マスクが 255.255.255.0 であるとき、宛先ネットワークのアドレスは、192.168.1.0 です。ネットワークマスクは、2 進数で連続した 1 と 0 で構成され、最上位から連続した 1 の数で表されます。またドットを用いて 10 進数で表現されることもあります。
- **Nexthop** － ネクストホップの IP アドレスです。
- **Flag** － ルートのフラグです。
- **OutInterface** － 出力インタフェースです。
- **Token** － MPLS ラベルスイッチングパスインデックス番号です。
- **Label** － 内部ラベルです。

13.2 FIBテーブルエントリの表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
FIBエントリを表示する	**display fib** [*ip-address* [*mask* | *mask-length*]]

目次

このセクションのページは**4-x-x** です。

14章 IPパフォーマンスの最適化 14-1
14.1 ダイレクトブロードキャストの送受信の有効化 14-1
14.1.1 設定手順 14-1
14.1.2 設定例 14-2
14.2 インタフェースのMTUサイズの設定 14-3
14.3 TCP path MTU discoveryの設定 14-3
14.4 TCPバッファサイズの設定 14-4
14.5 TCPタイマの設定 14-4
14.6 ICMPエラーパケットの送信設定 14-5
14.7 ICMPエラーメッセージのレートリミットの設定 14-7
14.8 ICMPパフォーマンスの最適化の表示と維持 14-7

14章 IP パフォーマンスの最適化

装置の設定を最適化することで、IP パフォーマンス全体を最適にすることができます。この章では設定を最適化するための、さまざまな技術について記載します。

14.1 ダイレクトブロードキャストの送受信の有効化

ダイレクトブロードキャストパケットは、特定のネットワークのすべてのホストに送信されるブロードキャストパケットのことです。ダイレクトブロードキャストパケットの宛先 IP アドレスの、ネットワーク ID は宛先ネットワークを識別し、ホスト ID は値がすべて 1 です。

インタフェースが、ダイレクトブロードキャストをネットワークに転送することを許可した場合、ハッカーがこの機能を悪用し、宛先ネットワークに攻撃する可能性があります。しかし、あるシナリオではインタフェースが UDP ヘルパー、Wake on LAN をサポートするため、ダイレクトブロードキャストパケットのように送受信する必要があります。

UDP ヘルパー機能によって、インタフェースが直接接続されたネットワークからダイレクトブロードキャストパケットの送受信を有効にすることができます。UDP ヘルパーはダイレクトブロードキャストパケットをユニキャストパケットに変換し、特定のサーバへ転送することにより、本機能を有効にできます。

この処理は、インタフェースが直接接続されたネットワークへのダイレクトブロードキャストパケットを転送し、Wake on LAN をサポートするため、別のサブネットから受信します。Wake on LAN は宛先ネットワークのホストを起動させるためにダイレクトブロードキャストを送信します。

14.1.1 設定手順

以下に、インタフェースで、直接接続されたネットワークにダイレクトブロードキャストの送受信を有効にする設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． interface view に移行する	**interface** *interface-type interface-number*	―
3． 直接接続されたネットワークにダイレクトブロードキャストの送受信を有効にする	**ip forward-broadcast**	デフォルト：無効

14.1.2 設定例

I. ネットワーク要件

図 14-1に示すように、Host のデフォルトゲートウェイは Switch の VLAN インタフェース 3 の IP アドレス 1.1.1.2/24 です。

Server が Host から IP アドレス 2.2.2.255 にダイレクトブロードキャストを受信できるようにするため、VLAN インタフェース 2 が直接接続されたネットワークへのブロードキャストを転送できるように有効にします。



図 14-1 ネットワーク図

II. 設定手順

1)　Switch A を設定します。

VLAN インタフェース 2、VLAN インタフェース 3 の IP アドレスを設定します。

```
<SwitchA> system-view
[SwitchA] interface vlan-interface 3
[SwitchA-Vlan-interface3] ip address 1.1.1.2 24
[SwitchA-Vlan-interface3] quit
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ip address 2.2.2.2 24
```

VLAN インタフェース 2 で直接接続されたネットワークのダイレクトブロードキャストの転送を有効にします。

```
[SwitchA-Vlan-interface2] ip forward-broadcast
```

2)　Switch B を設定します。

ホストへのスタティックルートを設定します。

```
<SwitchB> system-view
[SwitchB] ip route-static 1.1.1.1 24 2.2.2.2
```

VLAN インタフェース 2 の IP アドレスを設定します。

```
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] ip address 2.2.2.1 24
```

設定を行った後、ホストでサブネットに直接接続されたブロードキャストアドレス 2.2.2.255 に ping を行った場合、Switch B の VLAN インタフェース 2 は ping パケットを受信できます。Switch で **ip forward-broadcast** コマンドの設定を削除した場合、インタフェースは ping パケットを受信することができません。

14.2 インタフェースのMTUサイズの設定

IPv4 パケットが出力インタフェースの MTU サイズを超えたとき、装置は、以下のどちらかの処理を行います。

- パケットのフラグメントが禁止されている場合、装置はパケットを廃棄します。
- パケットのフラグメントが許可されている場合、装置はパケットを分割し、フラグメントしたパケットを転送します。

フラグメントと再構築は、システムリソースを消費します。フラグメントを防ぐため、ネットワーク環境にもとづいて、適切にインタフェースの MTU サイズを設定します。

以下にインタフェースの MTU サイズの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． interface view に移行する	**interface** *interface-type interface-number*	―
3． インタフェースの MTU サイズを設定する	**ip mtu** *mtu-size*	デフォルト：設定なし

注意：
自装置が発信元となるパケットに対してフラグメントの動作をします。
自装置が中継するパケットに対しては、IPv4 パケットが出力インタフェースの MTU サイズを超えたとき、装置はパケットを廃棄します。

14.3 TCP path MTU discoveryの設定

重要：
TCP 経路のすべての装置は **ip unreachables enable** コマンドを使用して、ICMP エラーメッセージの送信を有効にする必要があります。

TCP path MTU discovery（RFC1191）は、TCP 接続の送信元と宛先間の経路 MTU を探索します。以下のように動作します。

1) TCP 送信元の装置はフラグメント禁止（DF）ビットを設定して、パケットを送信します。
2) ルータは、出力インタフェースで MTU サイズを超過したパケットを廃棄します。出力インタフェースの MTU サイズが含まれた ICMP エラーメッセージを送信します。
3) ICMP エラーメッセージを受信した TCP 送信元の装置は、TCP 接続の現在の経路 MTU を計算します。
4) TCP 送信元の装置は、MSS よりも小さい TCP セグメントの次のパケットを送信します。（MSS ＝ 経路 MTU － IP ヘッダ長 － TCP ヘッダ長）

MSS が 32 バイトよりも小さい状態で、もし TCP 送信元の装置が ICMP エラーメッセージを受信する場合、TCP 送信元の装置はパケットをフラグメントします。

RFC1191 をサポートしていないルータから ICMP エラーメッセージを受信した場合、出カインタフェースの MTU は 0 に設定されます。ICMP エラーメッセージを受信した際、TCP 送信元の装置は、RFC1191 に記載されているように TCP MSS を計算するため、MTU テーブルから、現在の経路 MTU よりも小さい経路 MTU を選択します。MTU テーブルは、68、296、508、1006、1280、1492、2002、4352、8166、17914、32000、65535 バイトの MTU 値を含んでいます。最小 TCP MSS の値はシステムで 32 バイトと決められているため、実際の最小 MTU は 72 バイトです。

TCP path MTU discovery を有効にした後、すべての新しい TCP 接続は、経路 MTU を見つけます。装置は IP のフラグメントを発生させないように MSS の計算をするため、経路 MTU を使用します。

経路上で最小リンク MTU が増加したとき、送信元の装置の経路 MTU を増加させることができるように、経路 MTU は以下に示すエージングメカニズムを使用します。

- TCP 送信元の装置が ICMP エラーメッセージを受信したとき、経路 MTU を減少させ、経路 MTU のエージングタイマを開始します。
- エージングタイマが終了した後、送信元の装置は、RFC1191 に記載されているように、MTU テーブルで大きい値の MSS を使用します。
- ICMP エラーメッセージを 2 分以内に受信しない場合、送信元の装置は、TCP 3WAY ハンドシェイクでネゴシエートできる最大の MSS の値まで MSS を増加させます。

以下に TCP path MTU discovery の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. TCP path MTU discovery を有効にする	**tcp path-mtu-discovery** [**aging** *age-time* | **no-aging**]	デフォルト：無効

14.4 TCPバッファサイズの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. TCP 受信/送信バッファのサイズの設定をする	**tcp window** *window-size*	デフォルト：63KB

14.5 TCPタイマの設定

以下の TCP タイマを設定することができます。

- **SYN wait timer** – SYN パケットを送信したのち、TCP は SYN wait タイマを開始します。SYN wait タイマ間隔以内に応答パケットを受信しない場合、TCP 接続は確立しません。
- **FIN wait timer** – TCP 接続が FIN_WAIT_2 状態に変更されるとき、FIN wait タイマを開始します。タイマ間隔以内に FIN パケットを受信しない場合、TCP 接続は終了します。FIN パケットを受信した場合、TCP 接続状態は TIME_WAIT に変わります。FIN パケットを受信しない場合、タイマを再スタートします。タイマが満了した場合、接続は切断されます。

以下に TCP タイマの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． TCP タイマを設定する	● TCP SYN waitタイマを設定する： **tcp timer syn-timeout** *time-value* ● TCP FIN waitタイマを設定する： **tcp timer fin-timeout** *time-value*	デフォルト： ● TCP SYN waitタイマ：75秒 ● TCP FIN waitタイマ：675秒

14.6 ICMPエラーパケットの送信設定

ICMP エラーパケットには、リダイレクトパケット、タイムアウトパケット、宛先到達不能パケットの 3 種類のパケットがあります。この機能は ICMP エラーメッセージの送信を有効にします。

- ICMP リダイレクトメッセージ

ホストはすべてのパケットをデフォルトゲートウェイに送信します。デフォルトゲートウェイは、以降のパケットを送信するために正しいネクストホップを再選択するよう、以下のルールで、ホストに ICMP リダイレクトパケットを送信します。

- □ 受信と送信が同じインタフェースです。
- □ 選択したルートがリダイレクトパケットで作成されていない、あるいは変更されていません。
- □ 選択されたルートが 0.0.0.0 の装置へのデフォルトルートではありません。
- □ 受信したパケットに送信元ルートオプションがありません。

ICMP リダイレクトパケット機能はホストの管理を簡略化し、最適なルートを見つけ出すために、ホストが正しいルーティングテーブルを徐々に確立することができます。

- ICMP タイムアウトパケット

装置は以下のルールで ICMP タイムアウトパケットを送信します。

- □ 以下の場合、装置は送信元に ICMP TTL Expired の ICMP エラーパケットを送信します。
  - □ 受信パケットが装置へのパケットではありません。
  - □ パケットの TTL フィールドが 1 です。
- □ 宛先が装置自身である IP データグラムの最初のフラグメントパケットを、装置が受信したとき、タイマを始動します。データグラムのすべてのフラグメントパケットを受信する前にタイマが満了した場合、装置は ICMP Fragment Reassembly Timeout の ICMP エラーパケットを送信します。

- ICMP 宛先到達不能パケット

装置は以下のルールで ICMP 宛先不能パケットを送信します。

- □ パケットを転送するためのルートとデフォルトルートが入手できない場合、
- □ 以下の場合、装置は ICMP Network Unreachable の ICMP エラーパケットを送信元に送信します。
  - □ パケットを転送するためのルートがありません。
  - □ ルーティングテーブルにデフォルトルートが存在しません。
- □ 以下の場合、装置は ICMP Protocol Unreachable の ICMP エラーパケットを送信元に送信します。
  - □ パケットの宛先が装置です。

- □ パケットのトランスポート層プロトコルが装置でサポートしていません。

🕮 **メモ：**

DHCP 対応の装置が ICMP エコー要求を送信しないで、ICMP エコー返答を受信する場合、装置はどのようなプロトコルの ICMP 到達不能のエラーパケットも送信元に送信しません。DHCP の詳細はオペレーションマニュアルのセクション 4 *IP サービス*”*DHCP の概要*”を参照してください。

- □ 以下の場合、装置は ICMP Port Unreachable の ICMP エラーパケットを送信元に送信します。
  - □ UDP パケットの宛先が装置です。
  - □ パケットのポート番号が実行中のプロセスと一致していません。
- □ 以下の場合、装置は ICMP Source Route Failed の ICMP エラーパケットを送信元に送信します。
  - □ パケットの送信元が、Strict Source Routing を使用しています。
  - □ 中継装置が、送信元により指定されたネクストホップが直接接続されていないことを検出しました。
- □ 以下の場合、装置は ICMP Fragmentation Needed and DF-set の ICMP エラーパケットを送信元に送信します。
  - □ パケット転送とき、送信インタフェースの MTU がパケットより小さいです。
  - □ パケットに DF セット（フラグメント禁止）が付与されています。

以下に ICMP エラーパケットの送信の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． ICMP エラーパケットの送信を有効にする	• ICMPリダイレクトパケットの送信を有効にする：**ip redirects enable** • ICMPタイムアウトパケットの送信を有効にする：**ip ttl-expires enable** • ICMP宛先到達不能パケットの送信を有効にする：**ip unreachables enable**	デフォルト：無効

多くの ICMP パケットを送信するとネットワークトラフィックが増加します。多くの ICMP エラーによる悪意のあるパケットを受信した場合、装置のパフォーマンスが下がります。

このような問題を防止するために、装置は ICMP エラーパケットを送信しないように設定を無効にすることができます。ICMP タイムアウトパケットの送信が無効のとき、装置は ICMP TTL Expired メッセージの ICMP エラーパケットを送信しません。ICMP Fragment Reassembly Timeout の ICMP エラーパケットは正常に送信します。

14.7 ICMPエラーメッセージのレートリミットの設定

ネットワークの混雑状態を引き起こす可能性のある短い期間内に、過度の ICMP エラーメッセージを送信することを避けるため、ICMP エラーメッセージの送信レートを制限することができます。トークンバケット（bucket）アルゴリズムは、1 つの ICMP エラーメッセージを示す 1 つのトークンが用いられます。バケットに入ることができるトークンの最大数に達するまで、トークンは指定された間隔でバケットに配置されます。ICMP エラーメッセージが送信されるときに、トークンはバケットから取り除かれます。バケットが空のときに、新しいトークンがバケットに配置されるまで、ICMP エラーメッセージは送信されません。

以下に ICMP エラーメッセージのレートリミットの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． ICMP エラーメッセージの間隔とトークンバケットサイズを設定する	**ip icmp error-interval** *interval* [*bucketsize*]	デフォルト：100ミリ秒間隔で最大10トークンが配置されます。 ICMPレートリミットを無効にするには、間隔を0ミリ秒に設定します。

14.8 ICMPパフォーマンスの最適化の表示と維持

すべての view で **display** コマンドを実行でき、user view で **reset** コマンドを実行できます。

操作	コマンド
RawIP接続の概要情報を表示する	**display rawip** [**slot** *slot-number*]
RawIP接続の詳細情報を表示する	**display rawip verbose** [**slot** *slot-number* [**pcb** *pcb-index*]]
TCP接続の概要情報を表示する	**display tcp** [**slot** *slot-number*]
TCP接続の詳細情報を表示する	**display tcp verbose** [**slot** *slot-number* [**pcb** *pcb-index*]]
UDP接続の概要情報を表示する	**display udp** [**slot** *slot-number*]
UDP接続の詳細情報を表示する	**display udp verbose** [**slot** *slot-number* [**pcb** *pcb-index*]]
IPパケットの統計情報を表示する	**display ip statistics** [**slot** *slot-number*]
TCPトラフィックの統計情報を表示する	**display tcp statistics** [**slot** *slot-number*]
UDPトラフィックの統計情報を表示する	**display udp statistics** [**slot** *slot-number*]
ICMPの統計情報を表示する	**display icmp statistics** [**slot** *slot-number*]
IPパケットの統計情報を削除する	**reset ip statistics** [**slot** *slot-number*]
TCPトラフィックの統計情報を削除する	**reset tcp statistics**

操作	コマンド
UDPトラフィックの統計情報を削除する	**reset udp statistics**

目次

このセクションのページは **4-x-x** です。

15 章 UDP ヘルパー.....15-1
15.1 概要.....15-1
15.2 設定の制限とガイドライン.....15-1
15.3 ブロードキャストパケットからユニキャストパケットへの変換.....15-1
15.4 UDP ヘルパーの表示と維持.....15-2
15.5 UDP ヘルパー設定例.....15-2
15.5.1 ブロードキャストをユニキャストに変換するための設定例.....15-2

15章 UDP ヘルパー

15.1 概要

UDP ヘルパーは、指定した UDP 宛先ポート番号にパケットを変換することができます。

- 受信した UDP ブロードキャストパケットをユニキャストパケットに変換し、転送します。
- 受信した UDP ブロードキャストパケットをマルチキャストパケットに変換し、転送します。

15.2 設定の制限とガイドライン

UDP ヘルパーを設定するとき、以下の制限とガイドラインに従ってください。

- 装置のインタフェースでは、直接接続されたネットワークへのダイレクトブロードキャストの受信はデフォルトで無効となっています。UDP ヘルパーを使用するため、interface view で **ip forward-broadcast** コマンドを実行してください。ダイレクトブロードキャストの送受信についての詳細は、オペレーションマニュアルのセクション 4 *IP サービス* "*IP パフォーマンスの最適化*"を参照してください。
- UDP ヘルパーは宛先ポート 67 および 68 を使用する DHCP ブロードキャストパケットを転送できません。UDP ポート番号は、**udp-helper port** コマンドを使用してポート 67 および 68 を除外してください。
- UDP ポート番号は、最大で 256 個を設定可能です。
- UDP パケットを転送する宛先 IP アドレスとして、最大 20 個設定が可能です。

15.3 ブロードキャストパケットからユニキャストパケットへの変換

UDP ヘルパーでは、UDP 宛先ポート番号で、UDP ブロードキャストパケットを転送するかを判断します。

UDP ブロードキャストパケットを受信した場合、UDP ヘルパーはパケットの UDP 宛先ポート番号が、設定された UDP ポートに一致するか確認します。

- 受信した UDP ブロードキャストパケットの UDP 宛先ポート番号が、設定されたポート番号に一致した場合、UDP ヘルパーはパケットをコピーし、設定されたユニキャストアドレスにコピーした宛先 IP アドレスを変換します。UDP ヘルパーはユニキャストアドレスにパケットを転送します。
- 受信した UDP ブロードキャストパケットの UDP 宛先ポート番号が、設定されたポート番号に一致しない場合、UDP ヘルパーはパケットを処理しません。

以下にブロードキャストをユニキャストに変換する設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. UDP ヘルパーを有効にする	**udp-helper enable**	デフォルト：無効
3. UDP ポート番号を指定する	**udp-helper port** { *port-number* | **dns** | **netbios-ds** | **netbios-ns** | **tacacs** | **tftp** | **time** }	デフォルト：指定なし
4. interface view に移行する	**interface** *interface-type interface-number*	ー
5. 宛先サーバの IP アドレスを指定する	**udp-helper server** *ip-address*	デフォルト：指定なし 複数の宛先サーバを指定する場合、UDPヘルパーはサーバに1つのコピーを作成します。 ブロードキャストパケットを受信するインタフェースで指定してください。

15.4 UDPヘルパーの表示と維持

すべての view で **display** コマンドを実行でき、user view で **reset** コマンドを実行できます。

操作	コマンド
UDPヘルパー機能によって転送されたパケット情報を表示する	**display udp-helper interface** *interface-type interface-number*
UDPヘルパーの統計情報を削除する	**reset udp-helper statistics**

15.5 UDPヘルパー設定例

15.5.1 ブロードキャストをユニキャストに変換するための設定例

I. ネットワーク要件

図 15-1に示すように、Switch A の VLAN インタフェース 1のブロードキャストパケットをユニキャストパケットに変換します。UDP 宛先ポート番号が 55 のブロードキャストパケットを宛先サーバの IP アドレス 10.2.1.1/16 に転送します。

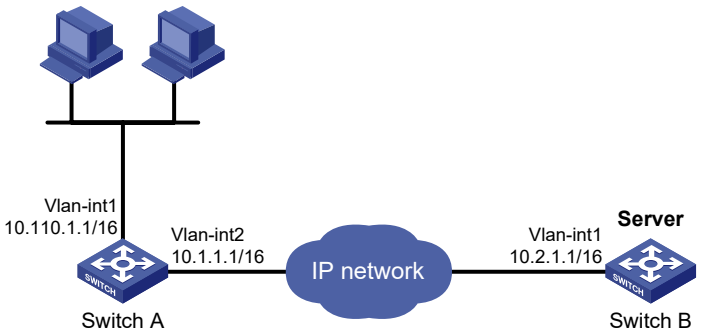


図 15-1 ネットワーク図

II. 設定手順

Switch A がサブネット 10.2.0.0/16 と通信可能であることを確認してください。

UDP ヘルパーを有効にします。

```
[SwitchA] System-view
[SwitchA] udp-helper  enable
```

UDP ポート番号 55 のブロードキャストパケットを転送するように設定します。

```
[SwitchA] udp-helper  port 55
```

VLAN インタフェース 1 のブロードキャストパケットをユニキャストパケットに変換するため、UDP ヘルパーの宛先サーバ 10.2.1.1 を指定します。

```
[SwitchA] interface  vlan-interface  1
[SwitchA-Vlan-interface1]  ip address  10.110.1.1  16
[SwitchA-Vlan-interface1]  udp-helper  server  10.2.1.1
```

III. 設定の確認

VLAN インタフェース 1 で UDP ヘルパーによって転送されたパケットの情報を表示します。

```
[SwitchA-Vlan-interface1]  display udp-helper  interface  vlan-interface  1
Interface              Server VPN instance          Server address Packets sent
Vlan-interface1          N/A                            10.2.1.1       5
```

目次

このセクションのページは **4-x-x** です。

16 章 IPv6 の基本 16-1
16.1 概要 16-1
16.1.1 IPv6 の機能 16-1
16.1.2 IPv6 アドレス 16-3
16.1.3 IPv6 ND プロトコル 16-6
16.1.4 IPv6 path MTU discovery（IPv6 PMTU 探索） 16-8
16.2 IPv6 変換技術 16-9
16.3 プロトコルと標準 16-9
16.4 IPv6 の基本の設定作業リスト 16-10
16.5 インタフェースへの IPv6 アドレスの割り当て 16-10
16.5.1 IPv6 グローバルユニキャストアドレスの設定 16-10
16.5.2 IPv6 リンクローカルアドレスの設定 16-12
16.5.3 IPv6 エニーキャストアドレスの設定 16-13
16.6 IPv6 ND の設定 16-13
16.6.1 スタティックネイバエントリの設定 16-13
16.6.2 動的に学習されるネイバの最大数の設定 16-14
16.6.3 STALE 状態での ND エントリのエージングタイマの設定 16-14
16.6.4 Hop Limit の設定 16-15
16.6.5 RA メッセージのパラメータの設定 16-15
16.6.6 DAD のための NS メッセージ送信試行回数の設定 16-17
16.7 PMTU 探索（ディスカバリ）の設定 16-18
16.7.1 インタフェースの MTU の設定 16-18
16.7.2 IPv6 アドレスのスタティック PMTU の設定 16-18
16.7.3 ダイナミック PMTU のエージングタイマの設定 16-18
16.8 ICMPv6 メッセージ送信の管理 16-19
16.8.1 ICMPv6 エラーメッセージのレートリミットの設定 16-19
16.8.2 マルチキャストエコー要求への応答の有効化 16-19
16.8.3 ICMPv6 宛先到達不能メッセージの有効化 16-20
16.8.4 ICMPv6 時間超過メッセージの送信の有効化 16-20
16.9 IPv6 の基本設定の表示と維持 16-21
16.10 IPv6 の基本設定例 16-22
16.10.1 IPv6 の基本設定例 16-22
16.11 IPv6 の基本のトラブルシューティング 16-26
16.11.1 症状 16-26
16.11.2 分析 16-26

16章 IPv6 の基本

16.1 概要

IPv6（Internet Protocol Version 6）は IPv4（Internet Protocol Version 4）の後継のプロトコルです。IPv4 はアドレス長が 32 ビットなので最大 4.3×10 の 9 乗個の割り当てが可能ですが、世界的に利用者が急増したことで、IP アドレスが枯渇する可能性があり、IPv6（Internet Protocol Version 6）が開発されました。IPv6 はアドレス長が 128 ビットなので最大 3.4×10 の 38 乗個と事実上無限に近い IP アドレスを割り当てることができます。

16.1.1 IPv6 の機能

I. ヘッダフォーマットの簡易化

IPv6 は IPv4 ヘッダフィールドを縮小、または IPv6 拡張ヘッダに移動することにより、基本の IPv6 ヘッダの長さを短くしました。IPv6 では固定長の基本ヘッダを使用し、IPv6 パケットの処理を簡単にして転送効率を高めています。IPv6 のアドレスサイズは IPv4 アドレスの 4 倍ですが、IPv6 の基本ヘッダのサイズは 40 バイトで、IPv4 ヘッダのわずか 2 倍となっています（Options フィールドを除きます）。

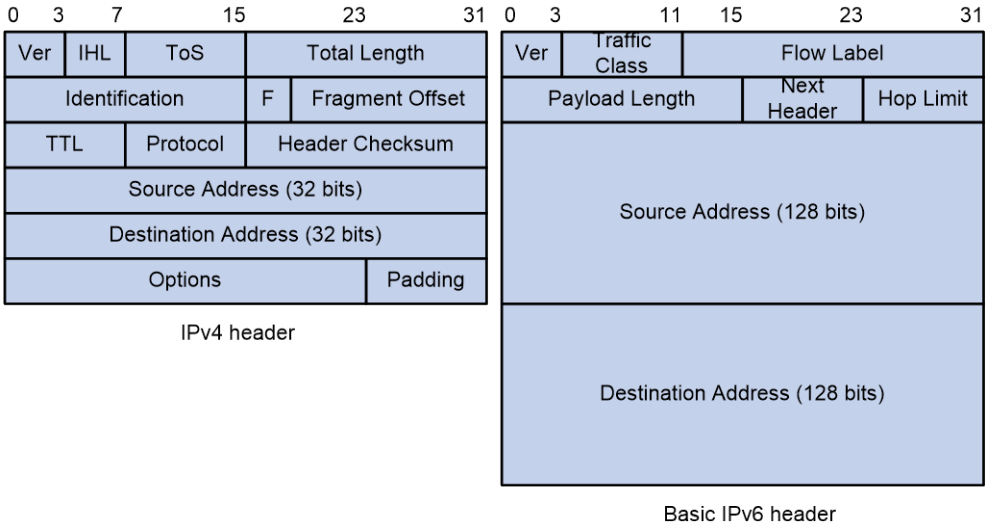


図 16-1 IPv4 パケットと基本 IPv6 パケットのヘッダフォーマットの違い

II. 大きなアドレス空間

IPv6 には 3.4 × 10^{38} アドレスが用意されており、パブリックネットワークとプライベートネットワークの階層的なアドレス割り当ての要件を満たします。

III. 階層アドレス構造

IPv6 は階層アドレス構造を使用しています。ルート検索を速め、ルートの集約を行い、IPv6 ルーティングテーブルに占有されるシステムリソースを減少させます。

IV. アドレス自動設定

ホストの設定を簡単にするために、IPv6 ではステートフルおよびステートレスのアドレス設定がサポートされています。

- ステートフルアドレス設定によって、ホストがサーバ（たとえば、DHCPv6 サーバ）から IPv6 アドレスおよび他の設定情報を取得します。
- ステートレスアドレス設定は、ホストがリンクレイヤアドレスとルータから広告されたプレフィックス情報にもとづいて、自動的に IPv6 アドレスおよび他の設定情報の作成を有効にします。

同一リンク上の他のホストと通信する場合、ホストはリンクレイヤアドレスとリンクローカルアドレスのプレフィックス（FE80::/10）にもとづいてリンクローカルアドレスを自動的に作成します。

V. ビルトインセキュリティ

IPv6 は IPsec を標準の拡張ヘッダとして使用し、エンドツーエンドのセキュリティを提供します。この機能はさまざまな IPv6 アプリケーション間の相互運用性を向上させます。

VI. QoS サポート

IPv6 ヘッダの Flow Label フィールドを使用すると、装置がフロー内のパケットにラベルを付けて、それらのパケットを特別に処理することができます。

VII. 強化されたネイバ検索（ディスカバリ）メカニズム

IPv6 ネイバ探索（ディスカバリ）プロトコルは、同一リンクにある隣接ノード間の情報交換を管理する ICMPv6（Internet Control Message Protocol Version 6）メッセージグループによって実行されます。ICMPv6 メッセージのグループは ARP（Address Resolution Protocol）メッセージ、ICMPv4（Internet Control Message Protocol version 4）ルータディスカバリメッセージ、および ICMPv4 リダイレクトメッセージに取って代わるもので、一連の他の機能を備えています。

VIII. 柔軟性のある拡張ヘッダ

IPv6 は IPv4 パケットのオプションフィールドを削除し、複数の拡張ヘッダを導入しています。このように、IPv6 によって柔軟性が大きく高められ、IP に拡張性がもたらされます。処理の効率も向上します。IPv4 パケットのオプションフィールドに含まれるものは

最大でも 40 バイトですが、IPv6 拡張ヘッダのサイズは IPv6 パケットのオプションフィールドによって制限されます。

16.1.2 IPv6 アドレス

I. IPv6 アドレスフォーマット

IPv6 アドレスは、コロン（:）で区切られた 16 ビットの 16 進数として表されます。IPv6 アドレスは 8 つのグループに分割されます。各グループの 16 ビットは、コロンで区切られ、4 つの 16 進数によって示されます。たとえば、2001:0000:130F:0000:0000:09C0:876A:130B です。

IPv6 アドレスの表現を簡単にするために、IPv6 アドレスのゼロを以下のように処理することができます。

- 各グループが 0000 の場合は 0 で表すことができます。たとえば、前述のアドレスは短縮した形式で表すと、2001:0:130F:0:0:9C0:876A:130B となります。
- ゼロの連続グループが 2 つ以上あれば、それらはダブルコロン（::）で置き換えることができます。たとえば、前述のアドレスは最短の形式で表すと、2001:0:130F::9C0:876A:130B となります。

⚠ **重要：**

ダブルコロン（::）は、IPv6 アドレスで 1 回だけ使用できます。複数回使用すると、ゼロに変換して 128 ビットの IPv6 アドレスに復元するとき、ダブルコロンがいくつのゼロを表しているのか判別できなくなります。

IPv6 アドレスは、アドレスプレフィックスとインタフェース ID から構成されます。アドレスプレフィックスとインタフェース ID はそれぞれ IPv4 アドレスのネットワーク ID とホスト ID に相当します。

IPv6 アドレスプレフィックスは IPv6 アドレス/プレフィックスの表記で記載されます。プレフィックス長はアドレスプレフィックスに相当する IPv6 アドレスの左端（先頭）からのビット数を示す 10 進数です。

II. IPv6 アドレスタイプ

IPv6 アドレスは以下のタイプに分類されます。

- **ユニキャストアドレス** － 単一インタフェースの識別番号で、IPv4 ユニキャストアドレスと同様です。ユニキャストアドレスに送られたパケットは、そのアドレスに識別されたインタフェースに配信されます。
- **マルチキャストアドレス** － （通常さまざまなノードに属している）インタフェースの集合の識別番号で、IPv4 マルチキャストアドレスに類似しています。マルチキャストアドレスに送られたパケットは、そのアドレスに識別されたすべてのインタフェースに配信されます。

  ブロードキャストはマルチキャストアドレスによって置き換えられます。

- **エニーキャストアドレス** － （通常はさまざまなノードに属している）インタフェースの集合の識別番号です。エニーキャストアドレスに送られたパケットは、そのアドレスに識別されたインタフェースに配信されます。インタフェースはルーティングプロトコルの距離測定に従って、もっとも近くにある装置のインタフェースです。

IPv6 アドレスのタイプは、フォーマットプレフィックスと呼ばれる先頭の数ビットによって指定されます。表 16-1に、アドレスのタイプとフォーマットプレフィックスの間のマッピング一覧を示します。

表 16-1 アドレスのタイプとフォーマットプレフィックスの間のマッピング

タイプ		フォーマットプレフィックス（バイナリ）	IPv6 プレフィックス ID
ユニキャストアドレス	未割り当てアドレス	00...0（128ビット）	::/128
	ループバックアドレス	00...1（128ビット）	::1/128
	リンクローカルアドレス	1111111010	FE80::/10
	グローバルユニキャストアドレス	他のフォーマット	－
マルチキャストアドレス		11111111	FF00::/8
エニーキャストアドレス		エニーキャストアドレスはユニキャストアドレス空間から取得されるもので、構文的にはユニキャストアドレスとの区別がつきません。	

III. ユニキャストアドレス

ユニキャストアドレスは、グローバルユニキャストアドレス、リンクローカルユニキャストアドレス、ループバックアドレス、未割り当てアドレスがあります。

- **グローバルユニキャストアドレス** － グローバルユニキャストアドレスは IPv4 のパブリックアドレスに相当し、インタネットサービスプロバイダ向けに提供されています。アドレスのタイプを使用すると、効率的なルートプレフィックス集約によってグローバルなルーティングエントリの数を制限することができます。
- **リンクローカルアドレス** － リンクローカルアドレスは、ネイバ探索やステートレス自動設定におけるリンクローカルノード間の通信に使用します。リンクローカルの送信元や宛先アドレスのパケットを他のリンクに転送することはできません。
- **ループバックアドレス** － ユニキャストアドレス 0:0:0:0:0:0:0:1（もっとも短縮した形式で表すと ::1）はループバックアドレスと呼ばれ、物理インタフェースに割り当てることはありません。IPv4 のループバックアドレスのように、ノードは、ループバックアドレス自体に IPv6 パケットを送信する場合があります。
- **未割り当てアドレス** － ユニキャストアドレス 0:0:0:0:0:0:0:0（もっとも短縮した形式で示すと:）は未割り当てアドレスと呼ばれ、ノードに割り当てることはできません。有効な IPv6 アドレスを取得する前に、ノードは未割り当てアドレスを IPv6 パケットの送信元アドレスフィールドに入力する場合があります。未割り当てアドレスは、宛先 IPv6 アドレスとして使用することはできません。

IV. マルチキャストアドレス

表 16-2に示す IPv6 マルチキャストアドレスは、特別な目的のために予約されています。

表 16-2 予約済みの IPv6 マルチキャストアドレス

アドレス	適用範囲
FF01::1	ノードローカルスコープ全ノードマルチキャストアドレス
FF02::1	リンクローカルスコープ全ノードマルチキャストアドレス
FF01::2	ノードローカルスコープ全ルータマルチキャストアドレス
FF02::2	リンクローカルスコープ全ルータマルチキャストアドレス

マルチキャストアドレスにはもう 1 つのタイプの要請（solicited）ノードアドレスがあります。要請ノードマルチキャストアドレスは、同一リンク上にあるネイバノードのリンクレイヤアドレスを取得するときに使用します。また、重複アドレス検出（DAD）にも使用します。IPv6 ユニキャストアドレスあるいはエニーキャストアドレスには、それぞれ 1 つずつ対応する要請ノードアドレスがあります。要請ノードマルチキャストアドレスの形式は FF02:0:0:0:0:1:FFXX:XXXX です。FF02:0:0:0:0:1 FF は固定値で、104 ビットで構成されています。XX:XXXX は、IPv6 ユニキャストアドレスまたはエニーキャストアドレスの下部 24 ビットです。

V. IEEE EUI-64 フォーマットのインタフェース識別子

インタフェース識別子は 64 ビット長です。IPv6 ユニキャストアドレスのインタフェース識別子は、リンク上のインタフェースを識別するために使用されます。インタフェースのリンクレイヤアドレス（通常 MAC アドレス）から派生したものです。MAC アドレスは 48 ビット長です。

IEEE EUI-64 フォーマットのインタフェース識別子を取得する場合、以下のステップに従います。

a) 16ビットの2進数1111111111111110（16進数でFFFEです）をMACアドレスの高位24ビットの後に挿入します。

b) U/L（ユニバーサル/ローカル）ビット（上位7番目のビット）を挿入します。この処理はインタフェース識別子がMACアドレスのように同じローカルあるいはグローバルで固有です。

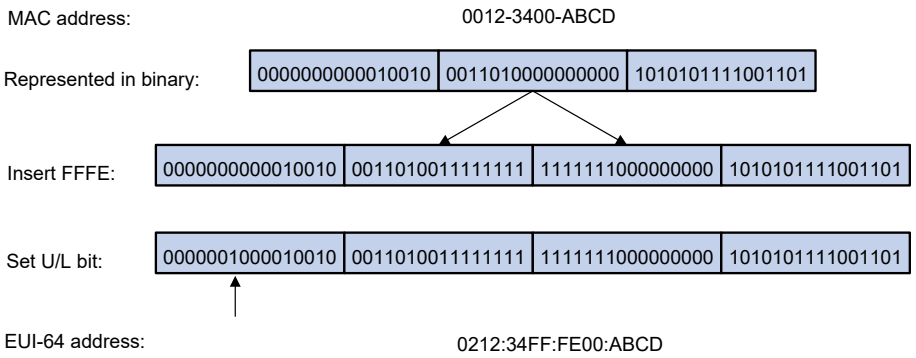


図 16-2 MAC アドレスから EUI-64 インタフェース識別子への変換

16.1.3 IPv6 ND プロトコル

IPv6 ND（Neighbor Discovery）プロトコルは、以下の ICMPv6 メッセージを使用します。

表 16-3 ND によって使用される ICMPv6 メッセージ

ICMPv6 メッセージ	タイプ	機能
ネイバ要請（NS）	135	ネイバのリンクレイヤアドレスの取得に使用します。
		ネイバに到達可能か確認するために使用します。
		DAD（重複アドレス検出）を行うために使用します。
ネイバ広告（NA）	136	NS メッセージへの応答に使用します。
		ネイバノードにリンクレイヤの変更を通知します。
ルータ要請（RS）	133	起動後、オートコンフィギュレーションのためノードはルータにアドレスプレフィックスおよびその他の設定情報を要求します。
ルータ広告（RA）	134	RS メッセージへの応答に使用します。
		ルータはプレフィックス情報オプションやフラグビットなどの情報が含まれる RA メッセージを送信します。
リダイレクト	137	一定の条件が満たされると、パケット転送に適したネクストホップルータを再選択できるように、デフォルトのゲートウェイが送信元ホストにリダイレクトメッセージを送信します。

I. アドレス解決

この機能は IPv4 の ARP に類似しています。IPv6 ノードは NS メッセージおよび NA メッセージを介して同一リンク上にあるネイバノードのリンクレイヤアドレスを取得します。図 16-3に Host A が同一リンク上の Host B のリンクレイヤアドレスを取得する方法を示します。

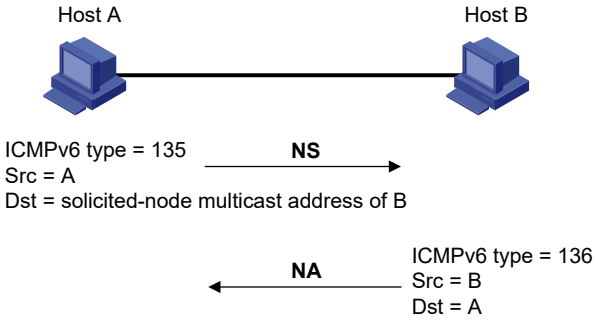


図 16-3 アドレス解決

以下にアドレス解決の手順を示します。

1) Host A は NS メッセージをマルチキャストします。NS メッセージの送信元アドレスは Host A の送信インタフェースの IPv6 アドレスです。宛先アドレスは Host B の要請ノードマルチキャストアドレスです。NS メッセージには、Host A のリンクレイヤアドレスと宛先 IPv6 アドレスが含まれています。
2) NS メッセージを受信した後、Host B はパケットの宛先アドレスが要請ノードマルチキャストアドレスであるかどうかを判断します。そうである場合は、Host B は Host A

のリンクレイヤアドレスを確認し、そのリンクレイヤアドレスが含まれる NA メッセージをユニキャストします。

3) Host A は NA メッセージから Host B のリンクレイヤアドレスを取得します。

II. ネイバ到達可能性探索

Host A がネイバの Host B のリンクレイヤアドレスを取得した後、Host A は NS メッセージと NA メッセージに従って、以下のように Host B が到達可能であるかどうかを確認することができます。

1) Host A は、Host B の IPv6 アドレスを宛先アドレスにした NS メッセージを送ります。
2) Host A が Host B から NA メッセージを受信すると、Host A は Host B が到達可能であると認識します。そうでない場合、Host B は到達不可能と認識します。

III. 重複アドレスの検出

Host A は IPv6 アドレスを取得すると、DAD（Duplicate Address Detection、重複アドレス検出）を実行してアドレスが他のノードに使用されているかどうかを判断します。IPv4 の gratuitous ARP 機能と同様です。DAD は NS メッセージおよび NA メッセージによって実行されます。

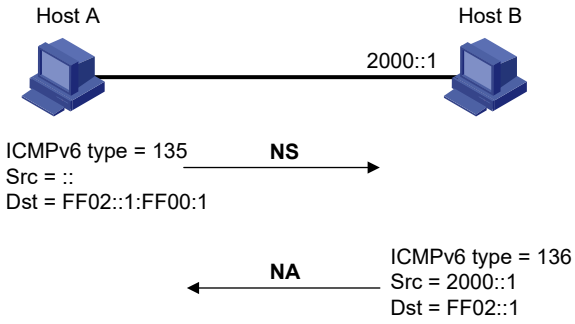


図 16-4 重複アドレスの検出

1) Host A は NS メッセージを送信します。この NS メッセージの送信元アドレスは未割り当てアドレスで、宛先アドレスは検出対象の IPv6 アドレスに対応する要請ノードマルチキャストアドレスです。NS メッセージには IPv6 アドレスが含まれています。
2) Host B がこの IPv6 アドレスを使用する場合、Host B は NA メッセージを返します。NA メッセージには Host B の IPv6 アドレスが含まれます。
3) Host A は Host B から NA メッセージを受信して、IPv6 アドレスが Host B によって使用されていることを知ります。NA メッセージを受信しない場合、Host B は IPv6 アドレスを使用していないと認識し、Host A がこの IPv6 アドレスを使用します。

IV. ルータ/プレフィックスの発見およびアドレスのオートコンフィギュレーション

ノードは、以下のようにルータ/プレフィックスの発見とオートコンフィギュレーションを行います。

1) 起動時、ノードは RS メッセージを送信し、オートコンフィギュレーションのためアドレスプレフィックスやその他の設定情報をルータに要求します。
2) ルータは、プレフィックス情報オプションや他の設定など情報が含まれる RA メッセージを返します。（ルータは定期的に RA メッセージを送信します）
3) RA メッセージのアドレスプレフィックスやその他の設定情報に従って、ノードはインタフェースに IPv6 アドレスおよびその他の設定情報を自動的に作成します。

プレフィックス情報オプションは、アドレスプレフィックスの preferred（推奨）期限と有効期限が含まれています。定期的な RA メッセージを受信すると、ノードはアドレスプレフィックスの preferred 期限と有効期限を更新します。

自動生成された IPv6 アドレスは有効期限内に適用できるものであり、有効期限が期限切れになると削除されます。

有効期限が期限切れになった後、ノードは、新しい接続を確立するために作成された IPv6 アドレスを使用することができませんが、IPv6 アドレスに関連づけられたパケットを受信することができます。preferred 期限は有効期限より大きくすることができません。

V. リダイレクション

ホストからパケットを受信する際、以下の条件である場合、ゲートウェイは最適なネクストホップのホストを通知するため、ICMPv6 リダイレクトメッセージをホストに通知します。

- 受信インタフェースがパケットを転送するインタフェースと同一です。
- 選択ルート自体は IPv6 ICMP リダイレクトメッセージによって作成、変更されることがありません。
- 選択ルートは装置のデフォルトルートではありません。
- 転送された IPv6 パケットに、ルーティング拡張ヘッダが含まれていません。

16.1.4 IPv6 path MTU discovery（IPv6 PMTU 探索）

パケットが送信元から宛先に通過するリンクは、さまざまな MTU を持つ可能性があります。MTU の最小値がパスの MTU です。IPv6 では、パケットサイズがリンクの MTU を超過している場合は、転送装置で処理を行う負荷を軽減し、ネットワークリソースを合理的に活用するために、パケットが送信元エンドでフラグメント化（分割）されます。

PMTU（path MTU）探索（ディスカバリ）メカニズムは、送信元から宛先までのパスにおけるすべてのリンクの MTU 最小値を発見します。

図 16-5に PMTU ディスカバリの動作手順を示します。

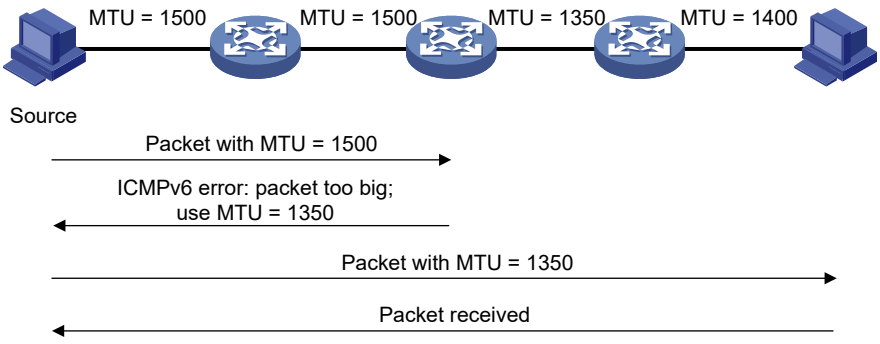


図 16-5 PMTU 探索（ディスカバリ）の処理

1) 送信元ホストは MTU よりも大きいパケットを宛先ホストに送信します。
2) 装置の出力インタフェースによってサポートされている MTU がパケットサイズよりも小さい場合、装置は以下の処理を行います。
   - □ パケットを破棄します。
   - □ インタフェースの MTU が含まれる ICMPv6 エラーパケットを送信元ホストに返します。
3) ICMPv6 エラーパケットを受信したのち、送信元ホストは以下の処理を行います。
   - □ 返された MTU を使用してパケットサイズを制限します。
   - □ パケットをフラグメント化します。
   - □ 宛先ホストに送信します。
4) 宛先ホストがパケットを受信するまで、手順 2～3 を繰り返します。このようにして、送信元ホストから宛先ホストまでのパスにある全リンクの最小 MTU が決定します。

16.2 IPv6変換技術

Dual Stack は、IPv6 ノードに IPv4 ノードとの互換性を持たせるためのもっとも直接的な方法です。Dual Stack ノードと呼ばれているネットワークノードは IPv4 と IPv6 の両方をサポートしています。IPv4 と IPv6 の両方をサポートする上位レイヤアプリケーションのために、トランスポート層で TCP か UDP を選択することができますが、ネットワーク層では IPv6 スタックが優先されます。

IPv4 アドレスと IPv6 アドレスが設定されている Dual Stack ノードは、IPv4 と IPv6 の両方のパケットを送信させることができます。Dual Stack ノードはグローバルで固有な IPv4 アドレスが必要なため、IPv4 アドレスの枯渇問題を解決することはできません。

16.3 プロトコルと標準

IPv6 に関連したプロトコルおよび規格を以下に示します。

- RFC 1881, *IPv6 Address Allocation Management*
- RFC 1887, *An Architecture for IPv6 Unicast Address Allocation*
- RFC 1981, *Path MTU Discovery for IP version 6*
- RFC 2375, *IPv6 Multicast Address Assignments*
- RFC 2460, *Internet Protocol, Version 6 (IPv6) Specification*
- RFC 2464, *Transmission of IPv6 Packets over Ethernet Networks*

- RFC 2526, *Reserved IPv6 Subnet Anycast Addresses*
- RFC 3307, *Allocation Guidelines for IPv6 Multicast Addresses*
- RFC 4191, *Default Router Preferences and More-Specific Routes*
- RFC 4291, *IP Version 6 Addressing Architecture*
- RFC 4443, *Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification*
- RFC 4861, *Neighbor Discovery for IP Version 6 (IPv6)*
- RFC 4862, *IPv6 Stateless Address Autoconfiguration*

16.4 IPv6の基本の設定作業リスト

作業リスト
（必須設定項目） インタフェースへのIPv6アドレスの割り当て • IPv6グローバルユニキャストアドレスの設定 • IPv6リンクローカルアドレスの設定 • IPv6エニーキャストアドレスの設定
（オプション設定項目） IPv6 NDの設定 • スタティックネイバエントリの設定 • 動的に学習されるネイバの最大数の設定 • STALE状態でのNDエントリのエージングタイマの設定 • Hop Limitの設定 • RAメッセージのパラメータの設定 • DADのためのNSメッセージ送信試行回数の設定
（オプション設定項目） PMTU探索（ディスカバリ）の設定 • インタフェースのMTUの設定 • IPv6アドレスのスタティックPMTUの設定 • ダイナミックPMTUのエージングタイマの設定
（オプション設定項目） ICMPv6メッセージ送信の管理: • ICMPv6エラーメッセージのレートリミットの設定 • マルチキャストエコー要求への応答の有効化 • ICMPv6宛先到達不能メッセージの有効化 • ICMPv6時間超過パケットの送信の有効化

16.5 インタフェースへのIPv6アドレスの割り当て

この章は IPv6 グローバルユニキャストアドレス、IPv6 リンクローカルアドレス、IPv6 エニーキャストアドレスの設定について記載します。

16.5.1 IPv6 グローバルユニキャストアドレスの設定

IPv6 グローバルユニキャストアドレスは、以下のいずれかの方法で設定することができます。

- **EUI-64 フォーマット IPv6 アドレス** － IPv6 アドレスプレフィックスは手動で設定し、インタフェース ID はインタフェースで自動作成されます。
- **手動設定** － IPv6 グローバルユニキャストアドレスが手動で設定されます。
- **ステートレスアドレス自動設定** － RA メッセージに含まれるアドレスプレフィックス情報をもとにして自動的に IPv6 グローバルユニキャストアドレスを作成します。

インタフェースに複数の IPv6 グローバルユニキャストアドレスを設定することができます。

手動で設定されたグローバルユニキャストアドレス（EUI-64 フォーマット IPv6 アドレスを含みます）は、自動で作成されたアドレスよりも優先されます。同じアドレスプレフィックスとは別の設定を行ったとき、インタフェースで自動生成されたグローバルユニキャストアドレスは、手動で設定されたアドレスで上書きされます。上書きされた自動生成されたグローバルユニキャストアドレスは、手動で設定されたアドレスが削除されても、もとに戻りません。そのかわり、次回インタフェースに受信された RA メッセージをもとにして、新しいグローバルユニキャストアドレスが自動で生成されます。

I. EUI-64 フォーマット IPv6 アドレス

以下に EUI-64 フォーマット IPv6 アドレスの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	－
2. interface view に移行する	**interface** *interface-type interface-number*	－
3. EUI-64 フォーマット IPv6 アドレスを作成するため、インタフェースを設定する	**ipv6 address** { *ipv6-address prefix-length* | *ipv6-address/prefix-length* } **eui-64**	デフォルト：設定なし

II. 手動設定

以下に IPv6 グローバルユニキャストアドレスの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	－
2. interface view に移行する	**interface** *interface-type interface-number*	－
3. 手動で IPv6 グローバルユニキャストアドレスを設定する	**ipv6 address** { *ipv6-address prefix-length* | *ipv6-address/prefix-length* }	デフォルト：設定なし

III. ステートレスアドレス自動設定

以下にステートレスアドレス自動設定での IPv6 アドレスの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	－
2. interface view に移行する	**interface** *interface-type interface-number*	－

操作	コマンド	補足
3. ステートレスアドレス自動設定を有効にする	**ipv6 address auto**	デフォルト：設定なし インタフェースで**undo ipv6 address auto** コマンドを使用して、インタフェースに自動で作成されたすべてのIPv6グローバルユニキャストアドレスとリンクローカルアドレスを削除できます。

16.5.2 IPv6 リンクローカルアドレスの設定

IPv6 リンクローカルアドレスは、以下のいずれかの方法で設定することができます。

- **自動生成** － インタフェースのリンクローカルアドレスプレフィックス（FE80::/10）およびリンクレイヤアドレスに従って、装置はインタフェースのリンクローカルアドレスを自動的に生成します。
- **手動割り当て** － インタフェースの IPv6 リンクローカルアドレスを手動で割り当てることができます。

インタフェースは 1 つの IPv6 リンクローカルアドレスのみ持つことができます。リンクローカルアドレスの重複を避けるため、自動生成方式を使用します。

手動割り当ては、自動生成より優先されます。

- 最初に自動生成を採用し、次に手動割り当てを行った場合、手動で割り当てたリンクローカルアドレスが自動生成アドレスを上書きします。
- 最初に手動割り当てを行い、次に自動生成を取り入れた場合は、以下の両方が発生します。
  - □ インタフェースのリンクローカルアドレスは手動割り当てのものがそのまま使われます。
  - □ 自動で生成されたリンクローカルアドレスは有効になりません。手動で割り当てられたアドレスを削除すると、自動生成のリンクローカルアドレスが有効になります。

I. IPv6 リンクローカルアドレスの自動生成の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	－
2. interface view に移行する	**interface** *interface-type interface-number*	－
3. IPv6 リンクローカルアドレスを自動生成するため、インタフェースを設定する	**ipv6 address auto link-local**	デフォルト：設定なし インタフェースにIPv6グローバルユニキャストアドレスが設定された後、リンクローカルアドレスが自動生成されます。

II. IPv6 リンクローカルアドレスの手動割り当ての設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. interface view に移行する	**interface** *interface-type interface-number*	―
3. IPv6 リンクローカルアドレスを手動で割り当てる	**ipv6 address** *ipv6-address* **link-local**	デフォルト：設定なし インタフェースにIPv6グローバルユニキャストアドレスが設定された後、リンクローカルアドレスが自動生成されます。

インタフェースに IPv6 グローバルユニキャストアドレスが設定された後、インタフェースはリンクローカルアドレスを自動的に生成します。自動的に生成されたリンクローカルアドレスは、**ipv6 address auto link-local** コマンドを使用して生成されたものと同じです。インタフェースにリンクローカルアドレスを手動で割り当てた場合、このリンクローカルアドレスが有効になります。手動で割り当てられたリンクローカルアドレスが削除されると、自動生成されたリンクローカルアドレスが有効になります。

インタフェースで **undo ipv6 address auto link-local** コマンドを使用することでのみ、**ipv6 address auto link-local** コマンドで生成されたリンクローカルアドレスを削除できます。インタフェースに IPv6 グローバルユニキャストアドレスが既に設定されている場合、インタフェースはリンクローカルアドレスを保持します。インタフェースに IPv6 グローバルユニキャストアドレスが設定されていない場合、インタフェースはリンクローカルアドレスを保持しません。

16.5.3 IPv6 エニーキャストアドレスの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. interface view に移行する	**interface** *interface-type interface-number*	―
3. IPv6 エニーキャストアドレスを設定する	**ipv6 address** { *ipv6-address prefix-length* | *ipv6-address/prefix-length* } **anycast**	デフォルト：設定なし

16.6 IPv6 NDの設定

この章は IPv6 ND プロトコルの設定方法について記載します。

16.6.1 スタティックネイバエントリの設定

ネイバエントリはリンクローカルノードの情報を記録します。エントリは、NS メッセージおよび NA メッセージを介して動的、あるいは手動で設定することができます。

装置はネイバの IPv6 アドレスとローカルのレイヤ 3 インタフェース番号によってスタティックネイバエントリを固有に識別します。以下のどちらかの方法を使用することでスタティックネイバエントリを設定することができます。

- **方法 1** – ローカルのレイヤ 3インタフェースにネイバの IPv6 アドレスとリンクレイヤアドレスを関連づけます。

  方法 1 を使用する場合、装置はネイバに接続するレイヤ 2 ポートを自動的に検索します。

- **方法 2** – VLAN のレイヤ 2 ポートにネイバの IPv6 アドレスとリンクレイヤアドレスを設定します。

  方法 2 を使用する場合、対応する VLAN インタフェースが存在しており、*port-type port-number* によって指定されたレイヤ 2 ポートが、*vlan-id* で指定されている VLAN に属していることを確認してください。装置はスタティックネイバエントリを識別するため、VLAN インタフェースをネイバの IPv6 アドレスに関連づけます。

以下にスタティックネイバエントリの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. スタティックネイバエントリを設定する	**ipv6 neighbor** *ipv6-address mac-address* { *vlan-id port-type port-number* | **interface** *interface-type interface-number* }	デフォルト：設定なし

16.6.2 動的に学習されるネイバの最大数の設定

装置は、ネイバノードのリンクレイヤアドレスを動的に取得して、NS メッセージおよび NA メッセージを介してネイバテーブルに追加することができます。ネイバエントリが動的に取得できるネイバテーブルが上限に到達すると、インタフェースはネイバ情報の学習を停止します。インタフェースでの多くのネイバテーブルによるリソースの枯渇を防ぐため、インタフェースが動的に学習できるネイバの最大数を設定することができます。

以下に動的に学習されるネイバの最大数の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. interface view に移行する	**interface** *interface-type interface-number*	―
3. 動的に学習されるネイバの最大数を設定する	**ipv6 neighbors max-learning-num** *max-number*	デフォルト：16384

16.6.3 STALE 状態での ND エントリのエージングタイマの設定

ND エントリは、エージングタイマを持っています。エージングタイマが終了する前に、STALE 状態の ND エントリがリフレッシュされない場合、NG エントリは DELAY 状態に遷移します。5 秒以内にリフレッシュされない場合、PROBE 状態に遷移し、装置は 3 回、NS メッセージを送信します。もし応答がない場合、ND エントリを削除します。

以下に ND エントリのエージングタイマの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. ND エントリのエージングタイマを設定する	**ipv6 neighbor stale-aging** *aging-time*	デフォルト：240分

16.6.4 Hop Limit の設定

装置は RA メッセージの Hop Limit を通知します。RA メッセージを受信するすべてのホストは送信する IPv6 パケットの Hop Limit フィールドの値を埋めるため、通知された値を使用します。

以下に Hop Limit の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. Hop Limit フィールドを設定する	**ipv6 hop-limit** *value*	デフォルト：64

16.6.5 RA メッセージのパラメータの設定

インタフェースが RA メッセージを送るかどうか、および RA メッセージを送信する間隔および RA メッセージのパラメータを設定することができます。RA メッセージを受信すると、ホストはこれらのパラメータを使用して、対応する動作を実行することができます。

表 16-4に RA メッセージに含まれる設定可能なパラメータを示します。

表 16-4 RA メッセージに含まれる設定可能なパラメータと説明

パラメータ	説明
Hop Limit	RAメッセージの最大ホップ数です。RAメッセージを受信したホストはIPv6パケットを送信するHop Limitフィールドに、この値を入れます。
Prefix information	装置によって広告されたプレフィックス情報を受信した後、同一リンク上のホストはステートレスオートコンフィギュレーションを実行することができます。
MTU	同じMTU値を使用するリンクのすべてのノードを保証します。
M flag	このフィールドは、ホストがIPv6アドレス取得のためにステートフルオートコンフィギュレーションを使用するかどうかを決定します。 Mフラグが1に設定されると、ホストはステートフルオートコンフィギュレーションを使用して（たとえばDHCPv6サーバ）IPv6アドレスを取得します。その他の場合は、ホストはステートレスオートコンフィギュレーションを使用してIPv6アドレスを取得します。
O flag	このフィールドは、ホストがIPv6アドレス以外の情報を取得するために、ステートフルオートコンフィギュレーションを使用するかどうかを決定します。 Oフラグが1に設定されると、ホストはステートフルオートコンフィギュレーション（たとえばDHCPv6サーバ）を使用してIPv6アドレス以外の情報を取得します。その他の場合は、ホストはステートレスオートコンフィギュレーションを使用してIPv6アドレス以外の情報を取得します。

パラメータ	説明
Router Lifetime	このフィールドは、RAメッセージを送信してホストのデフォルトルータとして機能するルータの有効期限を設定するときに使用します。 有効期限が0の場合、ルータはデフォルトゲートウェイとして使用することができません。
Retrans Timer	NSメッセージを送信した後、この指定時間内に応答メッセージを装置が受信できなかった場合、装置はNSメッセージを再送信します。
Reachable Time	ネイバの到達可能性を検出することによってネイバが到達可能であることが示されると、この到達可能時間内に到達できるものと装置はみなします。到達可能時間が終了した後、ネイバにパケットを送信する必要がある場合は、装置は宛先が到達可能か再確認します。
Router Preference	RAメッセージのルータ優先度です。ホストはRouter Preferenceの値に従ってデフォルトゲートウェイとしてルータを選択します。もしRouter Preferenceの値が同一である場合、ホストは最初にRAメッセージを受信したルータを選択します。

ルータが RA メッセージをアップデートできるように、RA メッセージ送信の最大間隔は、RA メッセージのルータ有効期限と等しいか、それよりも短くしてください。

インタフェースに対して設定された Retrans Timer フィールドと Reachable Time フィールドの値は、RA メッセージを介してホストに送られます。さらに、このインタフェースは Retrans Timer の間隔で NS メッセージを送信し、ネイバを Reachable Time の時間内に到達可能であるとみなします。

I. RA メッセージの送信の有効化

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. interface view に移行する	**interface** *interface-type interface-number*	ー
3. RA メッセージ送信の抑制を有効にする	**undo ipv6 nd ra halt**	デフォルト：無効
4. RA メッセージの送信間隔の最大値と最小値を設定する	**ipv6 nd ra interval** *max-interval min-interval*	デフォルト：RAメッセージの送信間隔は最長で600秒、最短で200秒です。 RAメッセージは最長と最短の間隔の中でランダムに送信されます。 最短間隔は最長間隔の0.75倍以内に設定してください。

II. RA メッセージのパラメータの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. interface view に移行する	**interface** *interface-type interface-number*	ー

操作	コマンド	補足
3. RA メッセージのプレフィックス情報のオプションを設定する	**ipv6 nd ra prefix** { *ipv6-prefix prefix-length* | *ipv6-prefix*/*prefix-length* } [*valid-lifetime preferred-lifetime* [**no-autoconfig** | **off-link**] *]	デフォルト：設定なし RAメッセージを送信するインタフェースのIPv6アドレスはプレフィックス情報として使用されます。 IPv6アドレスが手動で設定された場合、*valid-lifetime*は2592000秒（30日）、*preferred-lifetime*は604800秒（7日）の固定の値を使用します。 もしIPv6アドレスを自動で取得した場合、プレフィックスは設定された*valid-lifetime*と*preferred-lifetime*を使用します。
4. M フラグビットを 1に設定する	**ipv6 nd autoconfig managed-address-flag**	デフォルト：0 ホストがステートレスオートコンフィギュレーションによってIPv6アドレスを取得します。
5. O フラグビットを 1に設定する	**ipv6 nd autoconfig other-flag**	デフォルト：0 ホストがステートレスオートコンフィギュレーションによってその他の情報を取得します。
6. RA メッセージのルータの有効期限を設定する	**ipv6 nd ra router-lifetime** *time*	デフォルト：1800秒
7. NS retrans タイマを設定する	**ipv6 nd ns retrans-timer** *value*	デフォルト：1000ミリ秒の間隔でNSメッセージが送信され、RAメッセージのRetrans Timerフィールドは0です。
8. 到達可能な時間を設定する	**ipv6 nd nud reachable-time** *time*	デフォルト：ネイバ到達可能時間は30000ミリ秒で、RAメッセージのReachable Timerフィールドは0です。

16.6.6 DAD のための NS メッセージ送信試行回数の設定

IPv6 アドレスを取得した後、インタフェースは IPv6 アドレスが重複しているか検出する DAD（Duplicate Address Detection）を行うため、NS メッセージを送信します。インタフェースが（**ipv6 nd ns retrans-timer** コマンドによって決定される）指定時間内に応答を受信できなかった場合は、NS メッセージの送信を続けます。**ipv6 nd dad attempts** コマンドで設定される NS メッセージの送信試行回数が、最大に達しても応答が得られなかった場合は、取得したアドレスが使用可能であるとみなされます。

以下に DAD のための NS メッセージ送信試行回数の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. interface view に移行する	**interface** *interface-type interface-number*	—

操作	コマンド	補足
3. DAD のための NS メッセージ送信試行回数を設定する	**ipv6 nd dad attempts** *interval*	デフォルト：1 0はDADが無効であることを示します。

16.7 PMTU探索（ディスカバリ）の設定

16.7.1 インタフェースの MTU の設定

IPv6 ルータはパケットのフラグメントをサポートしていません。パケットサイズが出力インタフェースの MTU を超過すると、IPv6 ルータはパケットを廃棄し、送信元ホストに Packet Too Big メッセージを送信します。送信元ホストは MTU に従ってパケットを分割します。この問題を防ぐため、インタフェースで適切に MTU を設定します。

以下にインタフェースの MTU の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. interface view に移行する	**interface** *interface-type interface-number*	―
3. インタフェースの MTU を設定する	**ipv6 mtu** *size*	デフォルト：設定なし

16.7.2 IPv6 アドレスのスタティック PMTU の設定

宛先 IPv6 アドレスにスタティック PMTU を設定することができます。IPv6 アドレスのパケットを送信する前に、装置は出力インタフェースの MTU をスタティック PMTU と比較します。パケットサイズが 2 つの値で小さい方を超える場合は、ホストは小さい方の値に従ってパケットをフラグメント化します。フラグメントした後、装置はダイナミックに宛先ホストに PMTU を検出することができます。（オペレーションマニュアルのセクション 4 *IP サービス”IPv6 の基本”の”IPv6 path MTU discovery（IPv6 PMTU 探索）”* を参照してください。）

以下に指定した IPv6 アドレスのスタティック PMTU の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. 宛先 IPv6 アドレスにスタティック PMTU を設定する	**ipv6 pathmtu** *ipv6-address value*	デフォルト：設定なし

16.7.3 ダイナミック PMTU のエージングタイマの設定

送信元ホストから宛先ホストまでのパスの MTU が動的に決定すると（オペレーションマニュアルのセクション 4 *IP サービス "IPv6 の基本"の"IPv6 path MTU discovery（IPv6 PMTU 探索）"* を参照してください）、装置は以下の処理を行います。

- パスの MTU にもとづいて宛先ホストにパケットを送信します。
- エージングタイマを開始します。

エージングタイマが終了すると、動的に決定した PMTU が削除されます。送信元ホストは再度 MTU を決定し、PMTU メカニズムによってパケットを送信します。

以下にダイナミック PMTU のエージングタイマの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. ダイナミック PMTU のエージング時間を設定する	**ipv6 pathmtu age** *age-time*	デフォルト：10分 スタティックPMTUへのエージングタイマは無効です。

16.8 ICMPv6メッセージ送信の管理

この章は ICMPv6 メッセージの送信に関する設定方法について記載します。

16.8.1 ICMPv6 エラーメッセージのレートリミットの設定

ネットワークの混雑状態を引き起こす可能性のある短い期間内に、過度の ICMPv6 エラーメッセージを送信することを避けるため、ICMPv6 エラーメッセージの送信レートを制限することができます。トークンバケット（bucket）アルゴリズムは、1 つの ICMPv6 エラーメッセージを示す 1 つのトークンが用いられます。

バケットに入ることができるトークンの最大数に達するまで、トークンは指定された間隔でバケットに配置されます。

ICMPv6 エラーメッセージが送信されるときに、トークンはバケットから取り除かれます。バケットが空のとき、新しいトークンがバケットに配置されるまで、ICMPv6 エラーメッセージは送信されません。

以下に ICMPv6 エラーメッセージのレートリミットの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. ICMPv6 エラーメッセージの間隔とトークンバケットサイズを設定する	**ipv6 icmpv6 error-interval** *interval* [*bucketsize*]	デフォルト：100ミリ秒間隔で最大10トークンが配置されます。 ICMPv6レートリミットを無効にするには、間隔を0ミリ秒に設定します。

16.8.2 マルチキャストエコー要求への応答の有効化

装置はデフォルトでマルチキャストエコー要求の返答は無効です。しかし、いくつかのシナリオでは、送信元ホストが必要な情報を取得できるようにするため、マルチキャストエコー要求に応答する必要があります。

以下にマルチキャストエコー要求への応答の有効化の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. マルチキャストエコー要求への応答を有効にする	**ipv6 icmpv6 multicast-echo-reply enable**	デフォルト：無効

16.8.3 ICMPv6 宛先到達不能メッセージの有効化

装置は ICMPv6 宛先到達不能メッセージを以下のように送信します。

- **ICMPv6 No Route to Destination メッセージ**– 転送されたパケットがすべてのルートに一致しません。
- **ICMPv6 Communication with Destination Administratively Prohibited メッセージ**– 装置が宛先へのパケットの転送を禁止しています。通常、装置で Firewall フィルタや ACL などによって行われます。
- **ICMPv6 Beyond Scope of Source Address メッセージ**– 宛先が送信元 IPv6 アドレスの境界を超えています。たとえば、宛先 IPv6 アドレスがグローバルユニキャストアドレスで、送信元 IPv6 アドレスがリンクローカルアドレスです。
- **ICMPv6 Address Unreachable メッセージ**– 装置がパケットの宛先 IPv6 アドレスのリンクレイヤアドレスを解決できません。
- **ICMPv6 Port Unreachable メッセージ**– 装置向けの UDP パケットを受信したが UDP 宛先ポート番号が存在しません。

装置が間違って ICMPv6 宛先到達不能メッセージを作成する場合、攻撃リスクを防ぐため、ICMPv6 宛先到達不能メッセージの送信を無効にします。

以下に ICMPv6 宛先到達不能メッセージを送信する設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. ICMPv6 宛先到達不能メッセージの送信を有効にする	**ipv6 unreachables enable**	デフォルト：無効

16.8.4 ICMPv6 時間超過メッセージの送信の有効化

装置は、以下に従って ICMPv6 時間超過メッセージを送信します

- 受信した IPv6 パケットが装置向けではなく、Hop Limit が 1 のとき、装置は ICMPv6 Hop Limit Exceeded メッセージを送信元に送信します。
- 宛先 IP アドレスが装置向けである IPv6 データグラムのフラグメントされた最初のパケットを受信すると、タイマがスタートします。フラグメントされたすべてのパケットが届く前に、タイマが終了になったとき、ICMPv6 Fragment Reassembly Timeout メッセージを送信元に送信します。

悪意のあるパケットを大量に受信した場合、ICMP 時間超過メッセージにより装置のパフォーマンスが低下します。この攻撃を防ぐため、ICMPv6 時間超過メッセージの送信を無効にすることができます。

以下に ICMPv6 時間超過メッセージの送信の有効化の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. ICMPv6 時間超過メッセージの送信を有効にする	**ipv6 hoplimit-expires enable**	デフォルト：無効

16.9 IPv6の基本設定の表示と維持

すべての view で **display** コマンドを実行でき、user view で **reset** コマンドを実行できます。

操作	コマンド
IPv6 FIBエントリを表示する	**display ipv6 fib** [*ipv6-address* [*prefix-length*]]
インタフェースのIPv6情報を表示する	**display ipv6 interface** [*interface-type* [*interface-number*]] [**brief**]
ネイバ情報を表示する	**display ipv6 neighbors** { { *ipv6-address* | **all** | **dynamic** | **static** } [**slot** *slot-number*] | **interface** *interface-type interface-number* | **vlan** *vlan-id* } [**verbose**]
ネイバエントリの総数を表示する	**display ipv6 neighbors** { { **all** | **dynamic** | **static** } [**slot** *slot-number*] | **interface** *interface-type interface-number* | **vlan** *vlan-id* } **count**
VPNのネイバ情報を表示する	**display ipv6 neighbors vpn-instance** *vpn-instance-name* [**count**]
IPv6アドレスのPMTU情報を表示する	**display ipv6 pathmtu** { *ipv6-address* | { **all** | **dynamic** | **static** } [**count**] }
IPv6パケットとICMPv6パケットの統計情報を表示する	**display ipv6 statistics** [**slot** *slot-number*]
IPv6 RawIP接続の概要情報を表示する	**display ipv6 rawip** [**slot** *slot-number*]
IPv6 RawIP接続の詳細情報を表示する	**display ipv6 rawip verbose** [**slot** *slot-number* [**pcb** *pcb-index*]]
IPv6 TCP接続の概要情報を表示する	**display ipv6 tcp** [**slot** *slot-number*]
IPv6 TCP接続の詳細情報を表示する	**display ipv6 tcp verbose** [**slot** *slot-number* [**pcb** *pcb-index*]]
IPv6 UDP接続の概要情報を表示する	**display ipv6 udp** [**slot** *slot-number*]
IPv6 UDP接続の詳細情報を表示する	**display ipv6 udp verbose** [**slot** *slot-number* [**pcb** *pcb-index*]]
IPv6 TCP接続の統計情報を表示する	**display tcp statistics** [**slot** *slot-number*]
IPv6 UDP接続の統計情報を表示する	**display udp statistics** [**slot** *slot-number*]
IPv6ネイバ情報を削除する	**reset ipv6 neighbors** { **all** | **dynamic** | **interface** *interface-type interface-number* | **slot** *slot-number* | **static** }
IPv6アドレスのPMTU情報を削除する	**reset ipv6 pathmtu** { **all** | **dynamic** | **static** }
IPv6パケットとICMPv6パケットの統計情報を削除する	**reset ipv6 statistics** [**slot** *slot-number*]
IPv6 TCP接続の統計情報を削除する	**reset tcp statistics**
IPv6 UDP接続の統計情報を削除する	**reset udp statistics**

16.10 IPv6の基本設定例

16.10.1 IPv6 の基本設定例

I. ネットワーク要件

図 16-6に示すように、Host、Switch A、Switch B が Ethernet ポートを通して接続されています。Ethernet ポートに VLAN を設定し、VLAN インタフェースに IPv6 アドレスを設定します。Switch B と Host 間で通信可能となります。

Host で IPv6 を有効にし、IPv6 ND によって IPv6 アドレスを自動的に取得します。

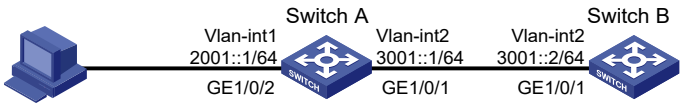


図 16-6 ネットワーク図

II. 設定手順

この例では、各 Switch で、各 VLAN インタフェースを事前に作成されていると仮定します。

1)　Switch A を設定します。

VLAN インタフェース 2 にグローバルユニキャストアドレスを設定します。

```
<SwitchA> system-view
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ipv6 address 3001::1/64
[SwitchA-Vlan-interface2] quit
```

VLAN インタフェース 1 にグローバルユニキャストアドレスを指定し、RA メッセージ（デフォルトでインタフェースは RA メッセージを送信しません）を送信するようにします。

```
[SwitchA] interface vlan-interface 1
[SwitchA-Vlan-interface1] ipv6 address 2001::1/64
[SwitchA-Vlan-interface1] undo ipv6 nd ra halt
[SwitchA-Vlan-interface1] quit
```

2)　Switch B を設定します。

VLAN インタフェース 2 にグローバルユニキャストアドレスを設定します。

```
<SwitchB> system-view
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] ipv6 address 3001::2/64
```

```
[SwitchB-Vlan-interface2] quit
```

宛先 IP アドレス 2001::/64 への IPv6 スタティックルート、ネクストホップアドレス 3001::1 を設定します。

```
[SwitchB] ipv6 route-static 2001:: 64 3001::1
```

3)　host を設定します。

IPv6 ND を通して、IPv6 アドレスを自動で取得する設定を有効にします。

Switch A の GigabitEthernet 1/0/2 のネイバ情報を表示します。

```
[SwitchA] display ipv6 neighbors interface gigabitethernet 1/0/2
Type: S-Static    D-Dynamic    O-Openflow     R-Rule    I-Invalid
IPv6 address              Link Layer      VID  Interface/Link ID   State T Age
FE80::215:E9FF:FEA6:7D14  0015-e9a6-7d14  1    GE1/0/2             STALE D 1238
2001::15B:E0EA:3524:E791  0015-e9a6-7d14  1    GE1/0/2             STALE D 1248
```

出力は、Host が取得した IPv6 グローバルユニキャストアドレスが 2001::15B:E0EA:3524:E791 であることを示しています。

III. 設定の確認

Switch A で IPv6 インタフェースの設定を表示します。インタフェースで設定されたすべての IPv6 グローバルユニキャストアドレスが表示されます。

```
[SwitchA] display ipv6 interface vlan-interface 2
Vlan-interface2 current state: UP
Line protocol current state: UP
IPv6 is enabled, link-local address is FE80::20F:E2FF:FE00:2
  Global unicast address(es):
    3001::1, subnet is 3001::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF00:1
    FF02::1:FF00:2
  MTU is 1500 bytes
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND retransmit interval is 1000 milliseconds
  Hosts use stateless autoconfig for addresses
IPv6 Packet statistics:
  InReceives:                  25829
  InTooShorts:                 0
  InTruncatedPkts:             0
  InHopLimitExceeds:           0
  InBadHeaders:                0
  InBadOptions:                0
  ReasmReqds:                  0
  ReasmOKs:                    0
  InFragDrops:                 0
  InFragTimeouts:              0
  OutFragFails:                0
  InUnknownProtos:             0
  InDelivers:                  47
  OutRequests:                 89
  OutForwDatagrams:            48
  InNoRoutes:                  0
  InTooBigErrors:              0
  OutFragOKs:                  0
  OutFragCreates:              0
  InMcastPkts:                 6
  InMcastNotMembers:           25747
```

```
  OutMcastPkts:                 48
  InAddrErrors:                 0
  InDiscards:                   0
  OutDiscards:                  0
```

[SwitchA] display ipv6 interface vlan-interface 1

```
Vlan-interface1 current state: UP
Line protocol current state: UP
IPv6 is enabled, link-local address is FE80::20F:E2FF:FE00:1C0
  Global unicast address(es):
    2001::1, subnet is 2001::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF00:1
    FF02::1:FF00:1C0
  MTU is 1500 bytes
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND retransmit interval is 1000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 600 seconds
  ND router advertisements live for 1800 seconds
  Hosts use stateless autoconfig for addresses
IPv6 Packet statistics:
  InReceives:                   272
  InTooShorts:                  0
  InTruncatedPkts:              0
  InHopLimitExceeds:            0
  InBadHeaders:                 0
  InBadOptions:                 0
  ReasmReqds:                   0
  ReasmOKs:                     0
  InFragDrops:                  0
  InFragTimeouts:               0
  OutFragFails:                 0
  InUnknownProtos:              0
  InDelivers:                   159
  OutRequests:                  1012
  OutForwDatagrams:             35
  InNoRoutes:                   0
  InTooBigErrors:               0
  OutFragOKs:                   0
  OutFragCreates:               0
  InMcastPkts:                  79
  InMcastNotMembers:            65
  OutMcastPkts:                 938
  InAddrErrors:                 0
  InDiscards:                   0
  OutDiscards:                  0
```

Switch B で IPv6 インタフェースの設定を表示します。インタフェースで設定されたすべての IPv6 グローバルユニキャストアドレスが表示されます。

[SwitchB] display ipv6 interface vlan-interface 2

```
Vlan-interface2 current state :UP
Line protocol current state :UP
IPv6 is enabled, link-local address is FE80::20F:E2FF:FE00:1234
  Global unicast address(es):
    3001::2, subnet is 3001::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF00:2
    FF02::1:FF00:1234
  MTU is 1500 bytes
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
```

```
  ND retransmit interval is 1000 milliseconds
  Hosts use stateless autoconfig for addresses
IPv6 Packet statistics:
  InReceives:                   117
  InTooShorts:                  0
  InTruncatedPkts:              0
  InHopLimitExceeds:            0
  InBadHeaders:                 0
  InBadOptions:                 0
  ReasmReqds:                   0
  ReasmOKs:                     0
  InFragDrops:                  0
  InFragTimeouts:               0
  OutFragFails:                 0
  InUnknownProtos:              0
  InDelivers:                   117
  OutRequests:                  83
  OutForwDatagrams:             0
  InNoRoutes:                   0
  InTooBigErrors:               0
  OutFragOKs:                   0
  OutFragCreates:               0
  InMcastPkts:                  28
  InMcastNotMembers:            0
  OutMcastPkts:                 7
  InAddrErrors:                 0
  InDiscards:                   0
  OutDiscards:                  0
```

Host で Switch A、Switch B 間で ping を行い、Switch A、Switch B、Host が接続されていることを確認します。

🕮 **メモ：**

リンクローカルアドレスに ping を行う際、パラメータ“**-i**”を使用してください

[SwitchB] ping ipv6 -c 1 3001::1

```
Ping6(56 data bytes) 3001::2 --> 3001::1, press CTRL_C to break
56 bytes from 3001::1, icmp_seq=0 hlim=64 time=4.404 ms

--- Ping6 statistics for 3001::1 ---
1 packet(s) transmitted, 1 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 4.404/4.404/4.404/0.000 ms
```

[SwitchB] ping ipv6 -c 1 2001::15B:E0EA:3524:E791

```
Ping6(56 data bytes) 3001::2 --> 2001::15B:E0EA:3524:E791, press CTRL_C to break
56 bytes from 2001::15B:E0EA:3524:E791, icmp_seq=0 hlim=64 time=5.404 ms

--- Ping6 statistics for 2001::15B:E0EA:3524:E791 ---
1 packet(s) transmitted, 1 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 5.404/5.404/5.404/0.000 ms
```

出力では、Switch B が Switch A、Host に ping が実行できることを示しています。また Host が Switch B、Switch A に ping が実行できることを示しています。

16.11 IPv6の基本のトラブルシューティング

16.11.1 症状

対向の IPv6 アドレスに対して ping ができません。

16.11.2 分析

1) 任意の view で **display ipv6 interface** コマンドを使用し、出力インタフェースの IPv6 アドレスが正常で、インタフェースが up であることを確認します。
2) IPv6 パケットのデバッグを有効にし、故障箇所を究明するため、user view で **debugging ipv6 packet** コマンドを使用します。

目次

このセクションのページは **4-x-x** です。

17 章 DHCPv6 の概要 17-1
17.1 DHCPv6 アドレス/プレフィックス割り当て 17-1
17.1.1 2 つのメッセージによる高速割り当て 17-1
17.1.2 4 つのメッセージによる割り当て 17-1
17.2 アドレス/プレフィックスのリース更新 17-2
17.3 ステートレス DHCPv6 17-3
17.4 DHCPv6 オプション 17-4
17.4.1 オプション 18 17-4
17.4.2 オプション 37 17-4
17.5 プロトコルと標準 17-5

17章 DHCPv6 の概要

DHCPv6 は、IPv6 プレフィックス、IPv6 アドレスやほかの設定パラメータをホストに割り当てます。

17.1 DHCPv6アドレス/プレフィックス割り当て

DHCPv6 アドレス/プレフィックスの割り当てのプロセスは 2 つあるいは 4 つのメッセージがあります。

17.1.1 2 つのメッセージによる高速割り当て

図 17-1に示すように高速割り当て(Rapid assignment)のプロセスの動作を以下に示します。

1) DHCPv6 クライアントは高速割り当てを行うため、Rapid Commit オプションを含む Solicit メッセージを送信します。
2) もし DHCPv6 サーバが高速割り当てをサポートしている場合、割り当てられる IPv6 アドレス/プレフィックスとほかの設定パラメータを含んだ Reply メッセージで応答します。もし DHCPv6 サーバが高速割り当てをサポートしていない場合、4 つのメッセージによる割り当てを行います。

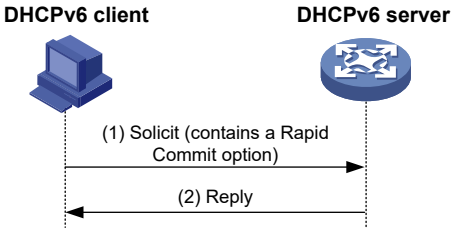


図 17-1 2つのメッセージによる高速割り当て

17.1.2 4 つのメッセージによる割り当て

図 17-2に示すように 4 メッセージ割り当て(Assignment)でのプロセスの動作を以下に示します。

1) DHCPv6 クライアントは、IPv6 アドレス/プレフィックスとほかの設定パラメータを要求するため、Solicit メッセージを送信します。
2) 以下のどちらかの状況である場合、DHCPv6 サーバは割り当て可能な IPv6 アドレス/プレフィックスとほかの設定パラメータを含む Advertise メッセージで応答します。
   - Solicit メッセージが Rapid Commit オプションを含んでいない場合
   - Solicit メッセージが Rapid Commit オプションを含んでいるが DHCPv6 サーバが高速割り当てをサポートしていない場合
3) DHCPv6 クライアントは異なる DHCPv6 サーバによって提供される複数の Advertise メッセージを受信することができます。受信した番号、サーバ優先度に従って

Advertise メッセージを選択し、確認のために選択したサーバに Request メッセージを送信します。

4) DHCPv6 サーバはアドレス/プレフィックスとほかの設定パラメータを割り当てるため、クライアントに Reply メッセージを送信します。

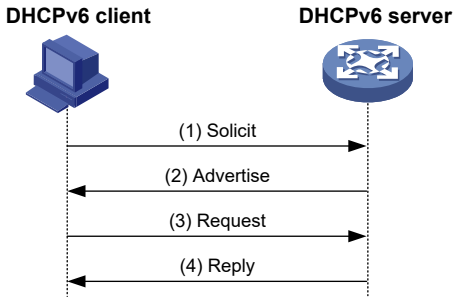


図 17-2 4 つのメッセージによる割り当て

17.2 アドレス/プレフィックスのリース更新

DHCPv6 サーバによって割り当てられた IPv6 アドレス/プレフィックスはリースできる有効期間があります。有効期間が終了すると、DHCPv6 クライアントは IPv6 アドレス/プレフィックスを使用することができません。IPv6 アドレス/プレフィックスを使用するため、DHCPv6 クライアントはリース期間を更新する必要があります。

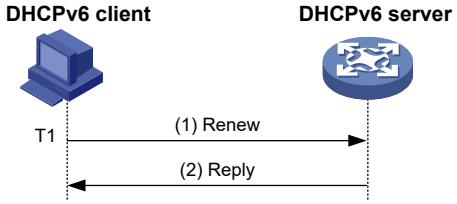


図 17-3 Renew メッセージを使用したアドレス/プレフィックスの更新

図 17-3に示すように、T1 で DHCPv6 クライアントは DHCPv6 サーバに Renew メッセージを送信します。T1 で推奨する値は、preferred 期限の半分の値です。DHCPv6 サーバは、クライアントに、リースが更新されるかどうかを通知するため、Reply メッセージで応答します。

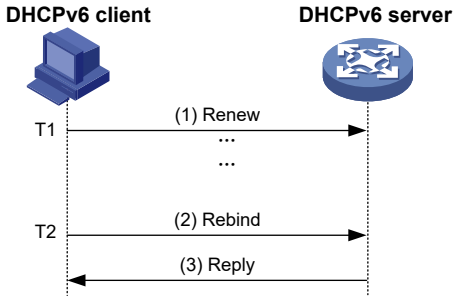


図 17-4 Rebind メッセージを使用したアドレス/プレフィックスリースの更新

図 17-4に示すように、処理します。

- DHCPv6 クライアントが T1 で Renew メッセージを送信した後、DHCPv6 サーバから応答が無い場合、T2 ですべての DHCPv6 サーバに Rebind メッセージをマルチキャストします。一般的に T2 は preferred 期限の 80%です。
- DHCPv6 サーバは、クライアントに、リースが更新されるかどうかを通知するため、Reply メッセージで応答します。
- DHCPv6 クライアントが、有効期限が終了する前にいずれの DHCPv6 サーバから応答を受信しない場合、クライアントはアドレス/プレフィックスの使用を中止します。
- 有効期限と preferred 期限についての詳細は、オペレーションマニュアルのセクション 4 *IP サービス* "*IPv6 の基本*"を参照してください。

17.3 ステートレスDHCPv6

IPv6 アドレス/プレフィックスを取得した装置は、ステートレス DHCPv6 を使用して DHCPv6 サーバからほかの設定パラメータを取得することができます。

装置はステートレス自動アドレス設定を行う間、ルータから受信した以下の RA メッセージのフラグによって、ステートレス DHCPv6 を実行します。

- 管理されたアドレス設定フラグ(M フラグ)が 0 に設定されています。
- ほかのステートフルフラグ(O フラグ)が 1 に設定されています。

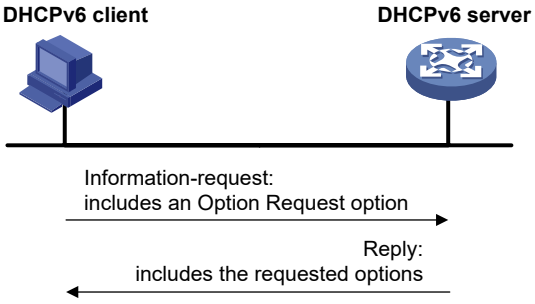


図 17-5 ステートレス DHCPv6 の動作

図 17-5におけるステートレス DHCPv6 の動作を以下に示します。

1) DHCPv6 クライアントは、すべての DHCPv6 サーバと DHCPv6 リレーエージェントに Information-request メッセージをマルチキャストします。Information-request メッセージは、DHCPv6 サーバからクライアントがリクエストする設定パラメータを指定した Option Request オプションが含まれます。
2) DHCPv6 サーバは、リクエストされた設定パラメータが含まれる Reply メッセージをクライアントに応答します。
3) クライアントは Reply メッセージをチェックします。もし取得した設定パラメータが Information-request メッセージのリクエストした内容にマッチした場合、クライアントはパラメータを使用してネットワーク設定を行います。もし一致しない場合、クライアントは設定パラメータを無視します。もしクライアントが複数の応答を受信した場合、最初に受信した応答を使用します。

17.4 DHCPv6オプション

17.4.1 オプション 18

オプション 18 はインタフェース ID と呼ばれます。RELAY-REPLY メッセージを転送するためにインタフェースを決定する DHCPv6 リレーエージェントによって使用されます。

DHCPv6 snooping 装置は DHCPv6 サーバに転送する前に受信した DHCPv6 要求メッセージにオプション 18 を追加します。サーバはオプション 18 のクライアント情報をもとにしてクライアントに IP アドレスを割り当てます。

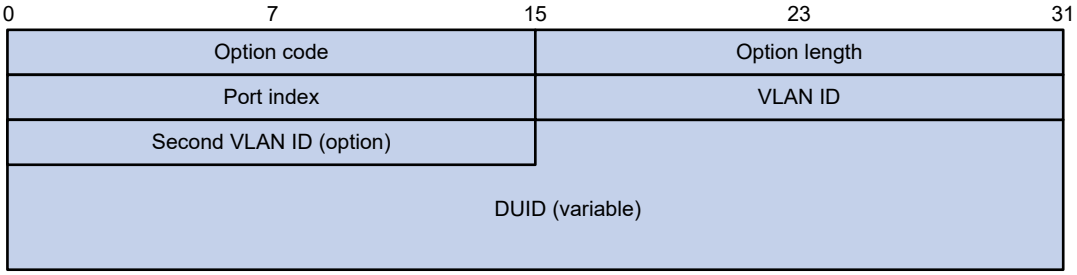


図 17-6 オプション 18 フォーマット

図 17-6にオプション 18 のフォーマットを示します。以下のフィールドを示します。

- Option code– オプションコードです。値は 18 です。
- Option length– オプションデータのサイズです。
- Port index– クライアントから DHCPv6 要求を受信したポートです。
- VLAN ID– 外部 VLAN の ID です。
- Second VLAN ID– 内部 VLAN の ID です。このフィールドはオプションです。受信した DHCPv6 要求に 2 番目の VLAN が含まれていない場合、オプション 18 も含まれません。
- DUID– DHCPv6 クライアントの DUID です。

17.4.2 オプション 37

オプションはリモート ID オプションと呼ばれます。クライアントを識別するために使用します。

DHCPv6 snooping 装置は DHCPv6 サーバに転送する前に受信した DHCPv6 要求メッセージにオプション 37 を追加します。オプションはアドレス割り当てについてのクライアント情報を提供します。

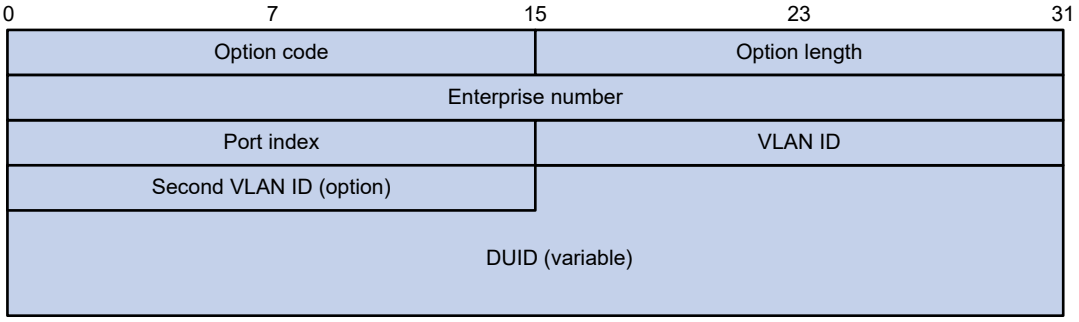


図 17-7 オプション 37 フォーマット

図 17-7にオプション 37 のフォーマットを示します。以下のフィールドを示します。

- Option code– オプションコードです。値は 37 です。
- Option length– オプションデータのサイズです。
- Enterprise number– エンタープライズ番号です。
- Port index– クライアントから DHCPv6 要求を受信したポートです。
- VLAN ID– 外部 VLAN の ID です。
- Second VLAN ID– 内部 VLAN の ID です。このフィールドはオプションです。受信した DHCPv6 要求に 2 番目の VLAN が含まれていない場合、オプション 37 も含まれません。
- DUID– DHCPv6 クライアントの DUID です。

17.5 プロトコルと標準

- RFC 3736, Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6
- RFC 3315, Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
- RFC 2462, IPv6 Stateless Address Autoconfiguration
- RFC 3633, IPv6 *Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6*

目次

このセクションのページは **4-x-x** です。

18 章 DHCPv6 リレーエージェント 18-1
18.1 概要.....18-1
18.1.1 一般的な用途.....18-1
18.1.2 DHCPv6 リレーエージェントの動作プロセス.....18-1
18.2 DHCPv6 リレーエージェント設定作業リスト 18-2
18.3 インタフェースでの DHCPv6 リレーエージェントの有効化.....18-2
18.4 リレーエージェントでの DHCPv6 サーバの指定 18-3
18.4.1 DHCPv6 サーバの IP アドレスの指定.....18-3
18.5 DHCPv6 リレーエージェントが送信した DHCPv6 パケットの DSCP 値の設定.....18-3
18.6 IPv6 プレフィックスを通知するための DHCPv6 リレーエージェントの有効化.....18-4
18.7 DHCPv6 リレーエージェントの表示とメンテナンスコマンド 18-4
18.8 DHCPv6 リレーエージェント設定の例 18-5
18.8.1 DHCPv6 リレーエージェントの設定例.....18-5

18章 DHCPv6 リレーエージェント

18.1 概要

18.1.1 一般的な用途

DHCPv6 クライアントは通常、マルチキャストアドレスを使用してローカルリンク上の DHCPv6 サーバに接続し、IPv6 アドレスおよびその他の設定パラメータを取得します。図 18-1に示すように、DHCPv6 サーバが別のサブネット上にある場合、DHCPv6 クライアントがサーバに接続するには DHCPv6 リレーエージェントが必要です。リレーエージェント機能は、各サブネットに DHCPv6 サーバを展開しないようにします。

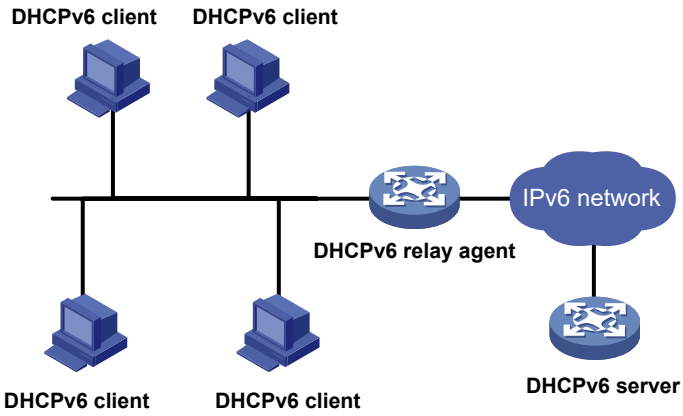


図 18-1 一般的な DHCPv6 リレーエージェントアプリケーション

18.1.2 DHCPv6 リレーエージェントの動作プロセス

図 18-2に示すように、DHCPv6 クライアントが DHCPv6 リレーエージェントを介して DHCPv6 サーバから IPv6 アドレスと他のネットワーク設定パラメータを取得しています。次の例では、高速割当てを使用してプロセスを説明します。

- DHCPv6 クライアントは、Rapid Commit オプションを含む Solicit メッセージを、すべての DHCPv6 サーバおよびリレーエージェントのマルチキャストアドレス FF02::1:2 に送信します。
- Solicit メッセージを受信した DHCPv6 リレーエージェントは、メッセージを Relay-forward メッセージの Relay Message オプションにカプセル化し、DHCPv6 サーバに送信します。
- Relay-forward メッセージから Solicit メッセージを取得した後、DHCPv6 サーバは次のタスクを実行します。IPv6 アドレスとその他の必要なパラメータを選択します。
  - □ Relay-reply メッセージの Relay Message オプション内にカプセル化された応答に追加します。
  - □ DHCPv6 リレーエージェントにリレー応答メッセージを送信します。
- DHCPv6 リレーエージェントは、リレー応答メッセージから応答を取得し、DHCPv6 クライアントに応答を送信します。

- DHCPv6 クライアントは、DHCPv6 サーバによって割り当てられた IPv6 アドレスとその他のネットワークパラメータを使用して、ネットワーク設定を完了します。

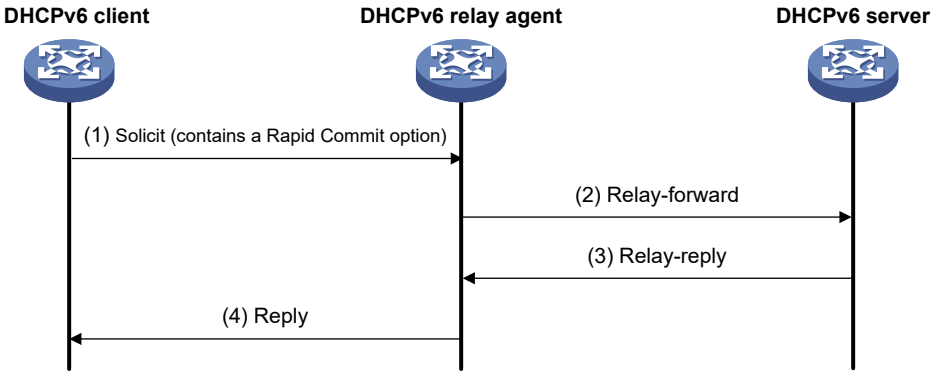


図 18-2 DHCPv6 リレーエージェントの動作プロセス

18.2 DHCPv6リレーエージェント設定作業リスト

作業リスト
（必須設定項目）インタフェースでのDHCPv6リレーエージェントの有効化
（必須設定項目）リレーエージェントでのDHCPv6サーバの指定
（オプション設定項目）DHCPv6リレーエージェントが送信したDHCPv6パケットのDSCP値の設定
（オプション設定項目）IPv6プレフィックスを通知するためのDHCPv6リレーエージェントの有効化

18.3 インタフェースでのDHCPv6リレーエージェントの有効化

I. 制限とガイドライン

ベストプラクティスとして、同じインタフェースで DHCPv6 リレーエージェントと DHCPv6 クライアントを有効にしないでください。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. interface view に移行する	**interface** *interface-type interface-number*	—
3. インタフェースで DHCPv6 リレーエージェントを有効にする	**ipv6 dhcp select relay**	デフォルト：無効

18.4 リレーエージェントでのDHCPv6サーバの指定

18.4.1 DHCPv6 サーバの IP アドレスの指定

I. 制限とガイドライン

- **ipv6 dhcp relay server-address** コマンドを使用すると、DHCPv6 リレーエージェントインタフェースで最大 8 台の DHCPv6 サーバを指定できます。DHCPv6 リレーエージェントは、指定されたすべての DHCPv6 サーバに DHCP 要求を転送します。
- DHCPv6 サーバアドレスがリンクローカルアドレスまたはマルチキャストアドレスの場合、このコマンドで interface キーワードを使用して送信インタフェースを指定する必要があります。そうしないと、DHCPv6 パケットが DHCPv6 サーバに到達できない可能性があります。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. interface view に移行する	**interface** *interface-type interface-number*	―
3. DHCPv6 サーバを指定する	**ipv6 dhcp relay server-address** *ipv6-address* [**interface** *interface-type interface-number*] [**public** | **vpn-instance** *vpn-instance-name*]	デフォルト：指定なし

18.5 DHCPv6リレーエージェントが送信したDHCPv6パケットのDSCP値の設定

I. DHCPv6 パケットの DSCP 値の設定について

パケットの DSCP 値は、パケットの優先度レベルを指定し、パケットの送信優先度に影響します。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. DHCPv6 リレーエージェントによって送信される DHCPv6 パケットの DSCP 値を設定する	**ipv6 dhcp dscp** *dscp-value*	デフォルト：56

18.6 IPv6プレフィックスを通知するためのDHCPv6リレーエージェントの有効化

I. IPv6 プレフィックスを通知する DHCPv6 リレーエージェントの有効化について

DHCPv6 クライアントは、DHCPv6 を介して IPv6 プレフィックスを取得し、この IPv6 プレフィックスを使用して、ダウンストリームネットワークのクライアントに IPv6 アドレスを割り当てることができます。IPv6 プレフィックスが DHCPv6 クライアントのアップストリームインタフェースの IPv6 アドレスと異なるサブネットにある場合、ダウンストリームネットワークのクライアントは外部ネットワークにアクセスできません。DHCPv6 クライアントと同じリンク上にある DHCPv6 リレーエージェントを有効にして、IPv6 プレフィックスを配信できます。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. DHCPv6 リレーエージェントが IPv6 プレフィックスを配信できるようにする	**ipv6 dhcp advertise pd-route**	デフォルトでは、DHCPv6リレーエージェントはIPv6プレフィックスを配信しません。このコマンドを使用する前に、DHCPv6リレーエージェントがDHCPv6リレーエントリを記録できるようになっていることを確認してください。

18.7 DHCPv6リレーエージェントの表示とメンテナンスコマンド

すべての view で **display** コマンドを実行でき、user view で **reset** コマンドを実行できます。

操作	コマンド
ローカル装置のDUIDを表示する	**display ipv6 dhcp duid**
DHCPv6リレーエージェントで指定されたDHCPv6サーバアドレスを表示します。	**display ipv6 dhcp relay server-address** [**interface** *interface-type interface-number*]
DHCPv6リレーエージェントのパケット統計情報を表示する	**display ipv6 dhcp relay statistics** [**interface** *interface-type interface-number*]
DHCPv6リレーエージェントのパケット統計情報を削除する	**reset ipv6 dhcp relay statistics** [**interface** *interface-type interface-number*]

18.8 DHCPv6リレーエージェント設定の例

18.8.1 DHCPv6 リレーエージェントの設定例

I. ネットワーク要件

図 18-3に示すように、Switch A の DHCPv6 リレーエージェントが DHCPv6 クライアントと DHCPv6 サーバの間で DHCPv6 パケットをリレーするように設定しています。

Switch A は、ネットワーク 1 ::/ 64 のゲートウェイとして機能します。 DHCPv6 を介して IPv6 アドレスと他の設定パラメータを取得するようにホストに通知するために RA メッセージを送信します。 RA メッセージの詳細はオペレーションマニュアルのセクション 4 *IP サービス* "*IPv6 の基本*"を参照してください。

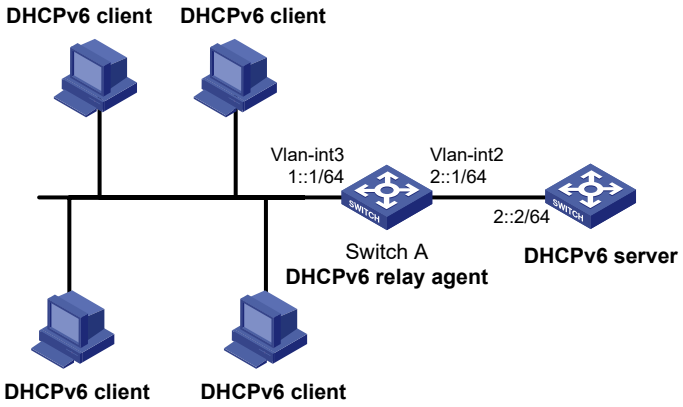


図 18-3 ネットワーク図

I. 設定手順

VLAN-interface 2 と VLAN-interface 3.の IPv6 アドレスを指定します。

```
<SwitchA> system-view
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ipv6 address 2::1 64
[SwitchA-Vlan-interface2] quit
[SwitchA] interface vlan-interface 3
[SwitchA-Vlan-interface3] ipv6 address 1::1 64
```

VLAN-interface 3 での RA メッセージ抑制を無効にします。

```
[SwitchA-Vlan-interface3] undo ipv6 nd ra halt
```

VLAN-interface 3 で送信する RA アドバタイズメントで、M flag を 1 に設定します。RA アドバタイズメントを受信するホストは、DHCPv6 を介して IPv6 アドレスを取得します。

```
[SwitchA-Vlan-interface3] ipv6 nd autoconfig managed-address-flag
```

VLAN-interface 3 で送信する RA アドバタイズメントの O flag を 1 に設定します。RA アドバタイズメントを受信するホストは、DHCPv6 を介して IPv6 アドレス以外の情報を取得します。

```
[SwitchA-Vlan-interface3] ipv6 nd autoconfig other-flag
```

VLAN-interface 3 で DHCPv6 リレーエージェントを有効にし、リレーエージェントで DHCPv6 サーバを指定します。

```
[SwitchA-Vlan-interface3] ipv6 dhcp select relay
[SwitchA-Vlan-interface3] ipv6 dhcp relay server-address 2::2
```

II. 設定の確認

Switch A の DHCPv6 サーバアドレス情報を表示します。

```
[SwitchA-Vlan-interface3] display ipv6 dhcp relay server-address
Interface: Vlan-interface3
 Server address      Outgoing Interface          Public/VRF name
 2::2                                            --/--
```

DHCPv6 リレーエージェントにパケット統計情報を表示します。

```
[SwitchA-Vlan-interface3] display ipv6 dhcp relay statistics
Packets dropped                : 0
Packets received               : 14
    Solicit                    : 0
    Request                    : 0
    Confirm                    : 0
    Renew                      : 0
    Rebind                     : 0
    Release                    : 0
    Decline                    : 0
    Information-request        : 7
    Relay-forward              : 0
    Relay-reply                : 7
Packets sent                   : 14
    Advertise                  : 0
    Reconfigure                : 0
    Reply                      : 7
    Relay-forward              : 7
    Relay-repl
```

目次

このセクションのページは **4-x-x** です。

19 章 DHCPv6 クライアント 19-1
19.1 概要 19-1
19.2 制限とガイドライン: DHCPv6 クライアント設定 19-1
19.3 DHCPv6 クライアント設定作業リスト 19-1
19.4 IPv6 アドレス取得の設定 19-1
19.5 DHCPv6 クライアントの表示および保守コマンド 19-2
19.6 DHCPv6 クライアント設定の例 19-2
19.6.1 IPv6 アドレス取得の設定例 19-2
19.6.2 ステートレス DHCPv6 の設定例 19-4

19章 DHCPv6 クライアント

装置は DHCPv6 クライアントが有効である場合、DHCPv6 クライアントとして機能し、DHCPv6 サーバから IP アドレスを含む設定パラメータを取得できます。

19.1 概要

DHCPv6 クライアントを設定すると、インタフェースは DHCPv6 サーバから設定パラメータを取得できます。

DHCPv6 クライアントは、DHCPv6 を使用して次の機能を実行できます。

- IPv6 アドレス、IPv6 プレフィックス、またはその両方を取得し、他の設定パラメータを取得します。DHCPv6 サーバが装置で有効になっている場合、クライアントは取得したパラメータを DHCPv6 オプショングループに自動的に保存できます。取得した IPv6 プレフィックスを使用して、クライアントはグローバルユニキャストアドレスを生成できます。
- ステートレス DHCPv6 をサポートし、IPv6 アドレスと IPv6 プレフィックスを除く設定パラメータを取得します。クライアントは、ステートレス IPv6 アドレス自動設定によって IPv6 アドレスを取得します。クライアントがアドレス取得中に、M フラグを 0、O フラグを 1に設定した RA メッセージを受信すると、ステートレス DHCPv6 が起動します。

19.2 制限とガイドライン: DHCPv6クライアント設定

DHCPv6 クライアントを DHCPv6 サーバまたは DHCPv6 リレーエージェントと同じインタフェースに設定しないでください。

19.3 DHCPv6クライアント設定作業リスト

作業リスト
(必須設定項目) IPv6アドレス取得の設定

19.4 IPv6アドレス取得の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. interface view に移行する	**interface** *interface-type interface-number*	―
3. DHCPv6 を使用して IPv6 アドレスとその他の設定パラメータを取得するようにインタフェースを設定する	**ipv6 address dhcp-alloc** [**option-group** *group-number* | **rapid-commit**] *	デフォルトでは、インタフェースはIPv6アドレス取得にDHCPv6を使用しません。

19.5 DHCPv6クライアントの表示および保守コマンド

操作	コマンド
DHCPv6クライアント情報を表示する	**display ipv6 dhcp client** [**interface** *interface-type interface-number*]
DHCPv6クライアント統計情報を表示する	**display ipv6 dhcp client statistics** [**interface** *interface-type interface-number*]
DHCPv6クライアント統計情報をクリアする	**reset ipv6 dhcp client statistics** [**interface** *interface-type interface-number*]

19.6 DHCPv6クライアント設定の例

19.6.1 IPv6 アドレス取得の設定例

I. ネットワーク要件

図 19-1に示すよう、DHCPv6 を使用して DHCPv6 サーバから設定パラメータを取得するようにスイッチを設定するパラメータには、IPv6 アドレス、DNS サーバアドレス、ドメイン名サフィックス、SIP サーバアドレス、および SIP サーバドメイン名が含まれます。

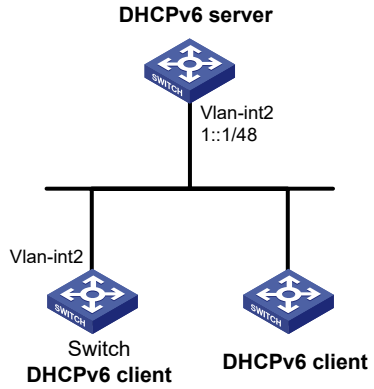


図 19-1 ネットワーク図

II. 設定手順

DHCPv6 クライアントを構成する前に、まず DHCPv6 サーバを構成する必要があります。

IPv6 アドレス取得のために DHCPv6 クライアントとして VLAN-interface 2 を設定します。DHCPv6 高速アドレス割り当てをサポートするために DHCPv6 クライアントを設定します。DHCPv6 クライアントを設定して、設定パラメータを保存するための動的 DHCPv6 オプショングループを作成します。

```
<Switch> system-view
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ipv6 address dhcp-alloc rapid-commit option-group 1
```

```
[Switch-Vlan-interface2]  quit
```

III. 設定の確認

クライアントがサーバから IPv6 アドレスと他の設定パラメータを取得したことを確認します。

```
[Switch] display ipv6 dhcp client
Vlan-interface2:
  Type: Stateful client requesting address
    State: OPEN
    Client DUID: 0003000100e002000000
    Preferred server:
      Reachable via address: FE80::2E0:1FF:FE00:18
      Server DUID: 0003000100e001000000
    IA NA: IAID 0x00000642, T1 50 sec, T2 80 sec
      Address: 1:1::2/128
       Preferred lifetime 100 sec, valid lifetime 200 sec
       Will expire on Mar 27 2014 at 08:06:57 (198 seconds left)
    DNS server addresses:
      2000::FF
    Domain name:
      example.com
    SIP server addresses:
      2:2::4
    SIP server domain names:
      bbb.com
```

装置で DHCPv6 サーバを有効にした後、設定パラメータが動的 DHCPv6 オプショングループに保存されていることを確認します。

```
[Switch] display ipv6 dhcp option-group  1
DHCPv6 option group: 1
  DNS server addresses:
    Type: Dynamic (DHCPv6 address allocation)
    Interface: Vlan-interface2
    2000::FF
  Domain name:
    Type: Dynamic (DHCPv6 address allocation)
    Interface: Vlan-interface2
    example.com
  SIP server addresses:
    Type: Dynamic (DHCPv6 address allocation)
    Interface: Vlan-interface2
    2:2::4
  SIP server domain names:
    Type: Dynamic (DHCPv6 address allocation)
    Interface: Vlan-interface2
    bbb.com
```

DHCPv6 クライアントが IPv6 アドレスを取得していることを確認します。

```
[Switch] display ipv6 interface brief
*down: administratively down
(s): spoofing
Interface                              Physical    Protocol    IPv6 Address
Vlan-interface2                        up          up          1:1::2
```

19.6.2 ステートレス DHCPv6 の設定例

I. ネットワーク要件

図 19-2に示すように、IPv6 アドレスと IPv6 プレフィックス以外の設定パラメータを取得するためにステートレス DHCPv6 を使用するようにスイッチ A を設定しています。 スイッチ B はゲートウェイとして機能し、RA メッセージを定期的に配信します。

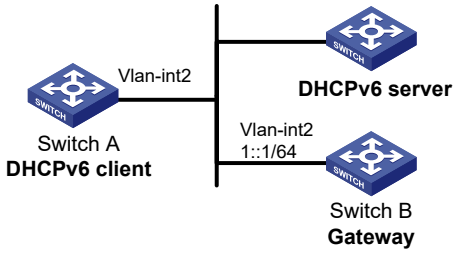


図 19-2 ネットワーク図

II. 設定手順

DHCPv6 クライアントを構成する前に、まず DHCPv6 サーバを構成する必要があります。

ゲートウェイ Switch B を設定に設定します。

VLAN-interface 2 のために IPv6 アドレスを設定してください。

```
<SwitchB> system-view
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] ipv6 address 1::1 64
```

VLAN-interface 2 で送信する RA アドバタイズメントの O flag を 1 に設定します。 RA アドバタイズメントを受信するホストは、DHCPv6 を介して IPv6 アドレス以外の情報を取得します。

```
[SwitchB-Vlan-interface2] ipv6 nd autoconfig other-flag
```

GigabitEthernet 1/0/1 で RA メッセージの抑制を無効にします。

```
[SwitchB-Vlan-interface2] undo ipv6 nd ra halt
```

1)　DHCPv6 クライアント Switch A を設定に設定します。

VLAN-interface 2 でステートレス IPv6 アドレス自動設定を有効にします。

```
<SwitchA> system-view
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ipv6 address auto
```

ステートレス IPv6 アドレス自動設定が有効になっているが、VLAN-interface 2 用に IPv6 アドレスが設定されていない場合、Switch A はリンクローカルアドレスを自動的に生成します。 Switch B に RS メッセージを送信し、IPv6 アドレス生成のための設定情報を要求します。 RS メッセージを受信すると、Switch B は RA メッセージを返信します。 M flag

を 0、O flag を 1 に設定した RA メッセージを受信した後、Switch A はステートレス DHCPv6 を実行して他の設定パラメータを取得します。

III. 設定の確認

DHCPv6 クライアント情報を表示します。

```
[SwitchA-Vlan-interface2] display ipv6 dhcp client interface vlan-interface 2
Vlan-interface2:
 Type: Stateless client
    State: OPEN
    Client DUID: 00030001000fe2ff0000
    Preferred server:
      Reachable via address: FE80::213:7FFF:FEF6:C818
      Server DUID: 0003000100137ff6c818
    DNS server addresses:
      1:2:4::5
      1:2:4::7
    Domain name:
      abc.com
```

DHCPv6 クライアント統計情報を表示します。

```
[SwitchA-Vlan-interface2] display ipv6 dhcp client statistics
Interface                    :  Vlan-interface2
Packets received             :  1
        Reply                :  1
        Advertise            :  0
        Reconfigure          :  0
        Invalid              :  0
Packets sent                 :  5
        Solicit              :  0
        Request              :  0
        Renew                :  0
        Rebind               :  0
        Information-request  :  5
        Release              :  0
        Decline              :  0
```

目次

このセクションのページは **4-x-x** です。

20 章 HTTP リダイレクト.....20-1
20.1 HTTP リダイレクトについて.....20-1
20.2 HTTPS リダイレクトポート番号の指定.....20-1
20.2.1 HTTPS リダイレクトポート番号の指定について.....20-1
20.2.2 制限とガイドライン.....20-1
20.2.3 設定手順.....20-1
20.3 SSL サーバポリシと HTTPS リダイレクトサービスの関連付け.....20-1
20.3.1 SSL サーバポリシと HTTPS リダイレクトサービスの関連付けについて.....20-1
20.3.2 制限とガイドライン.....20-2
20.3.3 設定手順.....20-2

20章 HTTP リダイレクト

20.1 HTTPリダイレクトについて

HTTP リダイレクトは、ユーザの HTTP または HTTPS 要求を指定した URL にリダイレクトします。以下の機能で使用されます。

- 802.1X認証、MAC 認証、ポートセキュリティのリダイレクト URL の割り当て
- 802.1X認証の EAD アシスタント URL リダイレクト
- Web 認証の URL リダイレクトサービス

20.2 HTTPSリダイレクトポート番号の指定

20.2.1 HTTPS リダイレクトポート番号の指定について

HTTPS リダイレクトで TCP ポート番号を指定することで装置は HTTPS リクエストをリダイレクトが可能になります。

20.2.2 制限とガイドライン

ポート衝突を回避するため、ウェルノンポートの指定はしないでください。他のサービスによって使われている TCP ポート番号を確認するために、**display tcp** コマンドを使ってください。

20.2.3 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. HTTPS リダイレクトポート番号を指定する	**http-redirect https-port** *port-number*	デフォルト：8443

20.3 SSLサーバポリシとHTTPSリダイレクトサービスの関連付け

20.3.1 SSL サーバポリシと HTTPS リダイレクトサービスの関連付けについて

HTTPS リダイレクトのセキュリティを改善するために、SSL サーバポリシを HTTPS リダイレクトサービスと関連付けすることができます。

20.3.2 制限とガイドライン

関連付けした SSL サーバポリシが存在していない場合、HTTPS リダイレクトは利用できません。最初に SSL サーバポリシを HTTPS リダイレクトサービスと関連付けして、それから SSL サーバポリシを設定することができます。

HTTPS リダイレクトサービスと関連した SSL サーバポリシを変更する場合、新しいポリシが直ちに適用されます。

20.3.3 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. SSL サーバポリシと HTTPS リダイレクトサービスを関連付ける	**http-redirect ssl-server-policy** *policy-name*	デフォルト：設定なし

QX-S5100G シリーズ Ethernet スイッチ

オペレーションマニュアル

5. ルーティングプロトコル

本マニュアルは以下に示す章で構成されています。

01-IP ルーティングの基本
02-スタティックルーティング
03-デフォルトルート
04-IPv6 スタティックルーティング
05-IPv6 デフォルトルート
06-RIP
07-OSPF
08-ポリシーベースルーティング
09-RIPng
10-OSPFv3
11-IPv6 ポリシーベースルーティング
12-ルーティングポリシー

目次

このセクションのページは **5-x-x** です。

1 章 IP ルーティングの基本 1-1
1.1 ルーティングテーブル 1-1
1.2 ダイナミックルーティングプロトコル 1-2
1.3 ルートの優先度 1-2
1.4 ロードバランス 1-3
1.5 ルートバックアップ 1-3
1.6 ルート再帰 1-3
1.7 ルート再分配 1-4
1.8 RIB NSR の設定 1-4
1.9 装置でサポートされるアクティブルートの最大数の設定 1-5
1.10 ルーティングテーブルの表示と維持 1-6

1章 IP ルーティングの基本

IP ルーティングはルーティングテーブルをもとにルータ上で IP パケットの転送を行います。この章はユニキャストルーティングプロトコルについて説明します。

⚠ **注意:**
動作が不安定になる可能性があるため、仕様で定められた数以上のルートを学習させないでください。

1.1 ルーティングテーブル

RIB (routing information base)はルート再帰、ルート再分配、ルート拡張情報を含んだグローバルルーティングテーブルと関連する情報が含まれます。ルータはルーティングテーブルから最適なルートを選択し、FIB (forwarding information base)テーブルに格納します。ルータはパケットを転送するために FIB テーブルを使用します。FIB テーブルの詳細は、オペレーションマニュアルのセクション 4 *IP サービス”IP フォワーディングの基本*”を参照してください。

表 1-1にルートのカテゴリを示します。

表 1-1 ルートのカテゴリ

基準	カテゴリ
宛先	• **ネットワークルート**—宛先がネットワークです。サブネットマスクは32ビット未満です。 • **ホストルート**—宛先がホストです。サブネットマスクは32ビットです。
宛先が直接接続されているかどうか	• **ダイレクトルート**—宛先が直接接続されています。 • **インダイレクトルート**—宛先が直接接続されていません。
作成元	• **ダイレクトルート**—ダイレクトルートがインタフェースのデータリンクプロトコルによって検出されました。インタフェースルートと呼ばれます。 • **スタティックルート**—管理者によって手動で設定されたルートです。 • **ダイナミックルート**—ルーティングプロトコルによって自動に検出されたルートです。

ルーティングテーブルの概要を表示する場合、**display ip routing-table** コマンドを使用します。

```
<Switch> display ip routing-table
Destinations : 9        Routes : 9
```

```
Destination/Mask    Proto   Pre Cost        NextHop         Interface
0.0.0.0/32          Direct  0   0           127.0.0.1       InLoop0
3.3.3.3/32          Direct  0   0           127.0.0.1       InLoop0
127.0.0.0/8         Direct  0   0           127.0.0.1       InLoop0
127.0.0.0/32        Direct  0   0           127.0.0.1       InLoop0
127.0.0.1/32        Direct  0   0           127.0.0.1       InLoop0
127.255.255.255/32  Direct  0   0           127.0.0.1       InLoop0
```

ルーティングエントリは以下の項目が含まれます。

- **Destination**(宛先アドレス)—宛先ホストあるいはネットワークの IP アドレスです。
- **Mask**(ネットワークマスク)—IP アドレスのマスク長です。
- **Proto**(プロトコル)—ルートを追加したプロトコルです。
- **Pre**(プリファレンス)—ルートの優先度です。同一宛先へのルートがある場合、最も高い優先度を持つルートが最適なルートとなります。
- **Cost**(コスト)— 宛先へのルートが複数あり、同一優先度である場合、最も小さいコストの値を持つルートが最適なルートとなります。
- **NextHop**(ネクストホップ)— ネクストホップの IP アドレスを示します。
- **Interface**(インタフェース)—IP パケットの転送に使用する出力先のインタフェースを示します。

1.2 ダイナミックルーティングプロトコル

スタティックルートは小規模で安定したネットワークで使われます。必要な設定とシステムリソースを少なくすることができます。構成が頻繁に変更するネットワークにおいては、ダイナミックルーティングプロトコルを設定することが一般的です。スタティックルーティングと比較して、ダイナミックルーティングは設定が複雑で、多くのルータとネットワークのリソースが必要となります。

ダイナミックルーティングは、構成の変更に適応した到達可能性の情報を、ダイナミックに収集し、報告します。ダイナミックルーティングは大規模のネットワークに適しています。

表 1-2 ダイナミックルーティングプロトコルのカテゴリ

基準	カテゴリ
ルーティングアルゴリズム	• **ディスタンスベクタプロトコル**－RIPがあります。 • **リンクステートプロトコル**－OSPFが含まれます。
IPバージョン	• **IPv4ルーティングプロトコル**－RIP、OSPFがあります。 • **IPv6ルーティングプロトコル**－RIPng、OSPFv3があります。

1.3 ルートの優先度

スタティックルーティング、ダイナミックルーティングを含むルーティングプロトコルは、デフォルトで優先度を持ちます。同一宛先に複数のルートがある場合、ルータは最適なルートとして最も高い優先度を持つルートを選択します。

ダイレクトルートのプリファレンスは 0 で、変更できません。各スタティックルートとダイナミックルーティングプロトコルのプリファレンスを設定することができます。表 1-3

にルートタイプとデフォルトのプリファレンスを示します。値が小さいほど優先度が高くなります。

表 1-3 ルートタイプとデフォルトルートプリファレンス

ルートタイプ	プリファレンス
Direct route	0
OSPF	10
Unicast static route	60
RIP	100
OSPF ASE	150
OSPF NSSA	150
Unknown(信用されていない送信元からのルート)	256

1.4 ロードバランス

ルーティングプロトコルは、同一宛先への複数の最適な同一コストのルートを持ちます。これらのルートの優先順位は同じであり、同一コストで複数パス(ECMP)のロードバランス（負荷分散）を行い転送できます。

スタティックルーティング、IPv6 スタティックルーティング、RIP、RIPng、OSPF、OSPFv3 がロードバランスをサポートしています。

1.5 ルートバックアップ

ルートバックアップはネットワークの信頼性を向上させます。ルートバックアップを用いて、最も優先度が高いルートをプライマリルートに設定し、残りをセカンダリルートにすることで、同一宛先に複数のルートを設定することができます。

通常時、パケットはプライマリルートで転送されます。障害などが発生したとき、セカンダリルートの中で最も優先度が高いルートでパケットが転送されます。障害が復旧したとき、ルートの選択が行われ、プライマリルートでパケットが転送されます。

1.6 ルート再帰

ネクストホップに直接接続されていない、スタティックルートを使用する場合、ルータはネクストホップに届く送信インタフェースを検索するため、ルート再帰を行う必要があります。

OSPF のようなリンクステートプロトコルはルート再帰の必要がありません。リンクステートプロトコルはルートの計算を通して直接接続されたネクストホップを取得します。

RIB は、関連したルート、ルート再帰のパス、およびルート再帰の depth についての概要情報を含めて、ルート再帰情報を記録し、保存します。

1.7 ルート再分配

ルート再分配はお互いにルート情報を学習するルーティングプロトコルで有効となります。ダイナミックルーティングプロトコルは、ダイレクト、スタティックルーティングを含む他のルーティングプロトコルからのルートを再分配することができます。詳細は、オペレーションマニュアルの関連する章を参照してください。

RIB はルーティングプロトコルの再分配の情報を記録します。

1.8 RIB NSRの設定

I. RIB NSR

アクティブ/スタンバイスイッチオーバーが発生すると、ノンストップルーティング (NSR) によってアクティブプロセスからスタンバイプロセスにルーティング情報がバックアップされ、ルーティングフラッピングが回避され、転送の継続性が確保されます。

RIB NSR は、アクティブ/スタンバイスイッチオーバー中にプロトコル NSR よりも高速なルートコンバージェンスを提供します。

II. 制限とガイドライン

ルートタイムアウトおよびトラフィック割り込みを回避するには、プロトコル GR または NSR とともにこの機能を使用します。

III. 設定手順(IPv4)

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. RIB view に移行する	**rib**	―
3. RIB IPv4 アドレスファミリーを作成し、RIB IPv4 address family view に移行する	**address-family ipv4**	―
4. IPv 4 RIB NSR を有効にする	**non-stop-routing**	デフォルト：無効

IV. 設定手順 (IPv 6)

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. RIB view に移行する	**rib**	―
3. RIB IPv6 アドレスファミリーを作成し、RIB IPv6 address family view に移行する	**address-family ipv6**	―

操作	コマンド	補足
4． IPv 6 RIB NSR を有効にする	**non-stop-routing**	デフォルト：無効

1.9 装置でサポートされるアクティブルートの最大数の設定

I. 装置でサポートされるアクティブルートの最大数の設定

この機能により、装置がサポートするアクティブな IPv4/IPv6 ルートの最大数を設定できます。アクティブな IPv4/IPv6 ルートの最大数を超えると、装置はまだ新しいアクティブルートを受け入れますが、システムログメッセージを生成します。メッセージにもとづいて関連するアクションを実行して、システムリソースを節約できます。

II. 設定手順(IPv4)

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． RIB view に移行する	**rib**	―
3． RIB IPv4 アドレスファミリーを作成し、RIB IPv4 address family view に移行する	**address-family ipv4**	―
4． 装置でサポートされるアクティブルートの最大数を設定する	**routing-table limit** *number* **simply-alert**	デフォルト：設定なし RIB IPv4 address family viewでの設定は、パブリックネットワークおよびVPNインスタンスのアクティブIPv4ルートの数を制限します。

III. 設定手順(IPv6)

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． RIB view に移行する	**rib**	―
3． RIB IPv6 アドレスファミリーを作成し、RIB IPv6 address family view に移行する	**address-family ipv6**	―
4． 装置でサポートされるアクティブルートの最大数を設定する	**routing-table limit** *number* **simply-alert**	デフォルト：設定なし RIB IPv6 address family viewでの設定は、パブリックネットワークおよびVPNインスタンスのアクティブIPv6ルートの数を制限します。

1.10 ルーティングテーブルの表示と維持

すべての view で **display** コマンドを実行でき、user view で **reset** コマンドを実行できます。

操作	コマンド
ルーティングテーブルの情報を表示する	**display ip routing-table** [**verbose**]
標準IPv4 ACLで許可されているルーティング情報を表示する	**display ip routing-table acl** *ipv4-acl-number* [**verbose**]
指定した宛先アドレスへのルート情報を表示する	**display ip routing-table** *ip-address* [*mask-length* | *mask*] [**longer-match**] [**verbose**]
指定した範囲内の宛先アドレスを持つルート情報を表示する	**display ip routing-table** *ip-address1* **to** *ip-address2* [**verbose**]
IPプレフィックスリストで許可されているルーティング情報を表示する	**display ip routing-table prefix-list** *prefix-list-name* [**verbose**]
ルートのルーティングプロトコルを表示する	**display ip routing-table protocol** *protocol* [**inactive** | **verbose**]
IPv4ルーティングテーブルの統計情報を表示する	**display ip routing-table statistics**
IPv4ルーティングテーブルの統計情報を削除する	**reset ip routing-table statistics protocol** { *protocol* | **all** }
IPv6ルーティングテーブルの統計情報を表示する	**display ipv6 routing-table** [**verbose**]
IPv6宛先アドレスへのルート情報を表示する	**display ipv6 routing-table** *ipv6-address* [*prefix-length*] [**longer-match**] [**verbose**]
標準IPv6 ACLで許可されているルーティング情報を表示する	**display ipv6 routing-table acl** *ipv6-acl-number* [**verbose**]
指定した範囲内のIPv6宛先アドレスを持つルート情報を表示する	**display ipv6 routing-table** *ipv6-address1* **to** *ipv6-address2* [**verbose**]
IPv6プレフィックスリストで許可されているルーティング情報を表示する	**display ipv6 routing-table prefix-list** *prefix-list-name* [**verbose**]
ルートのIPv6ルーティングプロトコルを表示する	**display ipv6 routing-table protocol** *protocol* [**inactive** | **verbose**]
IPv6ルーティングテーブルの統計情報を表示する	**display ipv6 routing-table statistics**
IPv6ルーティングテーブルの統計情報を削除する	**reset ipv6 routing-table statistics protocol** { *protocol* | **all** }

目次

このセクションのページは **5-x-x** です。

2 章 スタティックルーティング 2-1
2.1 スタティックルートの設定 2-1
2.2 スタティックルートでの BFD の設定 2-1
2.2.1 BFD コントロールパケットモード 2-2
2.2.2 Single ホップエコーパケットモード 2-2
2.3 スタティックルートの表示と維持 2-3
2.4 スタティックルートの設定例 2-3
2.4.1 基本的なスタティックルート設定例 2-3
2.4.2 BFD スタティックルートの設定例（ダイレクトネクストホップ） 2-5
2.4.3 BFD スタティックルートの設定例（インダイレクトネクストホップ） 2-8

2章 スタティックルーティング

スタティックルートは手動で設定します。ネットワークの構成が簡単であれば、スタティックルートの設定だけで問題なく運用することができます。ただし、ネットワーク障害やトポロジの変化が起きた場合、ネットワーク管理者がスタティックルートを修正する必要があります。

2.1 スタティックルートの設定

スタティックルートの設定を行う前に以下の設定が完了していることを確認してください。

- 関係するインタフェースの物理パラメータの設定
- 関係するインタフェースのリンクレイヤの設定
- 関係するインタフェースの IP アドレスの設定

以下にスタティックルートの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. スタティックルートを設定する	**ip route-static** *dest-address* { *mask-length* | *mask* } { *interface-type interface-number* [*next-hop-address*] | *next-hop-address* [**bfd control-packet bfd-source** *ip-address* | **permanent**] } [**preference** *preference*] [**description** *text*]	デフォルト：設定なし
3. （オプション設定項目）スタティックルートのデフォルトプリファレンスを設定する	**ip route-static default-preference** *default-preference*	デフォルト：60
4. （オプション設定項目）デフォルトルートを含むすべてのルートを削除する	**delete static-routes all**	1つのスタティックルートを削除するには、**undo ip route-static**コマンドを使用します。

2.2 スタティックルートでのBFDの設定

重要：

BFD が有効になっていると、ルートフラップを悪化させる可能性があります。

BFD（Bidirectional forwarding detection）は、一般的な用途、標準な用途、および手段、プロトコルから独立して、素早い障害検知メカニズムを提供します。BFD は、ルーティングプロトコルのような上位層のプロトコルの 2 台のルータ間の双方向の転送経路の障害を、一様で早急に検出することができます。

BFD に関する詳細は、オペレーションマニュアルのセクション 10 *高可用性* "*BFD*"を参照してください。

2.2.1 BFD コントロールパケットモード

2 つの装置間の双方向検知のために、BFD コントロールパケットを使用するには、各装置のピア宛のスタティックルートで BFD コントロールパケットモードを有効にする必要があります。

スタティックルートを設定し、BFD コントロールパケットモードを有効にするために、以下の 1 つを使用します。

- 出力インタフェースと直接接続されたネクストホップを指定します。
- 直接接続されていないネクストホップと指定された BFD パケットの送信元アドレスを指定します。

以下にスタティックルート（ダイレクトネクストホップ）での BFD コントロールモードの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. スタティックルートで BFD コントロールパケットモードを有効にする	**ip route-static** *dest-address* { *mask-length* | *mask* } *interface-type interface-number next-hop-address* **bfd control-packet** [**preference** *preference*] [**tag** *tag-value*] [**description** *text*]	デフォルト：設定なし

以下にスタティックルート（インダイレクトネクストホップ）での BFD コントロールモードの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. スタティックルートで BFD コントロールパケットモードを有効にする	**ip route-static** *dest-address* { *mask-length* | *mask* } { *next-hop-address* **bfd control-packet bfd-source** *ip-address* } [**preference** *preference*] [**tag** *tag-value*] [**description** *text*]	デフォルト：設定なし

2.2.2 Single ホップエコーパケットモード

スタティックルートで BFD エコーパケットモードを有効にすると、ローカル装置は BFD エコーパケットをピアへ送信します。ピアからの応答によって装置間のリンクのテストを行います。

重要:
BFD はスプーフィング属性の出力インタフェースでスタティックルートを設定することはできません。

以下にスタティックルートでの BFD エコーパケットモードの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. エコーパケットの送信元アドレスを設定する	**bfd echo-source-ip** *ip-address*	デフォルト：設定なし 詳細はコマンドマニュアルのセクション10 *高可用性" BFD"* を参照してください。
3. スタティックルートで BFD エコーパケットモードを有効にする	**ip route-static** *dest-address* { *mask-length* | *mask* } *interface-type interface-number next-hop-address* **bfd echo-packet** [**preference** *preference*] [**tag** *tag-value*] [**description** *text*]	デフォルト：設定なし

2.3 スタティックルートの表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
スタティックルート情報を表示する	**display ip routing-table protocol static** [**inactive** | **verbose**]

2.4 スタティックルートの設定例

2.4.1 基本的なスタティックルート設定例

I. ネットワーク要件

図 2-1に示すように、2 つのホスト間で相互接続できるように、スイッチでスタティックルートを設定します。

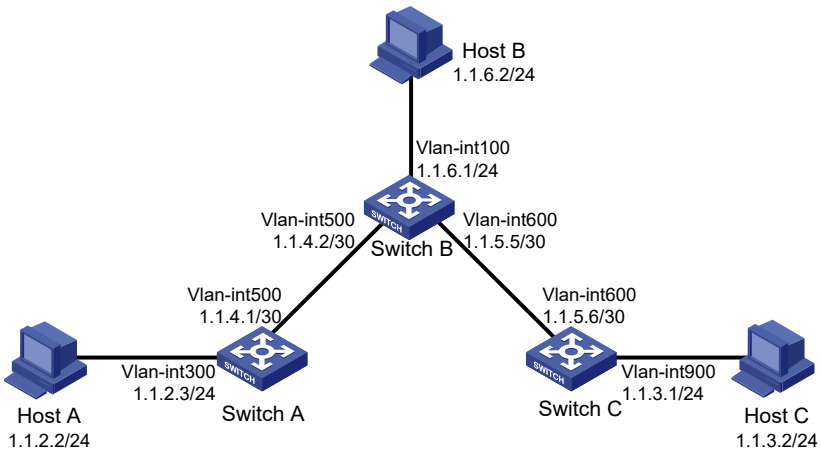


図 2-1 ネットワーク図

II. 設定手順

1) インタフェースの IP アドレスを設定します。（詳細は省略します）
2) スタティックルートを設定します。

Switch A にデフォルトルートを設定します。

```
<SwitchA> system-view
[SwitchA] ip route-static 0.0.0.0 0.0.0.0 1.1.4.2
```

Switch B に 2 つのスタティックルートを設定します。

```
<SwitchB> system-view
[SwitchB] ip route-static 1.1.2.0 255.255.255.0 1.1.4.1
[SwitchB] ip route-static 1.1.3.0 255.255.255.0 1.1.5.6
```

Switch C にデフォルトルートを設定します。

```
<SwitchC> system-view
[SwitchC] ip route-static 0.0.0.0 0.0.0.0 1.1.5.5
```

3) Host A、Host B、Host C にそれぞれ 1.1.2.3、1.1.6.1、1.1.3.1 のデフォルトゲートウェイアドレスを設定します。（詳細は省略します）

III. 設定の確認

Switch A のスタティックルートを表示します。

```
[SwitchA] display ip routing-table protocol static

Summary Count : 1

Static Routing table Status : <Active>
Summary Count : 1

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
0.0.0.0/0           Static 60   0            1.1.4.2         Vlan500
```

```
Static Routing table Status : <Inactive>
Summary Count : 0
```

Switch B のスタティックルートを表示します。

```
[SwitchB] display ip routing-table protocol static

Summary Count : 2

Static Routing table Status : <Active>
Summary Count : 2

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
1.1.2.0/24          Static 60   0            1.1.4.1         Vlan500

Static Routing table Status : <Inactive>
Summary Count : 0
```

Host B で **ping** コマンドを使用し、ホスト A への接続を確認します。（2 つのホストは Windows XP で動作していると仮定します。）

```
C:\Documents and Settings\Administrator>ping 1.1.2.2

Pinging 1.1.2.2 with 32 bytes of data:

Reply from 1.1.2.2: bytes=32 time=1ms TTL=126
Reply from 1.1.2.2: bytes=32 time=1ms TTL=126
Reply from 1.1.2.2: bytes=32 time=1ms TTL=126
Reply from 1.1.2.2: bytes=32 time=1ms TTL=126

Ping statistics for 1.1.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

Host B で **tracert** コマンドを使用し、Host A への接続を確認します。

```
C:\Documents and Settings\Administrator>tracert 1.1.2.2

Tracing route to 1.1.2.2 over a maximum of 30 hops

  1    <1 ms    <1 ms    <1 ms  1.1.6.1
  2    <1 ms    <1 ms    <1 ms  1.1.4.1
  3     1 ms    <1 ms    <1 ms  1.1.2.2

Trace complete.
```

2.4.2 BFD スタティックルートの設定例（ダイレクトネクストホップ）

I. ネットワーク要件

図 2-2に示すように設定します。

- Switch A のサブネット 120.1.1.0/24 にスタティックルートを設定します。
- Switch B のサブネット 120.1.1.0/24 にスタティックルートを設定します。
- 両方のルートに BFD を有効にします。
- Switch C のサブネット 120.1.1.0/24、121.1.1.0/24 にスタティックルートを設定します。

レイヤ 2 スイッチを経由した Switch A と Switch B 間のリンクが故障したとき、すぐに故障を検出し、Switch C を使用して Switch A と Switch B 間で通信ができるように BFD を有効にします。

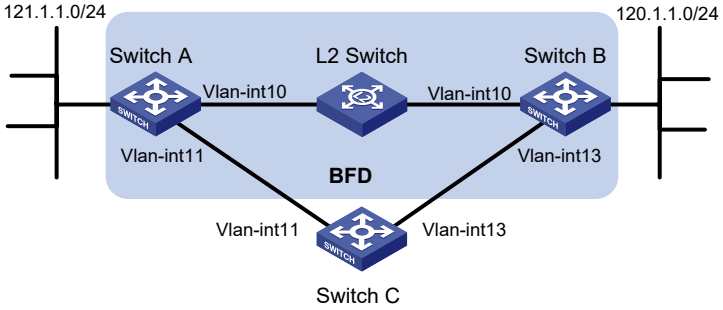


図 2-2 ネットワーク図

表 2-1 インタフェースと IP アドレスの割り当て

装置	インタフェース	IP アドレス	装置	インタフェース	IP アドレス
Switch A	VLAN-interface 10	12.1.1.1/24	Switch B	VLAN-interface 10	12.1.1.2/24
Switch A	VLAN-interface 11	10.1.1.102/24	Switch B	VLAN-interface 13	13.1.1.1/24
Switch C	VLAN-interface 11	10.1.1.100/24			
Switch C	VLAN-interface 13	13.1.1.2/24			

II. 設定手順

1)　インタフェースの IP アドレスを設定します。（詳細は省略します）
2)　スタティックルートと BFD を設定します。

Switch A にスタティックルートを設定し、レイヤ 2 スイッチを通してスタティックルートを行うため BFD コントロールパケットモードを有効にします。

```
<SwitchA> system-view
[SwitchA] interface vlan-interface 10
[SwitchA-vlan-interface10] bfd min-transmit-interval 500
[SwitchA-vlan-interface10] bfd min-receive-interval 500
[SwitchA-vlan-interface10] bfd detect-multiplier 9
[SwitchA-vlan-interface10] quit
[SwitchA] ip route-static 120.1.1.0 24 vlan-interface 10 12.1.1.2 bfd control-packet
[SwitchA] ip route-static 120.1.1.0 24 vlan-interface 11 10.1.1.100 preference 65
[SwitchA] quit
```

Switch B にスタティックルートを設定し、レイヤ 2 スイッチを通してスタティックルートを行うため BFD コントロールパケットモードを有効にします。

```
<SwitchB> system-view
[SwitchB] interface vlan-interface 10
```

```
[SwitchB-vlan-interface10] bfd min-transmit-interval 500
[SwitchB-vlan-interface10] bfd min-receive-interval 500
[SwitchB-vlan-interface10] bfd detect-multiplier 9
[SwitchB-vlan-interface10] quit
[SwitchB] ip route-static 121.1.1.0 24 vlan-interface 10 12.1.1.1 bfd control-packet
[SwitchB] ip route-static 121.1.1.0 24 vlan-interface 13 13.1.1.2 preference 65
[SwitchB] quit
```

Switch C にスタティックルートを設定します。

```
<SwitchC> system-view
[SwitchC] ip route-static 120.1.1.0 24 13.1.1.1
[SwitchC] ip route-static 121.1.1.0 24 10.1.1.102
```

III. 設定の確認

Switch A の BFD セッションを表示します。

```
<SwitchA> display bfd session

 Total Session Num: 1     Up Session Num: 1     Init Mode: Active

 IPv4 Session Working Under Ctrl Mode:

 LD/RD          SourceAddr      DestAddr        State    Holdtime    Interface
 4/7            12.1.1.1        12.1.1.2        Up       2000ms      Vlan10
```

出力は、BFD セッションが作成されたことを示しています。

Switch A のスタティックルート情報を表示します。

```
<SwitchA> display ip routing-table protocol static

Summary Count : 1

Static Routing table Status : <Active>
Summary Count : 1

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
120.1.1.0/24        Static 60   0            12.1.1.2        Vlan10

Static Routing table Status : <Inactive>
Summary Count : 0
```

出力では、Switch A は VLAN インタフェース 10 を経由して Switch B と通信していることを示しています。

そして VLAN インタフェース 10 を経由したリンクが故障します。

Switch A のスタティックルート情報を表示します。

```
<SwitchA> display ip routing-table protocol static

Summary Count : 1

Static Routing table Status : <Active>
```

```
Summary Count : 1

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
120.1.1.0/24        Static 65   0            10.1.1.100      Vlan11

Static Routing table Status : <Inactive>
Summary Count : 0
```

出力では、Switch A は VLAN インタフェース 11 を経由して Switch B と通信していることを示しています。

2.4.3 BFD スタティックルートの設定例（インダイレクトネクストホップ）

I. ネットワーク要件

図 2-3に示すように設定します。

- Switch A は、VLAN インタフェース 10 の出力インタフェースにて Switch B のループバック 1（2.2.2.9/32）へのルートを持っています。
- Switch B は、VLAN インタフェース 12 の出力インタフェースにて Switch B のループバック 1（1.1.1.9/32）へのルートを持っています。
- Switch D は、VLAN インタフェース 10 の出力インタフェースにて 1.1.1.9/32、VLAN インタフェース 12 の出力インタフェースにて 2.2.2.9/32 へのルートを持っています。

以下のようにスタティックルートを設定します。

- Switch A にサブネット 120.1.1.0/24 のスタティックルートを設定します。
- Switch B にサブネット 121.1.1.0/24 のスタティックルートを設定します。
- 両方のルートで BFD を有効にします。
- Switch C と Switch D の両方でサブネット 120.1.1.0/24 とサブネット 121.1.1.0/24 へのスタティックルートを設定します。

Switch A と Switch B 間の Switch D が故障したとき、すぐさま Switch C で検出し、通信できるように BFD を有効にします。

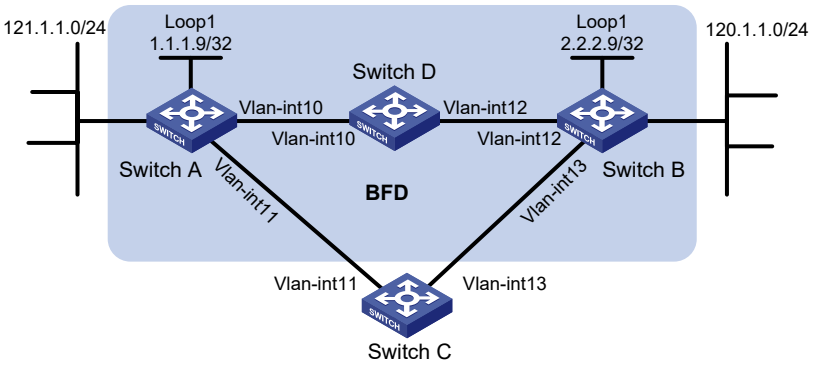


図 2-3 ネットワーク図

表 2-2 インタフェースと IP アドレスの割り当て

装置	インタフェース	IP アドレス	装置	インタフェース	IP アドレス
Switch A	Vlan-interface10	12.1.1.1/24	Switch B	Vlan-interface12	11.1.1.1/24
Switch A	Vlan-interface11	10.1.1.102/24	Switch B	Vlan-interface13	13.1.1.1/24

装置	インタフェース	IP アドレス	装置	インタフェース	IP アドレス
Switch A	Loop1	1.1.1.9/32	Switch B	Loop1	2.2.2.9/32
Switch C	Vlan-interface11	10.1.1.100/24	Switch D	Vlan-interface10	12.1.1.2/24
Switch C	Vlan-interface13	13.1.1.2/24	Switch D	Vlan-interface12	11.1.1.2/24

II. 設定手順

1)　インタフェースの IP アドレスを設定します。（詳細は省略します）
2)　スタティックルートと BFD を設定します。

Switch A にスタティックルートを設定し、Switch D を通してスタティックルートを行うため BFD コントロールパケットモードを有効にします。

```
<SwitchA> system-view
[SwitchA] bfd multi-hop min-transmit-interval 500
[SwitchA] bfd multi-hop min-receive-interval 500
[SwitchA] bfd multi-hop detect-multiplier 9
[SwitchA] ip route-static 120.1.1.0 24 2.2.2.9 bfd control-packet bfd-source 1.1.1.9
[SwitchA] ip route-static 120.1.1.0 24 vlan-interface 11 10.1.1.100 preference 65
[SwitchA] quit
```

Switch B にスタティックルートを設定し、Switch D を通してスタティックルートを行うため BFD コントロールパケットモードを有効にします。

```
<SwitchB> system-view
[SwitchB] bfd multi-hop min-transmit-interval 500
[SwitchB] bfd multi-hop min-receive-interval 500
[SwitchB] bfd multi-hop detect-multiplier 9
[SwitchB] ip route-static 121.1.1.0 24 1.1.1.9 bfd control-packet bfd-source 2.2.2.9
[SwitchB] ip route-static 121.1.1.0 24 vlan-interface 13 13.1.1.2 preference 65
[SwitchB] quit
```

Switch C にスタティックルートを設定します。

```
<SwitchC> system-view
[SwitchC] ip route-static 120.1.1.0 24 13.1.1.1
[SwitchC] ip route-static 121.1.1.0 24 10.1.1.102
```

Switch D にスタティックルートを設定します。

```
<SwitchD> system-view
[SwitchD] ip route-static 120.1.1.0 24 11.1.1.1
[SwitchD] ip route-static 121.1.1.0 24 12.1.1.1
```

III. 設定の確認

Switch A の BFD セッションを表示します。

```
<SwitchA> display bfd session

 Total Session Num: 1     Up Session Num: 1     Init Mode: Active

 IPv4 Session Working Under Ctrl Mode:

 LD/RD          SourceAddr      DestAddr        State    Holdtime     Interface
 4/7            1.1.1.9         2.2.2.9         Up       2000ms       N/A
```

出力では BFD セッションが作成されたことを示しています。

Switch A のスタティックルートを表示します。

```
<SwitchA> display ip routing-table protocol static

Summary Count : 1

Static Routing table Status : <Active>
Summary Count : 1

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
120.1.1.0/24        Static 60   0            12.1.1.2        Vlan10

Static Routing table Status : <Inactive>
Summary Count : 0
```

出力では、Switch A は VLAN インタフェース 10 を経由して Switch B と通信していることを示しています。

そして VLAN インタフェース 10 を経由したリンクが故障します。

Switch A のスタティックルートを表示します。

```
<SwitchA> display ip routing-table protocol static

Summary Count : 1

Static Routing table Status : <Active>
Summary Count : 1

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
120.1.1.0/24        Static 65   0            10.1.1.100      Vlan11

Static Routing table Status : <Inactive>
Summary Count : 0
```

出力では、Switch A は VLAN インタフェース 11 を経由して Switch B と通信していることを示しています。

目次

このセクションのページは **5-x-x** です。

3 章 デフォルトルート 3-1

3章 デフォルトルート

デフォルトルートはルーティングテーブルの指定したルーティングエントリにマッチしないパケットを転送するのに使用されます。デフォルトルートが設定されていない場合、ルーティングエントリにマッチしないパケットは廃棄され、ICMP 到達不能パケットが送信元に送信されます。

デフォルトルートは以下のいずれかの方法で設定することができます。

- ネットワーク管理者が宛先アドレスとマスクを 0.0.0.0 に設定します。詳細はオペレーションマニュアルのセクション 5 *ルーティングプロトコル "スタティックルーティング"*を参照してください。
- OSPF、RIP のようなダイナミックルーティングプロトコルは、デフォルトルートを作成できます。たとえば OSPF が動作している上流のルータはデフォルトルートを作成し、他のルータに配信することができます。そのルータは上流のルータがネクストホップとなるようにデフォルトルートを設定します。詳細は、関連するオペレーションマニュアルのセクション 5 *ルーティングプロトコル*を参照してください。

目次

このセクションのページは **5-x-x** です。

4 章 IPv6 スタティックルーティング 4-1
4.1 IPv6 スタティックルートの設定 4-1
4.2 IPv6 スタティックルートでの BFD の設定 4-1
4.2.1 BFD コントロールパケットモード 4-2
4.3 IPv6 スタティックルートの表示と維持 4-2
4.4 IPv6 スタティックルート設定例 4-3
4.4.1 基本的な IPv6 スタティックルート設定例 4-3
4.4.2 BFD の IPv6 スタティックルートの設定例(ダイレクトネクストホップ) 4-4
4.4.3 BFD の IPv6 スタティックルートの設定例(インダイレクトネクストホップ) 4-7

4章 IPv6 スタティックルーティング

スタティックルートは手動で設定されます。ネットワークのトポロジの変化に対応できません。ネットワークが故障、あるいはトポロジの変更が行われた場合、ネットワーク管理者は手動でスタティックルートを修正する必要があります。IPv6 スタティックルーティングも同様に簡単な IPv6 ネットワークで動作します。

4.1 IPv6スタティックルートの設定

IPv6 スタティックルートの設定を行う前に以下の設定が完了していることを確認してください。

- 関係するインタフェースのパラメータを設定してください。
- 関係するインタフェースのリンクレイヤを設定してください。
- 隣接ノードが互いに通信可能であることを確認してください。

以下に IPv6 スタティックルートの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. IPv6スタティックルートを設定する	**ipv6 route-static** *ipv6-address prefix-length interface-type interface-number next-hop-address* **bfd control-packet** [**preference** *preference*] [**description** *text*]	デフォルト：設定なし
3. (オプション設定項目)IPv6スタティックルートのデフォルトプリファレンスを設定する	**ipv6 route-static default-preference** *default-preference-value*	デフォルト：60
4. (オプション設定項目)デフォルトルートを含むすべての IPv6スタティックルートを削除する	**delete ipv6 static-routes all**	1つのIPv6スタティックルートを削除するには、**undo ipv6 route-static** コマンドを使用します。

4.2 IPv6スタティックルートでのBFDの設定

BFD(Bidirectional forwarding detection)は、一般的な用途、標準な用途、および手段、プロトコルから独立して、素早い障害検知メカニズムを提供します。BFD は、ルーティングプロトコルのようなプロトコルように、上位層のプロトコルの 2 台のルータ間の双方向の転送経路の障害を、一様で早急に検出することができます。BFD に関する詳細は、オペレーションマニュアルのセクション 10 *高可用性* "*BFD*"を参照してください。

⚠ **重要:**
BFD が有効になっていると、ルートフラップを悪化させる可能性があります。

4.2.1 BFD コントロールパケットモード

2 つの装置間の双方向検知のために、BFD コントロールパケットを使用するには、各装置のピア宛のスタティックルートで BFD コントロールパケットモードを有効にする必要があります。

スタティックルートを設定し、BFD コントロールパケットモードを有効にするために、以下の 1 つを使用します。

- 出力インタフェースと直接接続されたネクストホップを指定します。
- 直接接続されていないネクストホップと指定された BFD パケットの送信元アドレスを指定します。

以下に IPv6 スタティックルート(ダイレクトネクストホップ)での BFD コントロールモードの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. IPv6 スタティックルートで BFD コントロールパケットモードを有効にする	**ipv6 route-static** *ipv6-address prefix-length interface-type interface-number next-hop-address* **bfd control-packet** [**preference** *preference*] [**description** *text*]	デフォルト：設定なし

以下に IPv6 スタティックルート(インダイレクトネクストホップ)での BFD コントロールモードの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. IPv6 スタティックルートで BFD コントロールパケットモードを有効にする	**ipv6 route-static** *ipv6-address prefix-length* { *next-hop-address* **bfd control-packet bfd-source** *ipv6-address* } [**preference** *preference*] [**description** *description*]	デフォルト：設定なし

4.3 IPv6スタティックルートの表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
IPv6スタティックルート情報を表示する	**display ipv6 routing-table protocol static** [**inactive** | **verbose**]

4.4 IPv6スタティックルート設定例

4.4.1 基本的な IPv6 スタティックルート設定例

I. ネットワーク要件

図 4-1に示すように、2 つのホスト間で相互接続できるように、IPv6 スタティックルートを設定します。

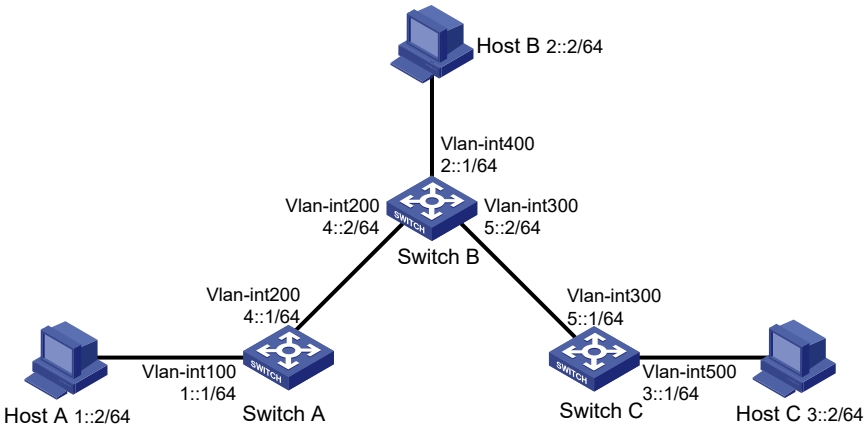


図 4-1 ネットワーク図

II. 設定手順

1) すべての VLAN インタフェースの IPv6 アドレスを設定します。(詳細は省略します)
2) IPv6 スタティックルートを設定します。

Switch A に IPv6 デフォルトスタティックルートを設定します。

```
<SwitchA> system-view
[SwitchA] ipv6 route-static :: 0 4::2
```

Switch B に 2 つの IPv6 スタティックルートを設定します。

```
<SwitchB> system-view
[SwitchB] ipv6 route-static 1:: 64 4::1
[SwitchB] ipv6 route-static 3:: 64 5::1
```

Switch C にデフォルト IPv6 スタティックルートを設定します。

```
<SwitchC> system-view
[SwitchC] ipv6 route-static :: 0 5::2
```

3) Host A、Host B、Host C にそれぞれ 1::1、2::1、3::1 のデフォルトゲートウェイアドレスを設定します。(詳細は省略します)

III. 設定の確認

Switch A の IPv6 スタティックルートを表示します。

```
[SwitchA] display ipv6 routing-table protocol static

Summary Count : 1

Static Routing table Status : <Active>
Summary Count : 1

Destination: ::                                          Protocol  : Static
NextHop    : 4::2                                        Preference: 60
Interface  : Vlan-interface200                           Cost      : 0

Static Routing table Status : <Inactive>
Summary Count : 0
```

Switch B の IPv6 スタティックルートを表示します。

```
[SwitchB] display ipv6 routing-table protocol static

Summary Count : 2

Static Routing table Status : <Active>
Summary Count : 2

Destination: 1::/64                                      Protocol  : Static
NextHop    : 4::1                                        Preference: 60
Interface  : Vlan-interface200                           Cost      : 0

Destination: 3::/64                                      Protocol  : Static
NextHop    : 5::1                                        Preference: 60
Interface  : Vlan-interface300                           Cost      : 0

Static Routing table Status : <Inactive>
Summary Count : 0
```

Host B で **ping** コマンドを使用し、接続を確認します。

```
[SwitchA] ping ipv6 3::1
Ping6(56 data bytes) 4::1 --> 3::1, press CTRL_C to break
56 bytes from 3::1, icmp_seq=0 hlim=62 time=0.700 ms
56 bytes from 3::1, icmp_seq=1 hlim=62 time=0.351 ms
56 bytes from 3::1, icmp_seq=2 hlim=62 time=0.338 ms
56 bytes from 3::1, icmp_seq=3 hlim=62 time=0.373 ms
56 bytes from 3::1, icmp_seq=4 hlim=62 time=0.316 ms

--- Ping6 statistics for 3::1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.316/0.416/0.700/0.143 ms
```

4.4.2 BFD の IPv6 スタティックルートの設定例(ダイレクトネクストホップ)

I. ネットワーク要件

図 4-2に示すように設定します。

- Switch A のサブネット 120::/64 に IPv6 スタティックルートを設定します。
- Switch B のサブネット 121::/64 に IPv6 スタティックルートを設定します。

- 両方のルートに BFD を有効にします。
- Switch C のサブネット 120::/64、121::/64 にスタティックルートを設定します。

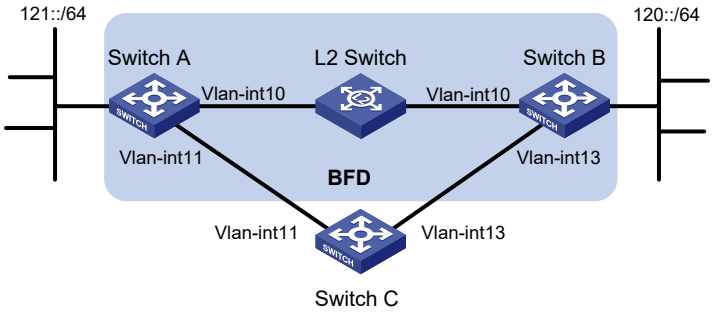


図 4-2 ネットワーク図

表 4-1 インタフェースと IPv6 アドレスの割り当て

装置	インタフェース	IPv6アドレス	装置	インタフェース	IPv6アドレス
Switch A	Vlan-interface10	12::1/64	Switch B	Vlan-interface13	13::1/64
Switch A	Vlan-interface11	10::102/64	Switch C	Vlan-interface11	10:: 100/64
Switch B	Vlan-interface10	12::2/64	Switch C	Vlan-interface13	13::2/64

II. 設定手順

1)　インタフェースの IPv6 アドレスを設定します。(詳細は省略します)
2)　IPv6 スタティックルートと BFD を設定します。

Switch A に IPv6 スタティックルートを設定し、レイヤ 2 スイッチを通してスタティックルートを行うため BFD コントロールパケットモードを有効にします。

```
<SwitchA> system-view
[SwitchA] interface vlan-interface 10
[SwitchA-vlan-interface10] bfd min-transmit-interval 500
[SwitchA-vlan-interface10] bfd min-receive-interval 500
[SwitchA-vlan-interface10] bfd detect-multiplier 9
[SwitchA-vlan-interface10] quit
[SwitchA] ipv6 route-static 120:: 64 vlan-interface 10 12::2 bfd control-packet
[SwitchA] ipv6 route-static 120:: 64 10::100 preference 65
[SwitchA] quit
```

Switch B に IPv6 スタティックルートを設定し、レイヤ 2 スイッチを通してスタティックルートを行うため BFD コントロールパケットモードを有効にします。

```
<SwitchB> system-view
[SwitchB] interface vlan-interface 10
[SwitchB-vlan-interface10] bfd min-transmit-interval 500
```

```
[SwitchB-vlan-interface10] bfd min-receive-interval 500
[SwitchB-vlan-interface10] bfd detect-multiplier 9
[SwitchB-vlan-interface10] quit
[SwitchB] ipv6 route-static 121:: 64 vlan-interface 10 12::1 bfd control-packet
[SwitchB] ipv6 route-static 121:: 64 vlan-interface 13 13::2 preference 65
[SwitchB] quit
```

Switch C に IPv6 スタティックルートを設定します。

```
<SwitchC> system-view
[SwitchC] ipv6 route-static 120:: 64 13::1
[SwitchC] ipv6 route-static 121:: 64 10::102
```

III. 設定の確認

Switch A の BFD セッションを表示します。

```
<SwitchA> display bfd session

 Total Session Num: 1     Up Session Num: 1     Init Mode: Active

 IPv6 Session Working Under Ctrl Mode:

       Local Discr: 513                 Remote Discr: 33
         Source IP: 12::1
    Destination IP: 12::2
     Session State: Up                      Interface: Vlan10
         Hold Time: 2012ms
```

出力は、BFD セッションが作成されたことを示しています。

Switch A の IPv6 スタティックルート情報を表示します。

```
<SwitchA> display ipv6 routing-table protocol static

Summary Count : 1

Static Routing table Status : <Active>
Summary Count : 1

Destination: 120::/64                                   Protocol  : Static
NextHop    : 12::2                                      Preference: 60
Interface  : Vlan10                                     Cost      : 0

Direct Routing table Status : <Inactive>
Summary Count : 0
```

出力では、Switch A は VLAN インタフェース 10 を経由して Switch B と通信していることを示しています。

そして VLAN インタフェース 10 を経由したリンクが故障します。

Switch A の IPv6 スタティックルート情報を表示します。

```
<SwitchA> display ipv6 routing-table protocol static

Summary Count : 1
```

```
Static Routing table Status : <Active>
Summary Count : 1

Destination: 120::/64                                   Protocol   : Static
NextHop    : 10::100                                    Preference: 65
Interface  : Vlan11                                     Cost       : 0

Static Routing table Status : < Inactive>
Summary Count : 0
```

出力では、Switch A は VLAN インタフェース 11 を経由して Switch B と通信していることを示しています。

4.4.3 BFD の IPv6 スタティックルートの設定例(インダイレクトネクストホップ)

I. ネットワーク要件

図 4-3に示すように設定します。

- Switch A は、VLAN インタフェース 10 の出力インタフェースにて Switch B のループバック 1(2::9/128)へのルートを持っています。
- Switch B は、VLAN インタフェース 12 の出力インタフェースにて Switch B のループバック 1(1::9/128)へのルートを持っています。
- Switch D は、VLAN インタフェース 10 の出力インタフェースにて 1.1.1.9/32、VLAN インタフェース 12 の出力インタフェースにて 2::9/128 へのルートを持っています。

以下のように IPv6 スタティックルートを設定します。

- Switch A にサブネット 120::/64 の IPv6 スタティックルートを設定します。
- Switch B にサブネット 121::/64 の IPv6 スタティックルートを設定します。
- 両方のルートで BFD を有効にします。
- Switch C と Switch D の両方でサブネット 120::/64 とサブネット 121::/64 への IPv6 スタティックルートを設定します。

Switch A と Switch B 間の Switch D が故障したとき、すぐさま Switch C で検出し、通信できるように BFD を有効にします。

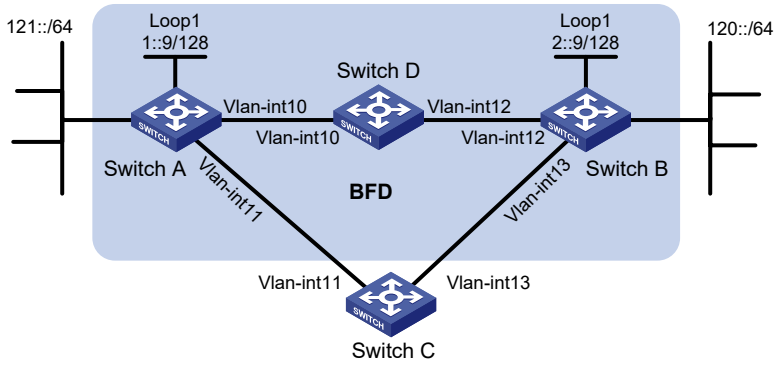


図 4-3 ネットワーク図

表 4-2 インタフェースと IPv6 アドレスの割り当て

装置	インタフェース	IPv6アドレス	装置	インタフェース	IPv6アドレス
Switch A	Vlan-interface10	12::1/64	Switch B	Vlan-interface12	11::2/64
Switch A	Vlan-interface11	10::102/64	Switch B	Vlan-interface13	13::1/64
Switch A	Loop1	1::9/128	Switch B	Loop1	2::9/128
Switch C	Vlan-interface11	10::100/64	Switch D	Vlan-interface10	12::2/64
Switch C	Vlan-interface13	13::2/64	Switch D	Vlan-interface12	11::1/64

II. 設定手順

1)　インタフェースの IPv6 アドレスを設定します。(詳細は省略します)
2)　IPv6 スタティックルートと BFD を設定します。

Switch A に IPv6 スタティックルートを設定し、Switch D を通して IPv6 スタティックルートを行うため BFD コントロールパケットモードを有効にします。

```
<SwitchA> system-view
[SwitchA] bfd multi-hop min-transmit-interval 500
[SwitchA] bfd multi-hop min-receive-interval 500
[SwitchA] bfd multi-hop detect-multiplier 9
[SwitchA] ipv6 route-static 120:: 64 2::9 bfd control-packet bfd-source 1::9
[SwitchA] ipv6 route-static 120:: 64 10::100 preference 65
[SwitchA] ipv6 route-static 2::9 128 12::2
[SwitchA] quit
```

Switch B に IPv6 スタティックルートを設定し、Switch D を通して IPv6 スタティックルートを行うため BFD コントロールパケットモードを有効にします。

```
<SwitchB> system-view
[SwitchB] bfd multi-hop min-transmit-interval 500
[SwitchB] bfd multi-hop min-receive-interval 500
[SwitchB] bfd multi-hop detect-multiplier 9
[SwitchB] ipv6 route-static 121:: 64 1::9 bfd control-packet bfd-source 2::9
[SwitchB] ipv6 route-static 121:: 64 13::2 preference 65
[SwitchB] ipv6 route-static 1::9 128 11::1
[SwitchB] quit
```

Switch C に IPv6 スタティックルートを設定します。

```
<SwitchC> system-view
[SwitchC] ipv6 route-static 120:: 64 13::1
[SwitchC] ipv6 route-static 121:: 64 10::102
```

Switch D に IPv6 スタティックルートを設定します。

```
<SwitchD> system-view
```

```
[SwitchD] ipv6 route-static 120:: 64 11::2
[SwitchD] ipv6 route-static 121:: 64 12::1
[SwitchD] ipv6 route-static 2::9 128 11::2
[SwitchD] ipv6 route-static 1::9 128 12::1
```

III. 設定の確認

Switch A の BFD セッションを表示します。

```
<SwitchA> display bfd session

 Total Session Num: 1     Up Session Num: 1     Init Mode: Active

 IPv6 Session Working Under Ctrl Mode:

       Local Discr: 513                Remote Discr: 33
         Source IP: 1::9
    Destination IP: 2::9
     Session State: Up                     Interface: N/A
         Hold Time: 2012ms
```

出力では BFD セッションが作成されたことを示しています。

Switch A の IPv6 スタティックルートを表示します。

```
<SwitchA> display ipv6 routing-table protocol static

Summary Count : 1

Static Routing table Status : <Active>
Summary Count : 1

Destination: 120::/64                                  Protocol  : Static
NextHop    : 2::9                                      Preference: 60
Interface  : Vlan10                                    Cost      : 0

Static Routing table Status : <Inactive>
Summary Count : 0
```

出力では、Switch A は VLAN インタフェース 10 を経由して Switch B と通信していることを示しています。

そして VLAN インタフェース 10 を経由したリンクが故障します。

Switch A の IPv6 スタティックルートを表示します。

```
<SwitchA> display ipv6 routing-table protocol static

Summary Count : 1

Static Routing table Status : <Active>
Summary Count : 1

Destination: 120::/64                                  Protocol  : Static
NextHop    : 10::100                                   Preference: 65
Interface  : Vlan11                                    Cost      : 0

Static Routing table Status : <Inactive>
Summary Count : 0
```

出力では、Switch A は VLAN インタフェース 11 を経由して Switch B と通信していることを示しています。

目次

このセクションのページは **5-x-x** です。

5 章 IPv6 デフォルトルート..... 5-1

5章 IPv6 デフォルトルート

IPv6 デフォルトルートは IPv6 ルーティングテーブルの指定した IPv6 ルーティングエントリにマッチしないパケットを転送するのに使用されます。

IPv6 デフォルトルートは以下のいずれかの方法で設定することができます。

- ネットワーク管理者が宛先アドレスとマスクを::/0 に設定します。詳細はオペレーションマニュアルのセクション 5 *ルーティングプロトコル”IPv6 スタティックルーティング”*を参照してください。
- ダイナミックルーティングプロトコル(OSPFv3、RIPng など)は、IPv6 デフォルトルートを作成できます。たとえば OSPFv3 が動作している上流のルータは既定の IPv6 デフォルトルートを作成し、他のルータに配信できます。これらのルータは、ネクストホップが上流のルータである IPv6 デフォルトルートを設定します。詳細は、オペレーションマニュアルのセクション 5 *ルーティングプロトコル*を参照してください。

目次

このセクションのページは **5-x-x** です。

6 章 RIP 6-1
6.1 概要 6-1
6.1.1 RIP ルーティングメトリック 6-1
6.1.2 RIP ルートエントリ 6-1
6.1.3 RIP の動作 6-1
6.1.4 ルーティングループの防止 6-2
6.1.5 RIP のバージョン 6-2
6.1.6 プロトコルと標準 6-2
6.2 RIP 設定作業リスト 6-3
6.3 RIP の基本設定 6-3
6.3.1 制限とガイドライン 6-3
6.3.2 RIP の有効化 6-4
6.3.3 RIP の受信とインタフェースへの配信の設定 6-4
6.3.4 RIP バージョンの指定 6-5
6.3.5 RIP ネイバ装置の指定 6-6
6.4 RIP ルート制御の設定 6-7
6.4.1 ルーティングメトリックの追加設定 6-7
6.4.2 RIPv2 ルート集約の設定 6-8
6.4.3 ホストルートの受信の無効化 6-9
6.4.4 デフォルトルートの配信 6-9
6.4.5 送受信ルートのフィルタリングの設定 6-10
6.4.6 RIP の優先順位の設定 6-10
6.4.7 RIP ルートの再配信の設定 6-11
6.5 RIP ネットワークの最適化の設定 6-11
6.5.1 RIP タイマの設定 6-11
6.5.2 スプリットホライズンとポイズンリバースの設定 6-12
6.5.3 RIP ECMP ルートの最大数の設定 6-13
6.5.4 RIP パケットの送信レートの設定 6-13
6.6 RIP ネットワーク管理の設定 6-14
6.7 RIP GR の設定 6-14
6.8 RIP NSR の有効化 6-15
6.9 RIP での BFD の設定 6-15
6.9.1 RIP での BFD の設定 6-15
6.9.2 制限とガイドライン 6-16
6.9.3 シングルホップエコー検知（直接接続された RIP ネイバ装置） 6-16
6.9.4 双方向コントロール検知 6-16
6.10 RIP セキュリティの拡張 6-17
6.10.1 受信 RIPv1 メッセージのゼロフィールドチェック機能の有効化 6-17
6.10.2 RIP アップデートの送信元 IP アドレスチェック機能の有効化 6-17
6.10.3 RIPv2 メッセージ認証の設定 6-18
6.11 RIP の表示と維持 6-18
6.12 RIP の設定例 6-19
6.12.1 RIP の基本機能の設定例 6-19
6.12.2 RIP ルート再配信の設定例 6-22

6.12.3 RIP インタフェースへのメトリックの追加設定例.....6-24
6.12.4 RIP の集約ルートの配信設定例 6-26
6.12.5 RIP GR の設定例 6-29
6.12.6 RIP NSR の設定例 6-29
6.12.7 RIP での BFD の設定例(直接接続されたネイバ装置のエコーパケットモードの片方向検知).....6-31
6.12.8 RIP での BFD の設定例(特定の宛先に対するシングルホップエコー検出).....6-34
6.12.9 RIP での BFD の設定例(BFD 制御パケットモードの双方向検出) 6-37

6章 RIP

6.1 概要

RIP(Routing Information Protocol)はディスタンスベクタの IGP で、小規模ネットワークに適しています。UDP のポート 520 パケットを使用してルート情報を交換します。

6.1.1 RIP ルーティングメトリック

RIP はホップ数を使用して宛先までの距離を測ります。ルータから直接接続されたネットワークへのホップ数は 0 です。ルータから直接接続されたルータへのホップ数は 1 です。収束時間を制限するため、RIP のメトリック値の範囲を 0～15 に制限しています。16 以上のメトリック値の宛先ネットワークへは到達不能とされます。そのため、RIP は大規模ネットワークには適しません。

6.1.2 RIP ルートエントリ

RIP はデータベースにルーティングエントリを記録します。各ルーティングエントリは以下の内容で構成されます。

- **宛先アドレス** – ホスト、もしくはネットワークの IP アドレス
- **ネクストホップ** – ネクストホップの IP アドレス
- **出力インタフェース** – ルートの出力インタフェース
- **メトリック** – ローカルルータから宛先へのコスト
- **ルートタイム** – ルーティングエントリが最後に更新された時間から経過した時間です。このタイムは、ルーティングエントリがアップデートされるたびに 0 にリセットされます。
- **ルートタグ** – ルートの識別に使用されます。詳細は、オペレーションマニュアルのセクション 5 *ルーティングプロトコル "ルーティングポリシー"*を参照してください。

6.1.3 RIP の動作

RIP は以下の動作を行います。

1) RIP はネイバルータにリクエストメッセージを送信します。ネイバルータはネイバルータのルーティングテーブル情報を含むレスポンスメッセージを返信します。
2) RIP はローカルルーティングテーブルの情報を受信した後、自身のルーティングテーブルをアップデートし、ネイバ装置に Triggered update メッセージを送信します。ネットワークのすべての RIP が同じように動作することで、最新のルーティング情報を学習します。
3) RIP は定期的にネイバ装置にローカルルーティングテーブルを送信します。RIP はメッセージを受信した後、ルーティングテーブルをアップデートし、最適なルートを選択し、他のネイバルータにアップデートを送信します。RIP は有効なルートのみを保存します。

6.1.4 ルーティングループの防止

ルーティングループを防ぐために、RIP は以下の機能を使用します。

- Counting to infinity – メトリック値 16 は、到達不能ルートとして定義されます。ルーティングループが発生したとき、ルートのメトリック値を 16 まで増加させます。
- Triggered updates – ネットワークのコンバージェンスを迅速に行うために、アップデート間隔が経過した後ではなく、ルートのメトリック値が変更される際に、アップデートを配信します。
- Split horizon – ルータはルーティングループを防ぎ、帯域幅を節約するために、ネイバ装置から学習したルーティング情報をそのネイバ装置宛に送信しません。
- Poison reverse – ルータはネイバ装置から受信したルートのメトリック値を 16 に設定し、ネイバ装置のルーティングテーブルから、それらの情報を削除するのを助けるために、ネイバ装置からのルートをネイバ装置に返します。

6.1.5 RIP のバージョン

RIP には RIPv1 と RIPv2 の 2 つのバージョンがあります。

RIPv1 は、クラスフルルーティングプロトコルです。メッセージは、ブロードキャストによる配信のみをサポートします。メッセージにマスク情報を付けて運びません。つまり、Class A、B、C のようなネットワークのルーティング情報のみ認識することができません。このため RIPv1 は離れているサブネットをサポートしません。

RIPv2 はクラスレスルーティングプロトコルです。以下に RIPv1 と比較した RIPv2 の利点を示します。

- ルーティングポリシーを柔軟に管理するためルートタグをサポートします。
- マスク、ルート集約、CIDR(Classless Inter-Domain Routing)をサポートします。
- ブロードキャストネットワークのベストネクストホップを選択するようにネクストホップの指定機能をサポートします。
- ネットワークリソースの消費を削減するため、RIPv2 ルータのみがルーティングアップデートを受信できるように、マルチキャストルーティングアップデートをサポートします。
- セキュリティを強化するために、プレーンテキスト認証と MD5 認証をサポートします。

RIPv2 は、ブロードキャストと、マルチキャストの 2 つのメッセージ転送タイプを持ちます。マルチキャストは、デフォルトでマルチキャストアドレスとして 224.0.0.9 を使用します。RIPv2 ブロードキャストモードで動作するインタフェースは、RIPv2 メッセージも受信することができます。

6.1.6 プロトコルと標準

- RFC 1058, Routing Information Protocol
- RFC 1723, RIP Version 2 - Carrying Additional Information
- RFC 1721, RIP Version 2 Protocol Analysis
- RFC 1722, RIP Version 2 Protocol Applicability Statement
- RFC 1724, RIP Version 2 MIB Extension
- RFC 2082, RIPv2 MD5 Authentication
- RFC 2091, Triggered Extensions to RIP to Support Demand Circuits
- RFC 2453, RIP Version 2

6.2 RIP設定作業リスト

作業リスト
RIPの基本設定: ● (必須設定項目) RIPの有効化 ● (オプション設定項目) RIPの受信とインタフェースへの配信の設定 ● (オプション設定項目) RIPバージョンの設定 ● RIPネイバ装置の指定 ブロードキャストあるいはマルチキャストをサポートしていないリンクでRIPを有効にするため、手動でRIPネイバ装置を指定する必要があります。
(オプション設定項目) RIPルート制御の設定: ● ルーティングメトリックの追加設定 ● RIPv2ルート集約の設定 ● ホストルートの受信の無効化 ● デフォルトルートの配信 ● 送受信ルートのフィルタリングの設定 ● RIPの優先順位の設定 ● RIPルートの再配信の設定
(オプション設定項目) RIPネットワークの最適化の設定: ● RIPタイマの設定 ● スプリットホライズンとポイズンリバースの設定 ● RIP ECMPルートの最大数の設定 ● RIPパケットの送信レートの設定
(オプション設定項目) RIPネットワーク管理の設定:
(オプション設定項目) RIPの可用性の向上の設定: ● RIP GRの設定 ● RIP NSRの有効化 ● RIPでのBFDの設定
(オプション設定項目) RIPセキュリティの拡張: ● 受信RIPv1メッセージのゼロフィールドチェック機能の有効化 ● RIPアップデートの送信元IPアドレスチェック機能の有効化 ● RIPv2メッセージ認証の設定

6.3 RIPの基本設定

6.3.1 制限とガイドライン

ルータで複数の RIP プロセスを有効にするため、各プロセスに ID を指定する必要があります。RIP プロセス ID はローカルで識別するために使われます。2 つの RIP ルータが異なるプロセス ID で RIP パケットを交換することができます。

6.3.2 RIP の有効化

I. RIP の有効化

ネットワークで RIP を有効にし、ワイルドカードのマスクを設定することができます。設定後、ネットワークに接続されたインタフェースでのみ RIP が動作します。

II. 制限とガイドライン

RIP を有効にする前に、interface view で RIP の設定を行う場合、RIP が有効になるまで設定は適用されません。

1つの物理インタフェースが複数のネットワークで使われる場合､異なる RIP プロセスで、これらのネットワークを配信することができません。

物理インタフェースで複数の RIP を有効にすることはできません。

III. ネットワークでの RIP の有効化

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. RIP を有効にし、RIP view に移行する	**rip** [*process-id*] [**vpn-instance** *vpn-instance-name*]	デフォルト：無効
3. ネットワークで RIP を有効にする	**network** *network-address* [*wildcard-mask*]	デフォルト：無効 **network** 0.0.0.0コマンドは1つのプロセスですべてのインタフェースでRIPを有効にすることができます。複数のプロセスに適用することはできません。

IV. インタフェースでの RIP の有効化

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. RIP を有効にし、RIP view に移行する	**rip** [*process-id*] [**vpn-instance** *vpn-instance-name*]	デフォルト：無効
3. system view に戻る	**quit**	ー
4. interface view に移行する	**interface** *interface-type interface-number*	ー
5. インタフェースで RIP を有効にする	**rip** *process-id* **enable** [**exclude-subip**]	デフォルト：無効

6.3.3 RIP の受信とインタフェースへの配信の設定

I. RIP の受信とインタフェースへの配信

この設定を行うと、以下の機能を設定できます。

- インタフェースの抑制を行います。抑制されたインタフェースは RIP メッセージを受信できますが、RIP メッセージを送信できません。

- インタフェースで RIP メッセージを送信しないようにします。
- インタフェースで RIP メッセージを受信できないようにします。

II. 制限とガイドライン

silent-interface コマンドを使用して抑制されたインタフェースは、RIP メッセージのみを受信できます。 RIP メッセージを送信できません。 すべてのインタフェースを抑制する場合、**silent-interface all** コマンドを使用します。**silent-interface** コマンドは、**rip input** コマンドと **rip output** コマンドより優先されます。

III. インタフェースの抑制

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. RIP view に移行する	**rip** [*process-id*] [**vpn-instance** *vpn-instance-name*]	―
3. インタフェースで RIP メッセージの送信を無効にする	**silent-interface** { *interface-type interface-number* | **all** }	デフォルト：すべてのRIPが有効なインタフェースはRIPメッセージを送信します。無効に設定されたインタフェースはRIPの受信ができますが、不明なポートを含むユニキャストリクエストに応答します。

IV. インタフェースでの RIP メッセージの受信の無効化

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. interface view に移行する	**interface** *interface-type interface-number*	―
3. RIP メッセージの受信を無効にする	**undo rip input**	デフォルト：RIPが有効なインタフェースはRIPメッセージを受信します。

V. インタフェースでの RIP メッセージの送信の無効化

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. interface view に移行する	**interface** *interface-type interface-number*	―
3. RIP メッセージの送信を無効にする	**undo rip output**	デフォルト：RIPが有効なインタフェースはRIPメッセージを送信します。

6.3.4 RIP バージョンの指定

I. RIP バージョンの指定

RIP view でグローバルに、あるいは interface view で指定したインタフェースの RIP バージョンを設定することができます。

インタフェースは、優先的にインタフェースで指定した RIP バージョンを使用します。インタフェースでバージョンが指定されていない場合、グローバルの RIP バージョンを使用します。グローバルおよびインタフェースの両方で RIP バージョンが設定されていない場合、インタフェースは RIPv1 ブロードキャストを送信し、以下のパケットを受信します。

- RIPv1 ブロードキャスト、ユニキャストパケット
- RIPv2 ブロードキャスト、マルチキャスト、ユニキャストパケット

II. 設定手順

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． RIP view に移行する	**rip** [*process-id*] [**vpn-instance** *vpn-instance-name*]	―
3． グローバルで RIP バージョンを指定する	**version** { **1** | **2** }	デフォルト：グローバルで RIPバージョンが指定されていません。 インタフェースはRIPv1ブロードキャストを送信し、RIPv1ブロードキャスト、ユニキャストパケットと、RIPv2ブロードキャスト、マルチキャスト、ユニキャストパケットを受信します。
4． system view に戻る	**quit**	―
5． interface view に移行する	**interface** *interface-type interface-number*	―
6． インタフェースで RIP バージョンを指定する	**rip version** { **1** | **2** [**broadcast** | **multicast**] }	デフォルト：インタフェースでRIPバージョンが指定されていません。 インタフェースはRIPv1ブロードキャストを送信し、RIPv1ブロードキャスト、ユニキャストパケットと、RIPv2ブロードキャスト、マルチキャスト、ユニキャストパケットを受信します。

6.3.5 RIP ネイバ装置の指定

I. RIP ネイバ装置

一般的に、RIP メッセージはブロードキャストあるいはマルチキャストで送信されます。ブロードキャストあるいはマルチキャストをサポートしていないリンクで RIP を有効にするため、手動で RIP ネイバ装置を指定する必要があります。

II. 制限とガイドライン

ネイバ装置が直接接続されている場合、**peer** *ip-address* コマンドを使用しないでください。使用した場合、同じルーティング情報のユニキャストメッセージ、マルチキャスト（あるいはブロードキャスト）メッセージの両方を受信してしまいます。

III. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. RIP view に移行する	**rip** [*process-id*] [**vpn-instance** *vpn-instance-name*]	―
3. RIP ネイバ装置を指定する	**peer** *ip-address*	デフォルト: ネイバ装置にアップデートをユニキャストしません。
4. RIP アップデートの送信元 IP アドレスチェック機能を無効にする	**undo validate-source-address**	デフォルト：有効 指定されたネイバ装置が直接接続されていない場合、受信アップデートの送信元アドレスチェック機能を無効にします。

6.4 RIPルート制御の設定

6.4.1 ルーティングメトリックの追加設定

I. ルーティングメトリックの追加

ルーティングメトリック(ホップカウント)は、送受信 RIP ルートのメトリックを追加することができます。

- 送信側へのメトリックの追加は、ルーティングテーブルのメトリックを変更しないで、送信ルートにメトリックを加えます。
- 受信側へのメトリックの追加は、受信したルートがルーティングテーブルに反映される前に、受信ルートにメトリックを追加します。したがって、受信ルートのメトリックは変更されます。追加メトリックの値と、オリジナルのメトリックが 16 を超える場合、ルートのメトリックは 16 になります。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. interface view に移行する	**interface** *interface-type interface-number*	―
3. 受信側に追加するルーティングメトリックを指定する	**rip metricin** [**route-policy** *route-policy-name*] *value*	デフォルト：0
4. 送信側に追加するルーティングメトリックを指定する	**rip metricout** [**route-policy** *route-policy-name*] *value*	デフォルト：1

6.4.2 RIPv2 ルート集約の設定

I. RIPv2 ルート集約の設定

ルート集約はネットワークにネイバしているサブネットを集約し、ネイバ装置にネットワーク情報を送信します。すべての集約されたルート間でもっとも小さいメトリックが集約ルートのメトリックとして使用されます。

次の方法を使用して、RIPv2 のルートを集約できます。

- 自動集約－連続したサブネットのナチュラルネットワークを作成するため、RIPv2 を設定します。たとえば、3 つのサブネットルート 10.1.1.0/24、10.1.2.0/24、および 10.1.3.0/24 があるとします。 自動集約は、より特定のルートではなく、集約ルート 10.0.0.0/8 を自動的に作成および配信します。
- 手動集約－集約ルートを手動で構成します。RIPv2 は、特定のルートではなく、集約ルートを配信します。たとえば、ネイバするサブネットが 10.1.1.0/24、10.1.2.0/24、および 10.1.3.0/24 がルーティングテーブルに存在するとします。集約ルート 10.1.0.0/16 を作成できます。GigabitEthernet 1/0/1 の特定のルートではなく、集約ルートを配信します。デフォルトでは、ナチュラルマスクは集約ルートを配信するために使用されます。インタフェースで集約ルートを手動で設定する場合、最初に RIPv2 自動ルート集約機能を無効にする必要があります。

II. 制限とガイドライン

ルート集約によるループを防止するために、集約ルートの出力インタフェースとしてインタフェース NULL0 を指定して、ブラックホールルートを作成します。 ブラックホールルートに一致するパケットが削除されます。

III. RIPv2 ルートの自動集約機能の有効化

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. RIP view に移行する	**rip** [*process-id*] [**vpn-instance** *vpn-instance-name*]	—
3. RIPv2 ルートの自動集約機能を有効にする	**summary**	デフォルト：有効 ルーティングテーブルのサブネットが隣接していない場合、自動集約機能は無効です。

IV. 集約ルートの配信

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. RIP view に移行する	**rip** [*process-id*] [**vpn-instance** *vpn-instance-name*]	—
3. RIPv2 ルートの自動集約機能を無効にする	**undo summary**	デフォルト：有効
4. system view に戻る	**quit**	—
5. interface view に移行する	**interface** *interface-type interface-number*	—
6. 集約ルートを設定する	**rip summary-address** *ip-address* { *mask-length* | *mask* }	デフォルト：設定なし

6.4.3 ホストルートの受信の無効化

I. ホストルートの受信の無効化

ネットワークリソースを節約するため、RIPv2 は、同一ネットワークからのホストルートの受信を無効にすることができます。RIPv1 はサポートしていません。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. RIP view に移行する	**rip** [*process-id*] [**vpn-instance** *vpn-instance-name*]	—
3. ホストルートの受信を無効にする	**undo host-route**	デフォルト：有効

6.4.4 デフォルトルートの配信

I. デフォルトルートの配信

RIP view で、すべての RIP インタフェース、あるいは interface view で指定した RIP インタフェースでデフォルトルートを配信することができます。interface view での設定は RIP view での設定よりも優先されます。

インタフェースでデフォルトルートの配信を無効にする場合、インタフェースで **rip default-route no-originate** コマンドを設定します。

デフォルトルートの配信機能が有効なルータは、RIP のネイバ装置からのデフォルトルートを受信しません。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. RIP view に移行する	**rip** [*process-id*] [**vpn-instance** *vpn-instance-name*]	—
3. デフォルトルートを配信する設定を有効にする	**default-route** { **only** | **originate** } [**cost** *cost-value* | *route-policy route-policy-name*]*	デフォルト：無効
4. system view に戻る	**quit**	—
5. interface view に移行する	**interface** *interface-type interface-number*	—
6. RIP インタフェースでデフォルトルートの配信する設定を有効にする	**rip default-route** { { **only** | **originate** } [**cost** *cost-value* | **route-policy** *route-policy-name*]* | **no-originate** }	デフォルト：デフォルトルートを配信する設定が有効化されている場合、RIPインタフェースはデフォルトルートを配信します。

6.4.5 送受信ルートのフィルタリングの設定

I. 送受信ルートのフィルタリング

ACL や IP プレフィックスリストなどのフィルタリングポリシーを使用することで送受信ルートをフィルタすることができます。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. RIP view に移行する	**rip** [*process-id*] [**vpn-instance** *vpn-instance-name*]	―
3. 受信ルートのフィルタリングを設定する	**filter-policy** { *ipv4-acl-number* | **gateway** *prefix-list-name* | **prefix-list** *prefix-list-name* [**gateway** *prefix-list-name*] } **import** [*interface-type interface-number*]	デフォルト：設定なし このコマンドは受信ルートをフィルタします。フィルタされたルートはルーティングテーブルに反映されず、ネイバ装置にも配信されません。
4. 再配信ルートのフィルタリングを設定する	**filter-policy** { *ipv4-acl-number* | **prefix-list** *prefix-list-name* } **export** [*protocol* [*process-id*] | *interface-type interface-number*]	デフォルト：設定なし このコマンドは**import-route** コマンドで再配信するルートを含む送信ルートをフィルタします。

6.4.6 RIP の優先順位の設定

I. RIP の優先順位の設定

複数の IGP で同一宛先のルートがある場合、もっとも高い優先順位を持っている IGP によって見つけられたルートが最適ルートとして選ばれます。この設定は RIP に優先順位を割り当てます。小さな優先順位の値を持つルートが、優先されます。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. RIP view に移行する	**rip** [*process-id*] [**vpn-instance** *vpn-instance-name*]	―
3. RIP の優先順位を設定する	**preference** { *preference* | **route-policy** *route-policy-name* } *	デフォルト：100

6.4.7 RIP ルートの再配信の設定

I. RIP ルートの再配信の設定

ルータで RIP と他のルーティングプロトコルが動作する場合、OSPF、IS-IS、スタティック、ダイレクトルートを含む他のルーティングプロトコルの再配信を設定することができます。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. RIP view に移行する	**rip** [*process-id*] [**vpn-instance** *vpn-instance-name*]	—
3. 他のプロトコルからのルートを再配信するように設定する	• ダイレクトあるいはスタティックルートからのルートを再配信する：**import-route** { **direct** | **static** } [**cost** *cost-value* | **route-policy** *route-policy-name* | **tag** *tag*]* • OSPF、IS-IS、あるいはほかのRIPプロセスからのルートを再配信する：**import-route** { **isis ospf** | **rip** } [*process-id* | **all-processes**] [**allow-direct** | **cost** *cost-value* | **route-policy** *route-policy-name* | **tag** *tag*]*	デフォルト：無効 このコマンドはアクティブなルートのみ再配信することができます。アクティブなルートを表示するには、**display ip routing-table protocol** コマンドを使用します。
4. (オプション設定項目) 再配信ルートにデフォルトメトリックを設定する	**default cost** *value*	デフォルト：0

6.5 RIPネットワークの最適化の設定

6.5.1 RIP タイマの設定

I. RIP タイマ

以下に示す RIP タイマを適切に設定することで、RIP ネットワークの収束速度を変更することができます。

- **Update timer** – ルートアップデートの間隔を指定します。
- **Timeout timer** – ルートエージングタイムを指定します。もしエージング時間内にルートを受信しない場合、ルートのメトリックを 16 に設定します。
- **Suppress timer** – RIP ルートがサプレス状態(到達不能状態)にとどまる時間を指定します。ルートのメトリックが 16 のとき、ルータはサプレス状態になります。停止した到達不能ルートは、アップデートされたルートによって置き換わります。このアップデートされたルートはサプレスタイマが終了する前に同一のネイバ装置から受信したルートに置き換わります。メトリックは 16 より小さい値を持ちます。

- **Garbage-collect timer** – ルートのメトリックが 16 になる時点から、そのルートがルーティングテーブルから削除されるまでの間隔を指定します。RIP はメトリックが 16 のルートを配信します。タイマの時間が過ぎた後も、そのルートへのルーティングアップデートが行われない場合、ルートはルーティグテーブルから削除されます。

II. 制限とガイドライン

不必要なトラフィックやルートの頻繁な変更を避けるため、RIP ルータ間の RIP タイマの設定は同一にしてください。

III. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. RIP view に移行する	**rip** [*process-id*] [**vpn-instance** *vpn-instance-name*]	—
3. RIP タイマの値を設定する	**timers** { **garbage-collect** *garbage-collect-value* | **suppress** *suppress-value* | **timeout** *timeout-value* | **update** *update-value* }*	デフォルト： ● garbage-collect timer ：120秒 ● suppress timer ： 120 秒 ● timeout timer ： 180 秒 ● update timer ： 30 秒

6.5.2 スプリットホライズンとポイズンリバースの設定

I. スプリットホライズンとポイズンリバース

スプリットホライズンとポイズンリバースはルーティングのループを防ぐための機能です。

- スプリットホライズンは、ネイバルータ間のルーティングループを防止するためにルートが学習されたインタフェース経由でルートを送信することを禁止します。
- ポイズンリバースは、RIP がルートを学習したインタフェース経由でルートを送信できるようにします。 ネイバルータ間のルーティングループを避けるため、これらのルートのメトリックを 16(到達不能)に設定します。

II. 制限とガイドライン

スプリットホライズンとポイズンリバースの両方を設定した場合、ポイズンリバース機能のみが適用されます。

III. スプリットホライズンの有効化

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. interface view に移行する	**interface** *interface-type interface-number*	—
3. スプリットホライズンを有効にする	**rip split-horizon**	デフォルト：有効

IV. ポイズンリバースの有効化

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. interface view に移行する	**interface** *interface-type interface-number*	―
3. ポイズンリバースを有効にする	**rip poison-reverse**	デフォルト：無効

6.5.3 RIP ECMP ルートの最大数の設定

I. RIP ECMP ルートの最大数の設定

ロードバランスのためイコールコストマルチパス(ECMP)ルートの最大数を指定します。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. RIP view に移行する	**rip** [*process-id*] [**vpn-instance** *vpn-instance-name*]	―
3. RIP ECMP ルートの最大数を指定する	**maximum load-balancing** *number*	デフォルトでは、RIP ECMPルートの最大数はECMPルートの最大数に等しく、max-ecmp-numコマンドを使用して設定できます。

6.5.4 RIP パケットの送信レートの設定

I. RIP パケットの送信レートの設定

パケットの送信間隔と各間隔で RIP パケットを送信できる最大数を指定します。この機能は、RIP パケットによるシステムの性能低下や多くの帯域幅を消費することを防ぐことができます。

II. 設定手順

次のコマンドを順番に実行して、すべてのインタフェースの RIP パケット送信レートを設定します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. RIP view に移行する	**rip** [*process-id*] [**vpn-instance** *vpn-instance-name*]	―
3. RIP パケットの送信間隔と最大数を設定する	**output-delay** *time* **count** *count*	デフォルト： 最大値：3パケット 間隔：20ms

6.6 RIPネットワーク管理の設定

I. RIP ネットワーク管理

MIB が割り当てられている RIP プロセスを管理するため、ネットワーク管理のソフトウェアを使用することができます。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. RIP プロセスに MIB を割り当てる	**rip mib-binding** *process-id*	デフォルト：MIBはもっとも小さいプロセスIDのRIPプロセスに割り当てられています。

6.7 RIP GRの設定

I. RIP GR

GR（グレースフルリスタート）は、ルーティングプロトコルの再起動あるいはアクティブ/スタンバイの切り替えが発生したときでも、パケット転送を継続することができます。

GR 機能を動作させるには 2 台のルータが必要です。GR のルータは以下の役割があります。

- GR リスタータ ― グレースフルリスタートルータです。GR 機能を持ちます。
- GR ヘルパー ― GR リスタータのネイバ装置です。GR プロセスを処理するために GR リスタータを補助します。

ルータで RIP を再起動したのち、ルータは RIP ルートを再学習し、FIB テーブルのアップデートを行います。これによりネットワークの切断とルートの収束が発生します。

GR 機能において、再起動するルータ（GR リスタータ）は、GR を行う能力があるネイバ装置にイベントを通知することができます。GR を行う能力があるネイバ装置（GR ヘルパー）は GR タイマの時間内にルータのネイバ関係を維持します。この処理の間、ルータの FIB テーブルは変更しません。

RIP が有効な装置はデフォルトで GR ヘルパーとして動作します。この作業は GR リスタータで行われます。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. RIP view に移行する	**rip** [*process-id*] [**vpn-instance** *vpn-instance-name*]	―
3. RIP の GR 機能を有効にする	**graceful-restart**	デフォルト：無効

6.8 RIP NSRの有効化

I. RIP NSR

ノンストップルーティング (NSR) を使用すると、装置はアクティブ RIP プロセスからスタンバイ RIP プロセスへのルーティング情報をバックアップできます。アクティブ/スタンバイスイッチオーバーの後、隣接関係を切断したり転送サービスに影響を与えたりすることなく、NSR はルートの再生成を完了できます。

NSR は、ルーティング情報をリカバリするために隣接装置の協力を必要とせず、一般に GR よりも頻繁に使用されます。

II. 制限とガイドライン

RIP NSR が有効になっている装置は、GR リスタータとして機能できません。

III. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. RIP view に移行する	**rip** [process-id] [**vpn-instance** *vpn-instance-name*]	—
3. RIP NSR を有効にする	**non-stop-routing**	デフォルト：無効 RIPプロセスに対して有効にされたRIP NSRは、そのプロセスだけで有効になります。ベストプラクティスとして、複数のRIPプロセスが存在する場合は、プロセスごとにRIP NSRを有効にします。

6.9 RIPでのBFDの設定

6.9.1 RIP での BFD の設定

RIP はルート更新要求を定期的にネイバ装置へ送信します。指定された間隔内に応答がない場合、RIP はそのルートを到達不能と認識します。このメカニズムではリンク障害をすばやく検出することができません。収束時間を早急に行うために、RIP で BFD を有効にします。BFD についてはオペレーションマニュアルのセクション 10 *高可用性”BFD”* を参照してください。

RIP は以下の BFD 検知モードをサポートしています。

- **シングルホップエコー検知**－直接接続されたネイバ装置のためのモードです。このモードでは直接接続されたネイバ装置がルート情報を持っているときのみ BFD セッションが確立されます。
- **特定の宛先のシングルホップエコー検知**－直接接続されたネイバの検出モード。このモードでは、ローカルインタフェース上で RIP が有効になっている場合、指定された RIP ネイバに BFD セッションが確立されます。 BFD が単方向リンクを検出すると、ローカル装置はコンバージェンス速度を向上させるためにインタフェース経由で

RIP パケットを送受信しません。リンクが回復すると、インタフェースは RIP パケットを再度送信できます。

- **双方向コントロール検知**－このモードは直接接続されていないネイバ装置のためのモードです。このモードは、両端が送信するルート情報を持っており、そして受信インタフェースで BFD が有効になっているときのみ、BFD セッションが確立されます。

6.9.2 制限とガイドライン

rip bfd enable および **rip bfd enable destination** コマンドは相互排他的です。**rip bfd enable destination** コマンドは未サポートです。

6.9.3 シングルホップエコー検知（直接接続された RIP ネイバ装置）

操作	コマンド	補足
1. system view に移行する	**system-view**	－
2. BFD エコーパケットの送信元 IP アドレスを設定する	**bfd echo-source-ip** *ip-address*	デフォルト：設定なし
3. interface view に移行する	**interface** *interface-type interface-number*	－
4. BFD を有効にする	**rip bfd enable**	デフォルト：無効

6.9.4 双方向コントロール検知

操作	コマンド	補足
1. system view に移行する	**system-view**	－
2. RIP view に移行する	**rip** [*process-id*] [**vpn-instance** *vpn-instance-name*]	－
3. RIP ネイバ装置を指定する	**peer** *ip-address*	デフォルト：ネイバ装置にアップデートをユニキャストしません。**undo peer** コマンドを使用しても、すぐにネイバ関係は削除されません。したがって、BFD セッションをすぐにダウン状態にすることはできません。
4. interface view に移行する	**interface** *interface-type interface-number*	－
5. インタフェースで BFD を有効にする	**rip bfd enable**	デフォルト：無効

6.10 RIPセキュリティの拡張

6.10.1 受信 RIPv1 メッセージのゼロフィールドチェック機能の有効化

I. 受信 RIPv1 メッセージのゼロフィールドチェック機能

RIPv1 メッセージのいくつかのフィールドはゼロである必要があり、それらのフィールドはゼロフィールドと呼ばれます。装置で、受信 RIPv1 メッセージのゼロフィールドチェック機能を有効にすることができます。ゼロフィールドにゼロ以外の値が含まれる場合、RIPv1 メッセージは処理されません。すべてのメッセージを信頼できる場合、ゼロフィールドチェック機能を無効化することで、CPU のリソースを節約することができます。

RIPv2 パケットはゼロフィールドを持たないため、この機能は適用されません。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. RIP view に移行する	**rip** [*process-id*] [**vpn-instance** *vpn-instance-name*]	—
3. 受信 RIPv1 メッセージのゼロフィールドチェック機能を有効にする	**checkzero**	デフォルト：無効

6.10.2 RIP アップデートの送信元 IP アドレスチェック機能の有効化

I. RIP アップデートの送信元 IP アドレスチェック機能

受信 RIP アップデートの送信元 IP アドレスのチェックを有効にすることができます。

- Ethernet インタフェースでメッセージを受信すると、RIP は、メッセージの送信元 IP アドレスをインタフェースの IP アドレスと比較します。そして、同一ネットワークセグメントでない場合、RIP はメッセージを破棄します。
- PPP インタフェースでメッセージを受信すると、RIP は、メッセージの送信元 IP アドレスが対向先のインタフェースの IP アドレスであるか確認します。異なる場合、RIP はメッセージを破棄します。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. RIP view に移行する	**rip** [*process-id*] [**vpn-instance** *vpn-instance-name*]	—
3. RIP アップデートの送信元 IP アドレスチェック機能を有効にする	**validate-source-address**	デフォルト：無効

6.10.3 RIPv2 メッセージ認証の設定

I. RIPv2 メッセージ認証

RIPv2 メッセージを認証することができます。

RIPv2 はプレーンテキストと MD5 の 2 つの認証モードをサポートします。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. interface view に移行する	**interface** *interface-type interface-number*	―
3. RIPv2 メッセージ認証を設定する	**rip authentication-mode** { **md5** { **rfc2082** { **cipher** *cipher-string* | **plain** *plain-string* } *key-id* | **rfc2453** { **cipher** *cipher-string* | **plain** *plain-string* } } | **simple** { **cipher** *cipher-string* | **plain** *plain-string* } }	デフォルト：設定なし この機能は認証をサポートしていないRIPv1では適用されません。interface viewでRIPv1用に認証を設定しても、設定は適用されません。

6.11 RIPの表示と維持

すべての view で **display** コマンドを実行でき、user view で **reset** コマンドを実行できます。

操作	コマンド
RIP の現在の状態と設定情報を表示する	**display rip** [*process-id*]
RIP GR 情報を表示する	**display rip** [*process-id*] **graceful-restart**
RIP NSR 情報を表示する	**display rip** [*process-id*] **non-stop-routing**
RIP データベースのすべての有効なルートを表示する	**display rip** *process-id* **database** [*ip-address* { *mask-length* | *mask* }]
RIP インタフェース情報を表示する	**display rip** *process-id* **interface** [*interface-type interface-number*]
RIP プロセスのネイバ情報を表示する	**display rip** *process-id* **neighbor** [*interface-type interface-number*]
指定した RIP プロセスのルーティング情報を表示する	**display rip** *process-id* **route** [*ip-address* { *mask-length* | *mask* } [**verbose**] | **peer** *ip-address* | **statistics**]
RIP プロセスをリセットする	**reset rip** *process-id* **process**
RIP プロセスの統計情報を削除する	**reset rip** *process-id* **statistics**

6.12 RIPの設定例

6.12.1 RIP の基本機能の設定例

I. ネットワーク要件

図 6-1 に示すように、Switch A と Switch B のすべてのルータで RIPv2 を有効にします。Switch B は Switch A にルート 10.2.1.0/24 のルートを配信しないように設定し、Switch A からルート 2.1.1.0/24 のみ受信するように設定します。

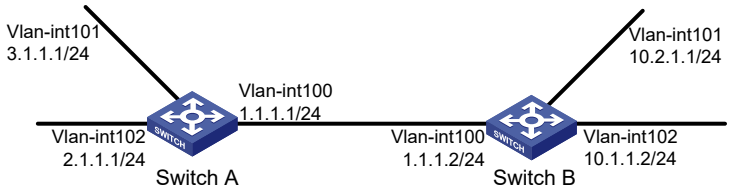


図 6-1 ネットワーク図

II. 設定手順

1)　インタフェースに IP アドレスを設定します。(詳細は省略します)
2)　RIP を有効にします。

Switch A の指定されたインタフェースで RIP を有効にします。

```
<SwitchA> system-view
[SwitchA] rip
[SwitchA-rip-1] network 1.0.0.0
[SwitchA-rip-1] network 2.0.0.0
[SwitchA-rip-1] network 3.0.0.0
[SwitchA-rip-1] quit
```

Switch B の指定されたインタフェースで RIP を有効にします。

```
<SwitchB> system-view
[SwitchB] rip
[SwitchB-rip-1] quit
[SwitchB] interface vlan-interface 100
[SwitchB-Vlan-interface100] rip 1 enable
[SwitchB-Vlan-interface100] quit
[SwitchB] interface vlan-interface 101
[SwitchB-Vlan-interface101] rip 1 enable
[SwitchB-Vlan-interface101] quit
[SwitchB] interface vlan-interface 102
```

```
[SwitchB-Vlan-interface102] rip 1 enable
[SwitchB-Vlan-interface102] quit
```

Switch A の RIP ルーティングテーブルを表示します。

```
[SwitchA] display rip 1 route
 Route Flags: R - RIP, T - TRIP
              P - Permanent, A - Aging, S - Suppressed, G - Garbage-collect
              D - Direct, O - Optimal, F - Flush to RIB
------------------------------------------------------------------------------
 Peer 1.1.1.2 on Vlan-interface100
      Destination/Mask        Nexthop          Cost    Tag     Flags   Sec
      10.0.0.0/8              1.1.1.2          1       0       RAOF    11
 Local route
      Destination/Mask        Nexthop          Cost    Tag     Flags   Sec
      1.1.1.0/24              0.0.0.0          0       0       RDOF    -
      2.1.1.0/24              0.0.0.0          0       0       RDOF    -
      3.1.1.0/24              0.0.0.0          0       0       RDOF    -
```

出力は、RIPv1 がクラスフルマスクを使用していることを示します。

3)　RIP バージョンを設定します。

Switch A に RIPv2 を設定します。

```
[SwitchA] rip
[SwitchA-rip-1] version 2
[SwitchA-rip-1] undo summary
[SwitchA-rip-1] quit
```

Switch B に RIPv2 を設定します。

```
[SwitchB] rip
[SwitchB-rip-1] version 2
[SwitchB-rip-1] undo summary
[SwitchB-rip-1] quit
```

Switch A の RIP ルーティングテーブルを表示します。

```
[SwitchA] display rip 1 route
 Route Flags: R - RIP, T - TRIP
              P - Permanent, A - Aging, S - Suppressed, G - Garbage-collect
              D - Direct, O - Optimal, F - Flush to RIB
------------------------------------------------------------------------------

 Peer 1.1.1.2 on Vlan-interface100
      Destination/Mask        Nexthop          Cost    Tag     Flags   Sec
      10.0.0.0/8              1.1.1.2          1       0       RAOF    50
      10.2.1.0/24             1.1.1.2          1       0       RAOF    16
      10.1.1.0/24             1.1.1.2          1       0       RAOF    16
 Local route
      Destination/Mask        Nexthop          Cost    Tag     Flags   Sec
      1.1.1.0/24              0.0.0.0          0       0       RDOF    -
      2.1.1.0/24              0.0.0.0          0       0       RDOF    -
      3.1.1.0/24              0.0.0.0          0       0       RDOF    -
```

出力は、RIPv2 がクラスレスマスクを使用していることを示します。

🕮 **メモ:**

RIPv2 が設定された後、RIPv1のルートはエージアウトするまでルーティングテーブルに存在します。

Switch B のルーティングテーブルを表示します。

```
[SwitchB] display rip 1 route
 Route Flags: R - RIP, T - TRIP
              P - Permanent, A - Aging, S - Suppressed, G - Garbage-collect
              D - Direct, O - Optimal, F - Flush to RIB
------------------------------------------------------------------------------
 Peer 1.1.1.1 on Vlan-interface100
      Destination/Mask        Nexthop          Cost    Tag     Flags   Sec
      2.1.1.0/24              1.1.1.1          1       0       RAOF    19
      3.1.1.0/24              1.1.1.1          1       0       RAOF    19
 Local route
      Destination/Mask        Nexthop          Cost    Tag     Flags   Sec
      1.1.1.0/24              0.0.0.0          0       0       RDOF    -
      10.1.1.0/24             0.0.0.0          0       0       RDOF    -
      10.2.1.0/24             0.0.0.0          0       0       RDOF    -
```

4) ルートのフィルタリングを設定します。

受信ルートと再配信ルートをフィルタするため、Switch B の IP プレフィックスリストを使用します。

```
[SwitchB] ip prefix-list aaa index 10 permit 2.1.1.0 24

[SwitchB] ip prefix-list bbb index 10 deny 10.2.1.0 24

[SwitchB] ip prefix-list bbb index 11 permit 0.0.0.0 0 less-equal 32

[SwitchB] rip 1

[SwitchB-rip-1] filter-policy prefix-list aaa import

[SwitchB-rip-1] filter-policy prefix-list bbb export

[SwitchB-rip-1] quit
```

Switch A のルーティングテーブルを表示します。

```
[SwitchA] display rip 100 route
 Route Flags: R - RIP, T - TRIP
              P - Permanent, A - Aging, S - Suppressed, G - Garbage-collect
------------------------------------------------------------------------------
 Peer 1.1.1.2 on Vlan-interface100
      Destination/Mask        Nexthop          Cost    Tag     Flags   Sec
      10.1.1.0/24             1.1.1.2          1       0       RAOF    19
 Local route
      Destination/Mask        Nexthop          Cost    Tag     Flags   Sec
      1.1.1.0/24              0.0.0.0          0       0       RDOF    -
      2.1.1.0/24              0.0.0.0          0       0       RDOF    -
      3.1.1.0/24              0.0.0.0          0       0       RDOF    -
```

Switch B のルーティングテーブルを表示します。

```
[SwitchB] display rip 1 route
 Route Flags: R - RIP, T - TRIP
              P - Permanent, A - Aging, S - Suppressed, G - Garbage-collect
              D - Direct, O - Optimal, F - Flush to RIB
------------------------------------------------------------------------------
 Peer 1.1.1.1 on Vlan-interface100
      Destination/Mask        Nexthop          Cost    Tag     Flags   Sec
```

```
      2.1.1.0/24              1.1.1.1         1         0         RAOF      19
Local route
      Destination/Mask        Nexthop         Cost      Tag       Flags     Sec
      1.1.1.0/24              0.0.0.0         0         0         RDOF      -
      10.1.1.0/24             0.0.0.0         0         0         RDOF      -
      10.2.1.0/24             0.0.0.0         0         0         RDOF      -
```

6.12.2 RIP ルート再配信の設定例

I. ネットワーク要件

図 6-2 に示すように、Switch B は RIP 100 を通して Switch A と通信し、RIP 200 を通して Switch C と通信します。

ダイレクトルートと RIP 100 からのルートを RIP 200 に再配信するために、Switch B にルートの再配信の設定を行います。Switch C は 10.2.1.0/24 と 11.1.1.0/24 宛のルートを学習できますが、Switch A は 12.3.1.0/24 と 16.4.1.0/24 宛のルートを学習できないようにします。

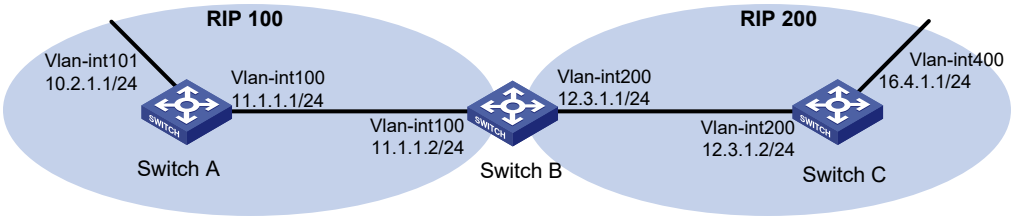


図 6-2 ネットワーク図

II. 設定手順

1) インタフェースに IP アドレスを設定します。(詳細は省略します)
2) RIP の基本機能を設定します。

Switch A で RIP100 を有効にし、RIPv2 を設定します。

```
<SwitchA> system-view
[SwitchA] rip 100
[SwitchA-rip-100] network 10.0.0.0
[SwitchA-rip-100] network 11.0.0.0
[SwitchA-rip-100] version 2
[SwitchA-rip-100] undo summary
[SwitchA-rip-100] quit
```

Switch B で RIP100、RIP200 を有効にし、RIPv2 を設定します。

```
<SwitchB> system-view
[SwitchB] rip 100
[SwitchB-rip-100] network 11.0.0.0
```

```
[SwitchB-rip-100] version 2
[SwitchB-rip-100] undo summary
[SwitchB-rip-100] quit
[SwitchB] rip 200
[SwitchB-rip-200] network 12.0.0.0
[SwitchB-rip-200] version 2
[SwitchB-rip-200] undo summary
[SwitchB-rip-200] quit
```

Switch C で RIP200 を有効にし、RIPv2 を設定します。

```
<SwitchC> system-view
[SwitchC] rip 200
[SwitchC-rip-200] network 12.0.0.0
[SwitchC-rip-200] network 16.0.0.0
[SwitchC-rip-200] version 2
[SwitchC-rip-200] undo summary
[SwitchC-rip-200] quit
```

Switch C の IP ルーティングテーブルを表示します。

```
[SwitchC] display ip routing-table

Destinations : 13        Routes : 13

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
0.0.0.0/32          Direct 0    0            127.0.0.1       InLoop0
12.3.1.0/24         Direct 0    0            12.3.1.2        Vlan200
12.3.1.0/32         Direct 0    0            12.3.1.2        Vlan200
12.3.1.2/32         Direct 0    0            127.0.0.1       InLoop0
12.3.1.255/32       Direct 0    0            12.3.1.2        Vlan200
16.4.1.0/24         Direct 0    0            16.4.1.1        Vlan400
16.4.1.0/32         Direct 0    0            16.4.1.1        Vlan400
16.4.1.1/32         Direct 0    0            127.0.0.1       InLoop0
16.4.1.255/32       Direct 0    0            16.4.1.1        Vlan400
127.0.0.0/8         Direct 0    0            127.0.0.1       InLoop0
127.0.0.0/32        Direct 0    0            127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0            127.0.0.1       InLoop0
127.255.255.255/32  Direct 0    0            127.0.0.1       InLoop0
```

3)　ルートの再配信を設定します。

Switch B で、RIP 200 にダイレクトルートと RIP 100 からのルートを再配信するように設定します。

```
[SwitchB] rip 200
[SwitchB-rip-200] import-route rip 100
[SwitchB-rip-200] import-route direct
[SwitchB-rip-200] quit
```

Switch C の IP ルーティングテーブルを表示します。

```
[SwitchC] display ip routing-table

Destinations : 15        Routes : 15

Destination/Mask    Proto  Pre  Cost        NextHop         Interface
0.0.0.0/32          Direct 0    0           127.0.0.1       InLoop0
10.2.1.0/24         RIP    100  1           12.3.1.1        Vlan200
11.1.1.0/24         RIP    100  1           12.3.1.1        Vlan200
12.3.1.0/24         Direct 0    0           12.3.1.2        Vlan200
12.3.1.0/32         Direct 0    0           12.3.1.2        Vlan200
12.3.1.2/32         Direct 0    0           127.0.0.1       InLoop0
12.3.1.255/32       Direct 0    0           12.3.1.2        Vlan200
16.4.1.0/24         Direct 0    0           16.4.1.1        Vlan400
16.4.1.0/32         Direct 0    0           16.4.1.1        Vlan400
16.4.1.1/32         Direct 0    0           127.0.0.1       InLoop0
16.4.1.255/32       Direct 0    0           16.4.1.1        Vlan400
127.0.0.0/8         Direct 0    0           127.0.0.1       InLoop0
127.0.0.0/32        Direct 0    0           127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0           127.0.0.1       InLoop0
127.255.255.255/32  Direct 0    0           127.0.0.1       InLoop0
```

6.12.3 RIP インタフェースへのメトリックの追加設定例

I. ネットワーク要件

図 6-3 に示すように、Switch A、Switch B、Switch C、Switch D、Switch E のすべてのインタフェースで RIPv2 を有効にします。

Switch A は Switch D への 2 つのリンクを持ちます。Switch B から Switch D へのリンクは Switch C から Switch D へのリンクに比べて安定しています。Switch A が Switch B から学習した 1.1.5.0/24 のネットワークを優先することができるように、Switch A の VLAN インタフェース 200 を通して受信した RIP ルートにメトリックを追加するように設定します。

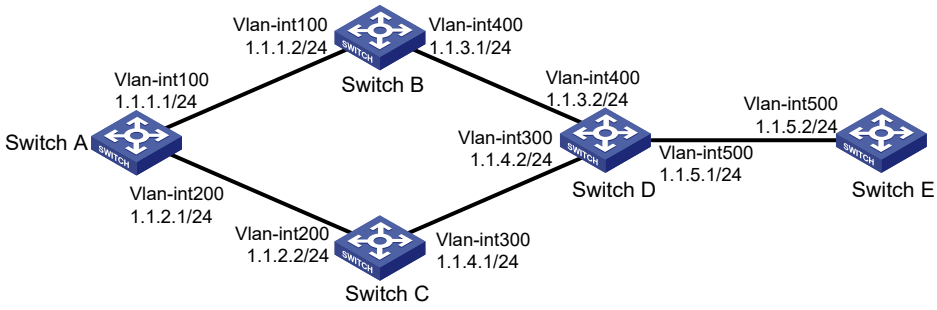


図 6-3 ネットワーク図

II. 設定手順

1)　インタフェースに IP アドレスを設定します。(詳細は省略します)
2)　RIP の基本機能を設定します。

Switch A を設定します。

```
<SwitchA> system-view

[SwitchA] rip 1

[SwitchA-rip-1] network 1.0.0.0
```

```
[SwitchA-rip-1] version 2
[SwitchA-rip-1] undo summary
[SwitchA-rip-1] quit
```

Switch B を設定します。

```
<SwitchB> system-view
[SwitchB] rip 1
[SwitchB-rip-1] network 1.0.0.0
[SwitchB-rip-1] version 2
[SwitchB-rip-1] undo summary
```

Switch C を設定します。

```
<SwitchC> system-view
[SwitchB] rip 1
[SwitchC-rip-1] network 1.0.0.0
[SwitchC-rip-1] version 2
[SwitchC-rip-1] undo summary
```

Switch D を設定します。

```
<SwitchD> system-view
[SwitchD] rip 1
[SwitchD-rip-1] network 1.0.0.0
[SwitchD-rip-1] version 2
[SwitchD-rip-1] undo summary
```

Switch E を設定します。

```
<SwitchE> system-view
[SwitchE] rip 1
[SwitchE-rip-1] network 1.0.0.0
[SwitchE-rip-1] version 2
[SwitchE-rip-1] undo summary
```

Switch A で RIP データベースにあるすべてのアクティブなルートを表示します。

```
[SwitchA] display rip 1 database
   1.0.0.0/8, auto-summary
       1.1.1.0/24, cost 0, nexthop 1.1.1.1, RIP-interface
       1.1.2.0/24, cost 0, nexthop 1.1.2.1, RIP-interface
       1.1.3.0/24, cost 1, nexthop 1.1.1.2
       1.1.4.0/24, cost 1, nexthop 1.1.2.2
       1.1.5.0/24, cost 2, nexthop 1.1.1.2
       1.1.5.0/24, cost 2, nexthop 1.1.2.2
```

出力はネットワーク 1.1.5.0/24 への 2 つの RIP ルートがあることを示します。それらのルートのネクストホップは、それぞれ、Switch B(1.1.1.2)と Switch C(1.1.2.2)です。ルートのコストは 2 です。

3)　RIP が有効なインタフェースに、メトリックを追加します。

Switch A の RIP が有効な VLAN インタフェース 200 に、メトリック 3 を追加するように設定します。

```
[SwitchA] interface vlan-interface 200
[SwitchA-Vlan-interface200] rip metricin 3
```

Switch A の RIP データベースのアクティブなルートを表示します。

```
[SwitchA-Vlan-interface200] display rip 1 database
   1.0.0.0/8, auto-summary
       1.1.1.0/24, cost 0, nexthop 1.1.1.1, RIP-interface
       1.1.2.0/24, cost 0, nexthop 1.1.2.1, RIP-interface
       1.1.3.0/24, cost 1, nexthop 1.1.1.2
       1.1.4.0/24, cost 2, nexthop 1.1.1.2
       1.1.5.0/24, cost 2, nexthop 1.1.1.2
```

出力は、ネットワーク 1.1.5.0/24 への RIP ルートが（ネクストホップが Switch B(1.1.1.2)、コストが 2）、ただ 1 つの RIP ルートであることを示します。

6.12.4 RIP の集約ルートの配信設定例

I. ネットワーク要件

図 6-4に示すように、Switch A と Switch B では OSPF が、Switch D では RIP が、Switch C では OSPF と RIP が動作しています。

Switch D が 10.1.1.0/24、10.2.1.0/24、10.5.1.0/24、10.6.1.0/24 宛てのネットワークを持てるように、Switch C に RIP で OSPF ルートを再配信できるように設定します。

Switch D のルーティングテーブルサイズを減らすことができるように、Switch C に集約ルート 10.0.0.0/8 のみを配信するように設定します。

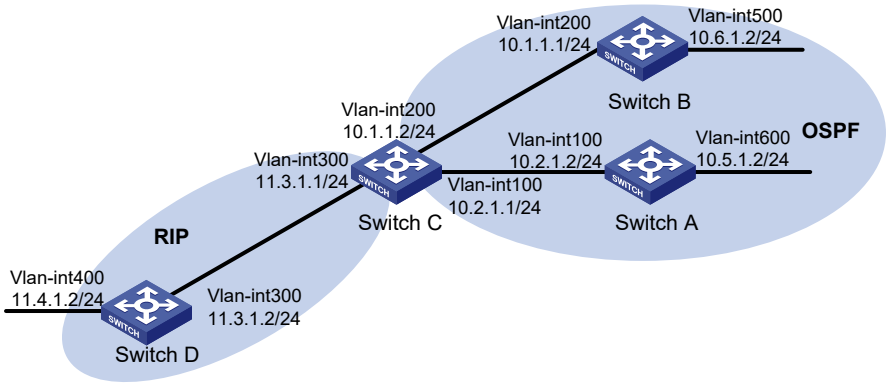


図 6-4 ネットワーク図

II. 設定手順

1) インタフェースに IP アドレスを設定します。(詳細は省略します)
2) RIP の基本機能を設定します。

Switch A を設定します。

```
<SwitchA> system-view
[SwitchA] ospf
[SwitchA-ospf-1] area 0
[SwitchA-ospf-1-area-0.0.0.0] network 10.5.1.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.0] network 10.2.1.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.0] quit
```

Switch B を設定します。

```
<SwitchB> system-view
[SwitchB] ospf
[SwitchB-ospf-1] area 0
[SwitchB-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] network 10.6.1.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] quit
```

Switch C を設定します。

```
<SwitchC> system-view
[SwitchC] ospf
[SwitchC-ospf-1] area 0
[SwitchC-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0] network 10.2.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0] quit
[SwitchC-ospf-1] quit
```

3) RIP の基本機能を設定します。

Switch C を設定します。

```
[SwitchC] rip 1
[SwitchC-rip-1] network 11.3.1.0
[SwitchC-rip-1] version 2
[SwitchC-rip-1] undo summary
```

Switch D を設定します。

```
<SwitchD> system-view
[SwitchD] rip 1
[SwitchD-rip-1] network 11.0.0.0
```

```
[SwitchD-rip-1] version 2
[SwitchD-rip-1] undo summary
[SwitchD-rip-1] quit
```

Switch C に RIP で、OSPF プロセス 1 からのルートとダイレクトルートを再配信するように設定します。

```
[SwitchC-rip-1] import-route direct
[SwitchC-rip-1] import-route ospf 1
[SwitchC-rip-1] quit
```

Switch D の IP ルーティングテーブルを表示します。

```
[SwitchD] display ip routing-table

Destinations : 15        Routes : 15

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
0.0.0.0/32          Direct 0    0            127.0.0.1       InLoop0
10.1.1.0/24         RIP    100  1            11.3.1.1        Vlan300
10.2.1.0/24         RIP    100  1            11.3.1.1        Vlan300
10.5.1.0/24         RIP    100  1            11.3.1.1        Vlan300
10.6.1.0/24         RIP    100  1            11.3.1.1        Vlan300
11.3.1.0/24         Direct 0    0            11.3.1.2        Vlan300
11.3.1.0/32         Direct 0    0            11.3.1.2        Vlan300
11.3.1.2/32         Direct 0    0            127.0.0.1       InLoop0
11.4.1.0/24         Direct 0    0            11.4.1.2        Vlan400
11.4.1.0/32         Direct 0    0            11.4.1.2        Vlan400
11.4.1.2/32         Direct 0    0            127.0.0.1       InLoop0
127.0.0.0/8         Direct 0    0            127.0.0.1       InLoop0
127.0.0.0/32        Direct 0    0            127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0            127.0.0.1       InLoop0
127.255.255.255/32  Direct 0    0            127.0.0.1       InLoop0
```

4) ルート集約を設定します。

Switch C で集約ルート 10.0.0.0/8 のみを配信するようにルート集約を設定します。

```
[SwitchC] interface vlan-interface 300
[SwitchC-Vlan-interface300] rip summary-address 10.0.0.0 8
```

Switch D の IP ルーティングテーブルを表示します。

```
[SwitchD] display ip routing-table

Destinations : 12        Routes : 12

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
0.0.0.0/32          Direct 0    0            127.0.0.1       InLoop0
10.0.0.0/8          RIP    100  1            11.3.1.1        Vlan300
11.3.1.0/24         Direct 0    0            11.3.1.2        Vlan300
11.3.1.0/32         Direct 0    0            11.3.1.2        Vlan300
11.3.1.2/32         Direct 0    0            127.0.0.1       InLoop0
11.4.1.0/24         Direct 0    0            11.4.1.2        Vlan400
11.4.1.0/32         Direct 0    0            11.4.1.2        Vlan400
11.4.1.2/32         Direct 0    0            127.0.0.1       InLoop0
127.0.0.0/8         Direct 0    0            127.0.0.1       InLoop0
127.0.0.0/32        Direct 0    0            127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0            127.0.0.1       InLoop0
127.255.255.255/32  Direct 0    0            127.0.0.1       InLoop0
```

6.12.5 RIP GR の設定例

I. ネットワーク要件

図 6-5 に示すように、Switch A、Switch B、および Switch C はすべて RIPv2 を実行します。

- Switch A で GR を有効にします。Switch A は GR リスタータとして機能します。
- Switch B と Switch C は GR ヘルパーとして機能し、GR を使用してルーティングテーブルを Switch A と同期させます。

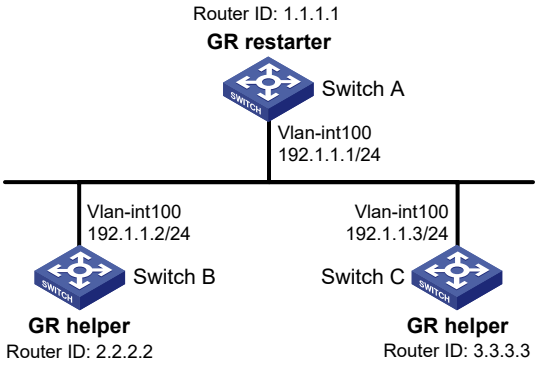


図 6-5 ネットワーク図

II. 設定手順

1) スイッチのインタフェースの IP アドレスとサブネットマスクを設定します。（詳細は示されていません）
2) スイッチに RIPv2 を設定して、次のことを確認します（詳細は省略します）。
   - Switch A、Switch B、および Switch C は、レイヤ 3 で相互に通信できます。
   - RIPv2 を使用して動的ルート更新を実装することができます。
3) Switch A で RIP GR を有効にします。

```
<SwitchA> system-view
[SwitchA] rip
[SwitchA-rip-1] graceful-restart
```

6.12.6 RIP NSR の設定例

I. ネットワーク要件

図 6-6に示すように、Switch A、Switch B、および Switch S はすべて RIPv 2 を実行します。

Switch S でアクティブ/スタンバイスイッチオーバーが発生したときに正しいルーティングを保証するには、Switch S で RIP NSR を有効にします。

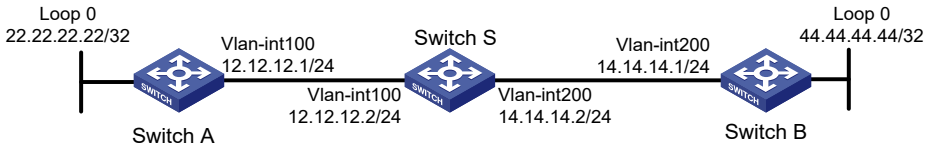


図 6-6 ネットワーク図

II. 設定手順

1) スイッチのインタフェースの IP アドレスとサブネットマスクを設定します。（詳細は表示されていません。）
2) スイッチで RIPv2 を設定して、次のことを確認します。（詳細は表示されていません。）
   - Switch A、Switch B、および Switch S は、レイヤ 3 で相互に通信できます。
   - 動的ルート更新は、RIPv2 を使用してそれらの間で実装できます。
3) Switch S で RIP NSR を有効にします。

```
<SwitchS> system-view
[SwitchS] rip 100
[SwitchS-rip-100] non-stop-routing
[SwitchS-rip-100] quit
```

III. 設定の確認

Switch S でアクティブ/スタンバイスイッチオーバーを実行します。

```
[SwitchS] placement reoptimize
Predicted changes to the placement
Program                          Current location       New location
-------------------------------------------------------------------------
lb                               0/0                    0/0
lsm                              0/0                    0/0
slsp                             0/0                    0/0
rib6                             0/0                    0/0
routepolicy                      0/0                    0/0
rib                              0/0                    0/0
staticroute6                     0/0                    0/0
staticroute                      0/0                    0/0
eviisis                          0/0                    0/0
ospf                             0/0                    1/0
Continue? [y/n]:y
Re-optimization of the placement start. You will be notified on completion
Re-optimization of the placement complete. Use 'display placement' to view the
new placement
```

Switch A のネイバ情報およびルート情報を表示します。

```
[SwitchA] display rip 1 neighbor
 Neighbor Address: 12.12.12.2
     Interface  : Vlan-interface200
     Version    : RIPv2      Last update: 00h00m13s
     Relay nbr  : No         BFD session: None
     Bad packets: 0          Bad routes : 0
[SwitchA] display rip 1 route
 Route Flags: R - RIP, T - TRIP
              P - Permanent, A - Aging, S - Suppressed, G - Garbage-collect
              D - Direct, O - Optimal, F - Flush to RIB
```

```
------------------------------------------------------------------------------
Peer 12.12.12.2 on Vlan-interface200
     Destination/Mask        Nexthop          Cost    Tag     Flags   Sec
     14.0.0.0/8              12.12.12.2       1       0       RAOF    16
     44.0.0.0/8              12.12.12.2       2       0       RAOF    16
Local route
     Destination/Mask        Nexthop          Cost    Tag     Flags   Sec
     12.12.12.0/24           0.0.0.0          0       0       RDOF    -
     22.22.22.22/32          0.0.0.0          0       0       RDOF    -
```

Switch B のネイバ情報およびルート情報を表示します。

```
[SwitchB] display rip 1 neighbor
Neighbor Address: 14.14.14.2
    Interface  : Vlan-interface200
    Version    : RIPv2     Last update: 00h00m32s
    Relay nbr  : No        BFD session: None
    Bad packets: 0         Bad routes : 0
[SwitchB] display rip 1 route
Route Flags: R - RIP, T - TRIP
             P - Permanent, A - Aging, S - Suppressed, G - Garbage-collect
             D - Direct, O - Optimal, F - Flush to RIB
------------------------------------------------------------------------------
Peer 14.14.14.2 on Vlan-interface200
     Destination/Mask        Nexthop          Cost    Tag     Flags   Sec
     12.0.0.0/8              14.14.14.2       1       0       RAOF    1
     22.0.0.0/8              14.14.14.2       2       0       RAOF    1
Local route
     Destination/Mask        Nexthop          Cost    Tag     Flags   Sec
     44.44.44.44/32          0.0.0.0          0       0       RDOF    -
     14.14.14.0/24           0.0.0.0          0       0       RDOF    -
```

出力には、Switch S でのアクティブ/スタンバイスイッチオーバー中に、Switch A および Switch B のネイバおよびルート情報が変更されないことが示されています。Switch A から Switch B へのトラフィックは影響を受けていません。

6.12.7 RIP での BFD の設定例(直接接続されたネイバ装置のエコーパケットモードの片方向検知)

I. ネットワーク要件

図 6-7に示すように、Switch A と Switch C の VLAN インタフェース 100 は、RIP プロセス 1 が動作します。Switch A の VLAN インタフェース 200 は、RIP プロセス 2 が動作します。Switch C の VLAN インタフェース 300 と Switch B の VLAN インタフェース 200 と VLAN インタフェース 300 は、RIP プロセス 1 が動作します。

- スタティックルート 100.1.1.1/24 を設定し、Switch C の RIP にスタティックルートを再配信するようにします。これは Switch A が、VLAN インタフェース 100 と VLAN インタフェース 200 を通して 100.1.1.1/24 の 2 つのルートを学習できるようにします。そして VLAN インタフェース 100 を通したルートを使用します。
- Switch A の VLAN インタフェース 100 で RIP の BFD を有効にします。VLAN インタフェース 100 が故障したときに、BFD がすぐさま故障を検出し、RIP に通知できるようにします。そして RIP はネイバ関係と VLAN インタフェース 100 で学習したルート情報を削除し、VLAN インタフェース 200 を通して 100.1.1.1/24 のルートを使用します。

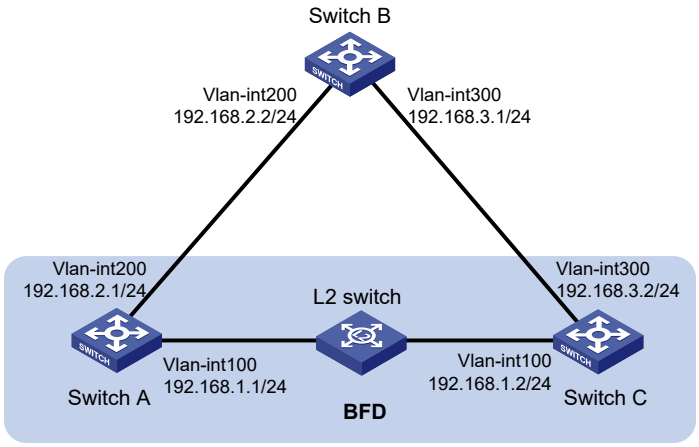


図 6-7 ネットワーク図

II. 設定手順

1)　インタフェースに IP アドレスを設定します。(詳細は省略します)
2)　RIP の基本機能を設定します。

Switch A を設定します。

```
<SwitchA> system-view
[SwitchA] rip 1
[SwitchA-rip-1] version 2
[SwitchA-rip-1] undo summary
[SwitchA-rip-1] network 192.168.1.0
[SwitchA-rip-1] quit
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] rip bfd enable
[SwitchA-Vlan-interface100] quit
[SwitchA] rip 2
[SwitchA-rip-2] version 2
[SwitchA-rip-2] undo summary
[SwitchA-rip-2] network 192.168.2.0
[SwitchA-rip-2] quit
```

Switch B を設定します。

```
<SwitchB> system-view
[SwitchB] rip 1
[SwitchB-rip-1] version 2
[SwitchB-rip-1] undo summary
```

```
[SwitchB-rip-1] network 192.168.2.0
[SwitchB-rip-1] network 192.168.3.0
[SwitchB-rip-1] quit
```

Switch C を設定します。

```
<SwitchC> system-view
[SwitchC] rip 1
[SwitchC-rip-1] version 2
[SwitchC-rip-1] undo summary
[SwitchC-rip-1] network 192.168.1.0
[SwitchC-rip-1] network 192.168.3.0
[SwitchC-rip-1] import-route static
[SwitchC-rip-1] quit
```

3) Switch A の VLAN インタフェース 100 の BFD パラメータを設定します。

```
[SwitchA] bfd echo-source-ip 11.11.11.11
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] bfd min-echo-receive-interval 500
[SwitchA-Vlan-interface100] bfd detect-multiplier 7
[SwitchA-Vlan-interface100] quit
[SwitchA] quit
```

4) Switch C のスタティックルートを設定します。

```
[SwitchC] ip route-static 120.1.1.1 24 null 0
```

III. 設定の確認

Switch A の BFD セッション情報を表示します。

```
<SwitchA> display bfd session
 Total Session Num: 1     Up Session Num: 1     Init Mode: Active

 IPv4 Session Working Under Echo Mode:

 LD          SourceAddr      DestAddr        State    Holdtime    Interface
 4           192.168.1.1     192.168.1.2     Up       2000ms      Vlan100
```

Switch A で学習された 120.1.1.0/24 の RIP ルートを表示します。

```
<SwitchA> display ip routing-table 120.1.1.0 24

Summary count : 1

Destination/Mask   Proto   Pre Cost        NextHop         Interface
120.1.1.0/24       RIP     100 1           192.168.1.2     Vlan-interface100
```

出力では、Switch A は VLAN インタフェース 100 を通して Switch C と通信しています。

そして VLAN インタフェース 100 を経由したリンクの障害を発生させます。

Switch A で学習された 120.1.1.0/24 の RIP ルートを表示します。

```
<SwitchA> display ip routing-table 120.1.1.0 24

Summary count : 1

Destination/Mask    Proto   Pre Cost        NextHop         Interface
120.1.1.0/24        RIP     100 1           192.168.2.2     Vlan-interface200
```

出力では、Switch A は VLAN インタフェース 200 を通して Switch C と通信しています。

6.12.8 RIP での BFD の設定例(特定の宛先に対するシングルホップエコー検出)

I. ネットワーク要件

図 6-8に示すように Switch A および Switch B の VLAN インタフェース 100 は、RIP プロセス 1 を実行します。 Switch B および Switch C の VLAN インタフェース 200 は、RIP プロセス 1 を実行します。

- 設定は、100.1.1.0/24 宛てのスタティックルートを設定し、Switch A と Switch C の両方でスタティックルートの RIP への再配送を有効にします。これにより、Switch B は、100.1.1.0/24 宛ての 2 つのルートを VLAN インタフェース 100 と VLAN インタフェース 200 を通じて学習できます。Switch A から再配信されたルートは、Switch C から再配信されたルートよりもコストが低いため、Switch B は VLAN インタフェース 200 を介したルートを使用します。
- Switch A の VLAN インタフェース 100 で RIP の BFD を有効にし、宛先として Switch B の VLAN インタフェース 100 を指定します。 Switch A と Switch B の間で片方向リンクが発生すると、BFDはリンク障害をすばやく検出し、RIPに通知できます。Switch B は次に、ネイバ関係と VLAN インタフェース 100 で学習したルート情報を削除します。 VLAN インタフェース 100 からのパケットの送受信は行いません。 ルートがスイッチから学習された場合 A Switch B は、VLAN インタフェース 200 を介して 100.1.1.124 宛てのルートを使用します。

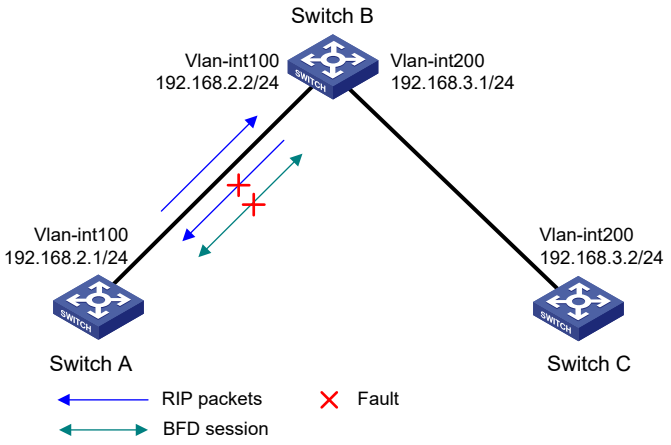


図 6-8 ネットワーク図

II. 設定手順

1) インタフェースのための IP アドレスを設定。(詳細は省略します)
2) RIP の基本機能の設定とインタフェースでの BFD の有効化

Switch A を設定します。

```
<SwitchA> system-view
[SwitchA] rip 1
[SwitchA-rip-1] network 192.168.2.0
[SwitchA-rip-1] import-route static
[SwitchA-rip-1] quit
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] rip bfd enable destination 192.168.2.2
[SwitchA-Vlan-interface100] quit
```

Switch B を設定します。

```
<SwitchB> system-view
[SwitchB] rip 1
[SwitchB-rip-1] network 192.168.2.0
[SwitchB-rip-1] network 192.168.3.0
[SwitchB-rip-1] quit
```

Switch C を設定します。

```
<SwitchC> system-view
[SwitchC] rip 1
[SwitchC-rip-1] network 192.168.3.0
[SwitchC-rip-1] import-route static cost 3
[SwitchC-rip-1] quit
```

3) Switch A の VLAN インタフェース 100 に BFD パラメータを設定します

```
[SwitchA] bfd echo-source-ip 11.11.11.11
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] bfd min-echo-receive-interval 500
[SwitchA-Vlan-interface100] return
```

4) スタティックルートを設定します。

Switch A でスタティックルートを設定します。

```
[SwitchA] ip route-static 100.1.1.0 24 null 0
```

Switch C でスタティックルートを設定します。

```
[SwitchA] ip route-static 100.1.1.0 24 null 0
```

III. 設定の確認

Switch A の BFD セッション情報を表示します。

```
<SwitchA> display bfd session

 Total Session Num: 1     Up Session Num: 1     Init Mode: Active

 IPv4 session working under Echo mode:

 LD             SourceAddr       DestAddr        State    Holdtime     Interface
 3              192.168.2.1      192.168.2.2     Up       2000ms       vlan100
```

100.1.1.0/24 宛てのルートを Switch B に表示します。

```
<SwitchB> display ip routing-table 100.1.1.0 24 verbose

Summary Count : 1

Destination: 100.1.1.0/24
   Protocol: RIP
 Process ID: 1
  SubProtID: 0x1                  Age: 00h02m47s
       Cost: 1                Preference: 100
      IpPre: N/A              QosLocalID: N/A
        Tag: 0                     State: Active Adv
  OrigTblID: 0x0                OrigVrf: default-vrf
    TableID: 0x2                 OrigAs: 0
      NibID: 0x12000002          LastAs: 0
     AttrID: 0xffffffff        Neighbor: 192.168.2.1
      Flags: 0x1008c         OrigNextHop: 192.168.2.1
      Label: NULL            RealNextHop: 192.168.2.1
    BkLabel: NULL              BkNextHop: N/A
  Tunnel ID: Invalid           Interface: vlan-interface 100
BkTunnel ID: Invalid         BkInterface: N/A
   FtnIndex: 0x0             TrafficIndex: N/A
  Connector: N/A                   PathID: 0x0
```

Switch A と Switch B 間のリンクに障害が発生した場合、Switch B に 100.1.1.0/24 宛てのルートを表示します。

```
<SwitchB> display ip routing-table 100.1.1.0 24 verbose

Summary Count : 1

Destination: 100.1.1.0/24
   Protocol: RIP
 Process ID: 1
  SubProtID: 0x1                  Age: 00h21m23s
       Cost: 4                Preference: 100
      IpPre: N/A              QosLocalID: N/A
        Tag: 0                     State: Active Adv
  OrigTblID: 0x0                OrigVrf: default-vrf
    TableID: 0x2                 OrigAs: 0
      NibID: 0x12000002          LastAs: 0
     AttrID: 0xffffffff        Neighbor: 192.168.3.2
      Flags: 0x1008c         OrigNextHop: 192.168.3.2
      Label: NULL            RealNextHop: 192.168.3.2
    BkLabel: NULL              BkNextHop: N/A
  Tunnel ID: Invalid           Interface: vlan-interface 200
BkTunnel ID: Invalid         BkInterface: N/A
   FtnIndex: 0x0             TrafficIndex: N/A
  Connector: N/A                   PathID: 0x0
```

6.12.9 RIP での BFD の設定例(BFD 制御パケットモードの双方向検出)

I. ネットワーク要件

図 6-9に示すように Switch A の VLAN インタフェース 100 および Switch C の VLAN インタフェース 200 は、RIP プロセス 1 を実行します。

Switch A の VLAN インタフェース 300 は RIP プロセス 2 を実行します。Switch C の VLAN インタフェース 400、および Switch D の VLAN インタフェース 300 と VLAN インタフェース 400 は、RIP プロセス 1 を実行します。

- Switch A で 100.1.1.0/24 宛てのスタティックルートを設定します。
- Switch C で 101.1.1.0/24 宛てのスタティックルートを設定します。
- Switch A と Switch C で RIP へのスタティックルート再配信を有効にします。これにより、Switch A は、VLAN インタフェース 100 と VLAN インタフェース 300 を介して 100.1.1.0/24 宛ての 2 つのルートを学習できます。 VLAN インタフェース 100 を経由するルートを使用します。
- Switch A の VLAN インタフェース 100 と Switch C の VLAN インタフェース 200 で BFD を有効にします。

VLAN インタフェース 100 上のリンクに障害が発生すると、BFD はリンク障害をすばやく検出し、RIP に通知できます。 RIP は、ネイバ関係と、VLAN インタフェース 100 で学習されたルート情報を削除します。それは、100.1.1.0/24 宛ての経路で VLAN インタフェース 300 を介して使用します。

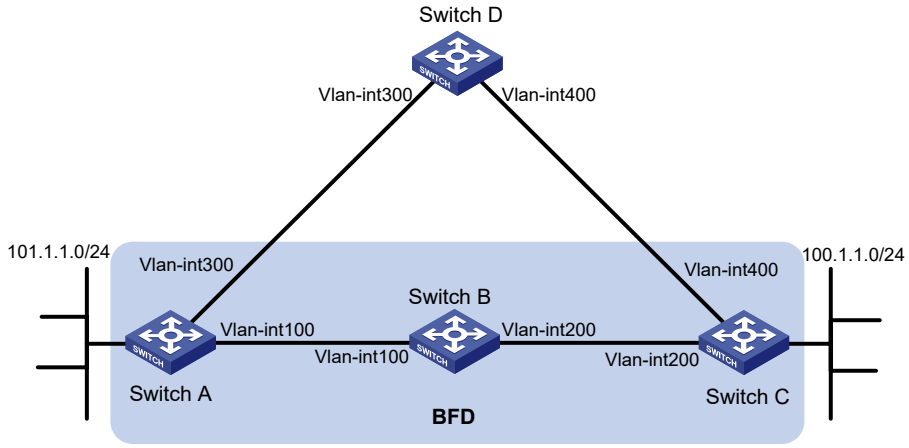


図 6-9 ネットワーク図

表 6-1 インタフェースと IP アドレスの割り当て

装置	インタフェース	IP アドレス
Switch A	VLAN-interface 300	192.168.3.1/24
Switch A	VLAN-interface 100	192.168.1.1/24
Switch B	VLAN-interface 100	192.168.1.2/24
Switch B	VLAN-interface 200	192.168.2.1/24
Switch C	VLAN-interface 200	192.168.2.2/24
Switch C	VLAN-interface 400	192.168.4.2/24
Switch D	VLAN-interface 300	192.168.3.2/24

装置	インタフェース	IP アドレス
Switch D	VLAN-interface 400	192.168.4.1/24

II. 設定手順

1) インタフェースのための IP アドレスを設定。(詳細は省略します)
2) RIP の基本設定とスタティックルートの RIP への再配信を有効にして、Switch A と Switch C が互いに送信するルートを持つようにします。

```
<SwitchA> system-view
[SwitchA] rip 1
[SwitchA-rip-1] version 2
[SwitchA-rip-1] undo summary
[SwitchA-rip-1] network 192.168.1.0
[SwitchA-rip-1] network 101.1.1.0
[SwitchA-rip-1] peer 192.168.2.2
[SwitchA-rip-1] undo validate-source-address
[SwitchA-rip-1] import-route static
[SwitchA-rip-1] quit
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] rip bfd enable
[SwitchA-Vlan-interface100] quit
[SwitchA] rip 2
[SwitchA-rip-2] version 2
[SwitchA-rip-2] undo summary
[SwitchA-rip-2] network 192.168.3.0
[SwitchA-rip-2] quit
```

Switch C を設定します。

```
<SwitchC> system-view
[SwitchC] rip 1
[SwitchC-rip-1] version 2
[SwitchC-rip-1] undo summary
[SwitchC-rip-1] network 192.168.2.0
[SwitchC-rip-1] network 192.168.4.0
[SwitchC-rip-1] network 100.1.1.0
[SwitchC-rip-1] peer 192.168.1.1
[SwitchC-rip-1] undo validate-source-address
```

```
[SwitchC-rip-1] import-route static
[SwitchC-rip-1] quit
[SwitchC] interface vlan-interface 200
[SwitchC-Vlan-interface200] rip bfd enable
[SwitchC-Vlan-interface200] quit
```

Switch D を設定します。

```
<SwitchD> system-view
[SwitchD] rip 1
[SwitchD-rip-1] version 2
[SwitchD-rip-1] undo summary
[SwitchD-rip-1] network 192.168.3.0
[SwitchD-rip-1] network 192.168.4.0
```

3) BDF パラメータを設定します。

Switch A を設定します。

```
[SwitchA] bfd session init-mode active
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] bfd min-transmit-interval 500
[SwitchA-Vlan-interface100] bfd min-receive-interval 500
[SwitchA-Vlan-interface100] bfd detect-multiplier 7
[SwitchA-Vlan-interface100] quit
```

Switch C を設定します。

```
[SwitchC] bfd session init-mode active
[SwitchC] interface vlan-interface 200
[SwitchC-Vlan-interface200] bfd min-transmit-interval 500
[SwitchC-Vlan-interface200] bfd min-receive-interval 500
[SwitchC-Vlan-interface200] bfd detect-multiplier 7
[SwitchC-Vlan-interface200] quit
```

4) スタティックルートを設定します。

Switch A の Switch C へのスタティックルートを設定します。

```
[SwitchA] ip route-static 192.168.2.0 24 vlan-interface 100 192.168.1.2
[SwitchA] quit
```

Switch C の Switch A へのスタティックルートを設定します。

```
[SwitchC] ip route-static 192.168.1.0 24 vlan-interface 200 192.168.2.1
```

III. 設定の確認

Switch A の BFD セッション情報を表示します。

```
<SwitchA> display bfd session

 Total Session Num: 1     Up Session Num: 1     Init Mode: Active

 IPv4 session working under Ctrl mode:

 LD/RD            SourceAddr      DestAddr        State    Holdtime    Interface
 513/513           192.168.1.1     192.168.2.2     Up       1700ms      vlan100
```

100.1.1.0/24 宛てのルートを Switch A に表示します。

```
<SwitchA> display ip routing-table 100.1.1.0 24

Summary count : 1

Destination/Mask   Proto   Pre Cost        NextHop         Interface
100.1.1.0/24       RIP     100 1           192.168.2.2     vlan-interface 100
```

出力は、Switch A が VLAN インタフェース 100 を介して Switch C と通信することを示しています。次に、VLAN インタフェース 100 上のリンクに障害が発生します。

Switch A で 100.1.1.0/24 宛ての RIP ルートを表示します。

```
<SwitchA> display ip routing-table 100.1.1.0 24

Summary count : 1

Destination/Mask   Proto   Pre Cost        NextHop         Interface
100.1.1.0/24       RIP     100 2           192.168.3.2     vlan-interface 300
```

出力は、Switch A が VLAN-インタフェース 300 を介して Switch C と通信することを示す。

目次

このセクションのページは**5-x-x** です。

7章 OSPF 7-1
7.1 概要 7-1
7.1.1 OSPFの特徴 7-1
7.1.2 OSPFパケット 7-1
7.1.3 LSAパケット 7-2
7.1.4 OSPFエリア 7-2
7.1.5 ルータタイプ 7-5
7.1.6 ルートタイプ 7-6
7.1.7 ルータID 7-6
7.1.8 ルートの計算 7-7
7.1.9 OSPFネットワークタイプ 7-7
7.1.10 DRおよびBDR 7-8
7.1.11 プロトコルと標準 7-9
7.2 制限とガイドライン 7-10
7.3 OSPF設定作業リスト 7-10
7.4 OSPF基本機能の設定 7-12
7.4.1 OSPFプロセスの有効化 7-12
7.4.2 OSPFエリアの作成 7-12
7.4.3 OSPFの有効化 7-13
7.5 OSPFスタブエリアとNSSAエリアの設定 7-14
7.5.1 OSPFスタブエリアとNSSAエリアの設定 7-14
7.5.2 スタブエリアの設定 7-14
7.5.3 NSSAエリアの設定 7-15
7.5.4 仮想リンクの設定 7-16
7.6 OSPFネットワークタイプの設定 7-16
7.6.1 制限とガイドライン 7-17
7.6.2 インタフェースのブロードキャストネットワークタイプの設定 7-17
7.6.3 インタフェースのNBMAネットワークタイプの設定 7-17
7.6.4 インタフェースのP2MPネットワークタイプの設定 7-18
7.6.5 インタフェースのP2Pネットワークタイプの設定 7-18
7.7 OSPFルート制御の設定 7-18
7.7.1 OSPF内部エリアルート集約の設定 7-19
7.7.2 再配信されたルート集約の設定 7-19
7.7.3 受信ルートのフィルタリングの設定 7-20
7.7.4 Type-3 LSAフィルタリングの設定 7-20
7.7.5 インタフェースのOSPFコストの設定 7-21
7.7.6 ECMPルートの最大数の設定 7-22
7.7.7 OSPFの優先順位の設定 7-22
7.7.8 別のルーティングプロトコルからOSPFへのルート再配信の設定 7-22
7.7.9 デフォルトルートの再配信の設定 7-23
7.7.10 ホストルートの配信の設定 7-24
7.8 OSPFのタイマの設定 7-24
7.8.1 OSPFのタイマの設定 7-24
7.8.2 OSPFパケットのタイマの設定 7-24

7.8.3 LSAの伝送遅延の設定 7-25
7.8.4 SPFの計算間隔の設定 7-26
7.8.5 LSAの到達間隔の設定 7-26
7.8.6 LSA生成間隔の設定 7-26
7.8.7 OSPFオーバーフローから終了する期間の設定 7-27
7.9 OSPFパケットパラメータの設定 7-27
7.9.1 インタフェースのOSPFパケット送受信の無効化 7-27
7.9.2 インタフェースMTUのDDパケットへの付加 7-28
7.9.3 送信OSPFパケットへのDSCP値の設定 7-28
7.10 LSAの生成、配信、受信の制御 7-29
7.10.1 LSDB内の外部LSAの最大数の設定 7-29
7.11 拡張OSPF機能の設定 7-29
7.11.1 スタブルータの設定 7-29
7.11.2 RFC 1583の互換性の有効化 7-30
7.12 OSPF GRの設定 7-30
7.12.1 OSPF GR 7-30
7.12.2 OSPF GRリスタータの設定 7-31
7.12.3 OSPF GRヘルパーの設定 7-31
7.12.4 OSPF GRの開始 7-32
7.13 OSPF NSRの設定 7-33
7.14 OSPFのBFDの設定 7-33
7.14.1 OSPFのBFD 7-33
7.14.2 双方向コントロールパケット検知の設定 7-34
7.14.3 シングルホップエコー検知の設定 7-34
7.15 OSPF FRRの設定 7-34
7.15.1 OSPF FRRについて 7-34
7.15.2 バックアップのネクストホップを計算するためにLFAアルゴリズムを使用するためにOSPF FRRを設定 7-35
7.16 OSPF認証の設定 7-35
7.16.1 OSPFエリアとインタフェースでのOSPF認証 7-35
7.16.2 エリアでのOSPF認証の設定 7-36
7.16.3 インタフェースでのOSPF認証の設定 7-36
7.17 OSPF用のGTSMの設定 7-36
7.18 OSPFのロギングとSNMP notificationの設定 7-36
7.18.1 ネイバ状態変更のロギング 7-36
7.18.2 OSPFロギング機能の設定 7-37
7.18.3 OSPFネットワーク管理の設定 7-37
7.19 OSPFの表示と維持 7-38
7.20 OSPFの設定例 7-39
7.20.1 OSPFの基本機能の設定例 7-39
7.20.2 OSPFルート再配信の設定例 7-42
7.20.3 ASBRでのOSPFルート集約の設定例 7-43
7.20.4 OSPFスタブエリアの設定例 7-46
7.20.5 OSPF NSSAエリアの設定例 7-49
7.20.6 OSPF DR選出の設定例 7-51
7.20.7 OSPF仮想リンクの設定例 7-55
7.20.8 OSPF GRの設定例 7-58
7.20.9 OSPF NSRの設定例 7-60
7.20.10 OSPFでのBFDの設定例 7-62
7.20.11 OSPF FRRの設定例 7-66
7.21 OSPFのトラブルシューティング 7-68
7.21.1 OSPFのネイバ関係が構築されない 7-68

7.22 ルーティング情報の誤り 7-69

7章 OSPF

7.1 概要

OSPF(Open Shortest Path First)は IETF の OSPF ワーキンググループによって開発されたリンクステート IGP です。OSPF バージョン 2 は IPv4 で使われます。この章では OSPFv2 に関して記載します。

7.1.1 OSPF の特徴

OSPF は以下の特徴があります。

- **広い適用範囲** – さまざまな規模のネットワークをサポートできます。また、OSPF ルーティングドメイン内で最大数百のルータをサポートできます。
- **高速収束** – ネットワークトポロジの変更があれば、直ちに更新パケットを送出します。
- **ループフリー** — OSPF は、収集したリンク状態に応じて最短パスツリーアルゴリズムを使用してルートを計算するので、アルゴリズム自体がルーティングループを生成しません。
- **エリア分割** — 管理しやすいように AS のネットワークを異なるエリアに分割できます。これによって、エリア間で転送するルーティング情報を大幅に集約し、ネットワーク帯域の消費を減らすことができます。
- **イコールコストマルチルート** — 特定宛先への複数の同一コストルートをサポートします。
- **ルーティング階層** — OSPF には 4 段階のルーティング階層があります。ルートに、内部エリア、中間エリア、外部タイプ 1、外部タイプ 2 という優先順位が付けられます。
- **認証** — ルート計算のセキュリティを保護するために、インタフェースベースのパケット認証をサポートします。
- **マルチキャスト転送** — パケットを送受信するマルチキャストアドレスをサポートします。

7.1.2 OSPF パケット

OSPF メッセージは直接 IP パケットによって送信されます。プロトコル番号は 89 です。

OSPF は以下のパケットタイプを使用します。

- **Hello パケット** — ルータからネイバルータの発見と状態を保持するために定期的に送信されます。Hello パケットには、タイマ、DR、BDR、既知のネイバルータの情報が含まれます。
- **DD パケット(データベース記述パケット)** — 各 LSA の集約を含む自身の LSDB を記述し、2 台のルータがデータベースの同期を取るときに交換されます。
- **LSR(リンク状態要求)パケット** — 必要な LSA をネイバルータに転送します。DD パケットをルータが交換した後、ローカル LDSB からなくなっているネイバルータの LSA を検出します。その際に、存在していない LSA をお互いに要求します。パケットには、要求する LSA の集約が含まれます。
- **LSU(リンク状態更新)パケット** — 必要な LSA をネイバルータに転送します。

- **LSAck(リンク状態確認)パケット** — このパケットを使用して、受信した LSU パケットに対して肯定応答を返します。LSA の HEAD(肯定応答を要求した) が含まれます。LSAck は複数の LSA に応答することができます。

7.1.3 LSA パケット

OSPF は LSA(Link State Advertisements)のルーティング情報を配信します。以下の LSA タイプが一般的に使用されます。

- ルータ LSA(Router-LSA) — タイプ-1 LSA は すべてのルータで生成され、ルータが所属するエリア内にだけ配信されます。この LSA は収集されたエリアのルータインタフェースの状態を記述します。
- ネットワーク LSA(Network-LSA) — タイプ-2 LSA はブロードキャストもしくは NBMA ネットワークの DR によって生成され､オリジナルエリアにのみ配信されます。この LSA はエリア内のルータのリストを記述します。
- ネットワーク集約 LSA(Network Summary-LSA) — タイプ-3 LSA は ABR(エリアボーダールータ)によって生成され、LSA に関連するエリアで配信されます。各 Summary-LSA には、AS の内部ルート(インターエリアルート)で、外部エリアへの宛先ルートが記載されています。
- ASBR 集約 LSA(ASBR Summary-LSA) — タイプ-4 LSA は ABR によって生成され、LSA に関連するエリアに配信されます。Type-4 summary-LSA は ASBR(自律システム境界ルータ)への宛先を記述します。
- AS 外部 LSA(AS External LSA) — Type-5 LSA は ASBR によって生成され、他のすべての AS（スタブエリアと NSSA エリアを除く）に配信されます。
- NSSA LSA — Type-7 LSA は RFC1587 で定義され、NSSA(Not-So-Stubby Area)の ASBR によって生成され単一の NSSA エリア内に配信されます。NSSA LSA は他のエリアの AS へのルートを記述します。
- Opaque LSA — 予約可能な LSA で、標準的な LSA ヘッダとアプリケーション固有情報から構成されます。Opaque LSA は、OSPF プロトコルまたはいくつかのアプリケーションで使われ、情報を OSPF ルーティング ドメインに配信します。Opaque LSA には、Type-9、Type-10、Type-11 の 3 タイプがあり、異なるエリアへの配信に使われます。Opaque LSA はローカル サブネット、Type-10 はローカル エリア、Type-11 は AS 全体に配信されます。

7.1.4 OSPF エリア

I. エリアベース OSPF ネットワークの分割

非常に大規模な OSPF ルーティングドメインでは、大量の記憶領域を占有し、SPF 計算によって CPU リソースが必要となります。ルートの同期を行うために非常に多くの OSPF パケットが作成され、帯域幅を過度に占有することがあります。

この問題を解消するため、OSPF は AS をエリア ID で識別される複数のエリアに分割します。エリアの境界はリンクではなくルータです。ネットワークセグメント (またはリンク)は 1 つのエリアにしか存在できず、図 7-1のように、OSPF インタフェースはエリアに所属するよう指定されなければなりません。

エリア分割後、ABR（エリア境界ルータ）はルート要約を行って他のエリアに配信される LSA の数を減らし、トポロジの変化の影響を最小限に抑えます。

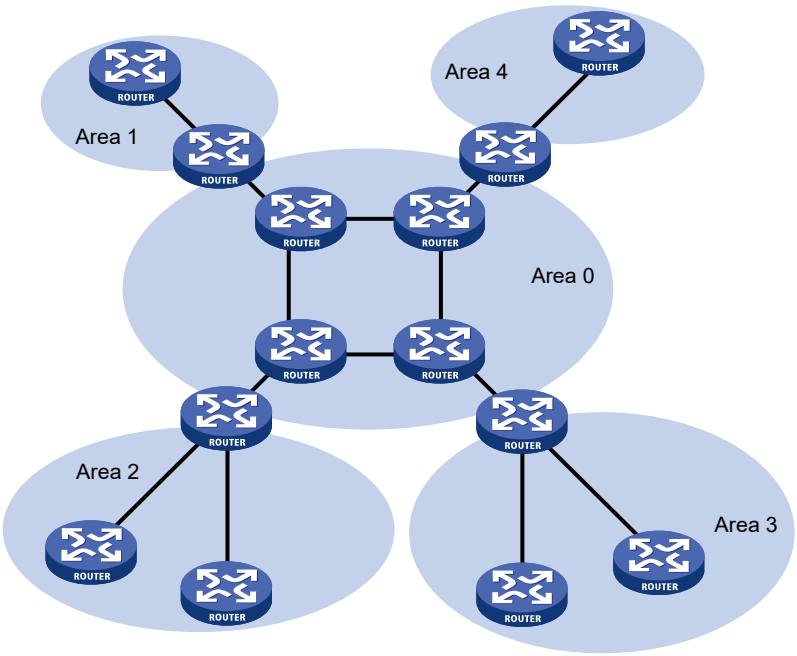


図 7-1 エリアで分割した OSPF ネットワーク

II. バックボーンエリア

各 AS にはバックボーンエリアと呼ばれるエリアがあり、バックボーン以外のエリア間のルーティング情報配信を行います。非バックボーンエリア間のルーティング情報はバックボーンエリアで転送されなければなりません。そのため、OSPF は以下が必要となります。

- 非バックボーンエリアはすべて、バックボーンエリアとの接続を維持する必要があります。
- バックボーンエリア自体が接続を維持する必要があります。

実際には、物理的な制約により要件を満たすことができない可能性があります。その場合、OSPF 仮想リンクを設定することが 1 つの解決策になります。

III. 仮想リンク

仮想リンクは、バックボーン以外のエリアを経由して 2 台の ABR 間に構築され、両方の ABR に設定されて有効になります。仮想リンク用の非バックボーンエリア内部ルートを提供するエリアは、通過エリアです。

図 7-2 において、Area 2 にはバックボーンエリア 0 への物理的な直接ルートはありません。ABR 間に仮想リンクを設定すれば、Area 2 はバックボーンエリアにつながります。

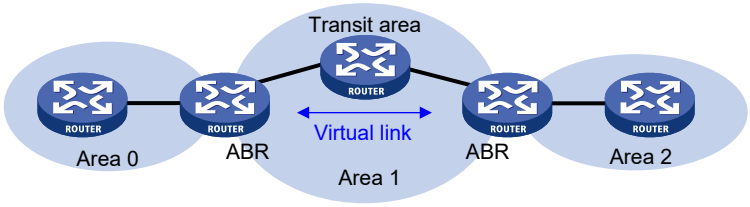


図 7-2 仮想リンクアプリケーション 1

仮想リンクのもう一つの用途は、冗長リンクとなることです。物理リンクの不具合でバックボーンエリアが内部接続を維持できないとき、仮想リンクを設定すれば、図 7-3のようにバックボーンエリアで論理的接続を確保できます。

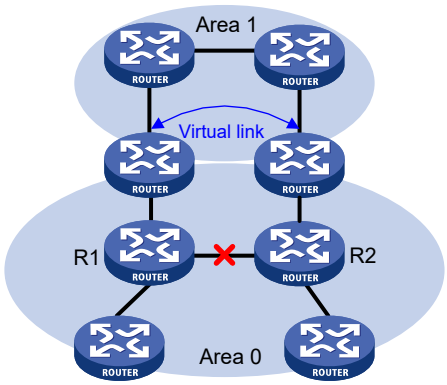


図 7-3 仮想リンクアプリケーション 2

2 台の ABR 間の仮想リンクは、ポイントツーポイント接続となります。このため、物理インタフェースで設定されるように、仮想リンクで Hello パケットの送信間隔などのインタフェースパラメータを設定できます。

仮想リンク上の 2 台の ABR は相互に OSPF パケットを直接交換し、その間にある OSPF ルータは、単にこれらの OSPF パケットを通常の IP パケットとして転送します。

IV. スタブエリアと完全スタブエリア

スタブエリアの ABR は、エリア内で Type-5 LSA を配布しません。そのため、このエリアのルーティングテーブルの大きさやルーティング情報の量はかなり削減されます。スタブエリアの ABR は、デフォルトルートを通して外部ネットワークにエリア内のルータが到達できるように、Type-3 LSA のデフォルトルートを配信します。

さらにルーティングテーブルサイズと配信される LSA を削減するため、スタブエリアを完全スタブエリアとして設定することができます。完全スタブエリアは他のエリアのルートも外部ルートも配信しません。完全スタブエリアの ABR は、デフォルトルートを通して外部ネットワークにエリア内のルータが到達できるように、Type-3 LSA のデフォルトルートを配信します。

V. NSSA エリアと完全 NSSA エリア

スタブエリアと同様、NSSA エリアは AS 外部 LSA (Type-5 LSA) をインポートしませんが、ASBR が生成し、NSSA エリアで配布された Type-7 LSA はインポートできます。NSSA ABR は、Type-7 LSA を Type-5 LSA に変換し、他のエリアに Type-5 LSA を配信します。

図 7-4において、OSPF AS は Area 1、Area 2、Area 0 があります。他の 2 つの AS は RIP プロトコルを採用しています。Area 1 は NSSA エリアで、そのエリア内の ASBR が RIP ルートを Type-7 LSA に変換し、Area 1 に配信します。この LSA が NSSA の ABR に向かうとき、ABR は Type-7 LSA を Type-5 LSA に変換し、Area 0 と Area 2 に配信します。

図の左側で、RIP ルートは Area 2 の ASBR により Type-5 LSA に変換され、OSPF AS に配布されます。しかし、Area 1 は NSSA であるため、これらの Type-5 LSA は Area 1 には配布されません。

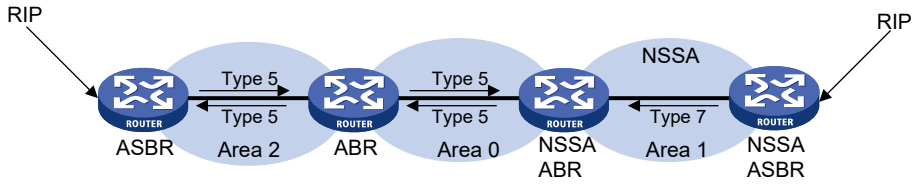


図 7-4 NSSA エリア

7.1.5 ルータタイプ

図 7-5に示すように、OSPF ルータは、異なるタイプに分類されます。内部ルータ、ABR、バックボーンルータ、ASBR が含まれます。

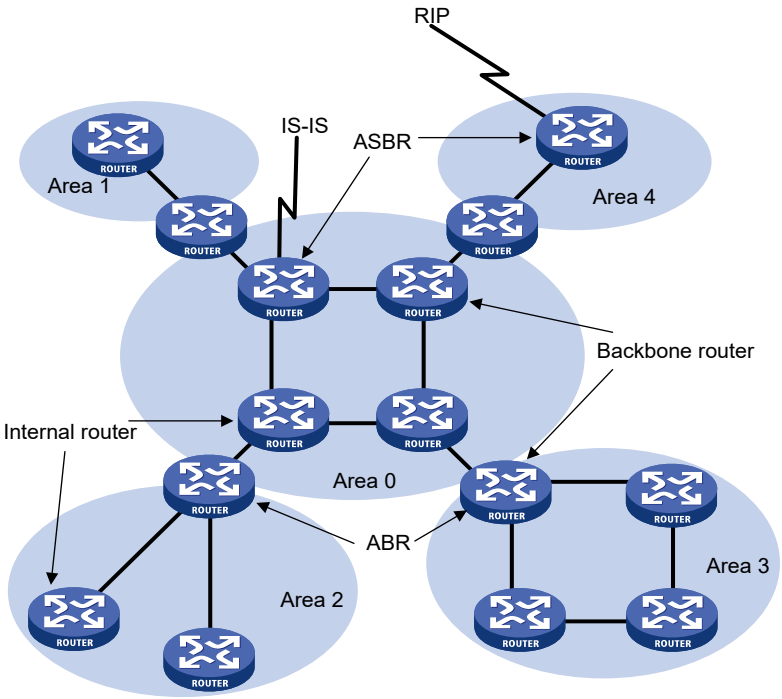


図 7-5 OSPF ルータタイプ

I. 内部ルータ

内部ルータのインタフェースはすべて 1 つの OSPF エリアに属します。

II. ABR

1 台の ABR は複数のエリアに属しますが、そのうちの 1 つは必ずバックボーンエリアで、バックボーンエリアとバックボーン以外のエリアを接続させます。ABR とバックボーンエリア間は物理的接続でも論理的接続でもかまいません。

III. バックボーンルータ

バックボーンルータの少なくとも 1 つのインタフェースはバックボーンエリアに付属しなくてはいけません。そのため、エリア 0 の ABR および内部ルータはすべてバックボーンルータです。

IV. ASBR

他の AS とルーティング情報をやり取りするルータが ASBR で、AS の境界には配置できません。内部ルータまたは ABR にもなります。

7.1.6 ルートタイプ

OSPF はルートを以下のレベルに優先付けします。

- エリア内ルート
- エリア外ルート
- 外部ルート Type-1
- 外部ルート Type-2

エリア内ルートおよびエリア間ルートは AS のネットワーク トポロジを記述し、外部ルートは AS の外側にある宛先へのルートを記述します。

外部ルート Type-1 は、RIP やスタティックルートなどの IGP ルートで、信頼性が高く、コストも OSPF 内部ルートと同程度です。ルータから外部ルート Type-1 の宛先までのコストは、ルータから対応する ASBR までのコストと ASBR から外部 ルートの宛先までのコストを足したものです。

外部ルート Type-2 は EGP ルートで、信頼性が低いため OSPF は ASBR から外部ルート Type-2 の宛先までのコストは、ASBR から OSPF 内部ルータまでのコストよりはるかに大きいと判断します。そのため、内部ルータから外部 ルート Type-2 までの宛先までのコストは、ASBR から外部ルート Type-2 の宛先までのコストとなります。宛先が同じ 2 台のルータのコストが同じであれば、ルータからの ASBR までのコストを考慮します。

7.1.7 ルータ ID

ルータ ID は、AS 内のルータを一意に識別します。 ルータが OSPF を実行するには、ルータ ID が必要です。手動でルータ ID を指定する、あるいは OSPF プロセスのグローバルのルータ ID を使用するかを選択できます。

I. 手動設定

OSPF プロセスを作成する場合は、手動でルータ ID を指定できます。ルータ ID が AS で固有であることを確認するために、ルータのインタフェースの IP アドレスをルータ ID として指定できます。

II. グローバルのルータ ID の使用

OSPF プロセスの作成時にルータ ID を指定しない場合、グローバルのルータ ID が使用されます。

ルータ ID を手動で指定する、あるいは OSPF プロセスを作成するとき、ルータ ID を自動的に取得するように OSPF プロセスを有効にすることを推奨します。

7.1.8 ルートの計算

OSPF はエリアのルートを以下のように計算します。

- 各ルータは周辺のネットワークトポロジにもとづいて LSA を作成し、アップデートパケットを他のルータに送信します。
- 各 OSPF ルータは LSDB を構成するため、他のルータからの LSA を収集します。LSA はルータ周囲のネットワークトポロジを記載しています。LSDB はエリアの全体のネットワークトポロジを記載しています。
- 各ルータは LSDB をエリアのトポロジを示す、重み付けしたグラフに変更します。エリア内にあるすべてのルータは同じグラフを持ちます。
- 各ルータは最小パスツリーを計算するため、SPF アルゴリズムを使用します。このアルゴリズムはエリア内のノードへのルートを示します。ルータ自体はツリーのルートとなります。

7.1.9 OSPF ネットワークタイプ

OSPF は、リンク レイヤ プロトコルに従って以下のタイプにネットワークを分類します。

- Broadcast － リンクレイヤプロトコルがイーサネットまたは FDDI のとき、OSPF はネットワーク タイプをデフォルトで Broadcast と判断します。Broadcast ネットワークでは、LSU パケットと LSAck パケットはマルチキャストアドレス 224.0.0.5(OSPF ルータとして予約されています)、と 224.0.0.6(OSPF DR として予約されています)で送信されます。DD パケットと LSR パケットはユニキャストで送信されます。
- NBMA(Non-Broadcast Multi-Access) － リンク レイヤ プロトコルが Frame Relay、ATM あるいは X.25 のとき、OSPF はネットワーク タイプをデフォルトで NBMA と判断します。NBMA ネットワークでは、パケットはユニキャストアドレスで送信されます。
- P2MP(point-to-multipoint) － デフォルトでは、OSPF はどのリンク レイヤ プロトコルも P2MP(通常は NBMA など他のネットワーク タイプから変換したもの) とみなされません。P2MP ネットワークでは、パケットはマルチキャスト アドレス (224.0.0.5) に送信されます。
- P2P(point-to-point) － リンク レイヤ プロトコルが PPP あるいは HDLC のとき、OSPF はネットワーク タイプを P2P と判断します。P2P ネットワークでは、パケットはマルチキャスト アドレス(224.0.0.5) に送信されます。

NBMA と P2MP 間の違いを以下に示します。

- NBMA ネットワークは、フルメッシュ接続の非ブロードキャスト、マルチアクセス ネットワークです。一方、P2MP ネットワークはフルメッシュ接続の必要はありません。
- NBMA ネットワークでは DR および BDR を選出する必要がありますが、P2MP ネットワークでは DR および BDR は使用できません。
- NBMA では、OSPF パケットはユニキャストパケットを使用し、ネイバは手動で設定します。P2MP では、デフォルトでマルチキャストパケットを使用しますが、ユニキャストパケットに設定することができます。

7.1.10 DR および BDR

I. DR および BDR のメカニズム

Broadcast または NBMA ネットワークでは、ルータ同士で相互にルーティング情報を交換します。ネットワークに n 台のルータがある場合、n(n-1)/2 個のネイバ関係 (adjacency) が必要です。ネットワークのルータに変更があると、ルーティング情報を同期化するためにトラフィックが生じ、ネットワーク リソースを消費します。

DR と BDR はこの問題を解決します。

- DR － 他のルータ間のルーティング情報を配信するために選出されます。もし DR が動作しなくなると、ネットワークのルータは別の DR を選出しその新しい DR と情報を同期化します。これには時間がかかり、ルーティングの計算間違いを起こしかねません。
- BDR(Backup Designated Router) — DR と共に選出され、他のすべてのルータとネイバ関係 (adjacency) を構築してルーティング情報を交換します。DR が機能しなくなると、非常に短時間で BDR が新しい DR になり、ネイバ関係 (adjacency) の構築や DR の再選出をしなくてもよくなります。一方で他のルータが別の BDR を選出し、これには比較的時間がかかりますが、ルーティングの計算には影響しません。

DR other と呼ばれる DR および BDR 以外のルータは、互いにネイバ関係 (adjacency) を構築したり、ルーティング情報を交換したりしません。よって、Broadcast および NBMA ネットワークのネイバ関係 (adjacency) の数は削減されます。

ルータの役割はサブネット(あるいはインタフェース)に固有です。インタフェースに 1 つの DR があり、他のインタフェースに BDR あるいは DR other があります。

図 7-6では、実線がイーサネットの物理的リンク、破線がネイバ関係 (adjacency) を表しています。DR や BDR のあるネットワークでは、7 つのネイバ関係 (adjacency) のみが確立されています。

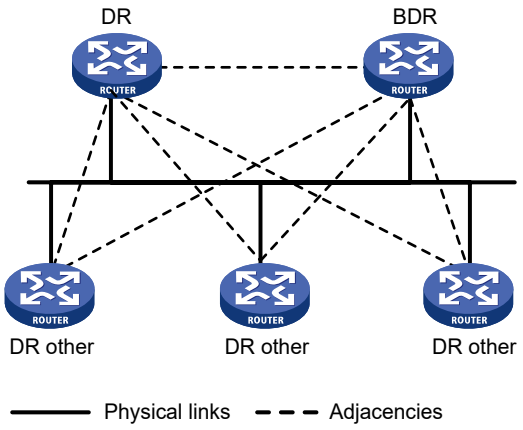


図 7-6 ネットワークの DR および BDR

🕮 **メモ：**

OSPF では、ネイバとネイバ関係で概念が異なります。起動後、OSPF は各 OSPF インタフェースで hello パケットを送信します。受信したルータはパケットのパラメータをチェックします。もしパラメータが自身のパラメータと一致する場合、受信したルータは送信したルータを OSPF のネイバルータと認識します。2 つの OSPF のネイバルータは、DD パケットと LSA の交換を行い、LSDB の同期化を行った後、ネイバ関係を確立します。

II. DR および BDR の選出

DR の選出はブロードキャストあるいは NBMA ネットワークで行われ、P2P や P2MP ネットワークでは行われません。

ブロードキャストあるいは NBMA ネットワークのルータは、ルータの優先度と ID によって DR と BDR を選出します。0 より高い優先度のルータが DR と BDR の選出に立候補します。

立候補は hello パケットで投票されます。各ルータは、それぞれが選出した DR を Hello パケットで他のすべてのルータに送信します。2 台のルータがそれ自体を DR と宣言した場合は、DR 優先度が高い方のルータが選ばれ、DR 優先度が同じ場合は、ルータ ID が高い方が選ばれます。

DR および BDR の選出が行われた後、もっとも高い優先度を持つルータがネットワークに追加されても、直ちに DR にはなれません。従ってネットワークの DR はもっとも高い優先度を持つルータでない可能性があり、BDR も 2 番目に高い優先度を持つルータでない可能性があります。

7.1.11 プロトコルと標準

- RFC 1245, *OSPF protocol analysis*
- RFC 1246, *Experience with the OSPF protocol*

- RFC 1370, *Applicability Statement for OSPF*
- RFC 1765, *OSPF Database Overflow*
- RFC 1793, *Extending OSPF to Support Demand Circuits*
- RFC 2154, *OSPF with Digital Signatures*
- RFC 2328, *OSPF Version 2*
- RFC 3101, *OSPF Not-So-Stubby Area (NSSA) Option*
- RFC 3166, *Request to Move RFC 1403 to Historic Status*
- RFC 3509, *Alternative Implementations of OSPF Area Border Routers*
- RFC 4167, *Graceful OSPF Restart Implementation Report*
- RFC 4750, *OSPF Version 2 Management Information Base*
- RFC 4811, *OSPF Out-of-Band LSDB Resynchronization*
- RFC 4812, *OSPF Restart Signaling*
- RFC 5088, *OSPF Protocol Extensions for Path Computation Element (PCE) Discovery*
- RFC 5250, *The OSPF Opaque LSA Option*
- RFC 5613, *OSPF Link-Local Signaling*
- RFC 5642, *Dynamic Hostname Exchange Mechanism for OSPF*
- RFC 5709, *OSPFv2 HMAC-SHA Cryptographic Authentication*
- RFC 5786, *Advertising a Router's Local Addresses in OSPF Traffic Engineering (TE) Extensions*
- RFC 6571, *Loop-Free Alternate (LFA) Applicability in Service Provider (SP) Networks*
- RFC 6860, *Hiding Transit-Only Networks in OSPF*
- RFC 6987, *OSPF Stub Router Advertisement*

7.2 制限とガイドライン

OSPF を動作させるには、最初にルータで OSPF を有効にする必要があります。ルートのブロックやルーティングループを引き起こす間違った設定を避けるため、正しい設定の計画であるか確認してください。

7.3 OSPF設定作業リスト

作業リスト
(必須設定項目) OSPFの基本機能の設定: • OSPFプロセスの有効化 • OSPFエリアの作成 • OSPFの有効化
(オプション設定項目) OSPFスタブエリアとNSSAエリアの設定: • スタブエリアの設定 • NSSAエリアの設定 • 仮想リンクの設定
(オプション設定項目) OSPFネットワークタイプの設定: • インタフェースのブロードキャストネットワークタイプの設定 • インタフェースのNBMAネットワークタイプの設定 • インタフェースのP2MPネットワークタイプの設定 • インタフェースのP2Pネットワークタイプの設定

作業リスト
(オプション設定項目) OSPFルート制御の設定: ● OSPF内部エリアルート集約の設定 ● 再配信されたルート集約の設定 ● 受信ルートのフィルタリングの設定 ● Type-3 LSAフィルタリングの設定 ● インタフェースのOSPFコストの設定 ● ECMPルートの最大数の設定 ● OSPFの優先順位の設定 ● 別のルーティングプロトコルからOSPFへのルート再配信の設定 ● デフォルトルートの再配信の設定 ● ホストルートの配信の設定
(オプション設定項目) OSPFのタイマの設定: ● OSPFパケットのタイマの設定 ● LSAの伝送遅延の設定 ● SPFの計算間隔の設定 ● LSAの到達間隔の設定 ● LSA生成間隔の設定 ● OSPFがオーバーフローから終了する期間の設定
(オプション設定項目) OSPFパケットパラメータの設定: ● インタフェースのOSPFパケット送受信の無効化 ● インタフェースMTUのDDパケットへの付加 ● 送信OSPFパケットへのDSCP値の設定
(オプション設定項目) LSAの生成、配信、受信の制御: ● LSDB内の外部LSAの最大数の設定
(オプション設定項目) 拡張OSPF機能の設定: ● スタブルータの設定 ● RFC1583の互換性の有効化
(オプション設定項目) OSPF可用性の拡張: ● OSPF GRの設定 ● OSPF NSRの設定 ● OSPFのBFDの設定 ● OSPF FRRの設定
(オプション設定項目) OSPFセキュリティ機能の設定: ● OSPF認証の設定 ● OSPFのGTSMの設定
(オプション設定項目) OSPFのロギングとSNMP notificationの設定: ● ネイバ状態変更のロギング ● OSPFロギング機能の設定 ● OSPFネットワーク管理の設定

7.4 OSPF基本機能の設定

7.4.1 OSPF プロセスの有効化

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. (オプション設定項目) グローバルルータ ID を設定する	**router id** *router-id*	デフォルト：設定なし グローバルルータIDが設定されていない場合、もっとも高いループバックインタフェースのIPアドレスがグローバルルータIDに適用されます。ループバックインタフェースが設定されていない場合、インタフェース状態(アップあるいはダウン)に従ってもっとも高い物理インタフェースのIPアドレスがグローバルルータIDに適用されます。
3. OSPF プロセスを有効にし、OSPF view に移行する	**ospf** [*process-id* | **router-id** *router-id* | **vpn-instance** *vpn-instance-name*] *	デフォルト：無効
4. (オプション設定項目) OSPF プロセスの記述を設定する	**description** *description*	デフォルト：設定なし 各OSPFプロセスに記述を設定することを推奨します。

7.4.2 OSPF エリアの作成

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. (オプション設定項目) グローバルルータ ID を設定する	**router id** *router-id*	デフォルト：設定なし
3. OSPF プロセスを有効にし、OSPF view に移行する	**ospf** [*process-id* | **router-id** *router-id* | **vpn-instance** *vpn-instance-name*] *	デフォルト：無効
4. (オプション設定項目) OSPF プロセスの記述を設定する	**description** *description*	デフォルト：設定なし 各OSPFプロセスに記述を設定することを推奨します。
5. OSPF エリアを作成し、OSPF area view に移行する	**area** *area-id*	デフォルト：設定なし
6. (オプション設定項目) エリアの記述を設定する	**description** *description*	デフォルト：設定なし 各OSPFエリアに記述を設定することを推奨します。

7.4.3 OSPF の有効化

I. 複数のプロセスと VPN

ルータで OSPF を有効にする場合、以下の処理を行う必要があります。

1) OSPF プロセスを作成します。
2) プロセスの OSPF エリアを作成します。
3) エリアでネットワークを指定します。

ネットワークに接続されたインタフェースでエリアの OSPF プロセスが動作します。OSPF はインタフェースのルートに直接配信します。

OSPF は複数のプロセスをサポートします。複数の OSPF プロセスを動作させるため、各プロセスの ID を指定する必要があります。プロセス ID はローカルでのみ適用し、ルータ間で交換されるパケットに影響しません。異なるプロセス ID を持つ 2 つのルータはパケットを交換できます。

OSPF は複数の VPN をサポートします。VPN インスタンスで OSPF プロセスを設定することができます。VPN インスタンスが指定されていない OSPF プロセスはパブリックネットワークで動作します。VPN の詳細はオペレーションマニュアルのセクション 7 *MCE* “*MCE*”を参照してください。

II. 制限とガイドライン

インタフェースで OSPF を設定する場合は､次の制限とガイドラインに従ってください。

- インタフェースが存在するネットワーク上で OSPF を有効にしたり、インタフェースで OSPF を直接有効にすることができます。両方を設定した場合、直接接続されているネットワークで OSPF を有効にした設定が優先されます。
- 指定された OSPF プロセスとエリアが存在しない場合、オペレーションはインタフェースの OSPF プロセスとエリアを作成します。インタフェースで OSPF プロセスを無効にすると、OSPF プロセスまたはエリアは削除されません。

III. ネットワークでの OSPF の有効化

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. OSPF プロセスを有効にし、OSPF view に移行する	**ospf** [*process-id* | **router-id** *router-id* | **vpn-instance** *vpn-instance-name*] *	デフォルト：無効
3. OSPF エリアを作成し、OSPF area view に移行する	**area** *area-id*	デフォルト：設定なし
4. ネットワークを指定し、そのネットワークに所属するインタフェースの OSPF を有効にする	**network** *ip-address wildcard-mask*	デフォルト：指定なし ネットワークは1つのエリアのみ追加することができます。

IV. インタフェースでの OSPF の有効化

操作	コマンド	補足
1. system view に移行する	**system-view**	―

操作	コマンド	補足
2． interface view に移行する	**interface** *interface-type interface-number*	―
3． インタフェースでの OSPF の有効にする	**ospf** *process-id* **area** *area-id* [**exclude-subip**]	―

7.5 OSPFスタブエリアとNSSAエリアの設定

7.5.1 OSPF スタブエリアと NSSA エリアの設定

スタブエリアあるいは NSSA エリアとして OSPF エリアを設定することができます。非バックボーンエリアとバックボーンエリア間、あるいはバックボーンエリア間の接続が確立されない場合、仮想リンクを作成することができます。

7.5.2 スタブエリアの設定

I. スタブエリアの設定

エリアに接続しているすべてのルータで **stub** コマンドによって、AS のエッジにある非バックボーンエリアをスタブエリアとして設定できます。AS 外部ルートを記述する Type-5 LSA はルーティングテーブルサイズを削減するために、スタブエリア内に配信されます。ABR は AS の外宛へのすべてのパケットがデフォルトルートを通って転送できるように、AS 内のデフォルトルートを作成します。

さらにルーティングテーブルのサイズとスタブエリアのルーティング情報の交換を削減するため、ABR 上で **stub** [**no-summary**]コマンドを使用することで、完全スタブエリアとして設定します。AS 外部ルートと内部ルートはエリアに配信しません。AS の外部あるいはエリアの外部へのすべてのパケットは、ABR に送信されます。

仮想リンクはスタブエリアあるいは完全スタブエリアを通過することができません。

外部ルートはエリアに配信することができないため、スタブあるいは完全スタブエリアは ASBR にすることができません。

II. 制限とガイドライン

スタブエリアあるいは完全スタブエリアとしてバックボーンエリアを設定しないでください。

スタブエリアを設定する場合、エリアに接続されるすべてのルータで **stub** コマンドを実行してください。

完全スタブエリアを設定する場合、エリアに接続されるすべてのルータで **stub** コマンドを実行して、ABR で **stub no-summary** コマンドを実行してください。

III. 設定手順

操作	コマンド	補足
1． system view に移行する	**system-view**	―

操作	コマンド	補足
2． OSPF view に移行する	**ospf** [*process-id* | **router-id** *router-id* | **vpn-instance** *vpn-instance-name*] *	―
3． area view に移行する	**area** *area-id*	―
4． エリアをスタブエリアとして設定する	**stub** [**default-route-advertise-always** | **no-summary**] *	デフォルト：設定なし
5． (オプション設定項目) スタブエリアに配信するデフォルトルートのコストを設定する	**default-cost** *cost*	デフォルト：1 **default-cost** *cost* コマンドはスタブエリアあるいは完全スタブエリアのABRでのみ適用できます。

7.5.3 NSSA エリアの設定

I. NSSA エリアの設定

スタブエリアは外部ルートを入手できませんが、NSSA エリアは他のスタブエリアの特徴を持ちながら OSPF ルーティングドメインに外部ルートをインポートできます。

完全 NSSA エリアを設定する場合、**nssa no-summary** コマンドを設定してください。完全 NSSA エリアの ABR はエリアに内部エリアルートを配信しません。

II. 制限とガイドライン

NSSA エリアあるいは完全 NSSA エリアとしてバックボーンエリアを設定することはできません。

NSSA エリアを設定する場合、エリアに接続されるすべてのルータに **nssa** コマンドを設定してください。

完全 NSSA エリアを設定する場合、エリアに接続されるすべてのルータに **nssa** コマンドを設定し、ABR で **nssa no-summary** コマンドを設定してください。

III. 設定手順

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． OSPF view に移行する	**ospf** [*process-id* | **router-id** *router-id* | **vpn-instance** *vpn-instance-name*] *	―
3． area view に移行する	**area** *area-id*	―

操作	コマンド	補足
4. エリアをNSSAエリアとして設定する	**nssa** [**default-route-advertise** | **no-import-route** | **no-summary** | **translate-always** | **translator-stability-interval** *value*] * **nssa** [**default-route-advertise** [**cost** *cost-value* | **nssa-only** | **route-policy** *route-policy-name* | **type** *type*] * | **no-import-route** | **no-summary** | **suppress-fa** | **[[[translate-always]** **[translate-ignore-checking-backbone]] | translate-never] |** **translator-stability-interval** *value*] *	デフォルト：設定なし
5. (オプション設定項目) NSSA エリアに配信されるデフォルトルートのコストを指定する	**default-cost** *cost-value*	デフォルト：1 このコマンドはNSSAエリアあるいは完全NSSAエリアのABR/ASBRでのみ適用できます。

7.5.4 仮想リンクの設定

I. 仮想リンク

非バックボーンエリアとバックボーンエリア、バックボーンエリア自体の間の接続を維持するために、仮想リンクを設定できます。

II. 制限とガイドライン

仮想リンクはスタブエリア、完全スタブエリア、NSSA エリア、完全 NSSA エリアを通過することができません。

III. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. OSPF view に移行する	**ospf** [*process-id* | **router-id** *router-id* | **vpn-instance** *vpn-instance-name*] *	―
3. area view に移行する	**area** *area-id*	―
4. 仮想リンクを設定する	**vlink-peer** *router-id* [**dead** *seconds* | **hello** *seconds* | { { **hmac-md5** | **md5** } *key-id* { **cipher** | **plain** } *string* | **simple** { **cipher** | **plain** } *string* } | **retransmit** *seconds* | **trans-delay** *seconds*] *	デフォルト：設定なし このコマンドは仮想リンクの両端に設定します。 仮想リンクの両端では、**hello** および **dead**パラメータは必ず同じにしてください。

7.6 OSPFネットワークタイプの設定

OSPF はリンクレイヤプロトコルにもとづいて、異なるタイプにネットワークを分類します。ネットワークタイプはブロードキャスト、NBMA、PSMP、P2P があります。

7.6.1 制限とガイドライン

ブロードキャストネットワーク中の幾つかのルータがマルチキャストをサポートしていないとき、ネットワークタイプを NBMA に変更できます。

ネットワークセグメント上に OSPF を実行しているルータが 2 つしかない場合、ネットワークタイプを P2P に変更してコストを節約できます

2 つのブロードキャスト、NBMA、および P2MP インタフェースは、同じネットワークセグメント上にある場合にのみネイバ関係を確立できます。

7.6.2 インタフェースのブロードキャストネットワークタイプの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. interface view に移行する	**interface** *interface-type interface-number*	ー
3. ネットワーク タイプをブロードキャストに設定する	**ospf network-type broadcast**	デフォルト : ブロードキャスト
4. (オプション設定項目) インタフェースに DR 優先度を設定する	**ospf dr-priority** *priority*	デフォルト : 1

7.6.3 インタフェースの NBMA ネットワークタイプの設定

I. 制限とガイドライン

NBMA としてネットワークタイプを設定した後、NBMA インタフェースはブロードキャスト Hello パケットでネイバノードを発見できないため、ネイバノードを識別するために DR 優先度が必要です。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. interface view に移行する	**interface** *interface-type interface-number*	ー
3. ネットワーク タイプに NBMA を設定する	**ospf network-type nbma**	デフォルト : ブロードキャスト
4. (オプション設定項目) インタフェースのルータの優先順位を設定する	**ospf dr-priority** *priority*	デフォルト : 1 DR選出用にルータの優先順位が設定されます。
5. system view に戻る	**quit**	ー
6. OSPF view に移行する	**ospf** [*process-id* | **router-id** *router-id* | **vpn-instance** *vpn-instance-name*] *	ー

操作	コマンド	補足
7． ネイバノードと DR 優先度を設定する	**peer** *ip-address* [**dr-priority** *dr-priority*]	デフォルト : ネイバノードの指定はありません。 この優先度はネイバノードに選出の権利があるかどうかを示します。あるネイバノードの DR 優先順位を0に設定したとき、ローカルルータはそのネイバノードに選出の権利がないとみなし、ネイバノードにHello パケットを送信しません。ただし、ローカルルータがDRまたはBDRのときは、優先順位が0のネイバノードにHello パケットを送り、ネイバ関係を確立します。

7.6.4 インタフェースの P2MP ネットワークタイプの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． interface view に移行する	**interface** *interface-type interface-number*	―
3． ネットワーク タイプに P2MP を設定する	**ospf network-type p2mp** [**unicast**]	デフォルト : ブロードキャスト
4． system view に戻る	**quit**	―
5． OSPF view に移行する	**ospf** [*process-id* | **router-id** *router-id* | **vpn-instance** *vpn-instance-name*] *	―
6． (オプション設定項目) ネイバノードと DR 優先度を設定する	**peer** *ip-address* [**cost** *value*]	デフォルト : ネイバノードの指定はありません。 ネットワークタイプがP2MP の場合、設定が必要です。

7.6.5 インタフェースの P2P ネットワークタイプの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． interface view に移行する	**interface** *interface-type interface-number*	―
3． ネットワーク タイプに P2P を設定する	**ospf network-type p2p**	デフォルト : ブロードキャスト

7.7 OSPFルート制御の設定

この章は OSPF ルーティング情報の配信および受信、他のプロトコルからのルートの再配信を制御する方法について説明します。

7.7.1 OSPF 内部エリアルート集約の設定

I. OSPF 内部エリアルート集約の設定

OSPF 内部エリアルートの集約により、エリア間で交換されるルーティング情報とルーティングテーブルのサイズが減少し、ルーティングパフォーマンスが向上します。

OSPF 間のエリア間ルート集約により、ABR は、ネイバするネットワークを単一のネットワークに集約し、ネットワークを他のエリアに配信することができます。 たとえば、エリア内では、3 つの内部ネットワーク 19.1.1.0/24、19.1.2.0/24、19.1.3.0/24 が使用可能です。 ABR を設定して、3 つのネットワークをネットワーク 19.1.0.0/16 に集約し、Type-3 LSA の他のエリアに集約ネットワークを配信するように設定できます。 この設定は他のエリアでのルータの LSDB の規模を減らし、トポロジの変更の影響を低減します。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. OSPF view に移行する	**ospf** [*process-id* | **router-id** *router-id* | **vpn-instance** *vpn-instance-name*] *	―
3. OSPF area view に移行する	**area** *area-id*	―
4. ABR のルート集約を設定する	**abr-summary** *ip-address* { *mask-length* | *mask* } [**advertise** | **not-advertise**] [**cost** *cost*]	デフォルト：設定なし

7.7.2 再配信されたルート集約の設定

I. 再配信されたルート集約

ASBR が指定されたアドレス範囲内の外部ルートを単一ルートに集約できるようにします。 ASBR は、LSDB の LSA の数を減らすために、Type-5 LSA のみを配信します。

ASBR は以下の LSA のルートを集約することができます。

- Type-5 LSA
- NSSA エリアの Type-7 LSA

II. 制限とガイドライン

ASBR(および ABR)が NSSA エリアを配信する場合、Type-7 LSA から変換された Type-5 LSA のルートを集約します。配信しない場合、Type-5 LSA から変換された Type-5 LSA のルートは集約されません。

III. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. OSPF view に移行する	**ospf** [*process-id* | **router-id** *router-id* | **vpn-instance** *vpn-instance-name*] *	―

操作	コマンド	補足
3． ASBR ルート集約を設定する	**asbr-summary** *ip-address* { *mask-length* | *mask* } [**cost** *cost* | **not-advertise** | **nssa-only** | **tag** *tag*] *	デフォルト：設定なし

7.7.3 受信ルートのフィルタリングの設定

I. フィルタリング方法

受信された LSA を使用して計算されるルートをフィルタすることができます。

以下にフィルタリングの方法を示します。

- 宛先アドレスでルーティング情報をフィルタするため、ACL あるいは IP アドレスプレフィックスを使用します。
- ネクストホップでルーティング情報をフィルタするため、gateway パラメータを使用します。
- 宛先アドレスでルーティング情報をフィルタするため、ACL あるいは IP アドレスプレフィックスを使用し、同時にネクストホップでルーティング情報をフィルタするため、gateway prefix-list-name パラメータを使用します。
- ルーティング情報をフィルタするため、route-policy route-policy-name を使用します。

II. 設定手順

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． OSPF view に移行する	**ospf** [*process-id* | **router-id** *router-id* | **vpn-instance** *vpn-instance-name*] *	―
3． 受信された LSA を使用して受信ルートのフィルタリングを設定する	**filter-policy** { *ipv4-acl-number* [**gateway** *prefix-list-name*] | **gateway** *prefix-list-name* | **prefix-list** *prefix-list-name* [**gateway** *prefix-list-name*] | **route-policy** *route-policy-name* } **import**	デフォルト：設定なし

7.7.4 Type-3 LSA フィルタリングの設定

I. Type-3 LSA フィルタリング

ネイバする非バックボーンエリアへの配信される Type-3 LSA と、ABR の他のエリアへ配信される Type-3 LSA をフィルタするために設定します。

II. 設定手順

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． OSPF view に移行する	**ospf** [*process-id* | **router-id** *router-id* | **vpn-instance** *vpn-instance-name*] *	―
3． area view に移行する	**area** *area-id*	―

操作	コマンド	補足
4． Type-3 LSA フィルタリングを設定する	**filter** { *ipv4-acl-number* | **prefix-list** *prefix-list-name* | **route-policy** *route-policy-name* } { **export** | **import** }	デフォルト：設定なし

7.7.5 インタフェースの OSPF コストの設定

I. インタフェースの OSPF コストの設定

下記のいずれかの方法でインタフェースに OSPF コストを設定できます。

- Interface view でコスト値を設定します。
- インタフェースに帯域の基準値を設定し、この基準値をもとに OSPF がコストを自動計算します。インタフェース OSPF コスト=帯域の基準値（100Mbps）/インタフェースの帯域幅（Mbps）。
  - 計算されたコストが 65535 よりも大きい場合は、この値は 65535 になります。計算された値が 1 よりも小さい場合、1 になります。
  - コストあるいは帯域の基準値が設定されていない場合、OSPF はインタフェースの帯域幅とデフォルトの帯域幅の基準値をもとにインタフェースのコストを計算します。

II. インタフェースの OSPF コストの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． interface view に移行する	**interface** *interface-type interface-number*	―
3． インタフェースに OSPF コストを設定する	**ospf cost** *value*	デフォルト：インタフェースは帯域に応じてコストを計算します。 ループバックインタフェースのOSPFコストはデフォルトで0です。

III. 帯域の基準値の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． OSPF view に移行する	**ospf** [*process-id* | **router-id** *router-id* | **vpn-instance** *vpn-instance-name*] *	―
3． 帯域の基準値を設定する	**bandwidth-reference** *value*	デフォルト：100Mbps

7.7.6 ECMP ルートの最大数の設定

I. ECMP ルートの最大数の設定

OSPF は、同じ宛先への複数の最適な等コストルートを検出することができます。これは、トラフィック負荷を共有するために使用できます。OSPF の ECMP ルートの最大数を設定できます。

II. 設定手順

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． OSPF view に移行する	**ospf** [*process-id* | **router-id** *router-id* | **vpn-instance** *vpn-instance-name*] *	―
3． ECMP ルートの最大数を設定する	**maximum load-balancing** *number*	デフォルト：8

7.7.7 OSPF の優先順位の設定

I. OSPF の優先順位

ルータは 1 台で複数のルーティングプロトコルを実行でき、各プロトコルの優先順位を設定します。ルートが複数のルーティングプロトコルで検出された場合、優先順位がもっとも高いプロトコルで検出されたルートが最適ルートとして選択されます。

II. 設定手順

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． OSPF view に移行する	**ospf** [*process-id* | **router-id** *router-id* | **vpn-instance** *vpn-instance-name*] *	―
3． OSPF の優先順位を設定する	**preference** [**ase**] { *preference* | **route-policy** *route-policy-name* } *	デフォルト:OSPF内部ルートの優先順位のデフォルトは10です。 OSPF外部ルートの優先順位のデフォルトは150です。

7.7.8 別のルーティングプロトコルから OSPF へのルート再配信の設定

I. 別のルーティングプロトコルから OSPF へのルート再配信

ルータが OSPF と他のルーティングプロトコルを動作させていた場合、RIP、BGP、スタティックルート、ダイレクトルートのような他のプロトコルを直接ルートまたは Type-5 LSA、Type-7 LSA でこれらのルートを OSPF に配信できます。加えて、許可されたルートのみを配信するため、再配信されるルートをフィルタすることができます。

II. 制限とガイドライン

OSPF はアクティブルートのみを再配信します。ルートステータス情報を表示するには、**display ip routing-table protocol** コマンドを使用します。

III. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. OSPF view に移行する	**ospf** [*process-id* | **router-id** *router-id* | **vpn-instance** *vpn-instance-name*] *	ー
3. 他のプロトコルからのルートを再配信するように OSPF を設定する	**import-route** { **direct** | **static** } [**cost** *cost-value* | **nssa-only** | **route-policy** *route-policy-name* | **tag** *tag* | *type type*] * **import-route** { **isis** | **ospf** | **rip** } [*process-id* | **all-processes**] [**allow-direct** | **cost** *cost-value* | **nssa-only** | **route-policy** *route-policy-name* | **tag** *tag* | *type type*] *	デフォルト：設定なし
4. (オプション設定項目) 再配信ルートをフィルタするように OSPF を設定する	**filter-policy** { *ipv4-acl-number* | **prefix-list** *prefix-list-name* } **export** [*protocol* [*process-id*]]	デフォルト：設定なし
5. 再配信されるルートのデフォルトパラメータ (コスト、タグ、タイプ) を設定する	**default** { **cost** *cost* | **tag** *tag* | **type** *type* } *	デフォルト：コストは 1、再配信ルートのタイプは Type-2 です。

7.7.9 デフォルトルートの再配信の設定

I. デフォルトルートの再配信

import-route コマンドを使用してもデフォルトの外部ルートは再配信できません。再配信するためには、デフォルトルートを再配信する **default-route-advertise** コマンドの設定を行います。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. OSPF view に移行する	**ospf** [*process-id* | **router-id** *router-id* | **vpn-instance** *vpn-instance-name*] *	ー
3. デフォルトルートを再配信するように設定する	**default-route-advertise** [[[**always** | **permit-calculate-other**] | **cost** *cost* | **route-policy** *route-policy-name* | **type** *type*] * | **summary cost** *cost*]	デフォルト : 再配信されません。 このコマンドはType-5 LSA（summary cost指定時はType-3 LSA）のデフォルトルートを再配信します。

操作	コマンド	補足
4． 再配信されるルートのデフォルトパラメータ(コスト、タグ、タイプ)を設定する	**default** { **cost** *cost* | **tag** *tag* | **type** *type* } *	デフォルト：コストは 1、再配信ルートのタイプは Type-2 です。

7.7.10 ホストルートの配信の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． OSPF view に移行する	**ospf** [*process-id* | **router-id** *router-id* | **vpn-instance** *vpn-instance-name*] *	―
3． area view に移行する	**area** *area-id*	―
4． ホストルートの配信を設定する	**host-advertise** *ip-address cost*	デフォルト：設定なし

7.8 OSPFのタイマの設定

7.8.1 OSPF のタイマの設定

OSPF パケットタイマを変更して収束速度とネットワーク負荷を調整し、低速リンクで LSA を送信する遅延時間を調整できます。

7.8.2 OSPF パケットのタイマの設定

I. OSPF パケットのタイマの設定

以下の OSPF インタフェースのタイマを、必要に応じて設定できます。

- Hello タイマ － Hello パケットの送信間隔です。OSPF ネイバノードで、統一されている必要があります。
- Poll タイマ － NBMA ネットワークで動作していないネイバノードに Hello パケットを送信する間隔です。
- Dead タイマ － この間隔内にネイバノードから Hello パケットを受け取らないと、インタフェースはネイバノードが動作していないと宣言します。
- LSA retransmission タイマ － ネイバノードに LSA を送信してからこの間隔内に確認応答パケットを受け取らないと、インタフェースは LSA を再送します。

II. 制限とガイドライン

hello タイマとネイバ dead タイマのデフォルト値は、ネットワークの種類によって異なります。インタフェースのネットワークタイプが変更されると、デフォルトの hello タイマとネイバ dead タイマがもとに戻ります。隣接する 2 つのインタフェースが同じ hello タイマとネイバ dead タイマで設定されていることを確認します。設定が矛盾している場合、OSPF ネイバ関係の確立に影響を与えます。

III. 設定手順

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． interface view に移行する	**interface** *interface-type interface-number*	―
3． hello タイマの間隔を指定する	**ospf timer hello** *seconds*	デフォルト：P2P および Broadcastインタフェースのデフォルト値は10 秒です。P2MPおよびNBMAインタフェースのデフォルト値は30 秒です。
4． poll タイマの間隔を指定する	**ospf timer poll** *seconds*	デフォルト：120秒 pollタイマの間隔は少なくともhelloタイマの間隔の4倍にしてください。
5． dead タイマの間隔を指定する	**ospf timer dead** *seconds*	デフォルト： P2PおよびBroadcastインタフェースのデフォルト値は40 秒です。P2MPおよび NBMA インタフェースのデフォルト値は120 秒です。deadタイマ間隔は少なくともhelloタイマの間隔の4倍にしてください。
6． retransmission タイマの間隔を指定する	**ospf timer retransmit** *interval*	デフォルト：5秒 retransmissionタイマの間隔は、不要なLSA の再送を防ぐため、あまり小さくしないでください。通常、この値はネイバ関係間のパケットの往復時間よりも大きくなります。

7.8.3 LSA の伝送遅延の設定

I. LSA の伝送遅延の設定

伝送中に、LSA がエージングアウトすることを防ぐため、LSA の伝送遅延を設定します。特に低速リンクでは、必要となります。

II. 設定手順

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． interface view に移行する	**interface** *interface-type interface-number*	―
3． LSA の伝送遅延を設定する	**ospf trans-delay** *seconds*	デフォルト：1秒

7.8.4 SPF の計算間隔の設定

I. SPF の計算間隔の設定

LSDB を変更すると SPF の計算が必要になります。OSPF ネットワークが頻繁に変わると、大量のネットワーク リソースが占有され、ルータの運用効率が下がります。ネットワークの SPF の計算間隔を調整することで、影響を減らすことができます。

ネットワークが頻繁に変わらないとき、*minimum-interval* で行われます。ネットワークの変更がしばしば起こると、計算の間隔は計算のたびに *incremental-interval* × 2^{n-2} ずつ増え、最後は *maximum-interval* になります。n は計算回数です。

II. 設定手順

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． OSPF view に移行する	**ospf** [*process-id* | **router-id** *router-id* | **vpn-instance** *vpn-instance-name*] *	―
3． SPF の計算間隔を指定する	**spf-schedule-interval** *maximum-interval* [*minimum-interval* [*incremental-interval*]]	デフォルト： ● 最大間隔：5秒 ● 最小間隔：50ミリ秒 ● 増加する間隔：200ミリ秒

7.8.5 LSA の到達間隔の設定

I. LSA の到達間隔の設定

OSPF が LSA 到達間隔以内に、先に受信した LSA と、同一の、LSA タイプ、LS ID、ルータ ID の LSA を受信した場合、OSPF は帯域幅とルータのリソースを節約するため、LSA を廃棄します。

II. 設定手順

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． OSPF view に移行する	**ospf** [*process-id* | **router-id** *router-id* | **vpn-instance** *vpn-instance-name*] *	―
3． LSA の到達間隔を設定する	**lsa-arrival-interval** *interval*	デフォルト：1000ミリ秒

7.8.6 LSA 生成間隔の設定

I. LSA 生成間隔の設定

LSA の生成間隔を適切に設定することで、ネットワークの頻繁な変更によってネットワークのリソースとルータが過度に消費されることを防ぐことができます。

ネットワークが頻繁に変わらないとき、*minimum-interval* で行われます。ネットワークの変更がしばしば起こると、計算の間隔は計算のたびに *incremental-interval*×2^{n-2} ずつ増え、最後は *maximum-interval* になります。n は計算回数です。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. OSPF view に移行する	**ospf** [*process-id* | **router-id** *router-id* | **vpn-instance** *vpn-instance-name*] *	ー
3. LSA 生成間隔を設定する	**lsa-generation-interval** *maximum-interval* [*minimum-interval* [*incremental-interval*]]	デフォルト： ● 最大間隔：5秒 ● 最小間隔：50ミリ秒 ● 増加する間隔：200ミリ秒

7.8.7 OSPF オーバーフローから終了する期間の設定

I. OSPF オーバーフローから終了する期間の設定

LSDB の LSA 数が上限を超えたとき、LSDB はオーバーフロー状態となります。リソースを節約するため、オーバーフロー状態の際、OSPF は外部 LSA の受信を行わず、作成された外部 LSA を削除します。

OSPF がオーバーフロー状態から終了するまでの期間を設定することができます。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. OSPF view に移行する	**ospf** [*process-id* | **router-id** *router-id* | **vpn-instance** *vpn-instance-name*] *	ー
3. オーバーフロー状態から終了する期間を設定する	**lsdb-overflow-interval** *interval*	デフォルト：300秒 0はオーバーフロー状態から終了しないことを示します。

7.9 OSPFパケットパラメータの設定

7.9.1 インタフェースの OSPF パケット送受信の無効化

I. インタフェースの OSPF パケット送受信の無効化

OSPF の適用性を拡張し、リソースの消費を削減するために、OSPF インタフェースでルーティング情報を送信しない、サイレント状態にすることができます。サイレント状態のインタフェースは、OSPF パケットをブロックし、OSPF ネイバ関係を確立することができません。しかし、他のインタフェースは Router LSA のインタフェースのダイレクトルートを配信することができます。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. OSPF view に移行する	**ospf** [*process-id* | **router-id** *router-id* | **vpn-instance** *vpn-instance-name*] *	ー
3. OSPF パケットの送受信を無効にする	**silent-interface** { *interface-type interface-number* | **all** }	デフォルト:OSPFパケットの送受信を行います。 この**silent-interface**コマンドは、現在のプロセスに関連したインタフェースのみ無効にします。複数のOSPFプロセスを同一インタフェースで無効化することができます。

7.9.2 インタフェース MTU の DD パケットへの付加

I. インタフェース MTU の DD パケットへの付加

通常、インタフェースは実際の MTU ではなく、DD パケットのインタフェースの MTU フィールドに 0 を追加します。DD パケットに MTU を追加するように設定することができます。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. interface view に移行する	**interface** *interface-type interface-number*	ー
3. DD パケットにインタフェース MTU を付加することを有効にする	**ospf mtu-enable**	デフォルト：無効 インタフェースは値0を書き込んでいます。

7.9.3 送信 OSPF パケットへの DSCP 値の設定

I. DSCP 値

DSCP 値は、送信パケットの優先順位を指定します。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. OSPF view に移行する	**ospf** [*process-id* | **router-id** *router-id* | **vpn-instance** *vpn-instance-name*] *	ー
3. OSPF パケットへの DSCP 値を設定する	**dscp** *dscp-value*	デフォルト：48

7.10 LSAの生成、配信、受信の制御

7.10.1 LSDB 内の外部 LSA の最大数の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． OSPF view に移行する	**ospf** [*process-id* | **router-id** *router-id* | **vpn-instance** *vpn-instance-name*] *	―
3． LSDB 内の外部 LSA の最大数を設定する	**lsdb-overflow-limit** *number*	デフォルト：制限なし

7.11 拡張OSPF機能の設定

7.11.1 スタブルータの設定

I. スタブルータ

スタブルータはトラフィックの制御に使われます。 そのステータスは、ネイバルータの OSPF ルータにスタブルータとして報告されます。 ネイバルータはスタブルータへのルートを持つことができますが、スタブルータを使用してデータを転送することはできません。

スタブルータからの Router LSA には、さまざまなリンクタイプの値が入ります。値 3 は、スタブネットワークとのリンクを意味し、リンクのコストはデフォルトで変わりません。リンクコストを 65535 に設定するには、**stub-router** コマンドで **include-stub** キーワードを指定します。値 1、2 または 4 は、ポイントツーポイントリンク、通過ネットワークとのリンクまたは仮想リンクを意味します。このような場合、最大コスト値 65535 が使われます。そのため、他のネイバノードはスタブルータとのリンクのコストが大きいことが分かり、よりコストの小さいルートがある限り、スタブルータに転送用のパケットを送信しません。

II. 設定手順

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． OSPF view に移行する	**ospf** [*process-id* | **router-id** *router-id* | **vpn-instance** *vpn-instance-name*] *	―
3． ルータをスタブルータに設定する	**stub-router [external-lsa [** *max-metric-value* **] | include-stub | on-startup** *seconds* **| summary-lsa [** *max-metric-value* **]]** *	デフォルト：設定なし スタブルータはスタブエリアとは関係ありません。

7.11.2 RFC 1583 の互換性の有効化

I. RFC 1583 の互換性

別の AS にある宛先への最適なルートを選択する場合、RFC1583 は RFC2328 と異なります。RFC1583 では、集約経路のコストは、集約された具体的な経路の最小コストになります。RFC2328 では、集約経路のコストは、集約された具体的な経路の最大コストとなります。

複数のルートは ASBR で有効なとき、OSPF は以下の優先順位で最適ルートを選択します。

1) もっとも高い優先順位のルートを選択します。
   - もし RFC2328 が RFC1583 で互換性がある場合、すべてのルートの優先度は同一です。
   - もし RFC2328 が RFC1583 と互換性がない場合、バックボーンエリアの負荷を軽減するために非バックボーンエリアの内部エリアルートが選択されます。バックボーンエリアの内部エリアと外部エリアの優先度は同一です。
2) 2 つのルートの優先度が同一である場合、コストの低いルートを選択します。
3) 2 つのルートのコストが同一である場合、もとのエリア ID が大きい値のルートを選択します。

II. 制限とガイドライン

ルーティングループを回避するために、RFC1583 と互換性があるようにルーティングドメインのすべてのルータに設定します。

III. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. OSPF view に移行する	**ospf** [*process-id* | **router-id** *router-id* | **vpn-instance** *vpn-instance-name*] *	ー
3. RFC153 の互換性を有効にする	**rfc1583 compatible**	デフォルト：有効

7.12 OSPF GRの設定

7.12.1 OSPF GR

GR（グレースフルリスタート）は、ルーティングプロトコルの再起動あるいはアクティブ/スタンバイの切り替えが発生したときでも、パケット転送を継続することができます。

GR 機能を動作させるには 2 台のルータが必要です。GR のルータは以下の役割があります。

- **GR リスタータ —** グレースフルリスタートルータです。GR 機能を持ちます。
- **GR ヘルパー —** GR リスタータのネイバ装置です。GR プロセスを処理するために GR リスタータを補助します。
- OSPF GR は以下のタイプがあります。
- **IETF 準拠の OSPF GR** － GR を実装するために Opaque LSA を使用します。

- **非 IETF 準拠の OSPF GR** – GR を配信するため、LLS(リンクローカルシグナリング)を使用し、LSDB を同期させるため、帯域外の同期化を使用します。
- 装置は、同時に GR リスタータと GR ヘルパーの両方で動作できます。

🕮 **メモ：**

- IRF スタック機能を使用している装置では、GR 機能を使用することを推奨します。
- IRF スタック装置で GR を使用する場合には、すべての IRF スタックユニットが同じ L3 ネットワークに所属するような構成にしてください。そうしない場合は、マスタ切り替え時にネットワークトポロジが変化して GR 機能が正常に動作を行いません。

7.12.2 OSPF GR リスタータの設定

I. IETF 準拠の OSPF GR リスタータの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. OSPF を有効にし、OSPF view に移行する	**ospf** [*process-id* | **router-id** *router-id* | **vpn-instance** *vpn-instance-name*] *	ー
3. opaque LSA の送受信を有効にする	**opaque-capability enable**	デフォルト：有効
4. IETF GR を有効にする	**graceful-restart ietf** [**global** | **planned-only**] *	デフォルト：無効
5. (オプション設定項目) GR 間隔を設定する	**graceful-restart interval** *interval-value*	デフォルト：120秒

II. 非 IETF 準拠の OSPF GR リスタータの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. OSPF を有効にし、OSPF view に移行する	**ospf** [*process-id* | **router-id** *router-id* | **vpn-instance** *vpn-instance-name*] *	ー
3. リンクローカルシグナリングを有効にする	**enable link-local-signaling**	デフォルト：無効
4. 帯域外の再同期機能を有効にする	**enable out-of-band-resynchronization**	デフォルト：無効.
5. 非 IETF GR を有効にする	**graceful-restart** [**nonstandard**] [**global** | **planned-only**] *	デフォルト：無効
6. (オプション設定項目) GR 間隔を設定する	**graceful-restart interval** *interval*	デフォルト：120秒

7.12.3 OSPF GR ヘルパーの設定

I. IETF 準拠の OSPF GR ヘルパーの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	ー

操作	コマンド	補足
2. OSPF を有効にし、OSPF view に移行する	**ospf** [*process-id* | **router-id** *router-id* | **vpn-instance** *vpn-instance-name*] *	ー
3. opaque LSA の送受信を有効にする	**opaque-capability enable**	デフォルト：有効
4. (オプション設定項目) GR ヘルパーを有効にする	**graceful-restart helper enable** [**planned-only**]	デフォルト：有効
5. (オプション設定項目) strict LSA 確認を有効にする	**graceful-restart helper strict-lsa-checking**	デフォルト：無効 GRヘルパー上でLSA変更が検出されると、GRヘルパー装置はGRヘルパーモードを終了します。

II. 非 IETF 準拠の OSPF GR ヘルパーの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. OSPF を有効にし、OSPF view に移行する	**ospf** [*process-id* | **router-id** *router-id* | **vpn-instance** *vpn-instance-name*] *	ー
3. リンクローカルシグナリングを有効にする	**enable link-local-signaling**	デフォルト：無効
4. 帯域外の再同期機能を有効にする	**enable out-of-band-resynchronization**	デフォルト：無効
5. (オプション設定項目) GR ヘルパーを有効にする	**graceful-restart helper enable**	デフォルト：有効
6. (オプション設定項目) strict LSA 確認を有効にする	**graceful-restart helper strict-lsa-checking**	デフォルト：無効 GRヘルパー上でLSA変更が検出されると、GRヘルパー装置はGRヘルパーモードを終了します。

7.12.4 OSPF GR の開始

I. OSPF GR の開始

アクティブ/スタンバイの切り替えを実行するか、**reset ospf process** コマンドを使用して OSPF GR を開始できます。

II. 設定手順

操作	コマンド
OSPFグレースフルリスタートを開始する	**reset ospf** [*process-id*] **process graceful-restart**

7.13 OSPF NSRの設定

I. OSPF NSR

ノンストップルーティング (NSR) は、アクティブプロセスからスタンバイプロセスへの OSPF リンクステート情報をバックアップします。アクティブ/スタンバイスイッチオーバーの後、隣接関係を切断したり転送サービスに影響を与えたりすることなく、NSR はリンクステートのリカバリとルートの再生成を完了できます。

NSR は、ルーティング情報をリカバリするために隣接装置の協力を必要とせず、一般に GR よりも頻繁に使用されます。

II. 制限とガイドライン

OSPF NSR が有効になっている装置は、GR リスタータとして機能できません。

III. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. OSPF view に移行する	**ospf** [*process-id* | **router-id** *router-id* | **vpn-instance** *vpn-instance-name*] *	―
3. OSPF NSR を有効にする	**non-stop-routing**	デフォルト：無効 このコマンドは、現在のプロセスに対してのみ有効です。ベストプラクティスとして、複数のOSPFプロセスが存在する場合は、プロセスごとにOSPF NSRを有効にします。

7.14 OSPFのBFDの設定

7.14.1 OSPF の BFD

BFD は、ネットワークの収束時間を改善する、OSPF ネイバ装置間のリンクの接続を早急に検出しモニタする共通の機能です。BFD についての詳細はオペレーションマニュアルのセクション 10 *高可用性* "*BFD*"を参照してください。

OSPF は以下の BFD 検出モードをサポートします。

- **双方向コントロールパケット検知** – リンクの両方の OSPF ルータで設定される、BFD 設定で必要な双方向コントロールパケット検知
- **シングルホップエコー検知** — リンクの片方の OSPF ルータで設定される、BFD 設定で必要なシングルホップエコー検知

7.14.2 双方向コントロールパケット検知の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. interface view に移行する	**interface** *interface-type interface-number*	―
3. 双方向コントロールパケット検知を有効にする	**ospf bfd enable**	デフォルト：無効 BFDセッションの両方のエンドは同じネットワークセグメントで同じエリアにする必要があります。

7.14.3 シングルホップエコー検知の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. エコーパケットの送信元アドレスを設定する	**bfd echo-source-ip** *ip-address*	デフォルト：設定なし
3. interface view に移行する	**interface** *interface-type interface-number*	―
4. シングルホップエコー検知を有効にする	**ospf bfd enable echo**	デフォルト：無効

7.15 OSPF FRRの設定

7.15.1 OSPF FRR について

パス上のリンクまたはルータの障害は、OSPF が新しいネットワークトポロジに基づいてルーティングコンバージェンスを完了するまで、パケット損失やルーティングループを引き起こす可能性があります。FRR では、リンクまたはノードの障害による影響を最小限に抑えるために、迅速な再ルーティングが可能です。

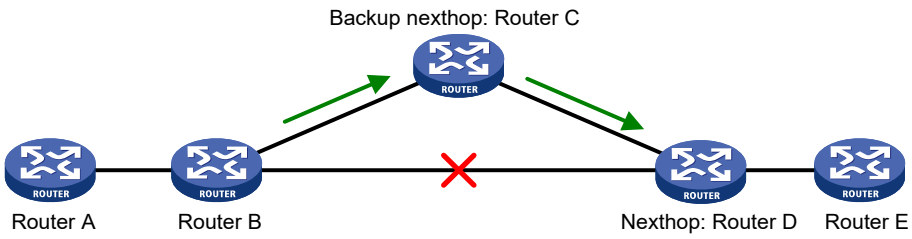


図 7-7 OSF FRR のネットワークダイアグラム

図 7-7に示すように、バックアップのネクストホップを指定するルーティングポリシーを使用して、ルータ B で FRR を設定します。プライマリリンクに障害が発生すると、OSPF はバックアップネクストホップにパケットを送信します。 同時に、OSPF は新しいネッ

トワークトポロジに基づいて最短パスを計算します。 ネットワークコンバージェンスの後、パス上でパケットを転送します。

ループフリー代替(LFA)アルゴリズムを使用してバックアップネクストホップを計算するように OSPF FRR を設定するか、ルーティングポリシーを使用してバックアップネクストホップを指定できます。

7.15.2 バックアップのネクストホップを計算するために LFA アルゴリズムを使用するために OSPF FRR を設定

I. 制限とガイドライン

fast-reroute lfa コマンドを **vlink-peer** コマンドと一緒に使用しないでください。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. interface view に移行する	**interface** *interface-type interface-number*	―
3. system view に戻る	**quit**	
4. OSPF view に移行する	**ospf** [*process-id* | **router-id** *router-id* | **vpn-instance** *vpn-instance-name*] *	―
5. OSPF FRR を有効にして、LFA アルゴリズムを使用してバックアップネクストホップを計算する	**fast-reroute lfa** [**abr-only**]	デフォルトでは、OSPF FRR は無効になっています。**abr-only**が指定されている場合は、ABRへのルートがバックアップパスとして選択されます。

7.16 OSPF認証の設定

7.16.1 OSPF エリアとインタフェースでの OSPF 認証

OSPF 認証の設定は、OSPF エリアとインタフェースで設定します。

OSPF は設定されたパスワードを送信されるパケットに追加し、受信したパケットの認証を行うためにパスワードを使用します。認証にパスしたパケットのみを受信することができます。認証に失敗した場合、OSPF ネイバ装置はネイバ関係を確立することができません。

OSPF 認証をエリアとインタフェースの両方で設定する場合、インタフェースの設定が適用されます。

7.16.2 エリアでの OSPF 認証の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. OSPF view に移行する	**ospf** [*process-id* | **router-id** *router-id* | **vpn-instance** *vpn-instance-name*] *	ー
3. area view に移行する	**area** *area-id*	ー
4. エリアで認証モードを設定する	● HMAC-MD5/MD5認証を設定する: **authentication-mode** { **hmac-md5** | **md5** } *key-id* { **cipher** | **plain** } *string* ● simple認証を設定する: **authentication-mode simple** { **cipher** | **plain** } *string*	デフォルト：設定なし エリアにあるすべての装置で同一の認証モードとパスワードを使用する必要があります。

7.16.3 インタフェースでの OSPF 認証の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. interface view に移行する	**interface** *interface-type interface-number*	ー
3. インタフェースで認証モードを設定する	● simple認証を設定する: **ospf authentication-mode simple** { **cipher** | **plain** } *string* ● HMAC-MD5/MD5認証を設定する: **ospf authentication-mode** { **hmac-md5** | **md5** } *key-id* { **cipher** | **plain** } *string*	デフォルト：設定なし ローカルインタフェースと対向先のインタフェースの両方で同一の認証モードとパスワードを使用する必要があります。

7.17 OSPF用のGTSMの設定

7.18 OSPFのロギングとSNMP notificationの設定

7.18.1 ネイバ状態変更のロギング

I. ネイバ状態変更のロギング

ネイバ状態の変更を information center にログ情報として出力することができます。information center は（ログを出力するか、どこにログを出力するか）ユーザが定義したルールに従ってログを出力します。information center の詳細は、オペレーションマニュアルのセクション 11 *システム管理* "*Information Center*"を参照してください。

II. 設定手順

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． OSPF view に移行する	**ospf** [*process-id* | **router-id** *router-id* | **vpn-instance** *vpn-instance-name*] *	―
3． ネイバ状態の変更に伴うログ作成を有効にする	**log-peer-change**	デフォルト：有効

7.18.2 OSPF ロギング機能の設定

I. OSPF ログ

OSPF ログには、LSA エージングログ、ルート計算ログ、隣接ログ、OSPF ルートログ、および自己発信および受信 LSA ログが含まれます。

II. 設定手順

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． OSPF view に移行する	**ospf** [*process-id* | **router-id** *router-id* | **vpn-instance** *vpn-instance-name*] *	―
3． OSPF ログの数を設定する	**event-log** { **lsa-flush** | **peer** | **spf** } **size** *count*	デフォルト：LSAエージングログ、隣接ログ、ルート計算ログの各タイプで最大10

7.18.3 OSPF ネットワーク管理の設定

I. OSPF ネットワーク管理

以下の設定を行うことで OSPF のネットワーク管理を行います。

- 指定した OSPF の管理を行うネットワーク管理ソフトウェアを使用するため、MIB に OSPF を組み込みます。
- 重要なイベントを報告するために OSPF の SNMP 通知を有効にします。
- 各間隔で出力できる SNMP 通知の出力間隔と SNMP 通知の最大数を設定します。

重要な OSPF イベントを NMS に通知するには、OSPF の SNMP 通知を有効にします。SNMP 通知が正しく送信されるようにするには、装置上の SNMP も設定する必要があります。SNMP 通知の詳細は、オペレーションマニュアルのセクション 11 *ネットワーク管理* "*SNMP*"を参照してください。

II. 設定手順

操作	コマンド	補足
1． system view に移行する	**system-view**	―

操作	コマンド	補足
2. OSPF プロセスに OSPF MIB を割り当てる	**ospf mib-binding** *process-id*	デフォルト : もっとも小さいプロセスIDのプロセスがOSPF MIB に割り当てられています。
3. OSPF トラップを有効にする	**snmp-agent trap enable ospf** [**authentication-failure** | **bad-packet** | **config-error** | **grhelper-status-change** | **grrestarter-status-change** | **if-state-change** | **lsa-maxage** | **lsa-originate** | **lsdb-approaching-overflow** | **lsdb-overflow** | **neighbor-state-change** | **nssatranslator-status-change** | **retransmit** | **virt-authentication-failure** | **virt-bad-packet** | **virt-config-error** | **virt-retransmit** | **virtgrhelper-status-change** | **virtif-state-change** | **virtneighbor-state-change**] *	デフォルト：有効
4. OSPF view に移行する	**ospf** [*process-id* | **router-id** *router-id* | **vpn-instance** *vpn-instance-name*] *	ー

7.19 OSPFの表示と維持

すべての view で **display** コマンドを実行でき、user view で **reset** コマンドを実行できます。

操作	コマンド
OSPF ABR 集約情報を表示する	**display ospf** [*process-id*] [**area** *area-id*] **abr-summary** [*ip-address* { *mask-length* | *mask* }] [**verbose**]
OSPF FRRバックアップネクストホップ情報を表示する。	**display ospf [** *process-id* **] [area** *area-id* **] fast-reroute lfa-candidate**
OSPFトポロジ情報を表示する。	**display ospf [** *process-id* **] [area** *area-id* **] spf-tree [verbose]**
OSPFプロセスの情報を表示する	**display ospf** [*process-id*] [**verbose**]
OSPF ABRおよびASBR情報を表示する	**display ospf** [*process-id*] **abr-asbr** [**verbose**]
OSPF ASBR 集約情報を表示する	**display ospf** [*process-id*] **asbr-summary** [*ip-address* { *mask-length* | *mask* }]
OSPFのログ情報を表示する	**display ospf** [*process-id*] **event-log** { **lsa-flush** | **peer** | **spf** }
OSPF GR情報を表示する	**display ospf** [*process-id*] **graceful-restart** [**verbose**]
OSPFインタフェース情報を表示する	**display ospf** [*process-id*] **interface** [*interface-type interface-number* | **verbose**]
OSPF LSDB情報を表示する	**display ospf** [*process-id*] [**area** *area-id*] **lsdb** { **asbr** | **network** | **nssa** | **opaque-area** | **opaque-link** | **router** | **summary** } [*link-state-id*] [**originate-router** *advertising-router-id* | **self-originate**] **display ospf** [*process-id*] **lsdb** [**brief** | **originate-router** *advertising-router-id* | **self-originate**] **display ospf** [*process-id*] **lsdb** { **ase** | **opaque-as ase** } [*link-state-id*] [**originate-router** *advertising-router-id* | **self-originate**]

操作	コマンド
OSPFのネクストホップの情報を表示する	**display ospf** [*process-id*] **nexthop**
OSPF NSR情報を表示する	**display ospf** [*process-id*] **non-stop-routing status**
OSPFネイバ情報を表示する	**display ospf** [*process-id*] **peer** [**verbose**] [*interface-type interface-number*] [*neighbor-id*]
OSPFエリアのネイバ統計情報を表示する	**display ospf** [*process-id*] **peer statistics**
OSPF要求キュー情報を表示する	**display ospf** [*process-id*] **request-queue** [*interface-type interface-number*] [*neighbor-id*]
OSPF再送キュー情報を表示する	**display ospf** [*process-id*] **retrans-queue** [*interface-type interface-number*] [*neighbor-id*]
OSPFルーティングテーブル情報を表示する	**display ospf** [*process-id*] **routing** [*ip-address* { *mask-length* | *mask* }] [**interface** *interface-type interface-number*] [**nexthop** *nexthop-address*] [**verbose**]
OSPF統計情報を表示する	**display ospf** [*process-id*] **statistics** [**error** | **packet** [*interface-type interface-number*]]
OSPF仮想リンク情報を表示する	**display ospf** [*process-id*] **vlink**
グローバルルータIDを表示する	**display router id**
OSPFのログ情報を削除する	**reset ospf** [*process-id*] **event-log** [**lsa-flush** | **peer** | **spf**]
OSPFプロセスをリセットする	**reset ospf** [*process-id*] **process** [**graceful-restart**]
OSPFルート再配信をリセットする	**reset ospf** [*process-id*] **redistribution**
OSPFの統計情報を削除する	**reset ospf** [*process-id*] **statistics**

7.20 OSPFの設定例

7.20.1 OSPF の基本機能の設定例

I. ネットワーク要件

図 7-8に示すように設定します。

- すべての Switch で OSPF を有効にし、3 つのエリアに AS を分割します。
- Switch A と Switch B を ABR として設定します。

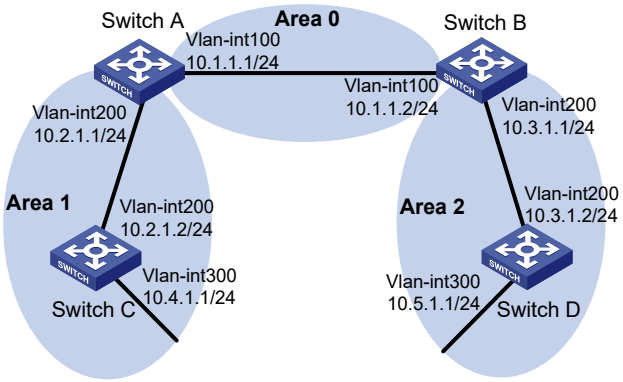


図 7-8 ネットワーク図

II. 設定手順

1) インタフェースに IP アドレスを設定します。(詳細は省略します)
2) OSPF を有効にします。

Switch A を設定します。

```
<SwitchA> system-view
[SwitchA] router id 10.2.1.1
[SwitchA] ospf
[SwitchA-ospf-1] area 0
[SwitchA-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.0] quit
[SwitchA-ospf-1] area 1
[SwitchA-ospf-1-area-0.0.0.1] network 10.2.1.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.1] quit
[SwitchA-ospf-1] quit
```

Switch B を設定します。

```
<SwitchB> system-view
[SwitchB] router id 10.3.1.1
[SwitchB] ospf
[SwitchB-ospf-1] area 0
[SwitchB-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] quit
[SwitchB-ospf-1] area 2
[SwitchB-ospf-1-area-0.0.0.2] network 10.3.1.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.2] quit
[SwitchB-ospf-1] quit
```

Switch C を設定します。

```
<SwitchC> system-view
[SwitchC] router id 10.4.1.1
[SwitchC] ospf
[SwitchC-ospf-1] area 1
[SwitchC-ospf-1-area-0.0.0.1] network 10.2.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.1] network 10.4.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.1] quit
[SwitchC-ospf-1] quit
```

Switch D を設定します。

```
<SwitchD> system-view
[SwitchD] router id 10.5.1.1
[SwitchD] ospf
[SwitchD-ospf-1] area 2
[SwitchD-ospf-1-area-0.0.0.2] network 10.3.1.0 0.0.0.255
[SwitchD-ospf-1-area-0.0.0.2] network 10.5.1.0 0.0.0.255
[SwitchD-ospf-1-area-0.0.0.2] quit
[SwitchD-ospf-1] quit
```

III. 設定の確認

Switch A のネイバ情報を表示します。

```
[SwitchA] display ospf peer verbose

          OSPF Process 1 with Router ID 10.2.1.1
                  Neighbors

 Area 0.0.0.0 interface 10.1.1.1(Vlan-interface100)'s neighbors
 Router ID: 10.3.1.1         Address: 10.1.1.2         GR State: Normal
   State: Full  Mode: Nbr is master  Priority: 1
   DR: 10.1.1.1  BDR: 10.1.1.2  MTU: 0
   Options is 0x02 (-|-|-|-|-|-|E|-)
   Dead timer due in 37  sec
   Neighbor is up for 06:03:59
   Authentication Sequence: [ 0 ]
   Neighbor state change count: 5

 Area 0.0.0.1 interface 10.2.1.1(Vlan-interface200)'s neighbors
 Router ID: 10.4.1.1         Address: 10.2.1.2         GR State: Normal
   State: Full  Mode: Nbr is master  Priority: 1
   DR: 10.2.1.1  BDR: 10.2.1.2  MTU: 0
   Options is 0x02 (-|-|-|-|-|-|E|-)
   Dead timer due in 32  sec
   Neighbor is up for 06:03:12
   Authentication Sequence: [ 0 ]
   Neighbor state change count: 5
```

Switch A の OSPF ルーティング情報を表示します。

```
[SwitchA] display ospf routing

          OSPF Process 1 with Router ID 10.2.1.1
                  Routing Table

                Topology base (MTID 0)

 Routing for network
 Destination        Cost     Type    NextHop         AdvRouter       Area
 10.2.1.0/24        1        Transit 10.2.1.1        10.2.1.1        0.0.0.1
 10.3.1.0/24        2        Inter   10.1.1.2        10.3.1.1        0.0.0.0
 10.4.1.0/24        2        Stub    10.2.1.2        10.4.1.1        0.0.0.1
 10.5.1.0/24        3        Inter   10.1.1.2        10.3.1.1        0.0.0.0
 10.1.1.0/24        1        Transit 10.1.1.1        10.2.1.1        0.0.0.0

 Total nets: 5
 Intra area: 3  Inter area: 2  ASE: 0  NSSA: 0
```

Switch D の OSPF ルーティング情報を表示します。

[SwitchD] display ospf routing

```
          OSPF Process 1 with Router ID 10.5.1.1
                  Routing Table

                Topology base (MTID 0)

 Routing for network
 Destination        Cost     Type    NextHop         AdvRouter       Area
 10.2.1.0/24        3        Inter   10.3.1.1        10.3.1.1        0.0.0.2
 10.3.1.0/24        1        Transit 10.3.1.2        10.3.1.1        0.0.0.2
 10.4.1.0/24        4        Inter   10.3.1.1        10.3.1.1        0.0.0.2
 10.5.1.0/24        1        Stub    10.5.1.1        10.5.1.1        0.0.0.2
 10.1.1.0/24        2        Inter   10.3.1.1        10.3.1.1        0.0.0.2

 Total nets: 5
 Intra area: 2  Inter area: 3  ASE: 0  NSSA: 0
```

Switch D で、IP アドレス 10.4.1.1 へ ping を実行し、接続を確認します。

[SwitchD] ping 10.4.1.1

```
Ping 10.4.1.1 (10.4.1.1): 56 data bytes, press CTRL_C to break
56 bytes from 10.4.1.1: icmp_seq=0 ttl=253 time=1.549 ms
56 bytes from 10.4.1.1: icmp_seq=1 ttl=253 time=1.539 ms
56 bytes from 10.4.1.1: icmp_seq=2 ttl=253 time=0.779 ms
56 bytes from 10.4.1.1: icmp_seq=3 ttl=253 time=1.702 ms
56 bytes from 10.4.1.1: icmp_seq=4 ttl=253 time=1.471 ms

--- Ping statistics for 10.4.1.1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.779/1.408/1.702/0.323 ms
```

7.20.2 OSPF ルート再配信の設定例

I. ネットワーク要件

図 7-9に示すように設定します。

- すべての Switch で OSPF を有効にします。
- 3 つのエリアで AS を分割します。
- Switch A と Switch B を ABR として設定します。
- ASBR として Switch C を設定し、外部ルート(スタティックルート)を再配信します。

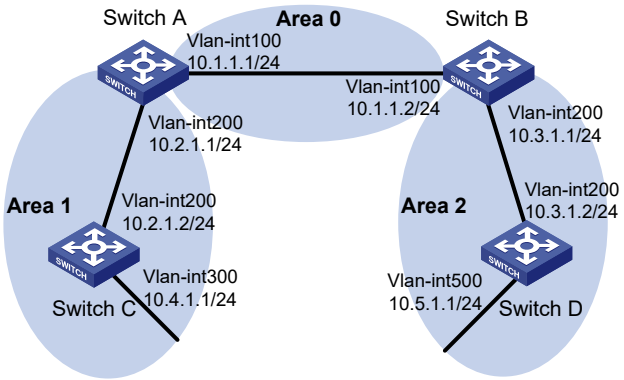


図 7-9 ネットワーク図

II. 設定手順

1) インタフェースに IP アドレスを設定します。(詳細は省略します)
2) OSPF を有効にします。(詳細はオペレーションマニュアルのセクション 5 *ルーティングプロトコル "OSPF"の"OSPF の基本機能の設定例"* を参照してください)
3) ルートを再配信するように設定します。

Switch C でネットワーク 3.1.2.0/24 のスタティックルートを設定します。

```
<SwitchC> system-view
[SwitchC] ip route-static 3.1.2.1 24 10.4.1.2
```

Switch C でスタティックルートを再配信するように設定します。

```
[SwitchC] ospf 1
[SwitchC-ospf-1] import-route static
```

III. 設定の確認

Switch D の ABR/ASBR 情報を表示します。

```
<SwitchD> display ospf abr-asbr

          OSPF Process 1 with Router ID 10.5.1.1
                  Routing Table to ABR and ASBR


                Topology base (MTID 0)
 Type        Destination     Area            Cost  Nexthop         RtType
 Intra       10.3.1.1        0.0.0.2         10    10.3.1.1        ABR
 Inter       10.4.1.1        0.0.0.2         22    10.3.1.1        ASBR
```

Switch D の OSPF ルーティング情報を表示します。

```
<SwitchD> display ospf routing

          OSPF Process 1 with Router ID 10.5.1.1
                   Routing Table

                Topology base (MTID 0)

 Routing for network
 Destination        Cost     Type    NextHop         AdvRouter       Area
 10.2.1.0/24        22       Inter   10.3.1.1        10.3.1.1        0.0.0.2
 10.3.1.0/24        10       Transit 10.3.1.2        10.3.1.1        0.0.0.2
 10.4.1.0/24        25       Inter   10.3.1.1        10.3.1.1        0.0.0.2
 10.5.1.0/24        10       Stub    10.5.1.1        10.5.1.1        0.0.0.2
 10.1.1.0/24        12       Inter   10.3.1.1        10.3.1.1        0.0.0.2

 Routing for ASEs
 Destination        Cost     Type    Tag         NextHop         AdvRouter
 3.1.2.0/24         1        Type2   1           10.3.1.1        10.4.1.1

 Total nets: 6
 Intra area: 2  Inter area: 3  ASE: 1  NSSA: 0
```

7.20.3 ASBR での OSPF ルート集約の設定例

I. ネットワーク要件

図 7-10に示すように：

- Switch A、Switch B、Switch C は Area2 にします。
- Switch A の VLAN インタフェース 200 に IP アドレス 2.1.1.1/24 を設定します。
- Switch B に、OSPF プロセス 2 を設定し、プロセス 1 とダイレクトルートを再配布します。
- Switch B で ASBR ルート集約を設定します。Switch B は、集約ルート 2.0.0.0/8 のみを配信します。

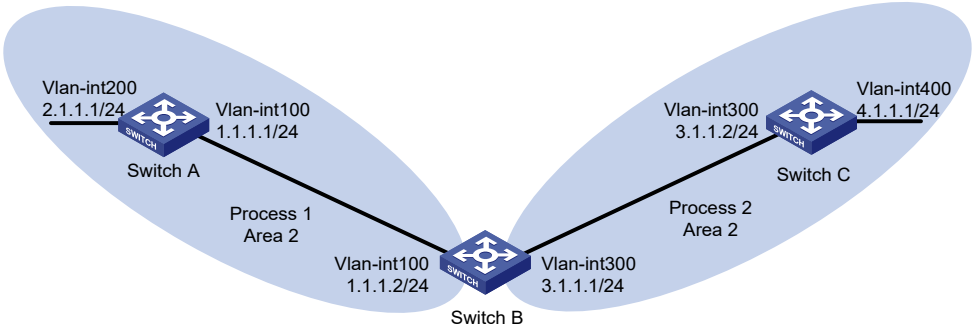


図 7-10 ネットワーク図

II. 設定手順

1)　インタフェースのための IP アドレスを設定。 (詳細は省略します)
2)　OSPF の設定

Switch A で OSPF プロセス 1 を有効にします。

```
<SwitchA> system-view
[SwitchA] router id 11.2.1.1
[SwitchA] interface vlan-interface 200
[SwitchA-Vlan-interface200] ip address 2.1.1.1 24
 [SwitchA-Vlan-interface200] quit
[SwitchA] ospf 1
[SwitchA-ospf-1] area 2
[SwitchA-ospf-1-area-0.0.0.2] network 1.1.1.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.2] network 2.1.0.0 0.0.255.255
[SwitchA-ospf-1-area-0.0.0.2] quit
[SwitchA-ospf-1] quit
```

Switch B で OSPF プロセス 1 とプロセス 2 を有効にします。

```
<SwitchB> system-view
[SwitchB] router id 11.2.1.2
[SwitchB] ospf 1
[SwitchB-ospf-1] area 2
[SwitchB-ospf-1-area-0.0.0.2] network 1.1.1.0 0.0.0.255
```

```
[SwitchB-ospf-1-area-0.0.0.2] quit
[SwitchB-ospf-1] quit
[SwitchB] ospf 2
[SwitchB-ospf-2] area 2
[SwitchB-ospf-2-area-0.0.0.2] network 3.1.1.0 0.0.0.255
[SwitchB-ospf-2-area-0.0.0.2] quit
[SwitchB-ospf-2] quit
```

Switch C で OSPF プロセス 2 を有効にします。

```
<SwitchC> system-view
[SwitchC] router id 11.1.1.2
[SwitchC] ospf 2
[SwitchC-ospf-2] area 2
[SwitchC-ospf-2-area-0.0.0.2] network 3.1.1.0 0.0.0.255
[SwitchC-ospf-2-area-0.0.0.2] network 4.1.0.0 0.0.255.255
[SwitchC-ospf-2-area-0.0.0.2] quit
[SwitchC-ospf-2] quit
```

3) ルートを再配信するための設定 OSPF:

Switch B の OSPF プロセス 2 を設定して、OSPF プロセス 1 からのルートとダイレクトルートを再配信します。

```
[SwitchB] ospf 2
[SwitchB-ospf-2]import-route direct
[SwitchB-ospf-2]import-route ospf 1
```

Switch C のルーティングテーブル情報を表示します。

```
[SwitchC] display ip routing-table
Destinations : 28       Routes : 28
Destination/Mask    Proto   Pre Cost        NextHop         Interface
0.0.0.0/32          Direct  0   0           127.0.0.1       InLoop0
1.1.1.0/24          O_ASE2  150 1           3.1.1.1         Vlan300
2.1.1.0/24          O_ASE2  150 1           3.1.1.1         Vlan300
3.1.1.0/24          Direct  0   0           3.1.1.2         Vlan300
3.1.1.0/32          Direct  0   0           3.1.1.2         Vlan300
3.1.1.2/32          Direct  0   0           127.0.0.1       InLoop0
3.1.1.255/32        Direct  0   0           3.1.1.2         Vlan300
4.1.1.0/24          Direct  0   0           4.1.1.1         Loop101
4.1.1.0/32          Direct  0   0           4.1.1.1         Loop101
4.1.1.1/32          Direct  0   0           127.0.0.1       InLoop0
4.1.1.255/32        Direct  0   0           4.1.1.1         Loop101
4.1.2.0/24          Direct  0   0           4.1.2.1         Loop102
4.1.2.0/32          Direct  0   0           4.1.2.1         Loop102
4.1.2.1/32          Direct  0   0           127.0.0.1       InLoop0
4.1.2.255/32        Direct  0   0           4.1.2.1         Loop102
4.1.3.0/24          Direct  0   0           4.1.3.1         Loop103
4.1.3.0/32          Direct  0   0           4.1.3.1         Loop103
4.1.3.1/32          Direct  0   0           127.0.0.1       InLoop0
4.1.3.255/32        Direct  0   0           4.1.3.1         Loop103
127.0.0.0/8         Direct  0   0           127.0.0.1       InLoop0
```

```
127.0.0.0/32        Direct  0    0           127.0.0.1       InLoop0
127.0.0.1/32        Direct  0    0           127.0.0.1       InLoop0
127.255.255.255/32 Direct  0    0           127.0.0.1       InLoop0
224.0.0.0/4         Direct  0    0           0.0.0.0         NULL0
224.0.0.0/24        Direct  0    0           0.0.0.0         NULL0
255.255.255.255/32 Direct  0    0           127.0.0.1       InLoop0
```

4) OSPF を設定して、ASBR 上のルートを集約します。

集約ルート 2.0.0.0/8 を配信するように、Switch B の OSPF プロセス 2 を設定します。

```
[SwitchB] ospf 2
[SwitchB-ospf-2] asbr-summary 2.0.0.0 8
[SwitchB-ospf-2] quit
```

Switch C のルーティングテーブル情報を表示します。

```
[SwitchC]display ip routing-table
Destinations : 26       Routes : 26
Destination/Mask    Proto   Pre Cost        NextHop         Interface
0.0.0.0/32          Direct  0   0           127.0.0.1       InLoop0
1.1.1.0/24          O ASE2  150 1           3.1.1.1         Vlan300
2.0.0.0/8           O_ASE2  150 1           3.1.1.1         Vlan300
3.1.1.0/24          Direct  0   0           3.1.1.2         Vlan300
3.1.1.0/32          Direct  0   0           3.1.1.2         Vlan300
3.1.1.2/32          Direct  0   0           127.0.0.1       InLoop0
3.1.1.255/32        Direct  0   0           3.1.1.2         Vlan300
4.1.1.0/24          Direct  0   0           4.1.1.1         Loop101
4.1.1.0/32          Direct  0   0           4.1.1.1         Loop101
4.1.1.1/32          Direct  0   0           127.0.0.1       InLoop0
4.1.1.255/32        Direct  0   0           4.1.1.1         Loop101
4.1.2.0/24          Direct  0   0           4.1.2.1         Loop102
4.1.2.0/32          Direct  0   0           4.1.2.1         Loop102
4.1.2.1/32          Direct  0   0           127.0.0.1       InLoop0
4.1.2.255/32        Direct  0   0           4.1.2.1         Loop102
4.1.3.0/24          Direct  0   0           4.1.3.1         Loop103
4.1.3.0/32          Direct  0   0           4.1.3.1         Loop103
4.1.3.1/32          Direct  0   0           127.0.0.1       InLoop0
4.1.3.255/32        Direct  0   0           4.1.3.1         Loop103
127.0.0.0/8         Direct  0   0           127.0.0.1       InLoop0
127.0.0.0/32        Direct  0   0           127.0.0.1       InLoop0
127.0.0.1/32        Direct  0   0           127.0.0.1       InLoop0
127.255.255.255/32 Direct  0   0           127.0.0.1       InLoop0
224.0.0.0/4         Direct  0   0           0.0.0.0         NULL0
224.0.0.0/24        Direct  0   0           0.0.0.0         NULL0
255.255.255.255/32 Direct  0   0           127.0.0.1       InLoop0
```

7.20.4 OSPF スタブエリアの設定例

I. ネットワーク要件

図 7-11に示すように設定します。

- すべての Switch で OSPF を有効にし、3 つのエリアに AS を分割します。
- エリア間のルーティング情報を転送するため、Switch A、Switch B を ABR として設定します。
- スタティックルートを再配信するため、Switch D を ASBR として設定します。
- 到達するかに関係なく、配信された LSA を削減するため、スタブエリア Area 1 を設定します。

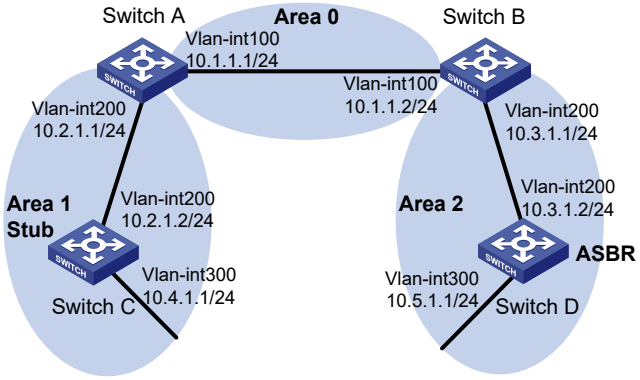


図 7-11 ネットワーク図

II. 設定手順

1) インタフェースに IP アドレスを設定します。(詳細は省略します)
2) OSPF を有効にします。(詳細はオペレーションマニュアルのセクション 5 *ルーティングプロトコル "OSPF"の"OSPF の基本機能の設定例"* を参照してください)
3) ルートの再配信を設定します。

Switch D でスタティックルートを再配信するように設定します。

```
<SwitchD> system-view
[SwitchD] ip route-static 3.1.2.1 24 10.5.1.2
[SwitchD] ospf
[SwitchD-ospf-1] import-route static
[SwitchD-ospf-1] quit
```

Switch C で ABR/ASBR 情報を表示します。

```
<SwitchC> display ospf abr-asbr

          OSPF Process 1 with Router ID 10.4.1.1
                  Routing Table to ABR and ASBR

              Topology base (MTID 0)
 Type        Destination     Area            Cost  Nexthop         RtType
 Intra       10.2.1.1        0.0.0.1         3     10.2.1.1        ABR
 Inter       10.5.1.1        0.0.0.1         7     10.2.1.1        ASBR
```

Switch C の OSPF ルーティング情報を表示します。

```
<SwitchC> display ospf routing

          OSPF Process 1 with Router ID 10.4.1.1
                  Routing Table

              Topology base (MTID 0)

 Routing for network
 Destination        Cost     Type    NextHop         AdvRouter       Area
 10.2.1.0/24        3        Transit 0.0.0.0         10.2.1.1        0.0.0.1
 10.3.1.0/24        7        Inter   10.2.1.1        10.2.1.1        0.0.0.1
 10.4.1.0/24        3        Stub    10.4.1.1        10.4.1.1        0.0.0.1
 10.5.1.0/24        17       Inter   10.2.1.1        10.2.1.1        0.0.0.1
 10.1.1.0/24        5        Inter   10.2.1.1        10.2.1.1        0.0.0.1
```

```
Routing for ASEs
Destination        Cost     Type    Tag         NextHop         AdvRouter
3.1.2.0/24         1        Type2   1           10.2.1.1        10.5.1.1

Total nets: 6
Intra area: 2  Inter area: 3  ASE: 1  NSSA: 0
```

出力は、Switch C のルーティングテーブルには AS 外部ルートが含まれることを示します。

4) スタブエリア Area 1 を設定します。

Switch A を設定します。

```
<SwitchA> system-view
[SwitchA] ospf
[SwitchA-ospf-1] area 1
[SwitchA-ospf-1-area-0.0.0.1] stub
[SwitchA-ospf-1-area-0.0.0.1] quit
[SwitchA-ospf-1] quit
```

Switch C を設定します。

```
<SwitchC> system-view
[SwitchC] ospf
[SwitchC-ospf-1] area 1
[SwitchC-ospf-1-area-0.0.0.1] stub
[SwitchC-ospf-1-area-0.0.0.1] quit
[SwitchC-ospf-1] quit
```

Switch C の OSPF ルーティング情報を表示します。

```
[SwitchC] display ospf routing

          OSPF Process 1 with Router ID 10.4.1.1
                  Routing Table

                Topology base (MTID 0)

Routing for network
Destination        Cost     Type    NextHop         AdvRouter       Area
0.0.0.0/0          4        Inter   10.2.1.1        10.2.1.1        0.0.0.1
10.2.1.0/24        3        Transit 0.0.0.0         10.2.1.1        0.0.0.1
10.3.1.0/24        7        Inter   10.2.1.1        10.2.1.1        0.0.0.1
10.4.1.0/24        3        Stub    10.4.1.1        10.4.1.1        0.0.0.1
10.5.1.0/24        17       Inter   10.2.1.1        10.2.1.1        0.0.0.1
10.1.1.0/24        5        Inter   10.2.1.1        10.2.1.1        0.0.0.1

Total nets: 6
Intra area: 2  Inter area: 4  ASE: 0  NSSA: 0
```

出力は、デフォルトルートが AS 外部ルートに置き換わることを示します。

完全スタブエリアとして Area 1 を設定します。

```
[SwitchA] ospf
[SwitchA-ospf-1] area 1
```

```
[SwitchA-ospf-1-area-0.0.0.1] stub no-summary
[SwitchA-ospf-1-area-0.0.0.1] quit
[SwitchA-ospf-1] quit
```

Switch C の OSPF ルーティング情報を表示します。

```
[SwitchC] display ospf routing

          OSPF Process 1 with Router ID 10.4.1.1
                  Routing Table

                Topology base (MTID 0)

 Routing for network
 Destination        Cost     Type    NextHop         AdvRouter       Area
 0.0.0.0/0          4        Inter   10.2.1.1        10.2.1.1        0.0.0.1
 10.2.1.0/24        3        Transit 0.0.0.0         10.4.1.1        0.0.0.1
 10.4.1.0/24        3        Stub    10.4.1.1        10.4.1.1        0.0.0.1

 Total nets: 3
 Intra area: 2  Inter area: 1  ASE: 0  NSSA: 0
```

出力は、内部エリアルートが削除され、1 つの外部ルート(デフォルトルート)のみが存在することを示します。

7.20.5 OSPF NSSA エリアの設定例

I. ネットワーク要件

図 7-12に示すように設定します。

- すべての Switch で OSPF を有効にし、3 つのエリアに AS を分割します。
- エリア間のルーティング情報を転送するため、Switch A、Switch B を ABR として設定します。

NSSA エリア Area 1 を設定します。ASBR として Switch C を設定し、AS にスタティックルートを再配信するように設定します。

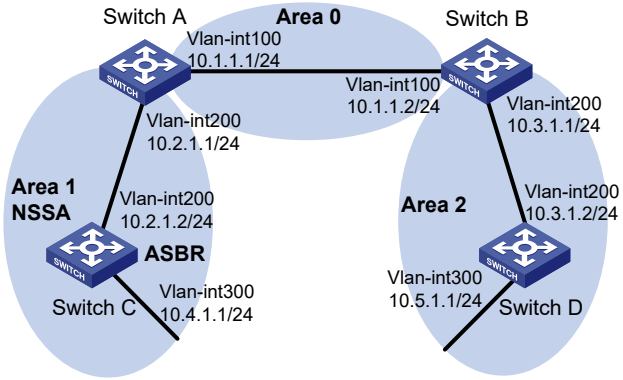


図 7-12 ネットワーク図

II. 設定手順

1) インタフェースに IP アドレスを設定します。(詳細は省略します)
2) OSPF の基本機能を設定します。(詳細はオペレーションマニュアルのセクション 5 *ルーティングプロトコル "OSPF"の"OSPF の基本機能の設定例"* を参照してください)
3) NSSA エリア Area 1 を設定します。

Switch A を設定します。

```
<SwitchA> system-view
[SwitchA] ospf
[SwitchA-ospf-1] area 1
[SwitchA-ospf-1-area-0.0.0.1] nssa
[SwitchA-ospf-1-area-0.0.0.1] quit
[SwitchA-ospf-1] quit
```

Switch C を設定します。

```
<SwitchC> system-view
[SwitchC] ospf
[SwitchC-ospf-1] area 1
[SwitchC-ospf-1-area-0.0.0.1] nssa
[SwitchC-ospf-1-area-0.0.0.1] quit
[SwitchC-ospf-1] quit
```

Switch C の OSPF ルーティング情報を表示します。

```
[SwitchC] display ospf routing

          OSPF Process 1 with Router ID 10.4.1.1
                  Routing Table

                Topology base (MTID 0)

 Routing for network
 Destination        Cost     Type    NextHop         AdvRouter       Area
 10.2.1.0/24        3        Transit 10.2.1.2        10.4.1.1        0.0.0.1
 10.3.1.0/24        7        Inter   10.2.1.1        10.2.1.1        0.0.0.1
 10.4.1.0/24        3        Stub    10.4.1.1        10.4.1.1        0.0.0.1
 10.5.1.0/24        17       Inter   10.2.1.1        10.2.1.1        0.0.0.1
 10.1.1.0/24        5        Inter   10.2.1.1        10.2.1.1        0.0.0.1

 Total nets: 5
 Intra area: 2  Inter area: 3  ASE: 0  NSSA: 0
```

4) ルートを再配信するように設定します。

Switch C でスタティックルートを再配信するように設定します。

```
[SwitchC] ip route-static 3.1.3.1 24 10.4.1.2
[SwitchC] ospf
[SwitchC-ospf-1] import-route static
[SwitchC-ospf-1] quit
```

Switch D の OSPF ルーティング情報を表示します。

```
<SwitchD> display ospf routing

                Topology base (MTID 0)

          OSPF Process 1 with Router ID 10.5.1.1
                    Routing Table

 Routing for network
 Destination        Cost     Type    NextHop         AdvRouter       Area
 10.2.1.0/24        22       Inter   10.3.1.1        10.3.1.1        0.0.0.2
 10.3.1.0/24        10       Transit 10.3.1.2        10.3.1.1        0.0.0.2
 10.4.1.0/24        25       Inter   10.3.1.1        10.3.1.1        0.0.0.2
 10.5.1.0/24        10       Stub    10.5.1.1        10.5.1.1        0.0.0.2
 10.1.1.0/24        12       Inter   10.3.1.1        10.3.1.1        0.0.0.2

 Routing for ASEs
 Destination        Cost     Type    Tag          NextHop         AdvRouter
 3.1.3.0/24         1        Type2   1            10.3.1.1        10.2.1.1

 Total nets: 6
 Intra area: 2  Inter area: 3  ASE: 1  NSSA: 0
```

出力は、NSSA エリアから入力された外部ルートが Switch D に存在していることを示します。

7.20.6 OSPF DR 選出の設定例

III. ネットワーク要件

図 7-13に示すように設定します。

- 同一ネットワークにある Switch A、Switch B、Switch C、Switch D で OSPF を有効にします。
- DR として Switch A を設定し、BDR として Switch C を設定します。

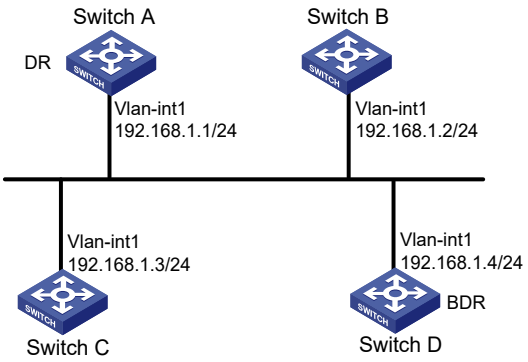


図 7-13 ネットワーク図

II. 設定手順

1) インタフェースに IP アドレスを設定します。(詳細は省略します)
2) OSPF を有効にします。

Switch A を設定します。

```
<SwitchA> system-view
[SwitchA] router id 1.1.1.1
[SwitchA] ospf
[SwitchA-ospf-1] area 0
[SwitchA-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.0] quit
[SwitchA-ospf-1] quit
```

Switch B を設定します。

```
<SwitchB> system-view
[SwitchB] router id 2.2.2.2
[SwitchB] ospf
[SwitchB-ospf-1] area 0
[SwitchB-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] quit
[SwitchB-ospf-1] quit
```

Switch C を設定します。

```
<SwitchC> system-view
[SwitchC] router id 3.3.3.3
[SwitchC] ospf
[SwitchC-ospf-1] area 0
[SwitchC-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0] quit
[SwitchC-ospf-1] quit
```

Switch D を設定します。

```
<SwitchD> system-view
[SwitchD] router id 4.4.4.4
[SwitchD] ospf
[SwitchD-ospf-1] area 0
[SwitchD-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[SwitchD-ospf-1-area-0.0.0.0] quit
[SwitchD-ospf-1] quit
```

Switch A の OSPF ネイバ情報を表示します。

```
[SwitchA] display ospf peer verbose

          OSPF Process 1 with Router ID 1.1.1.1
```

```
                Neighbors

 Area 0.0.0.0 interface 192.168.1.1(Vlan-interface1)'s neighbors
 Router ID: 2.2.2.2          Address: 192.168.1.2      GR State: Normal
   State: 2-Way  Mode: None  Priority: 1
   DR: 192.168.1.4  BDR: 192.168.1.3  MTU: 0
   Options is 0x02 (-|-|-|-|-|-|E|-)
   Dead timer due in 38  sec
   Neighbor is up for 00:01:31
   Authentication Sequence: [ 0 ]
   Neighbor state change count: 6
   BFD status: Disabled

 Router ID: 3.3.3.3          Address: 192.168.1.3      GR State: Normal
   State: Full  Mode: Nbr is master  Priority: 1
   DR: 192.168.1.4  BDR: 192.168.1.3  MTU: 0
   Options is 0x02 (-|-|-|-|-|-|E|-)
   Dead timer due in 31  sec
   Neighbor is up for 00:01:28
   Authentication Sequence: [ 0 ]
   Neighbor state change count: 6
   BFD status: Disabled

 Router ID: 4.4.4.4          Address: 192.168.1.4      GR State: Normal
   State: Full  Mode: Nbr is master  Priority: 1
   DR: 192.168.1.4  BDR: 192.168.1.3  MTU: 0
   Options is 0x02 (-|-|-|-|-|-|E|-)
   Dead timer due in 31  sec
   Neighbor is up for 00:01:28
   Authentication Sequence: [ 0 ]
   Neighbor state change count: 6
   BFD status: Disabled
```

出力は、Switch D が DR、Switch C が BDR であることを示します。

3) インタフェースのルータ優先順位を設定します。

Switch A を設定します。

```
[SwitchA] interface vlan-interface 1
[SwitchA-Vlan-interface1] ospf dr-priority 100
[SwitchA-Vlan-interface1] quit
```

Switch B を設定します。

```
[SwitchB] interface vlan-interface 1
[SwitchB-Vlan-interface1] ospf dr-priority 0
[SwitchB-Vlan-interface1] quit
```

Switch C を設定します。

```
[SwitchC] interface vlan-interface 1
[SwitchC-Vlan-interface1] ospf dr-priority 2
[SwitchC-Vlan-interface1] quit
```

Switch D のネイバ情報を表示します。

```
<SwitchD> display ospf peer verbose

          OSPF Process 1 with Router ID 4.4.4.4
                  Neighbors

 Area 0.0.0.0 interface 192.168.1.4(Vlan-interface1)'s neighbors
```

```
 Router ID: 1.1.1.1      Address: 192.168.1.1      GR State: Normal
   State: Full  Mode:Nbr is  slave  Priority: 100
   DR: 192.168.1.4  BDR: 192.168.1.3  MTU: 0
   Options is 0x02 (-|-|-|-|-|-|E|-)
   Dead timer due in 31  sec
   Neighbor is up for 00:11:17
   Authentication Sequence: [ 0 ]
   Neighbor state change count: 6
   BFD status: Disabled

 Router ID: 2.2.2.2      Address: 192.168.1.2      GR State: Normal
   State: Full  Mode:Nbr is  slave  Priority: 0
   DR: 192.168.1.4  BDR: 192.168.1.3  MTU: 0
   Options is 0x02 (-|-|-|-|-|-|E|-)
   Dead timer due in 35  sec
   Neighbor is up for 00:11:19
   Authentication Sequence: [ 0 ]
   Neighbor state change count: 6
   BFD status: Disabled

 Router ID: 3.3.3.3      Address: 192.168.1.3      GR State: Normal
   State: Full  Mode:Nbr is  slave  Priority: 2
   DR: 192.168.1.4  BDR: 192.168.1.3  MTU: 0
   Options is 0x02 (-|-|-|-|-|-|E|-)
   Dead timer due in 33  sec
   Neighbor is up for 00:11:15
   Authentication Sequence: [ 0 ]
   Neighbor state change count: 6
   BFD status: Disabled
```

出力は、優先順位が即座に適用されないため、DR と BDR が変更されていないことを示します。

4) OSPF プロセスを再起動します。

Switch D の OSPF プロセスを再起動します。

```
<SwitchD> reset ospf 1 process
Warning : Reset OSPF process? [Y/N]:y
```

Switch D のネイバ情報を表示します。

```
<SwitchD> display ospf peer verbose

          OSPF Process 1 with Router ID 4.4.4.4
                 Neighbors

 Area 0.0.0.0 interface 192.168.1.4(Vlan-interface1)'s neighbors
 Router ID: 1.1.1.1          Address: 192.168.1.1      GR State: Normal
   State: Full  Mode: Nbr is slave  Priority: 100
   DR: 192.168.1.1  BDR: 192.168.1.3  MTU: 0
   Options is 0x02 (-|-|-|-|-|-|E|-)
   Dead timer due in 39  sec
   Neighbor is up for 00:01:40
   Authentication Sequence: [ 0 ]
   Neighbor state change count: 6
   BFD status: Disabled

 Router ID: 2.2.2.2          Address: 192.168.1.2      GR State: Normal
   State: 2-Way  Mode: None  Priority: 0
   DR: 192.168.1.1  BDR: 192.168.1.3  MTU: 0
   Options is 0x02 (-|-|-|-|-|-|E|-)
   Dead timer due in 35  sec
   Neighbor is up for 00:01:44
   Authentication Sequence: [ 0 ]
   Neighbor state change count: 6
   BFD status: Disabled

 Router ID: 3.3.3.3          Address: 192.168.1.3      GR State: Normal
```

```
   State: Full  Mode: Nbr is slave  Priority: 2
   DR: 192.168.1.1  BDR: 192.168.1.3  MTU: 0
   Options is 0x02 (-|-|-|-|-|-|E|-)
   Dead timer due in 39  sec
   Neighbor is up for 00:01:41
   Authentication Sequence: [ 0 ]
   Neighbor state change count: 6
   BFD status: Disabled
```

出力は Switch A が DR で Switch C が bdr であることを示します。

もしネイバ状態が *full* である場合、Switch D がネイバとネイバ関係を確立しています。もしネイバ状態が *2-way* である場合、2 つの Switch は DR あるいは BDR でなく、LSA の交換が行われません。

OSPF インタフェース情報を表示します。

```
[SwitchA] display ospf interface

          OSPF Process 1 with Router ID 1.1.1.1
                  Interfaces

 Area: 0.0.0.0
 IP Address      Type       State   Cost  Pri   DR             BDR
 192.168.1.1     Broadcast  DR      1     100   192.168.1.1    192.168.1.3

[SwitchB] display ospf interface

          OSPF Process 1 with Router ID 2.2.2.2
                  Interfaces

 Area: 0.0.0.0
 IP Address      Type       State    Cost  Pri   DR             BDR
 192.168.1.2     Broadcast  DROther  1     0     192.168.1.1    192.168.1.3
```

インタフェース状態が *DR Other* である場合、インタフェースが DR あるいは BDR でないことを示します。

7.20.7 OSPF 仮想リンクの設定例

I. ネットワーク要件

図 7-14に示すように、Area2 とバックボーンエリアを接続するため、Switch B と Switch C 間で仮想リンクを設定します。設定後、Switch B が Area 2 へのルートを学習することができます。

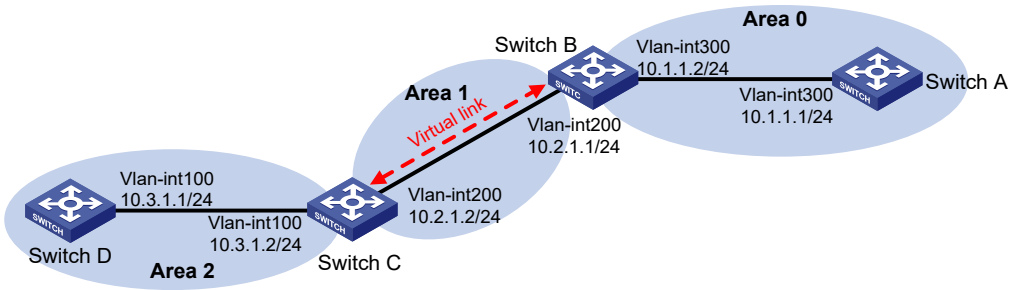


図 7-14 ネットワーク図

II. 設定手順

1) インタフェースに IP アドレスを設定します。(詳細は省略します)
2) OSPF を有効にします。

Switch A を設定します。

```
<SwitchA> system-view
[SwitchA] ospf 1 router-id 1.1.1.1
[SwitchA-ospf-1] area 0
[SwitchA-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.0] quit
[SwitchA-ospf-1] quit
```

Switch B を設定します。

```
<SwitchB> system-view
[SwitchB] ospf 1 router-id 2.2.2.2
[SwitchB-ospf-1] area 0
[SwitchB-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] quit
[SwitchB-ospf-1] area 1
[SwitchB‐ ospf-1-area-0.0.0.1] network 10.2.1.0 0.0.0.255
[SwitchB‐ ospf-1-area-0.0.0.1] quit
[SwitchB-ospf-1] quit
```

Switch C を設定します。

```
<SwitchC> system-view
[SwitchC] ospf 1 router-id 3.3.3.3
[SwitchC-ospf-1] area 1
[SwitchC-ospf-1-area-0.0.0.1] network 10.2.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.1] quit
[SwitchC-ospf-1] area 2
[SwitchC‐ ospf-1-area-0.0.0.2] network 10.3.1.0 0.0.0.255
[SwitchC‐ ospf-1-area-0.0.0.2] quit
[SwitchC-ospf-1] quit
```

Switch D を設定します。

```
<SwitchD> system-view
[SwitchD] ospf 1 router-id 4.4.4.4
```

```
[SwitchD-ospf-1] area 2
[SwitchD-ospf-1-area-0.0.0.2] network 10.3.1.0 0.0.0.255
[SwitchD-ospf-1-area-0.0.0.2] quit
[SwitchD-ospf-1] quit
```

Switch B の OSPF ルーティングテーブルを表示します。

```
[SwitchB] display ospf routing

          OSPF Process 1 with Router ID 2.2.2.2
                  Routing Table

                Topology base (MTID 0)

 Routing for network
 Destination        Cost     Type    NextHop         AdvRouter       Area
 10.2.1.0/24        2        Transit 10.2.1.1        3.3.3.3         0.0.0.1
 10.1.1.0/24        2        Transit 10.1.1.2        2.2.2.2         0.0.0.0
 Total nets: 2
 Intra area: 2  Inter area: 0  ASE: 0  NSSA: 0
```

Area 0 は Area 2 に直接接続されていないため、Switch B のルーティングテーブルに Area 2 へのルートがありません。

3) 仮想リンクを設定します。

Switch B を設定します。

```
[SwitchB] ospf
[SwitchB-ospf-1] area 1
[SwitchB-ospf-1-area-0.0.0.1] vlink-peer 3.3.3.3
[SwitchB-ospf-1-area-0.0.0.1] quit
[SwitchB-ospf-1] quit
```

Switch C を設定します。

```
[SwitchC] ospf 1
[SwitchC-ospf-1] area 1
[SwitchC-ospf-1-area-0.0.0.1] vlink-peer 2.2.2.2
[SwitchC-ospf-1-area-0.0.0.1] quit
[SwitchC-ospf-1] quit
```

Switch B の OSPF ルーティングテーブルを表示します。

```
[SwitchB] display ospf routing

          OSPF Process 1 with Router ID 2.2.2.2
                  Routing Table

                Topology base (MTID 0)

 Routing for network
 Destination        Cost     Type    NextHop         AdvRouter       Area
 10.2.1.0/24        2        Transit 10.2.1.1        3.3.3.3         0.0.0.1
 10.3.1.0/24        5        Inter   10.2.1.2        3.3.3.3         0.0.0.0
 10.1.1.0/24        2        Transit 10.1.1.2        2.2.2.2         0.0.0.0
```

```
Total nets: 3
Intra area: 2  Inter area: 1  ASE: 0  NSSA: 0
```

出力は、Switch B が Area 2 へのルート 10.3.1.0/24 を学習していることを示します。

7.20.8 OSPF GR の設定例

I. ネットワーク要件

図 7-15に示すように設定します。

- 同一 AS、同一 OSPF ルーティングドメインに属している Switch A、Switch B、Switch C は GR が有効です。
- Switch A は非 IETF GR リスタータとして動作します。Switch C、Switch C は GR ヘルパーです。GR の OOB 通信を通して Switch A と LSDB の同期化を行います。

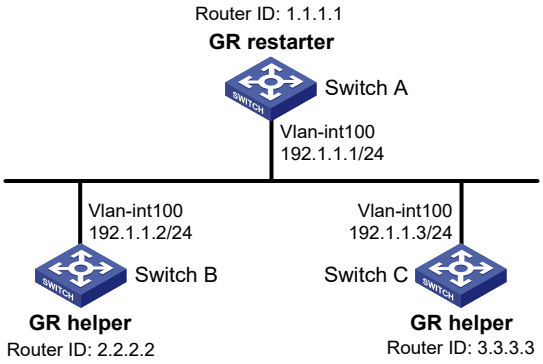


図 7-15 ネットワーク図

II. 設定手順

1) インタフェースに IP アドレスを設定します。(詳細は省略します)
2) OSPF を有効にします。

Switch A を設定します。

```
<SwitchA> system-view
[SwitchA] router id 1.1.1.1
[SwitchA] ospf 100
[SwitchA-ospf-100] area 0
[SwitchA-ospf-100-area-0.0.0.0] network 192.1.1.0 0.0.0.255
[SwitchA-ospf-100-area-0.0.0.0] quit
[SwitchA-ospf-1] quit
```

Switch B を設定します。

```
<SwitchB> system-view
[SwitchB] router id 2.2.2.2
```

```
[SwitchB] ospf 100
[SwitchB-ospf-100] area 0
[SwitchB-ospf-100-area-0.0.0.0] network 192.1.1.0 0.0.0.255
[SwitchB-ospf-100-area-0.0.0.0] quit
[SwitchB-ospf-1] quit
```

Switch C を設定します。

```
<SwitchC> system-view
[SwitchC] router id 3.3.3.3
[SwitchC] ospf 100
[SwitchC-ospf-100] area 0
[SwitchC-ospf-100-area-0.0.0.0] network 192.1.1.0 0.0.0.255
[SwitchC-ospf-100-area-0.0.0.0] quit
[SwitchC-ospf-1] quit
```

OSPF GR を設定します。

非 IETF GR リスタータとして Switch A を設定します。OSPF 100 のリンクローカルシグナリング、帯域外の再同期機能、非 IETF GR を有効にします。

```
[SwitchA-ospf-100] enable link-local-signaling
[SwitchA-ospf-100] enable out-of-band-resynchronization
[SwitchA-ospf-100] graceful-restart
[SwitchA-ospf-100] quit
```

GR ヘルパーとして Switch B を設定します。OSPF 100 のリンクローカルシグナリング、帯域外の再同期機能、非 IETF GR を有効にします。

```
[SwitchB-ospf-100] enable link-local-signaling
[SwitchB-ospf-100] enable out-of-band-resynchronization
```

GR ヘルパーとして Switch C を設定します。OSPF 100 のリンクローカルシグナリング、帯域外の再同期機能、非 IETF GR を有効にします。

```
[SwitchC-ospf-100] enable link-local-signaling
[SwitchC-ospf-100] enable out-of-band-resynchronization
```

III. 設定の確認

OSPF GR イベントのデバッグを有効にし、Switch A の GR を使用して OSPF をリスタートします。

```
<SwitchA> debugging ospf event graceful-restart
<SwitchA> terminal monitor
<SwitchA> terminal logging level 7
```

```
<SwitchA> reset ospf 100 process graceful-restart
Reset OSPF process? [Y/N]:y
%Oct 21 15:29:28:727 2011 SwitchA OSPF/5/OSPF_NBR_CHG: OSPF 100 Neighbor
192.1.1.2(Vlan-interface100) from Full to Down.
%Oct 21 15:29:28:729 2011 SwitchA OSPF/5/OSPF_NBR_CHG: OSPF 100 Neighbor
192.1.1.3(Vlan-interface100) from Full to Down.
*Oct 21 15:29:28:735 2011 SwitchA OSPF/7/DEBUG:
OSPF 100 nonstandard GR Started for OSPF Router
*Oct 21 15:29:28:735 2011 SwitchA OSPF/7/DEBUG:
OSPF 100 created GR wait timer,timeout interval is 40(s).
*Oct 21 15:29:28:735 2011 SwitchA OSPF/7/DEBUG:
OSPF 100 created GR Interval timer,timeout interval is 120(s).
*Oct 21 15:29:28:758 2011 SwitchA OSPF/7/DEBUG:
OSPF 100 created OOB Progress timer for neighbor 192.1.1.3.
*Oct 21 15:29:28:766 2011 SwitchA OSPF/7/DEBUG:
OSPF 100 created OOB Progress timer for neighbor 192.1.1.2.
%Oct 21 15:29:29:902 2011 SwitchA OSPF/5/OSPF_NBR_CHG: OSPF 100 Neighbor
192.1.1.2(Vlan-interface100) from Loading to Full.
*Oct 21 15:29:29:902 2011 SwitchA OSPF/7/DEBUG:
OSPF 100 deleted OOB Progress timer for neighbor 192.1.1.2.
%Oct 21 15:29:30:897 2011 SwitchA OSPF/5/OSPF_NBR_CHG: OSPF 100 Neighbor
192.1.1.3(Vlan-interface100) from Loading to Full.
*Oct 21 15:29:30:897 2011 SwitchA OSPF/7/DEBUG:
OSPF 100 deleted OOB Progress timer for neighbor 192.1.1.3.
*Oct 21 15:29:30:911 2011 SwitchA OSPF/7/DEBUG:
OSPF GR: Process 100 Exit Restart,Reason : DR or BDR change,for neighbor :
192.1.1.3.
*Oct 21 15:29:30:911 2011 SwitchA OSPF/7/DEBUG:
OSPF 100 deleted GR Interval timer.
*Oct 21 15:29:30:912 2011 SwitchA OSPF/7/DEBUG:
OSPF 100 deleted GR wait timer.
%Oct 21 15:29:30:920 2011 SwitchA OSPF/5/OSPF_NBR_CHG: OSPF 100 Neighbor
192.1.1.2(Vlan-interface100) from Full to Down.
%Oct 21 15:29:30:921 2011 SwitchA OSPF/5/OSPF_NBR_CHG: OSPF 100 Neighbor
192.1.1.3(Vlan-interface100) from Full to Down.
%Oct 21 15:29:33:815 2011 SwitchA OSPF/5/OSPF_NBR_CHG: OSPF 100 Neighbor
192.1.1.3(Vlan-interface100) from Loading to Full.
%Oct 21 15:29:35:578 2011 SwitchA OSPF/5/OSPF_NBR_CHG: OSPF 100 Neighbor
192.1.1.2(Vlan-interface100) from Loading to Full.
```

出力は Switch A が GR を完了したことを示します。

7.20.9 OSPF NSR の設定例

I. ネットワーク要件

図 7-16に示すように、Switch S、Switch A、および Switch B は同じ OSPF ルーティングドメインに属しています。Switch S でアクティブ/スタンバイスイッチオーバーが発生したときに正しいルーティングを保証するには、Switch S で OSPF NSR を有効にします。

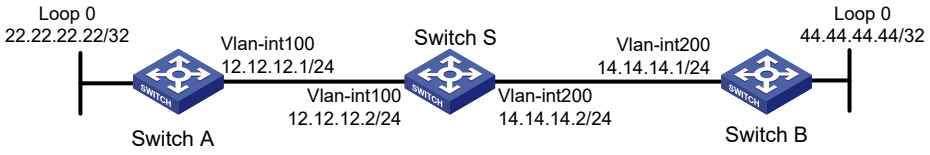


図 7-16 ネットワーク図

II. 設定手順

1) スイッチのインタフェースの IP アドレスとサブネットマスクを設定します。(詳細は表示されていません。)
2) スイッチで OSPF を設定して、次のことを確認します。(詳細は表示されていません。)
   - Switch S、Switch A、および Switch B は、レイヤ 3 で相互に通信できます。
   - 動的ルート更新は、OSPF を使用してそれらの間で実装できます。
3) Switch S で OSPF NSR を有効にします。

```
<SwitchS> system-view
[SwitchS] ospf 100
[SwitchS-ospf-100] non-stop-routing
[SwitchS-ospf-100] quit
```

III. 設定の確認

Switch S でアクティブ/スタンバイスイッチオーバーを実行します。

```
[SwitchS] placement reoptimize
Predicted changes to the placement
Program                              Current location       New location
-------------------------------------------------------------------------
rib                                  0/0                    0/0
staticroute                          0/0                    0/0
ospf                                 0/0                    0/0
Continue? [y/n]:y
Re-optimization of the placement start. You will be notified on completion
Re-optimization of the placement complete. Use 'display placement' to view the
new placement
```

スイッチオーバー期間中、Switch A の OSPF ネイバを表示して、Switch A と Switch S の間のネイバ関係を確認します。

```
<SwitchA> display ospf peer

          OSPF Process 1 with Router ID 2.2.2.1
               Neighbor Brief Information

 Area: 0.0.0.0
 Router ID       Address         Pri Dead-Time  State             Interface
 3.3.3.1         12.12.12.2      1   37         Full/BDR          Vlan100
```

Switch A の OSPF ルートを表示して、Switch A に Switch B のループバックインタフェースへのルートがあるかどうかを確認します。

```
<SwitchA> display ospf routing

          OSPF Process 1 with Router ID 2.2.2.1
                   Routing Table

                Topology base (MTID 0)
```

```
Routing for network
Destination         Cost     Type    NextHop         AdvRouter       Area
44.44.44.44/32      2        Stub    12.12.12.2      4.4.4.1         0.0.0.0
14.14.14.0/24       2        Transit 12.12.12.2      4.4.4.1         0.0.0.0
22.22.22.22/32      0        Stub    22.22.22.22     2.2.2.1         0.0.0.0
12.12.12.0/24       1        Transit 12.12.12.1      2.2.2.1         0.0.0.0

Total nets: 4
Intra area: 4  Inter area: 0  ASE: 0  NSSA: 0
```

Switch B の OSPF ネイバを表示して、Switch B と Switch S の間のネイバ関係を確認します。

```
<SwitchB> display ospf peer

          OSPF Process 1 with Router ID 4.4.4.1
               Neighbor Brief Information

Area: 0.0.0.0
Router ID       Address          Pri Dead-Time  State             Interface
3.3.3.1         14.14.14.2       1   39         Full/BDR          Vlan200
```

Switch B の OSPF ルートを表示して、Switch B に Switch A のループバックインタフェースへのルートがあるかどうかを確認します。

```
<SwitchB> display ospf routing

          OSPF Process 1 with Router ID 4.4.4.1
                   Routing Table

                Topology base (MTID 0)

Routing for network
Destination         Cost     Type    NextHop         AdvRouter       Area
44.44.44.44/32      0        Stub    44.44.44.44     4.4.4.1         0.0.0.0
14.14.14.0/24       1        Transit 14.14.14.1      4.4.4.1         0.0.0.0
22.22.22.22/32      2        Stub    14.14.14.2      2.2.2.1         0.0.0.0
12.12.12.0/24       2        Transit 14.14.14.2      2.2.2.1         0.0.0.0

Total nets: 4
Intra area: 4  Inter area: 0  ASE: 0  NSSA: 0
```

Switch S でアクティブ/スタンバイスイッチオーバーが発生した場合の出力は、次のとおりです。

- Switch A および Switch B のネイバ関係およびルーティング情報は変更されていません。
- Switch A から Switch B へのトラフィックは影響を受けていません。

7.20.10 OSPF での BFD の設定例

I. ネットワーク要件

図 7-17に示すようにネットワークレイヤで互いに通信できるように Switch A、Switch B、Switch C で OSPF を動作させます。

- レイヤ 2 スイッチを経由した Switch A と Switch B のリンクが故障したとき、BFD が故障を早急に検出し、OSPF に通知します。
- Switch A、Switch B は Switch C を通して通信します。

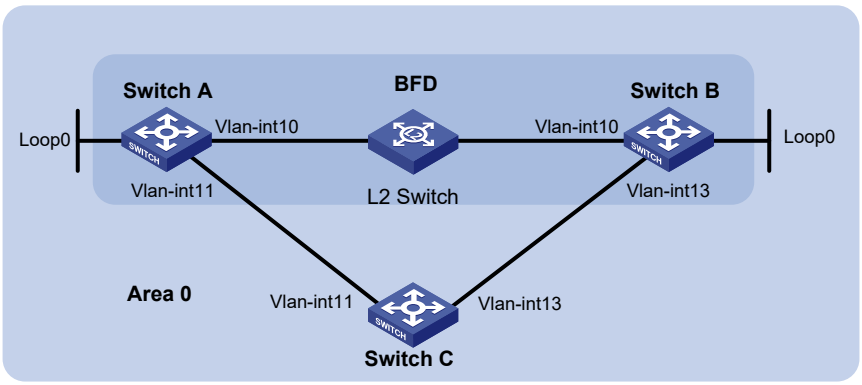


図 7-17 ネットワーク図

表 7-1 インタフェースと IP アドレスの割り当て

装置	インタフェース	IP アドレス
Switch A	Vlan-int10	192.168.0.102/24
Switch A	Vlan-int11	10.1.1.102/24
Switch A	Loop0	121.1.1.1/32
Switch B	Vlan-int10	192.168.0.100/24
Switch B	Vlan-int13	13.1.1.1/24
Switch B	Loop0	120.1.1.1/32
Switch C	Vlan-int11	10.1.1.100/24
Switch C	Vlan-int13	13.1.1.2/24

II. 設定手順

1)　インタフェースに IP アドレスを設定します。(詳細は省略します)
2)　OSPF を有効にします。

Switch A を設定します。

```
<SwitchA> system-view
[SwitchA] ospf
[SwitchA-ospf-1] area 0
[SwitchA-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.0] network 121.1.1.1 0.0.0.0
[SwitchA-ospf-1-area-0.0.0.0] quit
[SwitchA-ospf-1] quit
```

Switch B を設定します。

```
<SwitchB> system-view
[SwitchB] ospf
[SwitchB-ospf-1] area 0
```

```
[SwitchB-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] network 13.1.1.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] network 120.1.1.1 0.0.0.0
[SwitchB-ospf-1-area-0.0.0.0] quit
[SwitchB-ospf-1] quit
```

Switch C を設定します。

```
<SwitchC> system-view
[SwitchC] ospf
[SwitchC-ospf-1] area 0
[SwitchC-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0] network 13.1.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0] quit
[SwitchC-ospf-1] quit
```

3) BFD を設定します。

Switch A で BFD を有効にし、パラメータを設定します。

```
[SwitchA] bfd session init-mode active
[SwitchA] interface vlan-interface 10
[SwitchA-Vlan-interface10] ospf bfd enable
[SwitchA-Vlan-interface10] bfd min-transmit-interval 500
[SwitchA-Vlan-interface10] bfd min-receive-interval 500
[SwitchA-Vlan-interface10] bfd detect-multiplier 7
[SwitchA-Vlan-interface10] quit
```

Switch B で BFD を有効にし、パラメータを設定します。

```
[SwitchB] bfd session init-mode active
[SwitchB] interface vlan-interface 10
[SwitchB-Vlan-interface10] ospf bfd enable
[SwitchB-Vlan-interface10] bfd min-transmit-interval 500
[SwitchB-Vlan-interface10] bfd min-receive-interval 500
[SwitchB-Vlan-interface10] bfd detect-multiplier 6
[SwitchB-Vlan-interface10] quit
```

III. 設定の確認

Switch A の BFD 情報を表示します。

```
<SwitchA> display bfd session

 Total Session Num: 1     Up Session Num: 1     Init Mode: Active
```

```
 IPv4 Session Working Under Ctrl Mode:

 LD/RD          SourceAddr      DestAddr        State    Holdtime    Interface
 3/1            192.168.0.102   192.168.0.100   Up       1700ms      Vlan10
```

Switch A で宛先 120.1.1.1/32 のルートを表示します。

```
<SwitchA> display ip routing-table 120.1.1.1 verbose

Summary Count : 1

Destination: 120.1.1.1/32
   Protocol: O_INTRA
 Process ID: 1
  SubProtID: 0x1                  Age: 04h20m37s
       Cost: 1               Preference: 10
      IpPre: N/A             QosLocalID: N/A
        Tag: 0                    State: Active Adv
  OrigTblID: 0x0                OrigVrf: default-vrf
    TableID: 0x2                 OrigAs: 0
      NibID: 0x26000002          LastAs: 0
     AttrID: 0xffffffff        Neighbor: 0.0.0.0
      Flags: 0x1008c         OrigNextHop: 192.168.0.100
      Label: NULL            RealNextHop: 192.168.0.100
    BkLabel: NULL              BkNextHop: N/A
  Tunnel ID: Invalid           Interface: Vlan-interface10
BkTunnel ID: Invalid         BkInterface: N/A
   FtnIndex: 0x0             TrafficIndex: N/A
  Connector: N/A                  PathID: 0x0
```

出力は、Switch A は VLAN インタフェース 10 を通して Switch B と通信していることを示します。

そして VLAN インタフェース 10 が故障します。

Switch A で宛先 120.1.1.1/32 のルートを表示します。

```
<SwitchA> display ip routing-table 120.1.1.1 verbose

Summary Count : 1

Destination: 120.1.1.1/32
   Protocol: O_INTRA
 Process ID: 1
  SubProtID: 0x1                  Age: 04h20m37s
       Cost: 2               Preference: 10
      IpPre: N/A             QosLocalID: N/A
        Tag: 0                    State: Active Adv
  OrigTblID: 0x0                OrigVrf: default-vrf
    TableID: 0x2                 OrigAs: 0
      NibID: 0x26000002          LastAs: 0
     AttrID: 0xffffffff        Neighbor: 0.0.0.0
      Flags: 0x1008c         OrigNextHop: 10.1.1.100
      Label: NULL            RealNextHop: 10.1.1.100
    BkLabel: NULL              BkNextHop: N/A
  Tunnel ID: Invalid           Interface: Vlan-interface11
BkTunnel ID: Invalid         BkInterface: N/A
   FtnIndex: 0x0             TrafficIndex: N/A
  Connector: N/A                  PathID: 0x0
```

出力は、Switch A は VLAN インタフェース 11 を通して Switch B と通信していることを示します。

7.20.11 OSPF FRR の設定例

I. ネットワーク要件

図 7-18では、Switch A、Switch B、および Switch C が同じ OSPF ドメインに存在しています。 設定 OSPF FRR。これにより、Switch A と SwitchB 間のリンクに障害が発生した場合、トラフィックは即座にリンク B に切り替えられます。

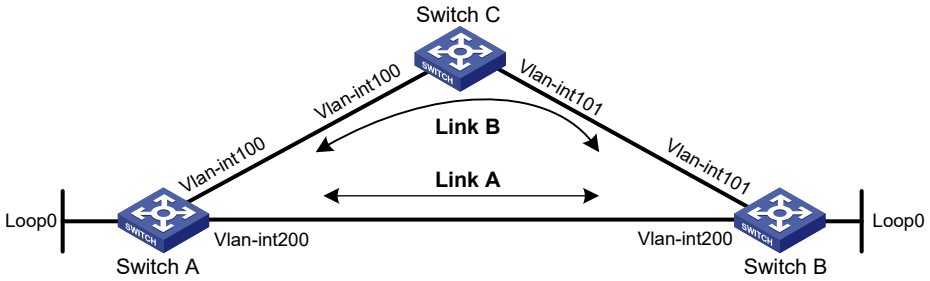


図 7-18 ネットワーク図

表 7-2 インタフェースと IP アドレスの割り当て

装置	インタフェース	IP アドレス
Switch A	Vlan-int100	12.12.12.1/24
Switch A	Vlan-int200	13.13.13.1/24
Switch A	Loop0	1.1.1.1/32
Switch B	Vlan-int101	24.24.24.4/24
Switch B	Vlan-int200	13.13.13.2/24
Switch B	Loop0	4.4.4.4/32
Switch C	Vlan-int100	12.12.12.2/24
Switch C	Vlan-int101	24.24.24.2/24

II. 設定手順

1) Switch 上のインタフェースの設定 IP アドレスとシーバマスク。 (詳細は表示されません。)
2) Switch 上の設定 OSPF を使用して、Switch A、Switch B、および Switch C がネットワークレイヤで相互に通信できるようにします。 (詳細は表示されません。)
3) バックアップネクストホップを自動的に計算する設定 OSPF FRR:

OSPF FRR では、LFA アルゴリズムを使用してバックアップネクストホップを計算するか、ルーティングポリシーを使用してバックアップネクストホップを指定できます。

- (方法 1.) LFA アルゴリズムを使用して、OSPF FRR がバックアップネクストホップを計算できるようにします。

```
<SwitchA> system-view
[SwitchA] ospf 1
[SwitchA-ospf-1] fast-reroute lfa
```

```
[SwitchA-ospf-1] quit
```

Switch B を設定します。

```
<SwitchB> system-view
[SwitchB] ospf 1
[SwitchB-ospf-1] fast-reroute lfa
[SwitchB-ospf-1] quit
```

- (方法 2.) ルーティングポリシーを使用して、OSPF FRR がバックアップネクストホップを指定できるようにします。

Switch A を設定します。

```
<SwitchA> system-view
[SwitchA] ip prefix-list abc index 10 permit 4.4.4.4 32
[SwitchA] route-policy frr permit node 10
[SwitchA-route-policy-frr-10] if-match ip address prefix-list abc
[SwitchA-route-policy-frr-10] apply fast-reroute backup-interface vlan-interface 100 backup-nexthop 12.12.12.2
[SwitchA-route-policy-frr-10] quit
[SwitchA] ospf 1
[SwitchA-ospf-1] fast-reroute route-policy frr
[SwitchA-ospf-1] quit
```

Switch B を設定します。

```
<SwitchB> system-view
[SwitchB] ip prefix-list abc index 10 permit 1.1.1.1 32
[SwitchB] route-policy frr permit node 10
[SwitchB-route-policy-frr-10] if-match ip address prefix-list abc
[SwitchB-route-policy-frr-10] apply fast-reroute backup-interface vlan-interface 101 backup-nexthop 24.24.24.2
[SwitchB-route-policy-frr-10] quit
[SwitchB] ospf 1
[SwitchB-ospf-1] fast-reroute route-policy frr
[SwitchB-ospf-1] quit
```

III. 設定の確認

Switch A のルート 4.4.4.4/32 を表示して、バックアップネクストホップ情報を表示します。

```
[SwitchA] display ip routing-table 4.4.4.4 verbose

Summary Count : 1
```

```
Destination: 4.4.4.4/32
   Protocol: O_INTRA
 Process ID: 1
  SubProtID: 0x1                    Age: 04h20m37s
       Cost: 1                Preference: 10
      IpPre: N/A              QosLocalID: N/A
        Tag: 0                     State: Active Adv
  OrigTblID: 0x0                OrigVrf: default-vrf
    TableID: 0x2                 OrigAs: 0
      NibID: 0x26000002          LastAs: 0
     AttrID: 0xffffffff        Neighbor: 0.0.0.0
      Flags: 0x1008c         OrigNextHop: 13.13.13.2
      Label: NULL            RealNextHop: 13.13.13.2
    BkLabel: NULL              BkNextHop: 12.12.12.2
  Tunnel ID: Invalid           Interface: Vlan-interface200
BkTunnel ID: Invalid         BkInterface: Vlan-interface100
   FtnIndex: 0x0            TrafficIndex: N/A
  Connector: N/A                 PathID: 0x0
```

Switch B のルート 1.1.1.1/32 を表示して、バックアップネクストホップ情報を表示します。

```
[SwitchB] display ip routing-table 1.1.1.1 verbose

Summary Count : 1

Destination: 1.1.1.1/32
   Protocol: O_INTRA
 Process ID: 1
  SubProtID: 0x1                    Age: 04h20m37s
       Cost: 1                Preference: 10
      IpPre: N/A              QosLocalID: N/A
        Tag: 0                     State: Active Adv
  OrigTblID: 0x0                OrigVrf: default-vrf
    TableID: 0x2                 OrigAs: 0
      NibID: 0x26000002          LastAs: 0
     AttrID: 0xffffffff        Neighbor: 0.0.0.0
      Flags: 0x1008c         OrigNextHop: 13.13.13.1
      Label: NULL            RealNextHop: 13.13.13.1
    BkLabel: NULL              BkNextHop: 24.24.24.2
  Tunnel ID: Invalid           Interface: Vlan-interface200
BkTunnel ID: Invalid         BkInterface: Vlan-interface101
   FtnIndex: 0x0            TrafficIndex: N/A
  Connector: N/A                 PathID: 0x0
```

7.21 OSPFのトラブルシューティング

7.21.1 OSPF のネイバ関係が構築されない

I. 症状

OSPF のネイバ関係が確立されません。

II. 分析

物理リンクおよび下位のレイヤプロトコルが正常に動作しているときは、インタフェースに設定されているOSPFパラメータを確認してください。ネイバノード同士は、エリア ID、ネットワークセグメントおよびマスク (P2P、仮想リンクはネットワークセグメントおよびマスクが異なることがあります)、ネットワーク タイプなどのパラメータが同じでなければなりません。

III. 解決策

1) **display ospf peer** コマンドで OSPF ネイバ情報を表示してください。
2) **display ospf interface** コマンドで OSPF インタフェース情報を表示してください。
3) ネイバルータの IP アドレスに **ping** を送信して接続を確認してください。
4) OSPF タイマをチェックしてください。インタフェースでは、dead 間隔は少なくとも hello 間隔の 4 倍にしてください。
5) NBMA ネットワークでは、**peer ip-address** コマンドでネイバノードを手動で指定することが必要です。
6) Broadcast または NBMA ネットワークでは、接続している少なくとも 1 つのインタフェースのルータ優先順位は 0 より大きくなければなりません。
7) 問題が解決しない場合、NEC に問い合わせてください。

7.22 ルーティング情報の誤り

I. 症状

OSPF が他のエリアへのルートを検出できません。

II. 分析

バックボーンエリアは、他のすべてのエリアとの接続を保持しなければなりません。1 台のルータが複数のエリアに接続している場合、少なくとも 1 つのエリアはバックボーンに接続されていなければなりません。バックボーンエリアはスタブエリアとしては設定できません。

スタブエリアでは、全部のルータが外部ルートを受信できるわけではなく、スタブエリアに接続しているインタフェースはすべて、スタブエリアに所属しなければなりません。

III. 解決策

1) **display ospf peer** コマンドでネイバルータを表示してください。
2) **display ospf interface** コマンドで OSPF インタフェース情報を表示してください。
3) **display ospf lsdb** コマンド LSDB を確認してください。
4) **display current-configuration configuration ospf** コマンドでエリア設定に関する情報を表示してください。2 つ以上のエリアが設定されている場合は、少なくとも 1 つのエリアをバックボーンに接続してください。
5) スタブエリアでは、所属しているルータはすべて、**stub** コマンドで設定してください。NSSA エリアでは、接続しているインタフェースはすべて、**nssa** コマンドで設定してください。
6) 仮想リンクが設定されている場合は、**display ospf vlink** コマンドで仮想リンクの状態をチェックしてください。
7) 問題が解決しない場合、NEC に問い合わせてください。

目次

このセクションのページは**5-x-x** です。

8章 ポリシーベースルーティング 8-1
8.1 概要 8-1
8.1.1 パケット転送プロセス 8-1
8.1.2 PBRのタイプ 8-1
8.1.3 ポリシー 8-1
8.1.4 PBRとTrack 8-2
8.2 PBR設定作業リスト 8-2
8.3 ポリシーの設定 8-3
8.3.1 ノードの作成 8-3
8.3.2 ノードのマッチ条件の設定 8-3
8.3.3 ノードのアクション設定 8-3
8.4 PBRのポリシーの指定 8-4
8.4.1 ローカルPBRのポリシーの指定 8-4
8.4.2 インタフェースPBRのポリシーの指定 8-4
8.5 PBRの表示と維持 8-5
8.6 PBRの設定例 8-5
8.6.1 パケットベースのローカルPBRの設定例 8-5
8.6.2 パケットベースのインタフェースPBRの設定例 8-7

8章 ポリシーベースルーティング

8.1 概要

ポリシーベースルーティング(PBR) は、ユーザが定義したルーティングポリシーに従ったルーティングメカニズムです。ポリシーは ACL で指定した条件にマッチしているパケットのネクストホップを指定することができます。

8.1.1 パケット転送プロセス

装置は以下のように受信したパケットを転送します。

1) 装置はマッチしているパケットを転送するため、PBR を使用します。
2) 以下のいずれかのイベントが発生した場合、装置はデフォルトルートを除いて、ルーティングテーブルを使用してパケットを転送します。
   - PBR ポリシーにマッチしません。
   - PBR をもとにしたパケットの転送に失敗しました。
3) パケット転送に失敗した場合、装置はデフォルトルートを使用してパケットを転送します。

8.1.2 PBR のタイプ

PBR はローカル PBR とインタフェース PBR の 2 種類があります。

- **ローカル PBR**－**ping** コマンドの ICMP パケットのような、ローカルで作成されたパケットの転送に適用されます。
- **インタフェース PBR**－インタフェースに転送されるパケットに対して適用されます。

8.1.3 ポリシー

ポリシーは、マッチ条件と、マッチしたパケットへのアクションから構成されます。ポリシーは 1 つ以上のノードから構成されます。

- ノードはノード番号によって指定されます。最も小さいノード番号が最も高い優先度となります。
- ノードは **if-match** と **apply** から構成されます。**if-match** でノードにマッチする条件を指定し、**apply** でアクションを適用します。
- ノードは **permit** や **deny** のモードがあります。

ポリシーは、パケットを順番にマッチさせます。もしパケットがノードのマッチ条件に適合する場合、ノードのアクションが適用されます。マッチ条件に適合しない場合、次のノードのマッチ条件と適合の確認を行います。いずれのノードのマッチ条件に適合しない場合、ルーティングテーブルに従って転送されます。

I. if-match

PBR は ACL にマッチする **if-match acl** のみをサポートします。ノードの各タイプの **if-match acl** は、1 つのみ指定することができます。

II. apply

PBR は、ネクストホップを設定するための **apply next-hop** のみをサポートします。

III. ノードのマッチモードの関係

すべての **if-match** にパケットが適合するか？	マッチモード	
	許可モード	**拒否モード**
Yes	• ノードに **apply** が設定されている場合、PBR は **apply** を実行します。 　○ PBR がパケットの転送に成功した場合、PBR は次のノードとマッチしません。 • ノードに **apply** が設定されていない場合、パケットはルーティングテーブルに従って転送されます。	パケットはルーティングテーブルに従って転送されます。
No	PBRは次のノードにパケットを移動します。	PBRは次のノードにパケットを移動します。

🕮 **メモ：**

if-match がないノードは、すべてのパケットにマッチします。

8.1.4 PBR と Track

PBR は **apply** の有効な状態を track されたネクストホップのリンク状態にダイナミックに適応するため、Track 機能と一緒に動作することができます。

- Track エントリが **Negative** に変更するオブジェクトに関連づけられているとき、apply は無効です。
- Track エントリが **Positive** あるいは **NotReady** に変更するオブジェクトに関連づけられているとき、**apply** は有効です。

Track と PBR の関連づけの詳細はオペレーションマニュアルのセクション 10 *高可用性*”*Track*”を参照してください。

8.2 PBR設定作業リスト

作業リスト
(必須設定項目) ポリシーの設定 1．ノードの作成 2．ノードのマッチ条件の設定 3．ノードのアクションの設定
(必須設定項目) PBRのポリシーの指定 必要に応じて以下の作業を選択してください。 • ローカル PBR のポリシーの指定 • インタフェース PBR のポリシーの指定

8.3 ポリシーの設定

8.3.1 ノードの作成

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. ノードを作成し、policy node view に移行する	**policy-based-route** *policy-name* [**deny** | **permit**] **node** *node-number*	ー

8.3.2 ノードのマッチ条件の設定

I. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. policy node view に移行する	**policy-based-route** *policy-name* [**deny** | **permit**] **node** *node-number*	ー
3. ACL のマッチ条件を設定する	**if-match acl** { *acl-number* | **name** *acl-name* }	デフォルト：設定なし ACLのマッチ条件はレイヤ2情報にマッチすることができません。 ACLマッチ条件は**permit**あるいは**deny**アクションを使用することができません。またACLを使用してタイムレンジを使用することができません。

8.3.3 ノードのアクション設定

I. 適用句について

ノードのパケットに一致するため、**apply next-hop** をネクストホップに設定することができます。

II. 制限とガイドライン

発信 PBR の場合は、ネクストホップを 1 つだけ指定できます。ネクストホップは直接接続する必要があります。

ネクストホップまたはデフォルトネクストホップを指定すると、PBR は定期的に FIB テーブルのルックアップを実行して、その可用性を判断します。一時的なサービス中断は、PBR がその可用性ステータスの変更後すぐにルートを更新しない場合に発生する可能性があります。

III. パケット転送を指示するためのアクションの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. policy node view に移行する	**policy-based-route** *policy-name* [**deny** | **permit**] **node** *node-number*	ー
3. ネクストホップを設定する	**apply next-hop** [**vpn-instance** *vpn-instance-name*] { *ip-address* [**direct**] [**track** *track-entry-number*] }&<1-2>	デフォルト : ネクストホップは指定されません。 バックアップあるいはロードバランスに、このステップを複数実行することで最大2つのネクストホップを設定することができます。

8.4 PBRのポリシーの指定

8.4.1 ローカル PBR のポリシーの指定

I. ローカル PBR

ローカルにポリシーを適用することで PBR を設定します。PBR はローカルに作成されたパケットの転送を行うため、ポリシーを使用します。

II. 制限とガイドライン

指定されるポリシーはすでに作成されている必要があります。新しいポリシーを適用する前に、現在のポリシーを削除する必要があります。

ローカル PBR は ping や Telnet のようなローカルサービスに適用します。装置のローカルサービスに与える影響を十分に理解したうえで設定してください。

III. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. ローカルに PBR を適用する	**ip local policy-based-route** *policy-name*	デフォルト：設定なし

8.4.2 インタフェース PBR のポリシーの指定

I. インタフェース PBR

インタフェースにポリシーを適用することで PBR を設定します。PBR はインタフェースで受信されたパケットの転送を処理するポリシーを使用します。

II. 制限とガイドライン

指定されるポリシーはすでに作成されている必要があります。インタフェースには 1 つのポリシーのみ適用することができます。新しいポリシーを適用する前にインタフェースから現在のポリシーを削除してください。

複数のインタフェースで同じポリシーを適用することができます。

III. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. interface view に移行する	**interface** *interface-type interface-number*	ー
3. インタフェースに PBR を適用する	**ip policy-based-route** *policy-name*	デフォルト：設定なし

8.5 PBRの表示と維持

すべての view で **display** コマンドを実行し、user view で **reset** コマンドを実行します。

操作	コマンド
PBRポリシー情報を表示する	**display ip policy-based-route** [**policy** *policy-name*]
インタフェースPBRと統計情報を表示する	**display ip policy-based-route interface** *interface-type interface-number* [**slot** *slot-number*]
PBR設定を表示する	**display ip policy-based-route setup**
PBRの統計情報を削除する	**reset ip policy-based-route statistics** [**policy** *policy-name*]

8.6 PBRの設定例

8.6.1 パケットベースのローカル PBR の設定例

I. ネットワーク要件

図 8-1に示すように、Switch A ですべての TCP パケットをネクストホップ 1.1.2.2 に転送します。他のパケットはルーティングテーブルに従って転送します。

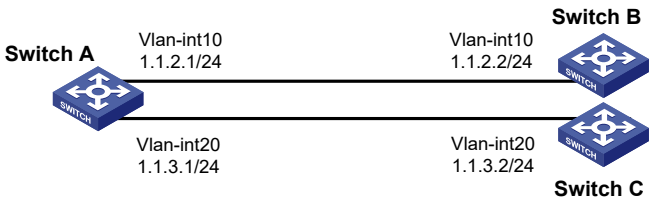


図 8-1 ネットワーク図

II. 設定手順

1)　Switch A を設定します。

VLAN10、VLAN20 を作成します。

```
<SwitchA> system-view
[SwitchA] vlan 10
[SwitchA-vlan10] quit
[SwitchA] vlan 20
[SwitchA-vlan20] quit
```

VLAN インタフェース 10、VLAN インタフェース 20 の IP アドレスを設定します。

```
[SwitchA] interface vlan-interface 10
[SwitchA-Vlan-interface10] ip address 1.1.2.1 24
[SwitchA-Vlan-interface10] quit
[SwitchA] interface vlan-interface 20
[SwitchA-Vlan-interface20] ip address 1.1.3.1 24
[SwitchA-Vlan-interface20] quit
```

TCP パケットにマッチする ACL 3101 を設定します。

```
[SwitchA] acl advanced 3101
[SwitchA-acl-ipv4-adv-3101] rule permit tcp
[SwitchA-acl-ipv4-adv-3101] quit
```

TCP パケットをネクストホップ 1.1.2.2 に転送するポリシー**aaa** のノード 5 を設定します。

```
[SwitchA] policy-based-route aaa permit node 5
[SwitchA-pbr-aaa-5] if-match acl 3101
[SwitchA-pbr-aaa-5] apply next-hop 1.1.2.2
[SwitchA-pbr-aaa-5] quit
```

Switch A にポリシー**aaa** を適用するようにローカル PBR を設定します。

```
[SwitchA] ip local policy-based-route aaa
```

2)　Switch B を設定します。

VLAN 10 を作成します。

```
<SwitchB> system-view
[SwitchB] vlan 10
[SwitchB-vlan10] quit
```

VLAN インタフェース 10 の IP アドレスを設定します。

```
[SwitchB] interface vlan-interface 10
[SwitchB-Vlan-interface10] ip address 1.1.2.2 24
```

3) Switch C を設定します。

VLAN 20 を作成します。

```
<SwitchC> system-view
[SwitchC] vlan 20
[SwitchC-vlan20] quit
```

VLAN インタフェース 20 の IP アドレスを設定します。

```
[SwitchC] interface vlan-interface 20
[SwitchC-Vlan-interface20] ip address 1.1.3.2 24
```

III. 設定の確認

Switch A 上で Switch B に Telnet を行います。Telnet は成功します。（詳細は省略します。）

Switch A 上で Switch C に Telnet を行います。Telnet は失敗します。（詳細は省略します。）

Switch A から Switch C に ping を行います。ping は成功します。（詳細は省略します。）

Telnet は TCP を使用し、ping は ICMP を使用します。結果を以下に示します。

- Switch A からのすべての TCP パケットはネクストホップ 1.1.2.2 に転送されます。
- 他のパケットは VLAN インタフェース 20 に従って転送されます。
- ローカル PBR の設定が有効です。

8.6.2 パケットベースのインタフェース PBR の設定例

I. ネットワーク要件

図 8-2に示すように、Switch A で、VLAN インタフェース 11 で受信されたすべての TCP パケットをネクストホップ 1.1.2.2 に転送します。他のパケットはルーティングテーブルに従って転送します。

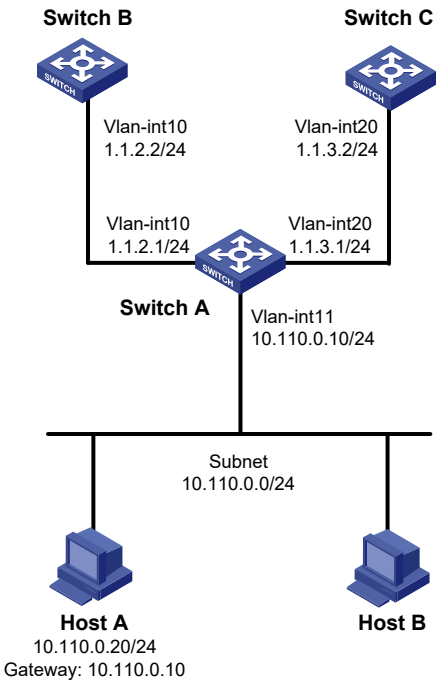


図 8-2 ネットワーク図

II. 設定手順

1) Switch B と Switch C が Host A に到達できることを確認してください。(詳細は省略します。)
2) Switch A を設定します。

VLAN10、VLAN20 を作成します。

```
<SwitchA> system-view
[SwitchA] vlan 10
[SwitchA-vlan10] quit
[SwitchA] vlan 20
[SwitchA-vlan20] quit
```

VLAN インタフェース 10、VLAN インタフェース 20 の IP アドレスを設定します。

```
[SwitchA] interface vlan-interface 10
[SwitchA-Vlan-interface10] ip address 1.1.2.1 24
[SwitchA-Vlan-interface10] quit
[SwitchA] interface vlan-interface 20
[SwitchA-Vlan-interface20] ip address 1.1.3.1 24
[SwitchA-Vlan-interface20] quit
```

TCP パケットにマッチする ACL 3101 を設定します。

```
[SwitchA] acl advanced 3101
[SwitchA-acl-ipv4-adv-3101] rule permit tcp
[SwitchA-acl-ipv4-adv-3101] quit
```

TCP パケットをネクストホップ 1.1.2.2 に転送するポリシー**aaa** のノード 5 を設定します。

```
[SwitchA] policy-based-route aaa permit node 5
[SwitchA-pbr-aaa-5] if-match acl 3101
[SwitchA-pbr-aaa-5] apply next-hop 1.1.2.2
[SwitchA-pbr-aaa-5] quit
```

VLAN インタフェース 11 にポリシー**aaa** を適用するようにインタフェース PBR を設定します。

```
[SwitchA] interface vlan-interface 11
[SwitchA-Vlan-interface11] ip address 10.110.0.10 24
[SwitchA-Vlan-interface11] ip policy-based-route aaa
[SwitchA-Vlan-interface11] quit
```

III. 設定の確認

Host A から Switch A に直接接続されている Switch B に Telnet を行います。Telnet は成功します。（詳細は省略します。）

Host A から Switch A に直接接続されている Switch C に Telnet を行います。Telnet は失敗します。（詳細は省略します。）

Host A から Switch C に ping を実行します。ping は成功します。（詳細は省略します。）

Telnet は TCP を使用し、ping は ICMP を使用しています。結果を以下に示します。

- Switch A の VLAN インタフェース 11 に到着するすべての TCP パケットは、ネクストホップ 1.1.2.2 に転送されます。
- 他のパケットは VLAN インタフェース 20 に転送されます。
- インタフェース PBR の設定が有効です。

目次

このセクションのページは **5-x-x** です。

9 章 RIPng 9-1
9.1 概要 9-1
9.1.1 RIPng ルーティングメトリック 9-1
9.1.2 RIPng ルートエントリ 9-1
9.1.3 RIPng パケットと配信 9-1
9.1.4 プロトコルと標準 9-2
9.2 RIPng 設定作業リスト 9-2
9.3 RIPng の基本設定 9-2
9.4 RIPng ルート制御の設定 9-3
9.4.1 ルーティングメトリックの追加設定 9-3
9.4.2 RIPng ルート集約の設定 9-3
9.4.3 デフォルトルートの配信 9-4
9.4.4 送受信/再配信ルートのフィルタリングの設定 9-4
9.4.5 RIPng の優先順位の設定 9-5
9.4.6 RIPng ルートの再配信の設定 9-5
9.5 RIPng ネットワークの調整と最適化 9-5
9.5.1 RIPng タイマの設定 9-5
9.5.2 スプリットホライズンとポイズンリバースの設定 9-6
9.5.3 ECMP ルートの最大数の設定 9-7
9.5.4 RIPng パケット送信レートの設定 9-7
9.6 RIPng GR の設定 9-7
9.7 RIPng NSR の設定 9-8
9.8 RIPng のセキュリティ機能の拡張 9-9
9.8.1 RIPng パケットのゼロフィールドチェック機能の有効化 9-9
9.9 RIPng の表示と維持 9-9
9.10 RIPng 設定例 9-10
9.10.1 RIPng の基本機能の設定例 9-10
9.10.2 RIPng ルート再配信の設定例 9-12
9.10.3 RIPng GR の設定例 9-15
9.10.4 RIPng NSR の設定例 9-16

9章 RIPng

9.1 概要

RIPng(Routing Information Protocol next generation)は IPv6 をサポートするために RIP-2 を拡張した機能です。RIPng はディスタンスベクタのプロトコルです。UDP パケットを使用し、ポート 521 を通してルート情報を交換します。RIP の概念の多くは、RIPng に適用されます。

9.1.1 RIPng ルーティングメトリック

RIPng はホップ数を使用して宛先までの距離を測ります。ホップ数はメトリックあるいはコストです。ルータから直接接続されたネットワークへのホップ数は 0 です。ルータから直接接続されたルータへのホップ数は 1 です。16 以上のメトリック値の宛先ネットワークへは到達不能とされます。

9.1.2 RIPng ルートエントリ

RIPng はデータベースにルートエントリを記録します。各ルートエントリは以下の構成があります。

- 宛先アドレス – ホスト、もしくはネットワークの IPv6 アドレス
- ネクストホップ – ネクストホップの IPv6 アドレス
- 出力インタフェース – ルートの出力インタフェース
- メトリック – ローカルルータから宛先へのコスト
- ルートタイム – ルーティングエントリが最後に更新された時間から経過した時間。このタイムは、ルーティングエントリがアップデートされるたびに 0 にリセットされます。
- ルートタグ – ルートの識別に使用されます。柔軟なルートの管理を行うため、ルーティングポリシーで使用されます。詳細は、オペレーションマニュアルのセクション 5 *ルーティングプロトコル”ルーティングポリシー”* を参照してください。

9.1.3 RIPng パケットと配信

RIPng はルーティング情報の交換を行うため、要求パケットと応答パケットをマルチキャストします。リンクローカルルータマルチキャストアドレスとして FF02::9 とリンクローカルソースアドレスとして FE80::/10 を使用します。RIPng はルーティング情報の交換を行うため、以下のように要求パケットと応答パケットを使用します。

1) RIPng が最初、またはルーティングテーブルの複数のエントリのアップデートが必要なとき、ネイバ装置にマルチキャストリクエストパケットを送信します。
2) RIPng ネイバ装置が要求パケットを受信したとき、ローカルルーティングテーブルを含む応答パケットを送信します。RIPng は、応答パケットのルートアップデートを周期的あるいはルートの変更が行ったときに配信することができます。
3) RIPng が応答を受信した後、応答の妥当性を確認し、ルーティングテーブルに追加する前に確認します。以下のことを確認します。

- 送信元 IPv6 アドレスがリンクローカルアドレスかどうかを確認します。

- ポート番号が正しいかどうかを確認します。

4) 確認に失敗した応答パケットは廃棄されます。

9.1.4 プロトコルと標準

- RFC 2080, RIPng for IPv6
- RFC 2081, RIPng Protocol Applicability Statement

9.2 RIPng設定作業リスト

作業リスト
(必須設定項目) RIPngの基本設定
(オプション設定項目) RIPngルート制御の設定: ● ルーティングメトリックの追加設定 ● RIPngルート集約の設定 ● デフォルトルートの配信 ● 送受信ルートのフィルタリングの設定 ● RIPngの優先順位の設定 ● RIPngルートの再配信の設定
(オプション設定項目) RIPngネットワークの調整と最適化: ● RIPngタイマの設定 ● スプリットホライズンとポイズンリバースの設定 ● ECMPルートの最大数の設定 ● RIPngパケット送信レートの設定
(オプション設定項目) ● RIPng GRの設定 ● RIPng NSRの設定
(オプション設定項目) RIPngのセキュリティ機能の拡張 ● RIPngパケットのゼロフィールドチェック機能の有効化

9.3 RIPngの基本設定

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. RIPng プロセスを作成し、その view に移行する	**ripng** [*process-id*] [**vpn-instance** *vpn-instance-name*]	デフォルト：設定なし
3. system view に戻る	**quit**	ー
4. interface view に移行する	**interface** *interface-type interface-number*	ー
5. インタフェースへの RIPng を有効にする	**ripng** *process-id* **enable**	デフォルト：無効 インタフェースでRIPngが有効でない場合、インタフェースはどのRIPngも送受信しません。

9.4 RIPngルート制御の設定

9.4.1 ルーティングメトリックの追加設定

I. ルーティングメトリックの追加

ルーティングメトリック(ホップカウント)の追加は、送受信 RIPng ルートのメトリックに追加のメトリックを加えることができます。

- 送信側へのメトリックの追加は、ルーティングテーブルのルートのメトリックを変更しないで、送信ルートのメトリックにメトリックを追加します。
- 受信側へのメトリックの追加は、受信したルートがルーティングテーブルに反映される前に、受信ルートのメトリックにメトリックが追加され、受信ルートのメトリックが変更されます。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. interface view に移行する	**interface** *interface-type interface-number*	―
3. 受信側に追加するルーティングメトリックを指定する	**ripng metricin** *value*	デフォルト：0
4. 送信側に追加するルーティングメトリックを指定する	**ripng metricout** *value*	デフォルト：1

9.4.2 RIPng ルート集約の設定

I. RIPng ルート集約の設定

インタフェースにルート集約を設定し、RIPng はロンゲストマッチにもとづいて、集約ルートを配信します。

RIPng ルート集約は、ネットワークのスケーラビリティを改良し、ルーティングテーブルサイズを削減し、ルーティングテーブルの検索効率を増加させます。

RIPng はすべての明確なルートのもっとも小さいメトリックによって集約ルートを配信します。

たとえば、RIPng は、メトリック 2 のインタフェース 1:11:11:24 から配信されるルートと、メトリック 3 のインタフェース 1:11:12:34 から配信されるルートの 2 つがあると仮定します。インタフェースのルート集約を設定し、メトリック 2 の 1 つのルート 11::0/16 が作成され、配信されます。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―

操作	コマンド	補足
2． interface view に移行する	**interface** *interface-type interface-number*	―
3． 集約 IPv6 プレフィックスを配信します。	**ripng summary-address** *ipv6-address prefix-length*	デフォルト：設定なし

9.4.3 デフォルトルートの配信

I. デフォルトルートの配信

指定したコストでネイバ装置にデフォルトルートを配信することができます。

II. 設定手順

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． interface view に移行する	**interface** *interface-type interface-number*	―
3． デフォルトルートを配信する設定を有効にする	**ripng default-route** { **only** | **originate** } [**cost** *cost-value*| **route-policy** *route-policy-name*]*	デフォルト：設定なし このコマンドは、デフォルトルートがローカルのIPv6ルーティングテーブルに存在するかどうかに関係なく、デフォルトルートを指定されたインタフェースを通して配信します。

9.4.4 送受信/再配信ルートのフィルタリングの設定

I. 送受信/再配信ルートのフィルタリング

IPv6 ACL あるいは IPv6 プレフィックスリストを使用することで送受信ルートをフィルタすることができます。他のルーティングプロトコルから再配信されたルートと指定されたネイバ装置からのルートのみフィルタするように RIPng を設定することができます。

II. 設定手順

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． RIPng view に移行する	**ripng** [*process-id*] [**vpn-instance** *vpn-instance-name*]	―
3． 受信ルートのフィルタリングを設定する	**filter-policy** { *ipv6-acl-number* | **prefix-list** *prefix-list-name* } **import**	デフォルト：設定なし
4． 再配信ルートのフィルタリングを設定する	**filter-policy** { *ipv6-acl-number* | **prefix-list** *prefix-list-name* } **export** [*protocol* [*process-id*]]	デフォルト：設定なし

9.4.5 RIPng の優先順位の設定

I. RIPng の優先順位

ルーティングプロトコルは優先順位を持ちます。同じ宛先のルートで複数の IGP プロトコルが動作するとき、他のルーティングプロトコルで学習したルートよりも、RIPng ルートに高い優先順位を持たせたいとき、最適ルートの選択に影響するように、RIPng に、より小さな優先順位の値を割り当てることができます。小さな優先順位の値を持つルートが、優先されます。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. RIPng view に移行する	**ripng** [*process-id*] [**vpn-instance** *vpn-instance-name*]	―
3. RIPng の優先順位を設定する	**preference** { *preference* | **route-policy** *route-policy-name* }*	デフォルト：100

9.4.6 RIPng ルートの再配信の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. RIPng view に移行する	**ripng** [*process-id*] [**vpn-instance** *vpn-instance-name*]	―
3. 他のプロトコルからのルートを再配信するように設定する	**import-route** { **direct** | **static** } [**cost** *cost-value* | **route-policy** *route-policy-name*]* **import-route** { **isisv6** | **ospfv3** | **ripng** } [*process-id*] [**allow-direct** | **cost** *cost-value* | **route-policy** *route-policy-name*]*	デフォルト：設定なし
4. (オプション設定項目) 再配信ルートにデフォルトメトリックを設定する	**default cost** *cost*	デフォルト：0

9.5 RIPngネットワークの調整と最適化

9.5.1 RIPng タイマの設定

RIPng ネットワークの性能を最適にするため、RIPng タイマを設定することができます。

RIPng タイマを調整するとき、不必要なネットワークの増加やルート変動を避けるために RIPng が動作しているルータで、ネットワークパフォーマンスを考慮し、設定を統一する必要があります。

I.

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. RIPng view に移行する	**ripng** [*process-id*] [**vpn-instance** *vpn-instance-name*]	―
3. RIPng タイマを設定する	**timers** { **garbage-collect** *garbage-collect-value* | **suppress** *suppress-value* | **timeout** *timeout-value* | **update** *update-value* }*	デフォルト： ● update timer ： 30 秒 ● timeout timer ： 180 秒 ● suppress timer ： 120 秒 ● garbage-collect timer ：120秒

9.5.2 スプリットホライズンとポイズンリバースの設定

I. 制限とガイドライン

スプリットホライズンとポイズンリバースの設定を行う時、以下の制限とガイドラインに従ってください。

- スプリットホライズンとポイズンリバースの両方を設定した場合、ポイズンリバース機能が適用されます。
- スプリットホライズン機能は、ネイバルータ間のルーティングループを防ぐために、そのインタフェースが学習したルートを送信するのを無効化します。一般的に、ルーティングループを防ぐため、スプリットホライズンを有効にすることを推奨します。
- ポイズンリバースは、インタフェースで受信したルートをそのインタフェースに配信するのを許可しますが、それらのルートのメトリックを 16(到達不能)にします。

II. スプリットホライズンの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. interface view に移行する	**interface** *interface-type interface-number*	―
3. スプリットホライズンを有効にする	**ripng split-horizon**	デフォルト：有効

III. ポイズンリバースの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. interface view に移行する	**interface** *interface-type interface-number*	―
3. ポイズンリバースを有効にする	**ripng poison-reverse**	デフォルト：無効

9.5.3 ECMP ルートの最大数の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. RIPng view に移行する	**ripng** [*process-id*] [**vpn-instance** *vpn-instance-name*]	―
3. ECMP ルートの最大数を指定する	**maximum load-balancing** *number*	デフォルトでは、RIPng ECMP ルートの最大数はECMPルートの最大数に等しく、**max-ecmp-num**コマンドを使用して設定できます。

9.5.4 RIPng パケット送信レートの設定

このタスクを実行して、RIPng パケットを送信する間隔と、各間隔で送信できる RIPng パケットの最大数を指定します。 この機能を使用すると、過剰な RIPng パケットがシステムパフォーマンスに影響を与えたり、過剰な帯域幅を消費したりするのを防ぐことができます。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. RIPng view に移行する	**ripng** [*process-id*] [**vpn-instance** *vpn-instance-name*]	―
3. RIPng パケット送信レートの設定する	RIPng view でRIPngパケット送信レートを設定するには、次のコマンドを順番に実行します。 **ripng** [*process-id*] [**vpn-instance** *vpn-instance-name*] **output-delay** *time* **count** *count*	• デフォルトでは、インタフェースは実行するRIPngプロセスのRIPngパケット送信レートを使用します。 • デフォルトでは、RIPngプロセスを実行するインタフェースは、20ミリ秒ごとに最大3つのRIPngパケットを送信します。

9.6 RIPng GRの設定

I. RIPng GR

GR（グレースフルリスタート）は、ルーティングプロトコルの再起動あるいはアクティブ/スタンバイの切り替えが発生したときでも、パケット転送を継続することができます。

GR 機能を動作させるには 2 台のルータが必要です。GR のルータは以下の役割があります。

- **GR リスタータ ―** グレースフルリスタートルータです。GR 機能を持ちます。
- **GR ヘルパー ―** GR リスタータのネイバ装置です。GR プロセスを処理するために GR リスタータを補助します。

ルータで RIPng を再起動したのち、ルータは RIPng ルートを再学習し、FIB テーブルのアップデートを行います。これによりネットワークの切断とルートの収束が発生します。

GR 機能において、再起動するルータ（GR リスタータ）は、GR を行う能力があるネイバ装置にイベントを通知することができます。GR を行う能力があるネイバ装置（GR ヘルパー）は GR タイマの時間内にルータのネイバ関係を維持します。この処理の間、ルータの FIB テーブルは変更しません。

RIPng が有効な装置はデフォルトで GR ヘルパーとして動作します。この作業は GR リスタータで行われます。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. RIPng を有効にし、RIPng view に移行する	**ripng** [*process-id*] [**vpn-instance** *vpn-instance-name*]	―
3. RIPng の GR 機能を有効にする	**graceful-restart**	デフォルト：無効

9.7 RIPng NSRの設定

I. RIPng NSR

ノンストップルーティング (NSR) は、RIPng ルーティング情報をアクティブプロセスからスタンバイプロセスにバックアップします。アクティブ/スタンバイスイッチオーバーの後、隣接関係を切断したり転送サービスに影響を与えたりすることなく、NSR はルートの再生成を完了できます。

NSR は、ルーティング情報をリカバリするために隣接装置の協力を必要とせず、一般に GR よりも頻繁に使用されます。

II. 制限とガイドライン

RIPng プロセスに対して有効化された RIPng NSR は、そのプロセスでのみ有効になります。複数の RIPng プロセスが存在する場合は、ベストプラクティスとして各プロセスに対して RIPng NSR を有効にします。

RIPng NSR が有効になっている装置は、GR リスタータとして機能できません。

III. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. RIPng view に移行する	**ripng** [*process-id*] [**vpn-instance** *vpn-instance-name*]	―
3. RIPng NSR を有効にする	**non-stop-routing**	デフォルト：無効

9.8 RIPngのセキュリティ機能の拡張

9.8.1 RIPng パケットのゼロフィールドチェック機能の有効化

I. RIPng パケットのゼロフィールドチェック機能

RIPng パケットのいくつかのフィールドはゼロである必要があり、それらのフィールドはゼロフィールドと呼ばれます。装置で、受信 RIPng パケットのゼロフィールドチェック機能を有効にすることができます。ゼロフィールドにゼロ以外の値が含まれる場合、RIPng パケットは処理されません。すべてのメッセージを信頼できる場合、ゼロフィールドチェック機能を無効化することで、CPU のリソースを節約することができます。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. RIPng view に移行する	**ripng** [*process-id*] [**vpn-instance** *vpn-instance-name*]	—
3. RIPng パケットのゼロフィールドチェック機能を有効にする	**checkzero**	デフォルト：有効

9.9 RIPngの表示と維持

すべての view で **display** コマンドを実行でき、user view で **reset** コマンドを実行できます。

操作	コマンド
RIPngプロセスの設定情報を表示する	**display ripng** [*process-id*]
RIPng GR情報を表示する	**display ripng** [*process-id*] **graceful-restart**
RIPng NSR情報を表示する	**display ripng** [*process-id*] **non-stop-routing**
RIPngデータベースのルートを表示する	**display ripng** *process-id* **database** [*ipv6-address prefix-length*]
RIPngインタフェース情報を表示する	**display ripng** *process-id* **interface** [*interface-type interface-number*]
RIPngプロセスのネイバ情報を表示する	**display ripng** *process-id* **neighbor** [*interface-type interface-number*]
RIPngプロセスのルーティング情報を表示する	**display ripng** *process-id* **route** [*ipv6-address prefix-length* [**verbose**] | **peer** *ipv6-address* | **statistics**]
RIPngプロセスをリセットする	**reset ripng** *process-id* **process**
RIPngプロセスの統計情報を削除する	**reset ripng** *process-id* **statistics**

9.10 RIPng設定例

9.10.1 RIPng の基本機能の設定例

I. ネットワーク要件

図 8-1に示すように、Switch A、Switch B、Switch C で RIPng を有効にします。Switch B は Switch A にルート 2::/64 のルートをフィルタし、Switch A からルート 4::/64 のみ配信するように設定します。

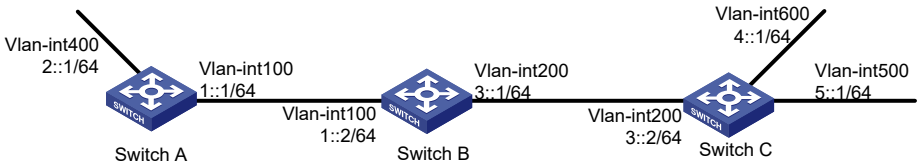


図 8-1 ネットワーク図

II. 設定手順

1)　インタフェースに IPv6 アドレスを設定します。(詳細は省略します)
2)　RIPng の基本機能の設定をします。

Switch A を設定します。

```
<SwitchA> system-view
[SwitchA] ripng 1
[SwitchA-ripng-1] quit
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] ripng 1 enable
[SwitchA-Vlan-interface100] quit
[SwitchA] interface vlan-interface 400
[SwitchA-Vlan-interface400] ripng 1 enable
[SwitchA-Vlan-interface400] quit
```

Switch B を設定します。

```
<SwitchB> system-view
[SwitchB] ripng 1
[SwitchB-ripng-1] quit
[SwitchB] interface vlan-interface 100
[SwitchB-Vlan-interface100] ripng 1 enable
[SwitchB-Vlan-interface100] quit
```

```
[SwitchB] interface vlan-interface 400
[SwitchB-Vlan-interface400] ripng 1 enable
[SwitchB-Vlan-interface400] quit
```

Switch C を設定します。

```
<SwitchC> system-view
[SwitchC] ripng 1
[SwitchC-ripng-1] quit
[SwitchC] interface vlan-interface 200
[SwitchC-Vlan-interface200] ripng 1 enable
[SwitchC-Vlan-interface200] quit
[SwitchC] interface vlan-interface 500
[SwitchC-Vlan-interface500] ripng 1 enable
[SwitchC-Vlan-interface500] quit
[SwitchC] interface vlan-interface 600
[SwitchC-Vlan-interface600] ripng 1 enable
[SwitchC-Vlan-interface600] quit
```

Switch B の RIPng ルーティングテーブルを表示します。

```
[SwitchB] display ripng 1 route
   Route Flags: A - Aging, S - Suppressed, G - Garbage-collect, D - Direct
                O - Optimal, F - Flush to RIB
 ------------------------------------------------------------------

 Peer FE80::20F:E2FF:FE23:82F5 on Vlan-interface100
 Destination 2::/64,
     via FE80::20F:E2FF:FE23:82F5, cost 1, tag 0, AOF, 6 secs
 Peer FE80::20F:E2FF:FE00:100  on Vlan-interface200
 Destination 4::/64,
     via FE80::20F:E2FF:FE00:100, cost 1, tag 0, AOF, 11 secs
 Destination 5::/64,
     via FE80::20F:E2FF:FE00:100, cost 1, tag 0, AOF, 11
 Local route
 Destination 1::/64,
     via ::, cost 0, tag 0, DOF
 Destination 3::/64,
     via ::, cost 0, tag 0, DOF
```

Switch A の RIPng ルーティングテーブルを表示します。

```
[SwitchA] display ripng 1 route
   Route Flags: A - Aging, S - Suppressed, G - Garbage-collect, D - Direct
                O - Optimal, F - Flush to RIB
 ------------------------------------------------------------------

 Peer FE80::200:2FF:FE64:8904 on Vlan-interface100
 Destination 3::/64,
     via FE80::200:2FF:FE64:8904, cost 1, tag 0, AOF, 31 secs
 Destination 4::/64,
     via FE80::200:2FF:FE64:8904, cost 2, tag 0, AOF, 31 secs
 Destination 5::/64,
     via FE80::200:2FF:FE64:8904, cost 2, tag 0, AOF, 31 secs
 Local route
```

```
 Destination 2::/64,
     via ::, cost 0, tag 0, DOF
 Destination 1::/64,
     via ::, cost 0, tag 0, DOF
```

3) ルートのフィルタリングを設定します

送受信ルートをフィルタするため、Switch B の IPv6 プレフィックスリストを使用します。

```
[SwitchB] ipv6 prefix-list aaa permit 4:: 64
[SwitchB] ipv6 prefix-list bbb deny 2:: 64
[SwitchB] ipv6 prefix-list bbb permit :: 0 less-equal 128
[SwitchB] ripng 1
[SwitchB-ripng-1] filter-policy prefix-list aaa export
[SwitchB-ripng-1] filter-policy prefix-list bbb import
[SwitchB-ripng-1] quit
```

Switch B と Switch A の RIPng ルーティングテーブルを表示します。

```
[SwitchB] display ripng 1 route
   Route Flags: A - Aging, S - Suppressed, G - Garbage-collect, D – Direct
                O - Optimal, F - Flush to RIB
 ------------------------------------------------------------------

 Peer FE80::1:100 on Vlan-interface100

 Peer FE80::3:200 on Vlan-interface200
 Destination 4::/64,
     via FE80::2:200, cost 1, tag 0, AOF, 11 secs
 Destination 5::/64,
     via FE80::2:200, cost 1, tag 0, AOF, 11 secs
 Local route
 Destination 1::/64,
     via ::, cost 0, tag 0, DOF
 Destination 3::/64,
     via ::, cost 0, tag 0, DOF
[SwitchA] display ripng 1 route
   Route Flags: A - Aging, S - Suppressed, G - Garbage-collect, D – Direct
                O - Optimal, F - Flush to RIB
 ------------------------------------------------------------------

 Peer FE80::2:100 on Vlan-interface100
 Destination 4::/64,
     via FE80::1:100, cost 2, tag 0, AOF, 2 secs
```

9.10.2 RIPng ルート再配信の設定例

I. ネットワーク要件

図 8-2に示すように、Switch B は RIPng 100 を通して Switch A と通信し、RIPng 200 を通して Switch C と通信します。

2 つの RIPng プロセスが、お互いからルートを再配信できるように Switch B にルートの再配信の設定を行います。

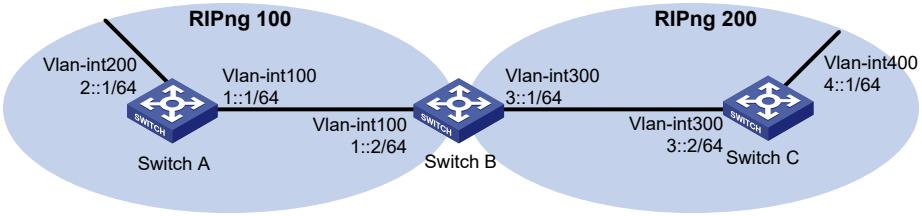


図 8-2 ネットワーク図

II. 設定手順

1)　インタフェースに IPv6 アドレスを設定します。(詳細は省略します)
2)　RIPng の基本機能の設定をします。

Switch A で RIPng100 を有効にします。

```
<SwitchA> system-view
[SwitchA] ripng  100
[SwitchA-ripng-100]  quit
[SwitchA] interface  vlan-interface  100
[SwitchA-Vlan-interface100]  ripng  100 enable
[SwitchA-Vlan-interface100]  quit
[SwitchA] interface  vlan-interface  200
[SwitchA-Vlan-interface200]  ripng  100 enable
[SwitchA-Vlan-interface200]  quit
```

Switch B で RIPng100 と RIPng200 を有効にします。

```
<SwitchB> system-view
[SwitchB] ripng  100
[SwitchB-ripng-100]  quit
[SwitchB] interface  vlan-interface  100
[SwitchB-Vlan-interface100]  ripng  100 enable
[SwitchB-Vlan-interface100]  quit
[SwitchB] ripng  200
[SwitchB-ripng-200]  quit
[SwitchB] interface  vlan-interface  300
[SwitchB-Vlan-interface300]  ripng  200 enable
[SwitchB-Vlan-interface300]  quit
```

Switch C で RIPng200 を有効にします。

```
<SwitchC> system-view
[SwitchC] ripng 200
```

```
[SwitchC] interface vlan-interface 300
[SwitchC-Vlan-interface300] ripng 200 enable
[SwitchC-Vlan-interface300] quit
[SwitchC] interface vlan-interface 400
[SwitchC-Vlan-interface400] ripng 200 enable
[SwitchC-Vlan-interface400] quit
```

Switch A のルーティングテーブルを表示します。

```
[SwitchA] display ipv6 routing-table

Destinations : 7 Routes : 7

Destination: ::1/128                                Protocol  : Direct
NextHop    : ::1                                    Preference: 0
Interface  : InLoop0                                Cost      : 0

Destination: 1::/64                                 Protocol  : Direct
NextHop    : ::                                   Preference: 0
Interface  : Vlan100                                Cost      : 0

Destination: 1::1/128                               Protocol  : Direct
NextHop    : ::1                                    Preference: 0
Interface  : InLoop0                                Cost      : 0

Destination: 2::/64                                 Protocol  : Direct
NextHop    : ::                                   Preference: 0
Interface  : Vlan200                                Cost      : 0

Destination: 2::1/128                               Protocol  : Direct
NextHop    : ::1                                    Preference: 0
Interface  : InLoop0                                Cost      : 0

Destination: FE80::/10                              Protocol  : Direct
NextHop    : ::                                     Preference: 0
Interface  : NULL0                                  Cost      : 0

Destination: FF00::/8                               Protocol  : Direct
NextHop    : ::                                     Preference: 0
Interface  : NULL0                                  Cost      : 0
```

3)　RIPng ルートの再配信の設定をします。

Switch B で、2 つの RIPng プロセス間ルートを再配信するように設定します。

```
[SwitchB] ripng 100
[SwitchB-ripng-100] import-route ripng 200
[SwitchB-ripng-100] quit
[SwitchB] ripng 200
[SwitchB-ripng-200] import-route ripng 100
[SwitchB-ripng-200] quit
```

Switch A のルーティングテーブルを表示します。

```
[SwitchA] display ipv6 routing-table

Destinations : 8 Routes : 8
```

```
Destination: ::1/128                                    Protocol  : Direct
NextHop    : ::1                                        Preference: 0
Interface  : InLoop0                                    Cost      : 0

Destination: 1::/64                                     Protocol  : Direct
NextHop    : ::                                       Preference: 0
Interface  : Vlan100                                    Cost      : 0

Destination: 1::1/128                                   Protocol  : Direct
NextHop    : ::1                                        Preference: 0
Interface  : InLoop0                                    Cost      : 0

Destination: 2::/64                                     Protocol  : Direct
NextHop    : ::                                       Preference: 0
Interface  : Vlan200                                    Cost      : 0

Destination: 2::1/128                                   Protocol  : Direct
NextHop    : ::1                                        Preference: 0
Interface  : InLoop0                                    Cost      : 0

Destination: 4::/64                                     Protocol  : RIPng
NextHop    : FE80::200:BFF:FE01:1C02                    Preference: 100
Interface  : Vlan100                                    Cost      : 1

Destination: FE80::/10                                  Protocol  : Direct
NextHop    : ::                                         Preference: 0
Interface  : NULL0                                      Cost      : 0

Destination: FF00::/8                                   Protocol  : Direct
NextHop    : ::                                         Preference: 0
Interface  : NULL0                                      Cost      : 0
```

9.10.3 RIPng GR の設定例

I. ネットワーク要件

図 8-3に示すように、Switch A、Switch B、および Switch C は、RIPng を通じて IPv6 ルーティング情報を学習します。

GR リスタータとしての設定 Switch A。GR ヘルパーとしての設定 Switch B と Switch C は、GR を使用してルーティングテーブルを SwitchA と同期させます。

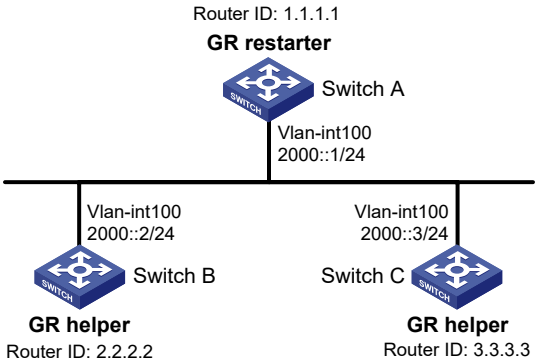


図 8-3 ネットワーク図

II. 設定手順

1) インタフェースに IPv6 アドレスを設定します。(詳細は省略します)
2) Switch で RIPng を設定して、次のことを確認します。(詳細は省略します)
   - Switch A、Switch B、および Switch C は、レイヤ 3 で相互に通信できます。
   - RIPng を使用して、動的ルート更新を実装することができます。
3) Switch A で RIPng GR を有効にします。

```
<SwitchA> system-view
[SwitchA] ripng 1
[SwitchA-ripng-1] graceful-restart
```

II. 設定の確認

RIPng を再起動するか、アクティブ/スタンバイ切り替えをトリガし、Switch A に GR ステータスを表示します。

```
<SwitchA> display ripng 1 graceful-restart
RIPng process: 1
 Graceful Restart capability     : Enabled
 Current GR state                : Normal
 Graceful Restart period         : 60  seconds
 Graceful Restart remaining time: 0   seconds
```

9.10.4 RIPng NSR の設定例

I. ネットワーク要件

図 8-4に示すように、Switch S、Switch A、および Switch B は、RIPng を介して IPv6 ルーティング情報を学習します。

Switch S でアクティブ/スタンバイスイッチオーバーが発生したときに正しいルーティングが行われるようにするには、Switch S で RIPng NSR を有効にします。

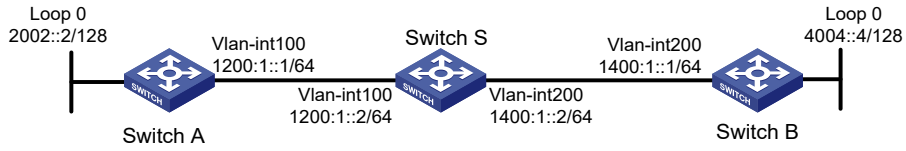


図 8-4 ネットワーク図

II. 設定手順

1) インタフェースの IPv6 アドレスを設定します。(詳細は表示されていません。)
2) スイッチで RIPng を設定して、次のことを確認します。(詳細は表示されていません。)
   - Switch S、Switch A、および Switch B は、レイヤ 3 で相互に通信できます。
   - 動的ルート更新は RIPng でそれらの間に実装できます。
3) Switch S で RIPng NSR を有効にします。

```
<SwitchS> system-view
```

```
[SwitchS] ripng 1
[SwitchS-ripng-1] non-stop-routing
[SwitchS-ripng-1] quit
```

III. 設定の確認

Switch S でアクティブ/スタンバイスイッチオーバーを実行します。

```
[SwitchS] placement reoptimize
Predicted changes to the placement
Program                              Current location       New location
-------------------------------------------------------------------------
lb                                   0/0                    0/0
lsm                                  0/0                    0/0
slsp                                 0/0                    0/0
rib6                                 0/0                    0/0
routepolicy                          0/0                    0/0
rib                                  0/0                    0/0
staticroute6                         0/0                    0/0
staticroute                          0/0                    0/0
eviisis                              0/0                    0/0
ospf                                 0/0                    1/0
Continue? [y/n]:y
Re-optimization of the placement start. You will be notified on completion
Re-optimization of the placement complete. Use 'display placement' to view the
new placement
```

#スイッチオーバー期間中に、Switch A の RIPng ネイバを表示して、Switch A と Switch S の間のネイバ関係を確認します。

```
[SwitchA] display ripng 1 neighbor
 Neighbor Address: FE80::AE45:5CE7:422E:2867
     Interface  : Vlan-interface100
     Version    : RIPng version 1     Last update: 00h00m23s
     Bad packets: 0                   Bad routes : 0
```

Switch A の RIPng ルートを表示して、Switch A に Switch B のループバックインタフェースへのルートがあるかどうかを確認します。

```
[SwitchA] display ripng 1 route
   Route Flags: A - Aging, S - Suppressed, G - Garbage-collect, D - Direct
                O - Optimal, F - Flush to RIB
 ------------------------------------------------------------
 Peer FE80::AE45:5CE7:422E:2867 on Vlan-interface100
 Destination 1400:1::/64,
     via FE80::AE45:5CE7:422E:2867, cost 1, tag 0, AOF, 1 secs
 Destination 4004::4/128,
     via FE80::AE45:5CE7:422E:2867, cost 2, tag 0, AOF, 1 secs
 Local route
 Destination 2002::2/128,
     via ::, cost 0, tag 0, DOF
 Destination 1200:1::/64,
     via ::, cost 0, tag 0, DOF
```

Switch B の RIPng ネイバを表示して、Switch B と Switch S のネイバ関係を確認します。

```
[SwitchB] display ripng 1 neighbor
 Neighbor Address: FE80::20C:29FF:FECE:6277
     Interface  : Vlan-interface200
     Version    : RIPng version 1     Last update: 00h00m18s
     Bad packets: 0                   Bad routes : 0
```

Switch B の RIPng ルートを表示して、Switch B に Switch A のループバックインタフェースへのルートがあるかどうかを確認します。

[SwitchB] display ripng 1 route

```
   Route Flags: A - Aging, S - Suppressed, G - Garbage-collect, D - Direct
                O - Optimal, F - Flush to RIB
 ------------------------------------------------------------
 Peer FE80::20C:29FF:FECE:6277 on Vlan-interface200
 Destination 2002::2/128,
     via FE80::20C:29FF:FECE:6277, cost 2, tag 0, AOF, 24 secs
 Destination 1200:1::/64,
     via FE80::20C:29FF:FECE:6277, cost 1, tag 0, AOF, 24 secs
 Local route
 Destination 4004::4/128,
     via ::, cost 0, tag 0, DOF
 Destination 1400:1::/64,
     via ::, cost 0, tag 0, DOF
```

Switch S でアクティブ/スタンバイスイッチオーバーが発生した場合の出力は、次のとおりです。

- Switch A および Switch B のネイバ関係およびルーティング情報は変更されていません。
- Switch A から Switch B へのトラフィックは影響を受けていません。

目次

このセクションのページは **5-x-x** です。

10 章 OSPFv3 10-1
10.1 概要 10-1
10.1.1 OSPFv3 と OSPFv2 の比較 10-1
10.1.2 OSPFv3 パケット 10-1
10.1.3 OSPFv3 LSA タイプ 10-2
10.1.4 プロトコルと標準 10-2
10.2 OSPFv3 設定作業リスト 10-3
10.3 OSPFv3 の有効化 10-4
10.4 OSPFv3 エリアパラメータの設定 10-4
10.4.1 OSPFv3 エリア 10-4
10.4.2 スタブエリアの設定 10-5
10.4.3 OSPFv3 仮想リンクの設定 10-5
10.5 OSPFv3 ネットワークタイプの設定 10-6
10.5.1 制限とガイドライン 10-6
10.5.2 OSPFv3 インタフェースのブロードキャストネットワークタイプの設定 10-6
10.5.3 OSPFv3 インタフェースの NBMA ネットワークタイプの設定 10-6
10.5.4 OSPFv3 インタフェースの P2MP ネットワークタイプの設定 10-7
10.5.5 OSPFv3 インタフェースの P2P ネットワークタイプの設定 10-7
10.6 OSPFv3 ルート制御の設定 10-8
10.6.1 OSPFv3 インターエリアルート集約の設定 10-8
10.6.2 再配信されたルート集約の設定 10-8
10.6.3 OSPFv3 受信ルートのフィルタリングの設定 10-9
10.6.4 インターエリアプレフィックス LSA のフィルタリングの設定 10-9
10.6.5 インタフェースの OSPFv3 コストの設定 10-9
10.6.6 OSPFv3 ECMP ルートの最大数の設定 10-10
10.6.7 OSPFv3 の優先順位の設定 10-11
10.6.8 OSPFv3 ルートの再配信 10-11
10.6.9 デフォルトルートの再配信 10-11
10.7 OSPFv3 タイマの設定 10-12
10.7.1 OSPFv3 パケットタイマの設定 10-12
10.7.2 LSA 伝送遅延の設定 10-12
10.7.3 SPF の計算間隔の設定 10-13
10.7.4 LSA 生成間隔の設定 10-13
10.8 インタフェースの DR 優先度の設定 10-14
10.9 OSPFv3 パケットパラメータの設定 10-14
10.9.1 DD パケットの MTU チェック無効化の設定 10-14
10.9.2 OSPFv3 パケットの送受信インタフェースの無効化の設定 10-15
10.10 プレフィックス抑制の設定 10-15
10.10.1 プレフィックスの抑制 10-15
10.10.2 プレフィックス抑制の制限とガイドライン 10-15
10.11 OSPFv3 GR の設定 10-16
10.11.1 OSPFv3 GR 10-16
10.11.2 GR リスタータの設定 10-16
10.11.3 GR ヘルパーの設定 10-16

10.11.4 OSPFv3 GR の始動 10-17
10.12 OSPFv 3 NSR の設定 10-17
10.13 OSPFv3 の BFD の設定 10-18
10.14 OSPFv3 ロギングと SNMP notification の設定 10-18
10.14.1 ネイバ状態変化のロギングの有効化 10-18
10.14.2 OSPFv3 ネットワーク管理の設定 10-19
10.15 OSPFv3 の表示と維持 10-20
10.16 OSPFv3 設定例 10-20
10.16.1 OSPFv3 スタブエリアの設定例 10-20
10.16.2 OSPFv3 DR 選択の設定例 10-25
10.16.3 OSPFv3 ルート再配信の設定例 10-28
10.16.4 OSPFv3 の GR の設定例 10-31
10.16.5 OSPFv 3 NSR の設定例 10-33

10章 OSPFv3

10.1 概要

この章は、IPv6 ネットワーク用の、RFC2740 に準拠した OSPFv3（Open Shortest Path First version 3）の設定について記載します。

10.1.1 OSPFv3 と OSPFv2 の比較

OSPFv3 と OSPFv2 の共通点は以下になります。

- 32 ビットのルータ ID とエリア ID
- パケット: Hello、DD (Data Description)、LSR (Link State Request)、LSU (Link State Update)、 LSAck (Link State Acknowledgment)
- ネイバ装置の探索とネイバ関係を確立するメカニズム
- LSA の配信とエージングのメカニズム
- OSPFv3 と OSPFv2 の相違点は以下になります。
- OSPFv3 はリンク単位で動作します。OSPFv2 は IP サブネット単位です。
- OSPFv3 はリンクごとの複数インスタンスをサポートしています。OSPFv2 はサポートしていません。
- OSPFv3 はルータ ID でネイバ装置を識別し、OSPFv2 は IP アドレスで識別します。
- OSPFv2 についての詳細は、オペレーションマニュアルのセクション 5 *ルーティングプロトコル"OSPF"*を参照してください。

10.1.2 OSPFv3 パケット

OSPFv3 は、以下のパケットタイプを使用します。

- **Hello パケット** — ルータからネイバルータの発見と状態を保持するために定期的に送信されます。Hello パケットには、いくつかのタイマ、DR、BDR、既知のネイバルータの情報が含まれます。
- **DD パケット(データベース記述パケット)** — 各 LSA の集約を含む自身の LSDB を記述し、2 台のルータがデータベースの同期を取るときに交換されます。
- **LSR(リンク状態要求)パケット** — 必要な LSA をネイバルータに転送します。DD パケットをルータが交換した後、ローカル LDSB からなくなっているネイバルータの LSA を検出します。その際に、存在していない LSA をお互いに要求します。パケットには、要求する LSA の集約が含まれます。
- **LSU(リンク状態更新)パケット** — 必要な LSA をネイバルータに転送します。
- **LSAck(リンク状態確認)パケット** — このパケットを使用して、受信した LSU パケットに対して肯定応答を返します。

10.1.3 OSPFv3 LSA タイプ

OSPFv3 は LSA でルーティング情報を送信します。以下の LSA を使用します。

- **ルータ LSA(Router LSA)** — Type-1 LSA です。この LSA は すべてのルータで生成され、ルータが所属するエリア内のみ配信されます。この LSA は収集されたエリアのルータインタフェースの状態を記述します。
- **ネットワーク LSA(Network LSA)** — Type-2 LSA です。この LSA はブロードキャストもしくは NBMA ネットワークの DR によって生成され、1 つのエリアのみ配信されます。この LSA はエリア内のルータのリストを記述します。
- **インターエリアプレフィックス LSA(Network Summary LSA)** — Type-3 LSA です。この LSA は ABR(エリアボーダールータ)によって生成され、LSA に関連するエリアに配信されます。各インターエリアプレフィックス LSA には、AS の内部ルート(インターエリアルート)で、外部エリアへの IPv6 アドレスプレフィックスのルートが記載されています。
- **インターエリアルータ LSA(Inter-Area-Router LSA)** — Type-4 LSA です。この LSA は ABR によって生成され、LSA に関連するエリアに配信されます。インターエリアルータ LSA は ASBR(自律システム境界ルータ)へのルートを記述します。
- **AS 外部 LSA(AS External LSA)** — Type-5 LSA です。この LSA は ASBR によって生成され、他のすべての AS(スタブエリアと NSSA エリアを除く)に配信されます。各 AS 外部 LSA は違う自律システムへのルートを記述します。デフォルトルートは AS 外部 LSA によって記述できます。
- **NSSA(Not-So-Stubby Area) LSA** – Type-7 LSA です。NSSA の ASBR によって生成され単一の NSSA エリア内に配信されます。NSSA LSA は他のエリアの AS へのルートを記述します。NSSA はサポートしていません。
- **リンク LSA(Link LSA)** – Type-8 LSA です。ルータは各接続リンク先について、別々のリンク LSA を生成します。リンク LSA はリンクローカルフラッディングスコープを備えており、各リンク LSA はリンク先の IPv6 アドレスのプリフィクス、およびルータのリンクローカルアドレスを記述します。
- **内部エリアプリフィクス LSA(Intra-Area-Prefix LSA)** – Type-9 LSA です。各内部エリアプリフィクス LSA はルータ、スタブエリアまたはトランジットエリアに関する IPv6 プリフィクス情報を含む他、エリアフラッディングスコープを備えています。現在、ルータ LSA やネットワーク LSA にはアドレス情報が含まれていないことから、この LSA が導入されました。
- **グレース LSA** – Type-11 LSA です。グレース LSA は、再起動時の GR Restarter(グレースフルリスタータ)によって生成され、ローカルリンク内に送信されます。リスタータはグレース LSA の中で、原因と再起動の間隔を記載し、GR 動作を実行するネイバ装置に伝えます。

10.1.4 プロトコルと標準

- RFC 2328, *OSPF Version 2*
- RFC 3101, *OSPF Not-So-Stubby Area (NSSA) Option*
- RFC 4552, *Authentication/Confidentiality for OSPFv3*
- RFC 5187, *OSPFv3 Graceful Restart*
- RFC 5329, *Traffic Engineering Extensions to OSPF Version 3*
- RFC 5340, *OSPF for IPv6*
- RFC 5523, *OSPFv3-Based Layer 1 VPN Auto-Discovery*

- RFC 5643, *Management Information Base for OSPFv3*
- RFC 6506, *Supporting Authentication Trailer for OSPFv3*
- RFC 6565, *OSPFv3 as a Provider Edge to Customer Edge (PE-CE) Routing Protocol*
- RFC 6969, *OSPFv3 Instance ID Registry Update*
- RFC 7166, *Supporting Authentication Trailer for OSPFv3*

10.2 OSPFv3設定作業リスト

作業リスト
(必須設定項目) OSPFv3の有効化
(オプション設定項目) OSPFv3エリアパラメータの設定: ● スタブエリアの設定 ● OSPFv3仮想リンクの設定 仮想リンクを設定することにより、ABRで非バックボーンエリアとバックボーンエリアまたはバックボーン自体との間の接続を維持することが可能です。
(オプション設定項目) OSPFv3ネットワークタイプの設定: ● OSPFv3インタフェースのブロードキャストネットワークタイプの設定 ● OSPFv3インタフェースのNBMAネットワークタイプの設定 ● OSPFv3インタフェースのP2MPネットワークタイプの設定 ● OSPFv3インタフェースのP2Pネットワークタイプの設定
(オプション設定項目) OSPFv3ルート制御の設定: ● OSPFv3インターエリアルート集約の設定 ● OSPFv3受信ルートのフィルタリングの設定 ● インターエリアプレフィックスLSAのフィルタリングの設定 ● インタフェースのOSPFv3コストの設定 ● OSPFv3 ECMPルートの最大数の設定 ● OSPFv3の優先順位の設定 ● OSPFv3ルートの再配信の設定 ● デフォルトルートの再配信の設定
(オプション設定項目) OSPFv3タイマの設定: ● OSPFv3パケットタイマの設定 ● LSA伝送遅延の設定 ● SPFの計算間隔の指定 ● LSA生成間隔の指定
(オプション設定項目)インタフェースのDRの優先度の設定
(オプション設定項目) OSPFv3パケットパラメータの設定: ● DDパケットのMTUチェック無効化の設定 ● OSPFv3パケットの送受信インタフェースの無効化の設定
(オプション設定項目) ● プレフィックス抑制の設定
(オプション設定項目) Enhancing OSPFv3 availability OSPFv3可用性の拡張: ● OSPFv3 GRの設定 ● OSPFv 3 NSRの設定 ● OSPFv3のBFDの設定

作業リスト
(オプション設定項目) OSPFv3ロギングとSNMP notificationの設定: ● ネイバ状態変化のロギングの有効化 ● OSPFv3ネットワーク管理の設定

10.3 OSPFv3の有効化

I. OSPFv3 の有効化

ルータの OSPFv3 プロセスを有効にするため、以下の設定を完了させてください。

1) グローバルで OSPFv3 プロセスを有効にします。
2) OSPFv3 プロセスにルータ ID を割り当てます。
3) 関連するインタフェースで OSPFv3 プロセスを有効にします。
4) ルータ ID は AS の中でルータを一意に識別します。OSPFv3 のプロセス ID はローカルでのみ使われます。ルータのプロセス 1 は別のルータのプロセス 2 のパケットと交換できます。

OSPFv3 は AS の各ルータのルータ ID を手動で指定する必要があります。AS のルータ ID が固有であることを確認してください。

II. 制限とガイドライン

ルータで複数の OSPFv3 プロセスを動作させる場合、各プロセスに固有のルータ ID を指定する必要があります。

III. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. OSPFv3 プロセスを有効にし、その view に移行する	**ospfv3** [*process-id* | **vpn-instance** *vpn-instance-name*] *	デフォルト：無効
3. ルータ ID を指定する	**router-id** *router-id*	デフォルト：設定なし
4. interface view に移行する	**interface** *interface-type interface-number*	―
5. インタフェースで OSPFv3 プロセスを有効にする	**ospfv3** *process-id* **area** *area-id* [**instance** *instance-id*]	デフォルト：無効

10.4 OSPFv3エリアパラメータの設定

10.4.1 OSPFv3 エリア

OSPFv3 のスタブエリアとバーチャルリンクの機能は、OSPFv2 のものと同じです。

ネットワーク上の LSA の数を減らし、OSPFv3 の活用を拡大するために、OSPFv3 AS を複数のエリアに分割します。AS の境界にある非バックボーンエリアについては、そのエ

リアのルータ上のルーティングテーブルのサイズ、および LSA の数を更に縮小するために、スタブエリアとして設定することができます。

スタブエリアは外部ルートをインポートすることができませんが、NSSA エリアは他のスタブエリアの特徴を維持したまま、OSPFv3 ルーティングドメインに外部エリアをインポートすることができます。

非バックボーンエリアではルーティング情報はバックボーンエリアを経由して交換されます。したがって、バックボーンエリアと非バックボーンエリア（バックボーン自体を含む）は必ず接続を維持している必要があります。実際には必要な物理的リンクを使って接続することはできませんが、バーチャルリンクを設定することにより、この問題を解決することができます。

10.4.2 スタブエリアの設定

I. 制限とガイドライン

スタブエリアに接続しているすべてのルータは **stub** コマンドを設定する必要があります。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. OSPFv3 view に移行する	**ospfv3** [*process-id* | **vpn-instance** *vpn-instance-name*] *	—
3. OSPFv3 area view に移行する	**area** *area-id*	—
4. スタブエリアとして設定する	**stub** [**default-route-advertise-always** | **no-summary**] *	デフォルト：設定なし **no-summary**パラメータはスタブエリアのABRでのみ有効です。 もしABRで**no-summary**パラメータを使用して**stub**コマンドを使用する場合、ABRはスタブエリアにインターエリアプレフィックスLSAにデフォルトルートを配信します。
5. (オプション設定項目) スタブエリアに配信するデフォルトルートコストを設定する	**default-cost** *value*	デフォルト：1

10.4.3 OSPFv3 仮想リンクの設定

I. OSPFv3 仮想リンク

仮想リンクを設定することにより、非バックボーンエリアとバックボーンエリアまたはバックボーン自体との間の接続を維持することが可能です。

II. 制限とガイドライン

仮想リンクの双方の終端は **vlink-peer** コマンドで設定された ABR である必要があります。

GR 対応プロセスのエリアでは仮想リンクを設定しないでください。

III. **設定手順**

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. OSPFv3 view に移行する	**ospfv3** [*process-id* | **vpn-instance** *vpn-instance-name*] *	―
3. OSPFv3 area view に移行する	**area** *area-id*	―
4. OSPFv3 仮想リンクを設定する	**vlink-peer** *router-id* [**dead** *seconds* | **hello** *seconds* | **instance** *instance-id* | **retransmit** *seconds* | **trans-delay** *seconds*]*	デフォルト：設定なし

10.5 OSPFv3ネットワークタイプの設定

10.5.1 制限とガイドライン

OSPFv3 はリンクレイヤプロトコルにもとづいて、ブロードキャスト、NBMA、P2MA、P2P の異なるタイプにネットワークを分類します。

- ブロードキャストネットワークのルータは、マルチキャストをサポートしません。ネットワークタイプを NBMA に変更する必要があります。
- ネットワークセグメントの OSPFv3 で動作するルータが 2 台の場合、コストを節約するためネットワークタイプを P2P に変更することができます。

10.5.2 OSPFv3 インタフェースのブロードキャストネットワークタイプの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. interface view に移行する	**interface** *interface-type interface-number*	―
3. OSPFv3 インタフェースのネットワークタイプをブロードキャストに設定する	**ospfv3 network-type broadcast** [**instance** *instance-id*]	デフォルト: ブロードキャスト

10.5.3 OSPFv3 インタフェースの NBMA ネットワークタイプの設定

I. **制限とガイドライン**

NBMA インタフェースでは、hello パケットのブロードキャストによってネイバを検出できないため、ネイバのリンクローカル IP アドレスおよび DR の優先度を指定する必要があります。

II. **設定手順**

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. interface view に移行する	**interface** *interface-type interface-number*	―
3. OSPFv3インタフェースのネットワークタイプを NBMA に設定する	**ospfv3 network-type nbma** [**instance** *instance-id*]	デフォルト : ブロードキャスト
4. （オプション設定項目）インタフェースの DR 優先度を設定する	**ospfv3 dr-priority** *priority*	デフォルト : 1 ルータの優先度は、DR/BDR を選択するときに使用されます。
5. NBMA または P2MP（ユニキャスト）ネイバと DR 優先度を設定する	**ospfv3 peer** *ipv6-address* [**cost** *cost-value* | **dr-priority** *priority*] [**instance** *instance-id*]	デフォルト : 設定なし

10.5.4 OSPFv3 インタフェースの P2MP ネットワークタイプの設定

I. **制限とガイドライン**

P2MP インタフェース（ユニキャストモードのみの場合）では、hello パケットのブロードキャストによってネイバを検出できないため、ネイバのリンクローカル IP アドレスを指定する必要があります。

II. **設定手順**

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. interface view に移行する	**interface** *interface-type interface-number*	―
3. OSPFv3インタフェースのネットワークタイプを設定する	**ospfv3 network-type p2mp** [**unicast**] [**instance** *instance-id*]	デフォルト : ブロードキャスト
4. NBMA または P2MP（ユニキャスト）ネイバと DR 優先度を設定する	**ospfv3 peer** *ipv6-address* [**cost** *cost-value* | **dr-priority** *priority*] [**instance** *instance-id*]	デフォルト : 設定なし

10.5.5 OSPFv3 インタフェースの P2P ネットワークタイプの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. interface view に移行する	**interface** *interface-type interface-number*	―
3. OSPFv3インタフェースのネットワークタイプを設定する	**ospfv3 network-type p2p** [**instance** *instance-id*]	デフォルト : ブロードキャスト

10.6 OSPFv3ルート制御の設定

10.6.1 OSPFv3 インターエリアルート集約の設定

I. OSPFv3 インターエリアルート集約

エリアに隣接しているネットワークセグメントがあった場合、ABR で一つのネットワークセグメントに集約するために、**abr-summary** コマンドを使うことができます。ABR は集約ルートだけを配信します。特定のネットワークセグメント中のすべての LSA を配信せずに、他のエリアの LSDB サイズを縮小します。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. OSPFv3 view に移行する	**ospfv3** [*process-id* | **vpn-instance** *vpn-instance-name*] *	—
3. OSPFv3 area view に移行する	**area** *area-id*	—
4. ルート集約を設定する	**abr-summary** *ipv6-address prefix-length* [**not-advertise**] [**cost** *cost-value*]	デフォルト：設定なし

10.6.2 再配信されたルート集約の設定

I. 再配信されたルート集約

ASBR が指定されたアドレス範囲内の外部ルートを単一ルートに集約できるようにします。

ASBR は以下の LSA のルートを集約することができます。

- Type-5 LSA
- NSSA エリアの Type-7 LSAs
- ASBR(および ABR)が配信する場合、NSSA エリアの Type-7 LSA から変換された Type-5 LSA。 配信しない場合、Type-5 LSA から変換された Type-5 LSA のルートは集約されません。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. OSPFv3 view に移行する	**ospfv3** [*process-id* | **vpn-instance** *vpn-instance-name*] *	—
3. ASBR ルート集約を設定する	**abr-summary** *ipv6-address prefix-length* [**cost** *cost-value* | **not-advertise** | **nssa-only** | **tag** *tag*] *	デフォルト：設定なし

10.6.3 OSPFv3 受信ルートのフィルタリングの設定

I. OSPFv3 受信ルートのフィルタリング

このコマンドは受信された LSA を使用して計算されたルートをフィルタすることができます。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. OSPFv3 view に移行する	**ospfv3** [*process-id* | **vpn-instance** *vpn-instance-name*] *	—
3. 受信された LSA を使用して、OSPFv3 受信ルートをフィルタする	**filter-policy** { *ipv6-acl-number* [**gateway** *prefix-list-name*] | **prefix-list** *prefix-list-name* [**gateway** *prefix-list-name*] | **gateway** *prefix-list-name* | **route-policy** *route-policy-name* } **import**	デフォルト：設定なし このコマンドはOSPFv3によって計算されたルートのみをフィルタすることができます。 取り除かれなかったルートのみ、ローカルルーティングテーブルに追加することができます。

10.6.4 インターエリアプレフィックス LSA のフィルタリングの設定

I. 制限とガイドライン

filter コマンドは ABR でのみ適用されます。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. OSPFv3 view に移行する	**ospfv3** [*process-id* | **vpn-instance** *vpn-instance-name*] *	—
3. OSPFv3 area view に移行する	**area** *area-id*	—
4. インターエリアプレフィックス LSA のフィルタリングを設定する	**filter** { *ipv6-acl-number* | **prefix-list** *prefix-list-name* | **route-policy** *route-policy-name* } { **export** | **import** }	デフォルト：設定なし

10.6.5 インタフェースの OSPFv3 コストの設定

I. インタフェースの OSPFv3 コストの設定

下記の方法のどちらかでインタフェースに OSPF コストを設定できます。

- Interface view でコスト値を設定します。
- インタフェースに帯域の基準値を設定し、この基準値をもとに OSPFv3 がコストを自動で計算します。

インタフェース OSPF コスト=帯域の基準値/インタフェースの通信速度。

- 計算されたコストが 65535 よりも大きい場合、この値は 65535 になります。
- 計算された値が 1 よりも小さい場合、1 になります。
- コスト値がインタフェースに設定されていない場合、OSPFv3 はインタフェースのコスト値を自動的に計算します。

II. interface view での OSPFv3 コストの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. interface view に移行する	**interface** *interface-type interface-number*	―
3. インタフェースの OSPFv3 コストを設定する	**ospfv3 cost** *value* [**instance** *instance-id*]	デフォルト : インタフェースは帯域に応じてコストを計算します。 VLAN の OSPFv3 のコストは 1 で、ループバックインタフェースの OSPFv3 コストはデフォルトで 0 です。

III. 帯域の基準値の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. OSPFv3 view に移行する	**ospfv3** [*process-id* | **vpn-instance** *vpn-instance-name*] *	―
3. 帯域の基準値を設定する	**bandwidth-reference** *value*	デフォルト : 100Mbps

10.6.6 OSPFv3 ECMP ルートの最大数の設定

I. OSPFv3 ECMP ルート

OSPFv3 はトラフィックの負荷を共有できるように、同一宛先に複数の等コストルートを検出します。ECMP ルートの最大数を設定することができます。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. OSPFv3 view に移行する	**ospfv3** [*process-id* | **vpn-instance** *vpn-instance-name*] *	―
3. OSPFv3 ルートの最大数を設定する	**maximum load-balancing** *number*	OSPFv3 ECMP ルートの最大数は、システムがサポートする ECMP ルートの最大数に等しくなります。

10.6.7 OSPFv3 の優先順位の設定

I. ルーティングプロトコルの優先順位

ルータは 1 台で複数のルーティングプロトコルを実行できます。システムは各プロトコルの優先順位を設定します。同一ルートが複数のルーティングプロトコルで検出された場合、優先順位がもっとも高いプロトコルで検出されたルートが選択されます。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. OSPFv3 view に移行する	**ospfv3** [*process-id* | **vpn-instance** *vpn-instance-name*] *	―
3. OSPFv3 の優先順位を設定する	**preference** [**ase**] { *preference* | **route-policy** *route-policy-name* } *	デフォルト： 内部ルートの優先順位：10 外部ルートの優先順位：150

10.6.8 OSPFv3 ルートの再配信

I. 制限とガイドライン

OSPFv3 はリンクステートをもとにしたルーティングプロトコルであるため、直接 LSA をフィルタすることはできません。OSPFv3 のフィルタリングは再配信ルートのみ行うことができます。フィルタされていないルートのみ LSA で配信されます。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. OSPFv3 view に移行する	**ospfv3** [*process-id* | **vpn-instance** *vpn-instance-name*] *	―
3. 他のプロトコルからのルートを再配信するように OSPFv3 を設定する	**import-route** { **direct** | **static** } [**cost** *cost-value* | **route-policy** *route-policy-name* | **type type**] * **import-route** { **ospfv3** | **ripng** } [*process-id* | **all-processes**]	デフォルト：無効
4. (オプション設定項目) OSPFv3 ルートの再配信をフィルタする	**filter-policy** { *ipv6-acl-number* | **prefix-list** *prefix-list-name* } **export** [*protocol* [*process-id*]]	デフォルト：設定なし このコマンドは**import-route** コマンドで再配信されたルートのみをフィルタします。**import-route**コマンドが設定されていない場合、このコマンドは適用されません。

10.6.9 デフォルトルートの再配信

I. デフォルトルートの再配信

import-route コマンドはデフォルト外部ルートを再配信することができません。

II. **設定手順**

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. OSPFv3 view に移行する	**ospfv3** [*process-id* | **vpn-instance** *vpn-instance-name*] *	―
3. (オプション設定項目) デフォルトルートを再配信するように OSPFv3 を設定する	**default-route-advertise** [[**always** | **permit-calculate-other**] | **cost** *cost* | **route-policy** *route-policy-name* | **type** *type*] *	デフォルト：設定なし

10.7 OSPFv3タイマの設定

10.7.1 OSPFv3 パケットタイマの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. interface view に移行する	**interface** *interface-type interface-number*	―
3. hello タイマの間隔を指定する	**ospfv3 timer hello** *seconds* [**instance** *instance-id*]	デフォルト：P2P および Broadcastインタフェースのデフォルト値は10 秒です。
4. dead タイマの間隔を指定する	**ospfv3 timer dead** *seconds* [**instance** *instance-id*]	デフォルト：P2Pおよび Broadcastインタフェースのデフォルト値は40 秒です。deadタイマの間隔はあまり短く設定することはできません。設定が短すぎると、容易にダウン状態であると判断されてしまいます。
5. poll タイマの間隔を指定する	**ospfv3 timer poll** *seconds* [**instance** *instance-id*]	デフォルト：120秒
6. LSA retransmission タイマの間隔を指定する	**ospfv3 timer retransmit** *interval* [**instance** *instance-id*]	デフォルト：5秒 LSA retransmissionタイマの間隔は、不要なLSA の再送を防ぐため、あまり小さくしないでください。

10.7.2 LSA 伝送遅延の設定

I. **LSA伝送遅延**

LSDB の各 LSA のエージングは、1 秒ごとに増加しますが、伝送時間の間、変更されません。伝送中に、LSA がエージングアウトすることを防ぐため、LSA の伝送遅延を設定します。特に低速リンクでは、必要となります。

II. **設定手順**

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. interface view に移行する	**interface** *interface-type interface-number*	―
3. LSA の伝送遅延を設定する	**ospfv3 trans-delay** *seconds* [**instance** *instance-id*]	デフォルト：1秒

10.7.3 SPF の計算間隔の設定

I. SPF の計算間隔の設定

LSDB を変更すると SPF の計算が必要になります。OSPF ネットワークが頻繁に変わると、大量のネットワーク リソースが占有され、ルータの運用効率が下がります。ネットワークの SPF の計算間隔を調整することで、影響を減らすことができます。

ネットワークが頻繁に変わらないとき、*minimum-interval* で行われます。ネットワークの変更がしばしば起こると、計算の間隔は計算の度に *incremental-interval* × 2^{n-2} ずつ増え、最後は *maximum-interval* になります。*n* は計算回数です。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. OSPFv3 view に移行する	**ospfv3** [*process-id* | **vpn-instance** *vpn-instance-name*] *	―
3. SPF の計算間隔を指定する	**spf-schedule-interval** *maximum-interval* [*minimum-interval* [*incremental-interval*]]	デフォルト： ● 最大間隔：5秒 ● 最小間隔：50ミリ秒 ● 増加する間隔：200ミリ秒

10.7.4 LSA 生成間隔の設定

I. LSA 生成間隔の設定

LSA の生成間隔を適切に設定することで、ネットワークの頻繁な変更によってネットワークのリソースとルータが過度に消費されることを防ぐことができます。

ネットワークが頻繁に変わらないとき、*minimum-interval* で行われます。ネットワークの変更がしばしば起こると、計算の間隔は計算の度に *incremental-interval* × 2^{n-2} ずつ増え、最後は *maximum-interval* になります。*n* は計算回数です。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. OSPFv3 view に移行する	**ospfv3** [*process-id* | **vpn-instance** *vpn-instance-name*] *	―

操作	コマンド	補足
3． LSA 生成間隔を設定する	**lsa-generation-interval** *maximum-interval* [*minimum-interval* [*incremental-interval*]]	デフォルト： ● 最大間隔：5秒 ● 最小間隔：0ミリ秒 ● 増加する間隔：0ミリ秒

10.8 インタフェースのDR優先度の設定

I. DR 優先度

ルータの優先度は、DR を選択するときに使用されます。優先度が 0 の場合、DR あるいは BDR はなれません。

II. 設定手順

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． interface view に移行する	**interface** *interface-type interface-number*	―
3． インタフェースの DR 優先度を設定する	**ospfv3 dr-priority** *priority* [**instance** *instance-id*]	デフォルト：1

10.9 OSPFv3パケットパラメータの設定

10.9.1 DD パケットの MTU チェック無効化の設定

I. DD パケットの MTU チェック無効化の設定

DD パケットに LSA がほとんどない場合には、処理効率の改善のために DD パケットの MTU をチェックする必要はありません。

II. 制限とガイドライン

インタフェースの MTU がピアと同一である場合､ネイバ関係を確立することができます。

III. 設定手順

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． interface view に移行する	**interface** *interface-type interface-number*	―
3． DD パケットの MTU チェックを無効にする	**ospfv3 mtu-ignore** [**instance** *instance-id*]	デフォルト：有効

10.9.2 OSPFv3 パケットの送受信インタフェースの無効化の設定

I. OSPFv3 パケットの送受信インタフェースの無効化

OSPF インタフェースが **silent** に設定された後、OSPF インタフェースの直接ルートが他のインタフェース経由で内部エリアプレフィックス LSA に配信することができますが、他の OSPFv3 パケットを配信することはできません。このため、OSPF インタフェースではネイバ関係を確立することはできません。この機能は OSPFv3 ネットワークの適合性を強化するものです。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. OSPFv3 view に移行する	**ospfv3** [*process-id* | **vpn-instance** *vpn-instance-name*] *	—
3. OSPFv3 パケットの送受信インタフェースを無効にする	**silent-interface** { *interface-type interface-number* | **all** }	デフォルト：有効 複数のプロセスは OSPFv3 パケットの受信と送信で同じインタフェースを無効にできますが、**silent-interface** コマンドは、現在のプロセスで有効なインタフェースにのみ適用されます。

10.10 プレフィックス抑制の設定

10.10.1 プレフィックスの抑制

デフォルトでは、OSPFv3 インタフェースは LSA 内のすべてのプレフィックスを配信します。OSPFv3 コンバージェンスを高速化するために、インタフェースがすべてのプレフィックスを配信するのを抑制できます。この機能は、抑制されたネットワークへの IP ルーティングを防止することで、ネットワークセキュリティを向上させます。

プレフィックスの省略が有効な場合:

- OSPFv3 は、Type-8 LSA 内の抑制されたインタフェースのプレフィックスを配信しません。
- ブロードキャストおよび NBMA ネットワークでは、DR は Type-2 LSA を参照する Type-9 LSA 内の抑制されたインタフェースのプレフィックスを配信しません。
- P2P および P2MP ネットワークでは、OSPFv3 は、Type-1 LSA を参照する Type-9 LSA 内の抑制されたインタフェースのプレフィックスを配信しません。

10.10.2 プレフィックス抑制の制限とガイドライン

プレフィックス抑制を使用する場合は、ベストプラクティスとして、すべての OSPFv3 ルータでプレフィックス抑制を設定します。

10.11 OSPFv3 GRの設定

10.11.1 OSPFv3 GR

GR は、ルーティングプロトコルの再起動あるいはアクティブ/スタンバイの切り替えが発生したときでも、パケット転送を継続することができます。

GR を処理するためには以下に示す 2 つの装置が必要です。

- **GR リスタータ** — グレースフルリスタートルータです。グレースフルリスタート機能を持ちます。
- **GR ヘルパー** — GR リスタータのネイバ装置です。GR プロセスを処理するために GR リスタータを補助します。

マスタ/バックアップの切り替え後のサービスの中断を防ぐため、GR リスタータが動作する OSPFv3 は以下の作業を完了しなければなりません。

- 再起動中に GR リスタータの転送エントリを安定に保ってください。
- すべてのネイバ関係を確立し、再起動後の完全なトポロジ情報を取得してください。

再起動後、GR リスタータは GR として機能するネイバルータに知らせるために Grace LSA を送信します。 Grace LSA を受信した後、GR ヘルパー機能のあるネイバルータはヘルパーモード（このため、GR ヘルパーと呼ばれます）となります。その後、GR リスタータが GR ヘルパーの支援でネイバ関係と LSDB を回復します。したがって、通常データの転送は保証されます。

10.11.2 GR リスタータの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. OSPFv3 view に移行する	**ospfv3** [*process-id* | **vpn-instance** *vpn-instance-name*] *	—
3. GR 機能を有効にする	**graceful-restart enable**	デフォルト：無効
4. (オプション設定項目)GR 間隔を設定する	**graceful-restart interval** *interval*	デフォルト：120秒

10.11.3 GR ヘルパーの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. OSPFv3 view に移行する	**ospfv3** [*process-id* | **vpn-instance** *vpn-instance-name*] *	—
3. GR ヘルパーを有効にする	**graceful-restart helper enable**	デフォルト：有効
4. GR ヘルパーの strict LSA checking を有効にする	**graceful-restart helper strict-lsa-checking**	デフォルト：無効

10.11.4 OSPFv3 GR の始動

I. OSPFv3 GR の始動

OSPFv3 GR はアクティブ/スタンバイの切り替えが発生した、あるいは以下のコマンドを実行したときに、始動します。

II. 設定手順

操作	コマンド
OSPFv3グレースフルリスタートを始動する	**reset ospfv3** [*process-id*] **process graceful-restart**

10.12 OSPFv 3 NSRの設定

I. OSPFv 3 NSR

ノンストップルーティング (NSR) は、OSPFv 3 リンクステート情報をアクティブプロセスからスタンバイプロセスにバックアップします。アクティブ/スタンバイスイッチオーバーの後、隣接関係を切断したり転送サービスに影響を与えたりすることなく、NSR はリンクステートのリカバリとルートの再生成を完了できます。

NSR は、ルーティング情報をリカバリするために隣接装置の協力を必要とせず、一般に GR よりも頻繁に使用されます。

II. 制限とガイドライン

OSPFv 3 NSR が有効になっている装置は、GR リスタータとして機能できません。

III. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. OSPFv3 view に移行する	**ospfv3** [*process-id* | **vpn-instance** *vpn-instance-name*] *	—
3. OSPFv 3 NSR を有効にする	**non-stop-routing**	デフォルト：無効 このコマンドは、現在のプロセスに対してのみ有効です。複数のOSPFv 3プロセスが存在する場合は、プロセスごとにOSPFv 3 NSRを有効にすることを推奨します。

10.13 OSPFv3のBFDの設定

I. OSPFv3 の BFD

BFD(Bidirectional forwarding detection)は、ネットワークの収束時間を改善する、OSPFv3 ネイバ装置間のリンクの接続を早急に検出しモニタする共通の機能です。BFD についての詳細はオペレーションマニュアルのセクション 10 *高可用性* "*BFD*"を参照してください。

hello パケットをネイバに送信することで検知した後、OSPFv3 はネイバアドレスの BFD を通知します。そして BFD はセッションを確立するために、ネイバアドレスを使用します。BFD セッションを確立される前、down 状態となります。この状態では、BFD コントロールパケットは、BFD コントロールパケットのトラフィックを削減させるため、1 秒以内の間隔で送信されます。BFD セッションが確立された後、BFD コントロールパケットはネゴシエートされた間隔で送信されます。そのため、早急な故障検知を行うことができます。

OSPFv3 の BFD の設定を行うために、最初に OSPFv3 の設定を行う必要があります。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. OSPFv3 view に移行する	**ospfv3** [*process-id* | **vpn-instance** *vpn-instance-name*] *	—
3. ルータ ID を指定する	**router-id** *router-id*	—
4. OSPFv3 view を終了する	**quit**	—
5. interface view に移行する	**interface** *interface-type interface-number*	—
6. インタフェースで OSPFv3 プロセスを有効にする	**ospfv3** *process-id* **area** *area-id* [**instance** *instance-id*]	—
7. インタフェースで BFD を有効にする	**ospfv3 bfd enable** [**instance** *instance-id*]	デフォルト：無効

10.14 OSPFv3ロギングとSNMP notificationの設定

10.14.1 ネイバ状態変化のロギングの有効化

I. ネイバ状態変化のロギング

この機能を有効にすることで、装置はネイバ状態が変化したログを information center に送信します。ユーザが定義したルールに従ってログを処理します。(ログを出力するか、どこに出力するか)。information center の詳細はオペレーションマニュアルのセクション 11 *システム管理* "*Information Center*"を参照してください。

II. **設定手順**

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． OSPFv3 view に移行する	**ospfv3** [*process-id* | **vpn-instance** *vpn-instance-name*] *	―
3． ネイバ状態変化のロギングを有効にする	**log-peer-change**	デフォルト：有効

10.14.2 OSPFv3 ネットワーク管理の設定

I. OSPFv3 ネットワーク管理の設定

以下の設定を行うことで OSPF のネットワーク管理を行います。

- 指定した OSPFv3 の管理を行うネットワーク管理ソフトウェアを使用するため、MIB に OSPFv3 を組み込みます。
- 重要なイベントを報告するために OSPFv3 の SNMP 通知を有効にします。
- 各間隔で出力できる SNMP 通知の出力間隔と SNMP 通知の最大数を設定します。

重要な OSPFv3 イベントを NMS に通知するには、OSPFv3 の SNMP 通知を有効にします。SNMP 通知が正しく送信されるようにするには、装置上の SNMP も設定する必要があります。SNMP 通知の詳細は、オペレーションマニュアルのセクション 11 *システム管理* "*SNMP*"を参照してください。

標準の OSPFv3MIB は、単一インスタンス MIB オブジェクトのみを提供します。標準の OSPFv3 MIB で複数の OSPFv3 プロセスを識別するには、各 OSPFv3 プロセスに一意のコンテキスト名を割り当てる必要があります。

Context は、複数インスタンス管理のために SNMPv3 に導入された方法です。SNMPv1/v2c では、プロトコル識別のコンテキスト名としてコミュニティ名を指定する必要があります。

II. 設定手順

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． OSPFv3 の SNMP 通知を有効にする	**snmp-agent trap enable ospfv3** [**grrestarter-status-change** | **grhelper-status-change** | **if-state-change** | **if-cfg-error** | **if-bad-pkt** | **neighbor-state-change** | **nssatranslator-status-change** | **virtif-bad-pkt** | **virtif-cfg-error** | **virtif-state-change** | **virtgrhelper-status-change** | **virtneighbor-state-change**]*	デフォルト有効
3． OSPFv3 view に移行する	**ospfv3** [*process-id* | **vpn-instance** *vpn-instance-name*] *	―

10.15 OSPFv3の表示と維持

すべての view で **display** コマンドを実行でき、user view で **reset** コマンドを実行できます。

操作	コマンド
OSPFv3 ABRの集約ルートの情報を表示する	**display ospfv3** [*process-id*] [**area** *area-id*] **abr-summary** [*ipv6-address prefix-length*] [**verbose**]
OSPFv3ネイバ情報を表示する	**display ospfv3** [*process-id*] [**area** *area-id*] **peer** [[*interface-type interface-number*] [**verbose**]	*peer-router-id*	**statistics**]
OSPFv3リクエストリスト情報を表示する	**display ospfv3** [*process-id*] [**area** *area-id*] **request-queue** [*interface-type interface-number*] [*neighbor-id*]
OSPFv3再送キューリスト情報を表示する	**display ospfv3** [*process-id*] [**area** *area-id*] **retrans-queue** [*interface-type interface-number*] [*neighbor-id*]
OSPFv3トポロジ情報を表示する	**display ospfv3** [*process-id*] [**area** *area-id*] **spf-tree** [**verbose**]
OSPFv3プロセスの情報を表示する	**display ospfv3** [*process-id*] [**verbose**]
OSPFv3 ABRおよびASBR情報を表示する	**display ospfv3** [*process-id*] **abr-asbr**
OSPFv3のGR状態を表示する.	**display ospfv3** [*process-id*] **graceful-restart**
OSPFv3インタフェース情報を表示する	**display ospfv3** [*process-id*] **interface** [*interface-type interface-number*	**verbose**]
OSPFv3 LSDB情報を表示する	**display ospfv3** [*process-id*] **lsdb** [{ **external**	**grace**	**inter-prefix**	**inter-router**	**intra-prefix**	**link**	**network**	**nssa**	**router**	**unknown** [*type*] } [*link-state-id*] [**originate-router** *router-id*	**self-originate**]	**statistics**	**total**	**verbose**]
OSPFv3のネクストホップの情報を表示する	**display ospfv3** [*process-id*] **nexthop**
OSPFv3 NSR情報を表示する	**display ospfv3** [*process-id*] **non-stop-routing**
OSPFv3ルーティング情報を表示する	**display ospfv3** [*process-id*] **routing** [*ipv6-address prefix-length*]
OSPFv3統計情報を表示する	**display ospfv3** [*process-id*] **statistics** [**error**]
OSPFv3仮想リンク情報を表示する	**display ospfv3** [*process-id*] **vlink**
OSPFv3プロセスをリセットする	**reset ospfv3** [*process-id*] **process** [**graceful-restart**]
OSPFv3ルート再配信をリセットする	**reset ospfv3** [*process-id*] **redistribution**
OSPFv3統計情報を削除する	**reset ospfv3** [*process-id*] **statistics**

10.16 OSPFv3設定例

10.16.1 OSPFv3 スタブエリアの設定例

I. ネットワーク要件

図 10-1に示すように、以下の設定を行います。

- すべての Switch で OSPFv3 を有効にします。
- AS を 3 つのエリアに分割します。

- エリア間のルーティング情報を転送するため、ABR として Switch B、Switch C を設定します。
- ルートの到達性に影響を与えずにエリア内の LSA を削減させるためには、エリア 2 をスタブエリアとして設定します。

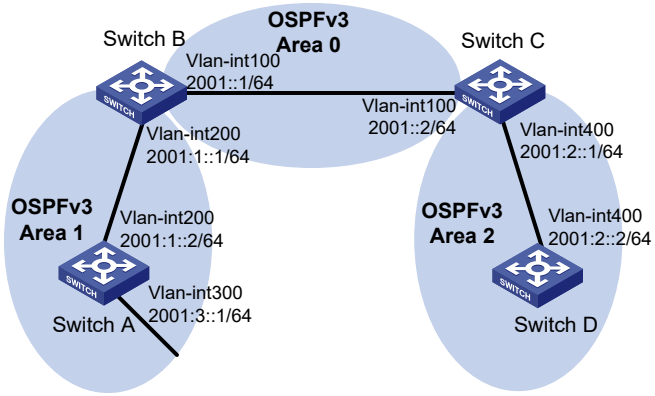


図 10-1 ネットワーク図

II. 設定手順

1) インタフェースに IPv6 アドレスを設定します。(詳細は省略します)
2) OSPFv3 を有効にします。

Switch A を設定します。OSPFv3 を有効にし、ルータ ID として 1.1.1.1 を指定します。

```
<SwitchA> system-view
[SwitchA] ospfv3
[SwitchA-ospfv3-1] router-id 1.1.1.1
[SwitchA-ospfv3-1] quit
[SwitchA] interface vlan-interface 300
[SwitchA-Vlan-interface300] ospfv3 1 area 1
[SwitchA-Vlan-interface300] quit
[SwitchA] interface vlan-interface 200
[SwitchA-Vlan-interface200] ospfv3 1 area 1
[SwitchA-Vlan-interface200] quit
```

Switch B を設定します。OSPFv3 を有効にし、ルータ ID として 2.2.2.2 を指定します。

```
<SwitchB> system-view
[SwitchB] ospfv3
[SwitchB-ospfv3-1] router-id 2.2.2.2
[SwitchB-ospfv3-1] quit
[SwitchB] interface vlan-interface 100
[SwitchB-Vlan-interface100] ospfv3 1 area 0
```

```
[SwitchB-Vlan-interface100] quit
[SwitchB] interface vlan-interface 200
[SwitchB-Vlan-interface200] ospfv3 1 area 1
[SwitchB-Vlan-interface200] quit
```

Switch C を設定します。OSPFv3 を有効にし、ルータ ID として 3.3.3.3 を指定します。

```
<SwitchC> system-view
[SwitchC] ospfv3
[SwitchC-ospfv3-1] router-id 3.3.3.3
[SwitchC-ospfv3-1] quit
[SwitchC] interface vlan-interface 100
[SwitchC-Vlan-interface100] ospfv3 1 area 0
[SwitchC-Vlan-interface100] quit
[SwitchC] interface vlan-interface 400
[SwitchC-Vlan-interface400] ospfv3 1 area 2
[SwitchC-Vlan-interface400] quit
```

Switch D を設定します。OSPFv3 を有効にし、ルータ ID として 4.4.4.4 を指定します。

```
<SwitchD> system-view
[SwitchD] ospfv3
[SwitchD-ospfv3-1] router-id 4.4.4.4
[SwitchD-ospfv3-1] quit
[SwitchD] interface vlan-interface 400
[SwitchD-Vlan-interface400] ospfv3 1 area 2
[SwitchD-Vlan-interface400] quit
```

Switch B の OSPFv3 ネイバ情報を表示します。

```
[SwitchB] display ospfv3 peer

               OSPFv3 Process 1 with Router ID 2.2.2.2

 Area: 0.0.0.0
--------------------------------------------------------------------------
 Router ID       Pri State             Dead-Time InstID Interface
 3.3.3.3         1   Full/BDR          00:00:40  0      Vlan100

 Area: 0.0.0.1
--------------------------------------------------------------------------
 Router ID       Pri State             Dead-Time InstID Interface
 1.1.1.1         1   Full/DR           00:00:40  0      Vlan200
```

Switch C の OSPFv3 ネイバ情報を表示します。

```
[SwitchC] display ospfv3 peer

               OSPFv3 Process 1 with Router ID 3.3.3.3
```

```
 Area: 0.0.0.0
----------------------------------------------------------------------
 Router ID       Pri State            Dead-Time InstID Interface
 2.2.2.2         1   Full/DR          00:00:40  0      Vlan100

 Area: 0.0.0.2
----------------------------------------------------------------------
 Router ID       Pri State            Dead-Time InstID Interface
 4.4.4.4         1   Full/BDR         00:00:40  0      Vlan400
```

Switch D の OSPFv3 ルーティングテーブル情報を表示します。

```
[SwitchD] display ospfv3 routing

              OSPFv3 Process 1 with Router ID 4.4.4.4
----------------------------------------------------------------------
 I  - Intra area route,  E1 - Type 1 external route,  N1 - Type 1 NSSA route
 IA - Inter area route,  E2 - Type 2 external route,  N2 - Type 2 NSSA route
 *  - Selected route

 *Destination: 2001::/64
  Type       : IA                                    Cost     : 2
  NextHop    : FE80::F40D:0:93D0:1                   Interface: Vlan400
  AdvRouter  : 3.3.3.3                               Area     : 0.0.0.2
  Preference : 10

 *Destination: 2001:1::/64
  Type       : IA                                    Cost     : 3
  NextHop    : FE80::F40D:0:93D0:1                   Interface: Vlan400
  AdvRouter  : 3.3.3.3                               Area     : 0.0.0.2
  Preference : 10

 *Destination: 2001:2::/64
  Type       : I                                     Cost     : 1
  Nexthop    : ::                                    Interface: Vlan400
  AdvRouter  : 4.4.4.4                               Area     : 0.0.0.2
  Preference : 10

 *Destination: 2001:3::/64
  Type       : IA                                    Cost     : 4
  NextHop    : FE80::F40D:0:93D0:1                   Interface: Vlan400
  AdvRouter  : 3.3.3.3                               Area     : 0.0.0.2
  Preference : 10

 Total: 4
 Intra area: 1         Inter area: 3         ASE: 0         NSSA: 0
```

3) スタブエリアとしてエリア 2 を設定します。

Switch D を設定します。

```
[SwitchD] ospfv3
[SwitchD-ospfv3-1] area 2
[SwitchD-ospfv3-1-area-0.0.0.2] stub
```

Switch C を設定し、スタブエリアに送信するデフォルトルートのコストを 10 に指定します。

```
[SwitchC] ospfv3
[SwitchC-ospfv3-1] area 2
[SwitchC-ospfv3-1-area-0.0.0.2] stub
[SwitchC-ospfv3-1-area-0.0.0.2] default-cost 10
```

Switch D の OSPFv3 ルーティングテーブル情報を表示します。

```
[SwitchD] display ospfv3 routing

              OSPFv3 Process 1 with Router ID 4.4.4.4
------------------------------------------------------------------------
 I  - Intra area route,  E1 - Type 1 external route,  N1 - Type 1 NSSA route
 IA - Inter area route,  E2 - Type 2 external route,  N2 - Type 2 NSSA route
 *  - Selected route

 *Destination: ::/0
  Type       : IA                                    Cost     : 11
  NextHop    : FE80::F40D:0:93D0:1                   Interface: Vlan400
  AdvRouter  : 4.4.4.4                               Area     : 0.0.0.2
  Preference : 10

 *Destination: 2001::/64
  Type       : IA                                    Cost     : 2
  NextHop    : FE80::F40D:0:93D0:1                   Interface: Vlan400
  AdvRouter  : 3.3.3.3                               Area     : 0.0.0.2
  Preference : 10

 *Destination: 2001:1::/64
  Type       : IA                                    Cost     : 3
  NextHop    : FE80::F40D:0:93D0:1                   Interface: Vlan400
  AdvRouter  : 3.3.3.3                               Area     : 0.0.0.2
  Preference : 10

 *Destination: 2001:2::/64
  Type       : I                                     Cost     : 1
  Nexthop    : ::                                    Interface: Vlan400
  AdvRouter  : 4.4.4.4                               Area     : 0.0.0.2
  Preference : 10

 *Destination: 2001:3::/64
  Type       : IA                                    Cost     : 4
  NextHop    : FE80::F40D:0:93D0:1                   Interface: Vlan400
  AdvRouter  : 3.3.3.3                               Area     : 0.0.0.2
  Preference : 10

 Total: 5
 Intra area: 1         Inter area: 4         ASE: 0         NSSA: 0
```

出力は、デフォルトルートが追加され、直接接続されたルートのコストに設定したコストがプラスされていることを示します。

4) 完全スタブエリアとしてエリア 2 を設定します。

Switch C で完全スタブエリアとしてエリア 2 を設定します。

```
[SwitchC-ospfv3-1-area-0.0.0.2] stub no-summary
```

Switch D の OSPFv3 ルーティングテーブル情報を表示します。

```
[SwitchD] display ospfv3 routing

              OSPFv3 Process 1 with Router ID 4.4.4.4
------------------------------------------------------------------------
 I  - Intra area route,  E1 - Type 1 external route,  N1 - Type 1 NSSA route
 IA - Inter area route,  E2 - Type 2 external route,  N2 - Type 2 NSSA route
 *  - Selected route

 *Destination: ::/0
  Type       : IA                                    Cost     : 11
  NextHop    : FE80::F40D:0:93D0:1                   Interface: Vlan400
  AdvRouter  : 4.4.4.4                               Area     : 0.0.0.2
  Preference : 10

 *Destination: 2001:2::/64
```

```
  Type       : I                                    Cost      : 1
  Nexthop    : ::                                   Interface: Vlan400
  AdvRouter  : 4.4.4.4                              Area      : 0.0.0.2
  Preference : 10

 Total: 2
 Intra area: 1         Inter area: 1         ASE: 0         NSSA: 0
```

出力は、ルートエントリが削減されていることを示します。デフォルトルートを除く、すべての直接接続されてないルートが削除されています。

10.16.2 OSPFv3 DR 選択の設定例

I. ネットワーク要件

- Switch A の優先度を 100 と設定し、ネットワークで最高の優先度とし、DR になるようにします。
- Switch C の優先度を 2 と設定し、ネットワークで 2 番目の優先度とし、BDR になるようにします。
- Switch B の優先度を 0 と設定し、DR あるいは BDR にならないようにします。
- Switch D の優先度をデフォルトの 1 とします。

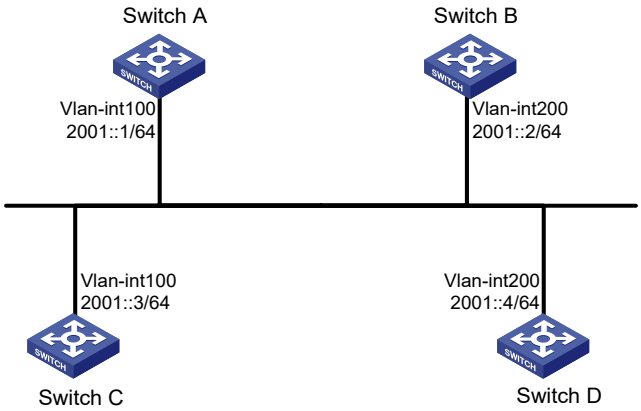


図 10-2 ネットワーク図

I. 設定手順

1) インタフェースに IPv6 アドレスを設定します。(詳細は省略します)
2) OSPFv3 を有効にします。

Switch A で OSPFv3 を有効にし、ルータ ID として 1.1.1.1 を指定します。

```
<SwitchA> system-view
[SwitchA] ospfv3
[SwitchA-ospfv3-1] router-id 1.1.1.1
[SwitchA-ospfv3-1] quit
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] ospfv3 1 area 0
```

```
[SwitchA-Vlan-interface100] quit
```

Switch B で OSPFv3 を有効にし、ルータ ID として 2.2.2.2 を指定します。

```
<SwitchB> system-view
[SwitchB] ospfv3
[SwitchB-ospfv3-1] router-id 2.2.2.2
[SwitchB-ospfv3-1] quit
[SwitchB] interface vlan-interface 200
[SwitchB-Vlan-interface200] ospfv3 1 area 0
[SwitchB-Vlan-interface200] quit
```

Switch C で OSPFv3 を有効にし、ルータ ID として 3.3.3.3 を指定します。

```
<SwitchC> system-view
[SwitchC] ospfv3
[SwitchC-ospfv3-1] router-id 3.3.3.3
[SwitchC-ospfv3-1] quit
[SwitchC] interface vlan-interface 100
[SwitchC-Vlan-interface100] ospfv3 1 area 0
[SwitchC-Vlan-interface100] quit
```

Switch D で OSPFv3 を有効にし、ルータ ID として 3.3.3.3 を指定します。

```
<SwitchD> system-view
[SwitchD] ospfv3
[SwitchD-ospfv3-1] router-id 4.4.4.4
[SwitchD-ospfv3-1] quit
[SwitchD] interface vlan-interface 200
[SwitchD-Vlan-interface200] ospfv3 1 area 0
[SwitchD-Vlan-interface200] quit
```

Switch A でネイバ情報を表示します。複数の Switch でデフォルトの DR 優先度の値が 1 に設定されています。この場合、ルータ ID が最高の優先度の Switch が DR として選出されます。このため、Switch D は DR、Switch C は BDR となります。

```
[SwitchA] display ospfv3 peer

              OSPFv3 Process 1 with Router ID 1.1.1.1

 Area: 0.0.0.0
--------------------------------------------------------------------------
 Router ID       Pri State             Dead-Time InstID Interface
 2.2.2.2         1   2-Way/DROther     00:00:36  0      Vlan200
 3.3.3.3         1   Full/BDR          00:00:35  0      Vlan100
 4.4.4.4         1   Full/DR           00:00:33  0      Vlan200
```

Switch D のネイバ情報を表示します。ネイバ状態はすべて full になっています。

```
[SwitchD] display ospfv3 peer

               OSPFv3 Process 1 with Router ID 4.4.4.4

 Area: 0.0.0.0
--------------------------------------------------------------------------
 Router ID       Pri State             Dead-Time InstID Interface
 1.1.1.1         1   Full/DROther      00:00:30  0      Vlan100
 2.2.2.2         1   Full/DROther      00:00:37  0      Vlan200
 3.3.3.3         1   Full/BDR          00:00:31  0      Vlan100
```

3)　インタフェースのルータ優先順位を設定します。

Switch A で VLAN インタフェース 100 の DR の優先度の値を 100 に設定します。

```
[SwitchA] interface Vlan-interface 100
[SwitchA-Vlan-interface100] ospfv3 dr-priority 100
[SwitchA-Vlan-interface100] quit
```

Switch B で VLAN インタフェース 200 の DR の優先度の値を 0 に設定します。

```
[SwitchB] interface vlan-interface 200
[SwitchB-Vlan-interface200] ospfv3 dr-priority 0
[SwitchB-Vlan-interface200] quit
```

Switch C で VLAN インタフェース 100 の DR の優先度の値を 2 に設定します。

```
[SwitchC] interface Vlan-interface 100
[SwitchC-Vlan-interface100] ospfv3 dr-priority 2
[SwitchC-Vlan-interface100] quit
```

Switch A のネイバ情報を表示します。DR の優先度は更新されていますが、DR と BDR は変わっていないことがわかります。

```
[SwitchA] display ospfv3 peer
               OSPFv3 Process 1 with Router ID 1.1.1.1

 Area: 0.0.0.0
--------------------------------------------------------------------------
 Router ID       Pri State             Dead-Time InstID Interface
 2.2.2.2         0   2-Way/DROther     00:00:36  0      Vlan200
 3.3.3.3         2   Full/BDR          00:00:35  0      Vlan200
 4.4.4.4         1   Full/DR           00:00:33  0      Vlan200
```

Switch D のネイバ情報を表示します。Switch D はまだ DR のままになっています。

```
[SwitchD] display ospfv3 peer

               OSPFv3 Process 1 with Router ID 4.4.4.4

 Area: 0.0.0.0
--------------------------------------------------------------------------
 Router ID       Pri State             Dead-Time InstID Interface
 1.1.1.1         100 Full/DROther      00:00:30  0      Vlan100
 2.2.2.2         0   Full/DROther      00:00:37  0      Vlan200
 3.3.3.3         2   Full/BDR          00:00:31  0      Vlan100
```

4)　DR、BDR の選出の更新を行います。

インタフェースで shutdown コマンドと undo shutdown コマンドを実行し、DR/BDR 選定をやり直します。(詳細は省略します)

Switch A のネイバ情報を表示します。Switch C が BDR になっていることがわかります。

```
[SwitchA] display ospfv3 peer

               OSPFv3 Process 1 with Router ID 1.1.1.1

 Area: 0.0.0.0
--------------------------------------------------------------------------
 Router ID       Pri State             Dead-Time InstID Interface
 2.2.2.2         0   Full/DROther      00:00:36  0      Vlan200
 3.3.3.3         2   Full/BDR          00:00:35  0      Vlan100
 4.4.4.4         1   Full/DROther      00:00:33  0      Vlan200
```

Switch D のネイバ情報を表示します。

```
[SwitchD] display ospfv3 peer

               OSPFv3 Process 1 with Router ID 4.4.4.4

 Area: 0.0.0.0
--------------------------------------------------------------------------
 Router ID       Pri State             Dead-Time InstID Interface
 1.1.1.1         100 Full/DR           00:00:30  0      Vlan100
 2.2.2.2         0   2-Way/DROther     00:00:37  0      Vlan200
 3.3.3.3         2   Full/BDR          00:00:31  0      Vlan100
```

出力は、Switch A が DR になったことを示します。

10.16.3 OSPFv3 ルート再配信の設定例

I. ネットワーク要件

図 10-3に示すように設定します。

- Switch A、Switch B、Switch C は Area2 にします。
- Switch B で OSPFv3 プロセス 1 と OSPFv3 プロセス 2 を動作させます。Switch B は OSPFv3 プロセス 1 と OSPFv3 プロセス 2 を通して、Switch A と Switch C と通信します。
- Switch B でダイレクトルートと OSPFv3 プロセス 1 のルートを OSPFv3 プロセス 2 に再配信します。そして再配信されたルートのデフォルトメトリックを 3 に設定します。Switch C は 1::0/64 と 2::0/64 のルートを学習できますが、Switch A は 3::0/64 と 4::0/64 のルートを学習できないようにします。

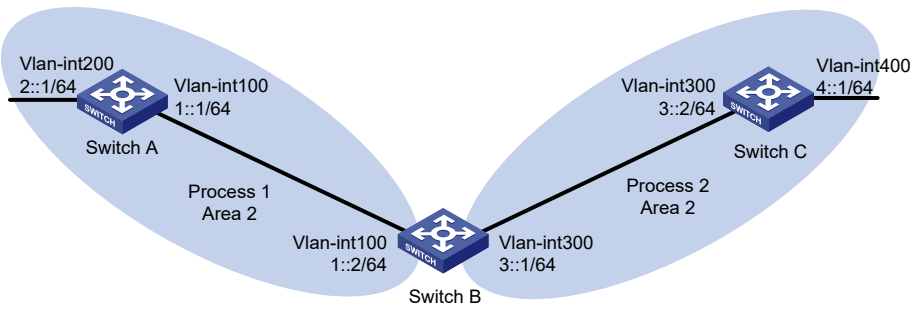


図 10-3 ネットワーク図

II. **設定手順**

1) インタフェースに IPv6 アドレスを設定します。(詳細は省略します)
2) OSPFv3 を有効にします。

Switch A で OSPFv3 プロセス 1 を有効にします。

```
<SwitchA> system-view
[SwitchA] ospfv3 1
[SwitchA-ospfv3-1] router-id 1.1.1.1
[SwitchA-ospfv3-1] quit
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] ospfv3 1 area 2
[SwitchA-Vlan-interface100] quit
[SwitchA] interface vlan-interface 200
[SwitchA-Vlan-interface200] ospfv3 1 area 2
[SwitchA-Vlan-interface200] quit
```

Switch B で OSPFv3 プロセス 1 と OSPFv3 プロセス 2 を有効にします。

```
<SwitchB> system-view
[SwitchB] ospfv3 1
[SwitchB-ospfv3-1] router-id 2.2.2.2
[SwitchB-ospfv3-1] quit
[SwitchB] interface vlan-interface 100
[SwitchB-Vlan-interface100] ospfv3 1 area 2
[SwitchB-Vlan-interface100] quit
[SwitchB] ospfv3 2
[SwitchB-ospfv3-2] router-id 3.3.3.3
[SwitchB-ospfv3-2] quit
[SwitchB] interface vlan-interface 300
[SwitchB-Vlan-interface300] ospfv3 2 area 2
[SwitchB-Vlan-interface300] quit
```

Switch C で OSPFv3 プロセス 2 を有効にします。

```
<SwitchC> system-view
[SwitchC] ospfv3 2
[SwitchC-ospfv3-2] router-id 4.4.4.4
[SwitchC-ospfv3-2] quit
[SwitchC] interface vlan-interface 300
[SwitchC-Vlan-interface300] ospfv3 2 area 2
```

```
[SwitchC-Vlan-interface300] quit
[SwitchC] interface vlan-interface 400
[SwitchC-Vlan-interface400] ospfv3 2 area 2
[SwitchC-Vlan-interface400] quit
```

Switch C のルーティングテーブル情報を表示します。

```
[SwitchC] display ipv6 routing-table

Destinations : 7 Routes : 7

Destination: ::1/128                                    Protocol  : Direct
NextHop    : ::1                                        Preference: 0
Interface  : InLoop0                                    Cost      : 0

Destination: 3::/64                                     Protocol  : Direct
NextHop    : ::                                         Preference: 0
Interface  : Vlan300                                    Cost      : 0

Destination: 3::2/128                                   Protocol  : Direct
NextHop    : ::1                                        Preference: 0
Interface  : InLoop0                                    Cost      : 0

Destination: 4::/64                                     Protocol  : Direct
NextHop    : ::                                         Preference: 0
Interface  : Vlan400                                    Cost      : 0

Destination: 4::1/128                                   Protocol  : Direct
NextHop    : ::1                                        Preference: 0
Interface  : InLoop0                                    Cost      : 0

Destination: FE80::/10                                  Protocol  : Direct
NextHop    : ::                                         Preference: 0
Interface  : NULL0                                      Cost      : 0

Destination: FF00::/8                                   Protocol  : Direct
NextHop    : ::                                         Preference: 0
Interface  : NULL0
```

3) OSPFv3 ルート再配信を設定します。

Switch B にダイレクトルートと OSPFv3 プロセス 1 のルートを OSPFv3 プロセス 2 に再配信する設定をします。

```
[SwitchB] ospfv3 2
[SwitchB-ospfv3-2] default cost 3
[SwitchB-ospfv3-2] import-route ospfv3 1
[SwitchB-ospfv3-2] import-route direct
[SwitchB-ospfv3-2] quit
```

Switch C のルーティングテーブル情報を表示します。

```
[SwitchC] display ipv6 routing-table

Destinations : 9 Routes : 9

Destination: ::1/128                                    Protocol  : Direct
NextHop    : ::1                                        Preference: 0
Interface  : InLoop0                                    Cost      : 0

Destination: 1::/64                                     Protocol  : O ASE2
```

```
NextHop    : FE80::200:CFF:FE01:1C03                Preference: 150
Interface  : Vlan300                                Cost      : 3

Destination: 2::/64                                 Protocol  : O_ASE2
NextHop    : FE80::200:CFF:FE01:1C03                Preference: 150
Interface  : Vlan300                                Cost      : 3

Destination: 3::/64                                 Protocol  : Direct
NextHop    : ::                                     Preference: 0
Interface  : Vlan300                                Cost      : 0

Destination: 3::2/128                               Protocol  : Direct
NextHop    : ::1                                    Preference: 0
Interface  : InLoop0                                Cost      : 0

Destination: 4::/64                                 Protocol  : Direct
NextHop    : ::                                     Preference: 0
Interface  : Vlan400                                Cost      : 0

Destination: 4::1/128                               Protocol  : Direct
NextHop    : ::1                                    Preference: 0
Interface  : InLoop0                                Cost      : 0

Destination: FE80::/10                              Protocol  : Direct
NextHop    : ::                                     Preference: 0
Interface  : NULL0                                  Cost      : 0

Destination: FF00::/8                               Protocol  : Direct
NextHop    : ::                                     Preference: 0
Interface  : NULL0
```

10.16.4 OSPFv3 の GR の設定例

I. ネットワーク要件

図 10-4に示すように以下の設定を行います。

- Switch A、Switch B、Switch C は同一 AS、同一 OSPFv3 ルーティングドメイン内にあり、GR が有効です。
- Switch A は GR リスタータとして動作します。Switch B、Switch C は GR ヘルパーとして動作します。GR を通して Switch A と LSDB の同期化を行います。

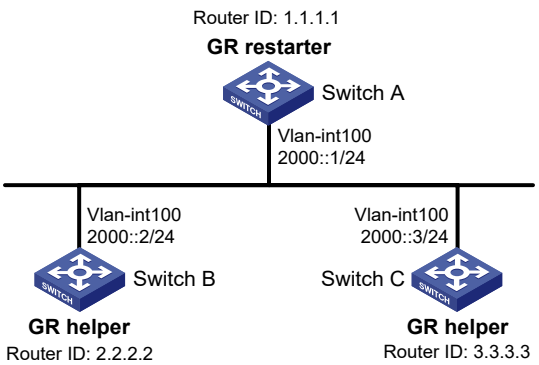


図 10-4 ネットワーク図

II. 設定手順

1) インタフェースに IPv6 アドレスを設定します。(詳細は省略します)
2) OSPFv3 を有効にします。

Switch A で OSPFv3 プロセス 1、GR を有効にし、ルータ ID を 1.1.1.1 に設定します。

```
<SwitchA> system-view
[SwitchA] ospfv3 1
[SwitchA-ospfv3-1] router-id 1.1.1.1
[SwitchA-ospfv3-1] graceful-restart enable
[SwitchA-ospfv3-1] quit
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] ospfv3 1 area 1
[SwitchA-Vlan-interface100] quit
```

Switch B で OSPFv3 を有効にし、ルータ ID を 2.2.2.2 に設定します。Switch B はデフォルトで GR ヘルパーが有効です。

```
<SwitchB> system-view
[SwitchB] ospfv3 1
[SwitchB-ospfv3-1] router-id 2.2.2.2
[SwitchB-ospfv3-1] quit
[SwitchB] interface vlan-interface 100
[SwitchB-Vlan-interface100] ospfv3 1 area 1
[SwitchB-Vlan-interface100] quit
```

Switch C で OSPFv3 を有効にし、ルータ ID を 3.3.3.3 に設定します。Switch C はデフォルトで GR ヘルパーが有効です。

```
<SwitchC> system-view
[SwitchC] ospfv3 1
[SwitchC-ospfv3-1] router-id 3.3.3.3
[SwitchC-ospfv3-1] quit
[SwitchC] interface vlan-interface 100
[SwitchC-Vlan-interface100] ospfv3 1 area 1
[SwitchC-Vlan-interface100] quit
```

III. 設定の確認

OSPFv3 の GR を起動させるため、Switch A でマスタ/スタンバイの切り替えを行います（詳細は省略します）。

10.16.5 OSPFv 3 NSR の設定例

I. ネットワーク要件

図 10-5に示すように、Switch S、Switch A、および Switch B は、同じ AS および OSPFv3 ルーティングドメインに属しています。Switch S でアクティブ/スタンバイスイッチオーバーが発生したときに正しいルーティングを保証するには、Switch S で OSPFv3 NSR を有効にします。

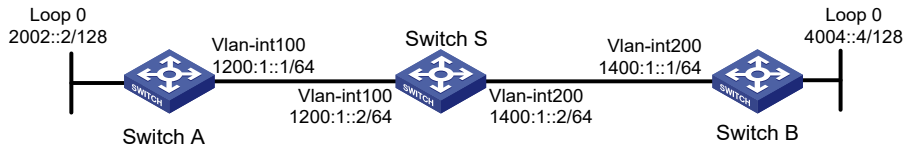


図 10-5 ネットワーク図

II. 設定手順

1) スイッチのインタフェースの IP アドレスとサブネットマスクを設定します。（詳細は表示されていません。）
2) スイッチで OSPFv3 を設定して、Switch S、Switch A、および Switch B がレイヤ 3 で相互に通信できるようにします。（詳細は表示されていません）
3) OSPFv3 を設定します。

Switch A で OSPFv 3 を有効にし、ルータ ID を 1.1.1.1 に設定します。

```
<SwitchA> system-view
[SwitchA] ospfv3 1
[SwitchA-ospfv3-1] router-id 1.1.1.1
[SwitchA-ospfv3-1] quit
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] ospfv3 1 area 1
[SwitchA-Vlan-interface100] quit
```

Switch B で OSPFv 3 を有効にし、ルータ ID を 2.2.2.2 に設定します。

```
<SwitchB> system-view
[SwitchB] ospfv3 1
[SwitchB-ospfv3-1] router-id 2.2.2.2
[SwitchB-ospfv3-1] quit
[SwitchB] interface vlan-interface 200
[SwitchB-Vlan-interface200] ospfv3 1 area 1
[SwitchB-Vlan-interface200] quit
```

Switch S で、OSPFv 3 を有効にし、ルータ ID を 3.3.3.3 に設定して、NSR を有効にします。

```
<SwitchS> system-view
[SwitchS] ospfv3 1
[SwitchS-ospfv3-1] router-id 3.3.3.3
[SwitchS-ospfv3-1] non-stop-routing
[SwitchS-ospfv3-1] quit
[SwitchS] interface vlan-interface 100
[SwitchS-Vlan-interface100] ospfv3 1 area 1
[SwitchS-Vlan-interface100] quit
[SwitchS] interface vlan-interface 200
[SwitchS-Vlan-interface200] ospfv3 1 area 1
[SwitchS-Vlan-interface200] quit
```

III. 設定の確認

以下を確認します。

- Switch S でアクティブ/スタンバイスイッチオーバーが発生した場合、Switch A と Switch B のネイバ関係およびルーティング情報は変更されていません。(詳細は表示されません。)
- Switch A から Switch B へのトラフィックは影響を受けていません。(詳細は表示されません。)

目次

このセクションのページは **5-x-x** です。

11 章 IPv6 ポリシーベースルーティング 11-1
11.1 概要.....11-1
11.1.1 IPv6 パケット転送プロセス.....11-1
11.1.2 IPv6 PBR タイプ.....11-1
11.1.3 ポリシー.....11-1
11.1.4 PBR と Track.....11-2
11.2 IPv6 PBR 設定作業リスト.....11-2
11.3 IPv6 ポリシーの設定.....11-3
11.3.1 IPv6 ノードの作成.....11-3
11.3.2 IPv6 ノードのマッチ条件の設定.....11-3
11.3.3 IPv6 ノードのアクションの設定.....11-3
11.4 IPv6 PBR ポリシーの指定.....11-4
11.4.1 IPv6 ローカル PBR の IPv6 ポリシーの指定.....11-4
11.4.2 IPv6 インタフェース PBR の IPv6 ポリシーの指定.....11-4
11.5 IPv6 PBR の表示と維持.....11-5
11.6 IPv6 PBR の設定例.....11-5
11.6.1 パケットベースの IPv6 ローカル PBR の設定例.....11-5
11.6.2 パケットベースの IPv6 インタフェース PBR の設定例.....11-7

11章 IPv6 ポリシーベースルーティング

11.1 概要

IPv6 ポリシーベースルーティング(PBR) は、ユーザが定義したルーティングポリシーに従ったルーティングメカニズムです。ポリシーは ACL のような指定した条件にマッチしているパケットにネクストホップを指定することができます。

11.1.1 IPv6 パケット転送プロセス

装置は以下のように受信した IPv6 パケットを転送します。

1) 装置はマッチしているパケットを転送するため、PBR を使用します。
2) 以下のイベントのいずれかが発生したとき、装置はパケットを転送するためルーティングテーブルのルート（デフォルトルートを除きます）を検索します。
   - パケットが PBR ポリシーにマッチしません。
   - PBR をもとにしたパケットの転送に失敗します。
3) パケット転送に失敗した場合、デフォルトルートを使用してパケットを転送します。

11.1.2 IPv6 PBR タイプ

PBR はローカル PBR とインタフェース PBR の 2 種類があります。ローカル PBR はサポートしていません。

- **ローカル PBR**－**ping** コマンドの ICMP パケットのような、ローカルで作成されたパケットの転送に適用されます。
- **インタフェース PBR**－インタフェースに転送されるパケットに対して適用されます。

11.1.3 ポリシー

Ipv6 ポリシーは、マッチ条件と、マッチしたパケットへのアクションから構成されます。ポリシーは 1 つ以上のノードから構成されます。

- ノードはノード番号によって指定されます。最も小さいノード番号が最も高い優先度となります。
- ノードは **if-match** と **apply** から構成されます。**if-match** でノードにマッチする条件を指定し、**apply** でアクションを適用します。
- ノードは **permit** や **deny** のモードがあります。

ポリシーは、パケットを順番にマッチさせます。もしパケットがノードのマッチ条件に適合する場合、ノードのアクションが適用されます。マッチ条件に適合しない場合、次のノードのマッチ条件と適合の確認を行います。いずれのノードのマッチ条件に適合しない場合、ルーティングテーブルに従って転送されます。

I. if-match

IPv6 PBR は ACL にマッチする **if-match acl** のみをサポートします。ノードで指定できる **if-match acl** は、1 つのみです。

II. apply

IPv6 PBR はパケットのネクストホップを設定する **apply next-hop** のみサポートします。

III. ノードのマッチモードの関係

すべての if-match にパケットが適合するか？	マッチモード	
	許可モード	拒否モード
Yes	• ノードに**apply**が設定されている場合、IPv6 PBRは**apply**を実行します。IPv6 PBRがパケットの転送に成功した場合、IPv6 PBRは次のノードとマッチしません。 • ノードに**apply**が設定されていない場合、パケットはルーティングテーブルに従って転送されます。	パケットはルーティングテーブルに従って転送されます。
No	IPv6 PBRは次のノードにパケットを移動します。	IPv6 PBRは次のノードにパケットを移動します。

🕮 **メモ：**

if-match がないノードは、すべてのパケットにマッチします。

11.1.4 PBR と Track

PBRは **apply**の有効な状態を track されたネクストホップのリンク状態にダイナミックに適応するため、Track 機能と一緒に動作することができます。

- Track エントリが **Negative** に変更するオブジェクトに関連づけられているとき、apply は無効です。
- Track エントリが **Positive** あるいは **NotReady** に変更するオブジェクトに関連づけられているとき、**apply** は有効です。

Track と PBR の関連づけの詳細はオペレーションマニュアルのセクション 10 *高可用性*” *Track*” を参照してください。

11.2 IPv6 PBR設定作業リスト

作業リスト
(必須設定項目) IPv6ポリシーの設定: 1. IPv6ノードの作成 2. IPv6ノードのマッチ条件の設定 3. IPv6ノードのアクションの設定
(必須設定項目) IPv6 PBRポリシーの指定: • IPv6ローカルPBRのIPv6ポリシーの指定 • IPv6インタフェースPBRのIPv6ポリシーの指定

11.3 IPv6ポリシーの設定

11.3.1 IPv6 ノードの作成

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. IPv6 ノードあるいはポリシーノードを作成し、IPv6 policy node view に移行する	**ipv6 policy-based-route** *policy-name* [**deny** | **permit**] **node** *node-number*	―

11.3.2 IPv6 ノードのマッチ条件の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. IPv6 policy node view に移行する	**ipv6 policy-based-route** *policy-name* [**deny** | **permit**] **node** *node-number*	―
3. ACL のマッチ条件を設定する	**if-match acl** { *ipv6-acl-number* | **name** *ipv6-acl-name* }	デフォルト：設定なし ACLのマッチ条件はレイヤ2情報と一致することができません。 ACLのマッチ条件は**permit**あるいは**deny**アクション、指定したACLのタイムレンジを使用することができません。

11.3.3 IPv6 ノードのアクションの設定

I. apply

IPv6 PBR は **apply next-hop** のみをサポートして、一致するパケットのネクストホップを設定します。

II. 制限とガイドライン

IPv6 PBR は、IPv6 PBR ポリシーで指定されたネクストホップまたはデフォルトネクストホップの有効性を決定するために、定期的に FIB テーブル内を検索します。 ネクストホップでルート変更が発生した場合、IPv6 PBR はすぐにルートを更新しない場合があります。この結果、一時的な通信中断が発生します。

III. IPv6 ノードのアクションの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―

操作	コマンド	補足
2. IPv6 policy node view に移行する	**ipv6 policy-based-route** *policy-name* [**deny** | **permit**] **node** *node-number*	―
3. ネクストホップを設定する	**apply next-hop** [**vpn-instance** *vpn-instance-name*] { *ipv6-address* [**direct**] [**track** *track-entry-number*] }&<1-2>	デフォルト : ネクストホップは指定されません。 バックアップ用に、このステップを複数実行することで複数ネクストホップを設定することができます。 ネクストホップの最大は2です。

11.4 IPv6 PBRポリシーの指定

11.4.1 IPv6 ローカル PBR の IPv6 ポリシーの指定

I. IPv6 ローカル PBR

ローカルで生成されたパケットの転送をガイドする IPv6 ローカル PBR の IPv6 ポリシーを指定するには、次の作業を実行します。

II. 制限とガイドライン

IPv6 ローカル PBR に指定できるポリシーは 1 つだけです。指定したポリシーがすでに存在することを確認する必要があります。新しいポリシーを適用する前に、まず現在のポリシーを削除する必要があります。

IPv6 ローカル PBR は、ping や Telnet などのローカルサービスに影響を与える可能性があります。IPv6 ローカル PBR を使用する場合は、装置のローカルサービスへの影響を十分に理解してください。

III. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. ローカルに IPv6 PBR を適用する	**ipv6 local policy-based-route** *policy-name*	デフォルト：設定なし

11.4.2 IPv6 インタフェース PBR の IPv6 ポリシーの指定

I. インタフェース PBR

インタフェースで受信したパケットの転送を行うため、インタフェースに IPv6 ポリシーを適用します。

II. 制限とガイドライン

インタフェースには 1 つのポリシーのみ適用することができます。指定したポリシーが存在することを確認してください。新しいポリシーを適用する前にインタフェースから現在のポリシーを削除してください。

複数のインタフェースで同じポリシーを適用することができます。

III. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. interface view に移行する	**interface** *interface-type interface-number*	ー
3. インタフェースに IPv6 PBR を適用する	**ipv6 policy-based-route** *policy-name*	デフォルト：設定なし

11.5 IPv6 PBRの表示と維持

すべての view で **display** コマンドを実行し、user view で **reset** コマンドを実行します。

操作	コマンド
IPv6 PBRポリシー情報を表示する	**display ipv6 policy-based-route** [**policy** *policy-name*]
IPv6インタフェースPBRと統計情報を表示する	**display ipv6 policy-based-route interface** *interface-type interface-number*
IPv6 PBR設定を表示する	**display ipv6 policy-based-route setup**
IPv6 PBRの統計情報を削除する	**reset ipv6 policy-based-route statistics** [**policy** *policy-name*]

11.6 IPv6 PBRの設定例

11.6.1 パケットベースの IPv6 ローカル PBR の設定例

I. ネットワーク要件

図 11-1に示すように、Switch B と Switch C は Switch A を介して接続されています。Switch B と Switch C には、互いに到達するルートがありません。

Switch A で IPv6 PBR を設定し、すべての TCP パケットをネクストホップ 1::2 (Switch B) に転送します。

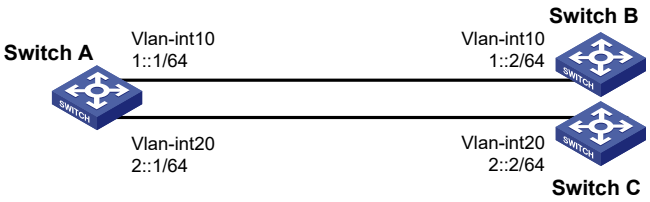


図 11-1 ネットワーク図

II. 設定手順

1)　Switch A を設定します。

VLAN10、VLAN20 を作成します。

```
<SwitchA> system-view
[SwitchA] vlan 10
[SwitchA-vlan10] quit
[SwitchA] vlan 20
[SwitchA-vlan20] quit
```

VLAN インタフェース 10 および VLAN インタフェース 20 の IPv6 アドレスを設定します。

```
[SwitchA] interface vlan-interface 10
[SwitchA-Vlan-interface10] ipv6 address 1::1 64
[SwitchA-Vlan-interface10] quit
[SwitchA] interface vlan-interface 20
[SwitchA-Vlan-interface20] ipv6 address 2::1 64
[SwitchA-Vlan-interface20] quit
```

TCP パケットにマッチする ACL 3001 を設定します。

```
[SwitchA] acl ipv6 advanced 3001
[SwitchA-acl-ipv6-adv-3001] rule permit tcp
[SwitchA-acl-ipv6-adv-3001] quit
```

TCP パケットをネクストホップ 1::2 に転送するポリシー**aaa** のノード 5 を設定します。

```
[SwitchA] ipv6 policy-based-route aaa permit node 5
[SwitchA-pbr6-aaa-5] if-match acl 3001
[SwitchA-pbr6-aaa-5] apply next-hop 1::2
[SwitchA-pbr6-aaa-5] quit
```

ポリシー**aaa** を Switch A に適用して、IPv6 ローカル PBR を設定します。

```
[SwitchA] ipv6 local policy-based-route aaa
```

2)　Switch B を設定します。

VLAN 10 を作成します。

```
<SwitchB> system-view
[SwitchB] vlan 10
[SwitchB-vlan10] quit
```

VLAN インタフェース 10 の IPv6 アドレスを設定します。

```
[SwitchB] interface vlan-interface 10
[SwitchB-Vlan-interface10] ipv6 address 1::2 64
```

3)　Switch C を設定します。

VLAN 20 を作成します。

```
<SwitchC> system-view
[SwitchC] vlan 20
[SwitchC-vlan20] quit
```

VLAN インタフェース 20 の IPv6 アドレスを設定します。

```
[SwitchC] interface vlan-interface 20
[SwitchC-Vlan-interface20] ipv6 address 2::2 64
```

III. 設定の確認

Switch A の Switch B に Telnet を行います。Telnet は成功します。

Switch A の Switch C に Telnet を行います。Telnet は失敗します。

Switch A から Switch C に ping を実行します。ping は成功します。

Telnet は TCP を使用し、ping は ICMP を使用しています。結果を以下に示します。

- Switch A から送信されたすべての TCP パケットは、ネクストホップ 1 :: 2 に転送されます。
- 他のパケットは VLAN インタフェース 20 に転送されます。
- IPv6 ローカル PBR の設定が有効です。

11.6.2 パケットベースの IPv6 インタフェース PBR の設定例

I. ネットワーク要件

図 11-2に示すように、Switch B と Switch C は互いに通信できるルートがありません。

Switch A で IPv6 PBR を設定し、VLAN インタフェース 11 で受信されたすべての TCP パケットをネクストホップ 1::2（Switch B）に転送します。

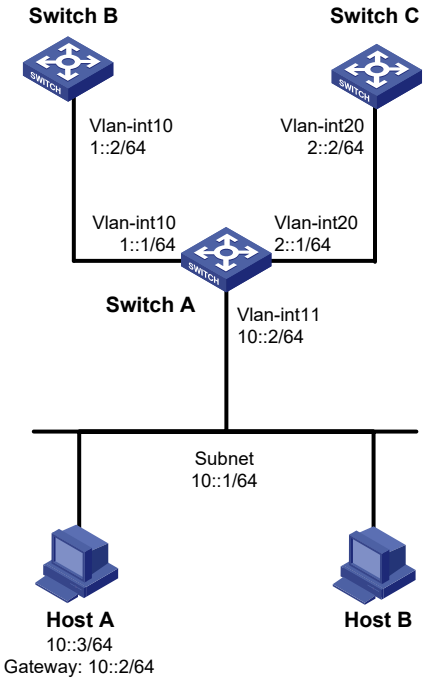


図 11-2 ネットワーク図

II. 設定手順

1)　Switch A を設定します。

VLAN10、VLAN20 を作成します。

```
<SwitchA> system-view
[SwitchA] vlan 10
[SwitchA-vlan10] quit
[SwitchA] vlan 20
[SwitchA-vlan20] quit
```

RIPng を設定します。

```
[SwitchA] ripng 1
[SwitchA-ripng-1] quit
[SwitchA] interface vlan-interface 10
[SwitchA-Vlan-interface10] ipv6 address 1::1 64
[SwitchA-Vlan-interface10] ripng 1 enable
[SwitchA-Vlan-interface10] quit
[SwitchA] interface vlan-interface 20
[SwitchA-Vlan-interface20] ipv6 address 2::1 64
[SwitchA-Vlan-interface20] ripng 1 enable
[SwitchA-Vlan-interface20] quit
```

TCP パケットにマッチする ACL 3001 を設定します。

```
[SwitchA] acl ipv6 advanced 3001
[SwitchA-acl-ipv6-adv-3001] rule permit tcp
[SwitchA-acl-ipv6-adv-3001] quit
```

TCP パケットをネクストホップ 1::2 に転送するポリシー**aaa** のノード 5 を設定します。

```
[SwitchA] ipv6 policy-based-route aaa permit node 5
[SwitchA-pbr6-aaa-5] if-match acl 3001
[SwitchA-pbr6-aaa-5] apply next-hop 1::2
[SwitchA-pbr6-aaa-5] quit
```

VLAN インタフェース 11 にポリシー**aaa** を適用するように IPv6 インタフェース PBR を設定します。

```
[SwitchA] interface vlan-interface 11
[SwitchA-Vlan-interface11] ipv6 address 10::2 64
[SwitchA-Vlan-interface11] undo ipv6 nd ra halt
[SwitchA-Vlan-interface11] ripng 1 enable
[SwitchA-Vlan-interface11] ipv6 policy-based-route aaa
```

2)　Switch B を設定します。

VLAN 10 を作成します。

```
<SwitchB> system-view
[SwitchB] vlan 10
[SwitchB-vlan10] quit
```

RIPng を設定します。

```
[SwitchB] ripng 1
[SwitchB-ripng-1] quit
[SwitchB] interface vlan-interface 10
[SwitchB-Vlan-interface10] ipv6 address 1::2 64
[SwitchB-Vlan-interface10] ripng 1 enable
[SwitchB-Vlan-interface10] quit
```

3)　Switch C を設定します。

VLAN 20 を作成します。

```
<SwitchC> system-view
[SwitchC] vlan 20
[SwitchC-vlan20] quit
```

RIPng を設定します。

```
[SwitchC] ripng 1
[SwitchC-ripng-1] quit
[SwitchC] interface vlan-interface 20
[SwitchC-Vlan-interface20] ipv6 address 2::2 64
[SwitchC-Vlan-interface20] ripng 1 enable
[SwitchC-Vlan-interface20] quit
```

III. 設定の確認

IPv6 を有効にし、Host A の IPv6 アドレス 10::3 を設定します。

```
C:\>ipv6 install
Installing...
Succeeded.
C:\>ipv6 adu 4/10::3
```

Host A から Switch A に直接接続されている Switch B に Telnet を行います。Telnet は成功します。

Host A から Switch A に直接接続されている Switch C に Telnet を行います。Telnet は失敗します。

Host A から Switch C に ping を実行します。ping は成功します。

Telnet は TCP を使用し、ping は ICMP を使用しています。結果を以下に示します。

- Switch A の VLAN インタフェース 11 に到着するすべての TCP パケットは、ネクストホップ 1::2 に転送されます。
- 他のパケットは VLAN インタフェース 20 に転送されます。
- IPv6 インタフェース PBR の設定が有効です。

目次

このセクションのページは **5-x-x** です。

12 章 ルーティングポリシー.....12-1
12.1 概要.....12-1
12.1.1 ルーティングポリシーの実装.....12-1
12.1.2 フィルタ.....12-1
12.2 ルーティングポリシーの設定作業リスト.....12-2
12.3 IPv4 プレフィックスリストの設定.....12-2
12.4 IPv6 プレフィックスリストの設定.....12-3
12.5 AS パスリストの設定.....12-3
12.6 コミュニティリストの設定.....12-4
12.7 拡張コミュニティリストの設定.....12-4
12.8 ルーティングポリシーの設定.....12-5
12.8.1 ルーティングポリシーの作成.....12-5
12.8.2 if-match の設定.....12-5
12.8.3 apply の設定.....12-6
12.9 ルーティングポリシーの表示と維持.....12-7
12.10 ルーティングポリシーの設定例.....12-7
12.10.1 スタティックルートを RIP に再配信するためのルーティングポリシーの適用例12-7
12.10.2 IPv6 ルートの再配信ルートへのルーティングポリシーの設定例.....12-9

12章 ルーティングポリシー

12.1 概要

ルーティングポリシーは、ルータでルートをフィルタしたり、ルーティング情報を修正したりするために使用されます。

ルーティングポリシーは配信、受信、再配信されたルートをフィルタしたり、ルートを受信、配信、再配信するときの属性を修正したりするために使用されます。

12.1.1 ルーティングポリシーの実装

ルーティングポリシーを設定するために、以下のことを行います。

1) 宛先アドレスや配信するルータのアドレスのようなルーティングの属性に従ってフィルタリングを設定します。
2) ルーティングポリシーを作成し、ルーティングポリシーにフィルタリングを適用します。

12.1.2 フィルタ

ルーティングポリシーはルートにマッチする以下のフィルタリングを使用することができます。

I. ACL

ACL はルーティング情報の宛先、あるいはネクストホップにマッチするように設定されます。

ACL についての詳細は、オペレーションマニュアルのセクション 8 *ACL and QoS*”*ACL*”を参照してください。

II. IP プレフィックスリスト

IP プレフィックスリストはルーティング情報の宛先アドレスにマッチするように設定されます。

IP プレフィックスリストには、プレフィックス範囲を指定する複数の項目を含めることができます。 ルートの各宛先 IP アドレスプレフィックスは、インデックス番号の昇順でこれらの項目と比較されます。 リスト内の 1 つの項目と一致する場合、プレフィックスは IP プレフィックスリストと一致します。

III. ルーティングポリシー

ルーティングポリシーは複数のノードで構成することができ、それらは論理和の関係にあります。各ルーティングポリシーノードはマッチする単位で、小さい番号から先にマッチします。一度特定のノードにマッチした場合、ルーティングポリシーをパスし、次のノードでは参照されません。

各ノードは **permit** と **deny** の設定で構成されます。

- **permit** － ルーティングポリシーノードに **permit** を指定します。ルートがノードのすべての **if-match** にマッチする場合、ノードの **apply** が実行されていれば、次のノードのマッチングを行いません。ルートは次のノードと比較されません。ノードのすべての **if-match** にマッチしない場合、次のノードのマッチングを行います。
- **deny** － ルーティングポリシーノードに **deny** を指定します。**deny** ノードの **apply** は実行されません。ルートがノードのすべての **if-match** にマッチする場合、ルートを廃棄し、次のノードのマッチングを行いません。もしルートがノードのすべての **if-match** にマッチしない場合、次のノードのマッチングを行います。
- ノードは **if-match**、**apply** から構成されます。
- **if-match** － マッチする基準を定義します。マッチする対象はルーティング情報のいくつかの属性です。ルーティングポリシーのノードの **if-match** は論理積の関係にあります。つまり、パケットはルーティングポリシーをパスするためには、ノードのすべての **if-match** にマッチする必要があります。
- **apply** － ルート属性の修正のような許可されたパケットで実行されるアクションを指定します。

if-match、**apply** を設定する際、以下のガイドラインに従います。

- ルーティングフィルタのみ実装する場合、apply は設定する必要がありません。
- permit モードノードの if-match を設定しない場合、ノードはすべてのルートを許可します。
- マッチしていないルートを許可するため、複数の deny モードノードの後に if-match あるいは apply がないように **permit** モードノードを設定してください。

12.2 ルーティングポリシーの設定作業リスト

作業リスト
(オプション設定項目) フィルタの設定: ● IPv4プレフィックスリストの設定 ● IPv6プレフィックスリストの設定 ● ASパスリストの設定 ● コミュニティリストの設定 ● 拡張コミュニティリストの設定
ルーティングポリシーの設定: 1． ルーティングポリシーの作成 2． if-match の設定 3． apply の設定

12.3 IPv4プレフィックスリストの設定

I. 制限とガイドライン

すべてのアイテムが **deny** モードで設定されている場合、IPv4 プレフィックスリストをパスすることはできません。他の IPv4 ルーティング情報をパスするには、複数の **deny** アイテムの次に **permit** 0.0.0.0 0 **less-equal** 32 を定義する必要があります。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. IPv4 プレフィックスリストを設定する	**ip prefix-list** *prefix-list-name* [**index** *index-number*] { **deny** | **permit** } *ip-address mask-length* [**greater-equal** *min-mask-length*] [**less-equal** *max-mask-length*]	—

12.4 IPv6プレフィックスリストの設定

I. 制限とガイドライン

すべてのアイテムが **deny** モードで設定されている場合、IPv6 プレフィックスリストをパスすることはできません。他の IPv4 ルーティング情報をパスするには、複数の **deny** アイテムの次に **permit** :: 0 **less-equal** 128 を定義する必要があります。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. IPv6 プレフィックスリストを設定する	**ipv6 prefix-list** *prefix-list-name* [**index** *index-number*] { **deny** | **permit** } *ipv6-address* { **inverse** *inverse-prefix-length* | *prefix-length* [**greater-equal** *min-prefix-length*] [**less-equal** *max-prefix-length*] }	—

12.5 ASパスリストの設定

I. AS パスリストの設定

番号で識別された AS パスリストとして複数のアイテムを定義することができます。アイテム間の関係は論理和です。つまり、ルートは、定義されたアイテムのうちの 1 つにマッチする場合、AS パスリストをパスします。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AS パスリストを設定する	**ip as-path** *as-path-number* { **deny** | **permit** } *regular-expression*	—

12.6 コミュニティリストの設定

I. コミュニティリストの設定

番号で識別されたコミュニティリストとして複数のアイテムを定義することができます。アイテム間の関係は論理和です。つまり、ルートは、定義されたアイテムのうちの 1 つにマッチする場合、コミュニティリストをパスします。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. コミュニティリストを設定する	• 標準コミュニティリストを設定する: **ip community-list** { *basic-comm-list-num* | **basic** *basic-comm-list-name* } { **deny** | **permit** } [*community-number*&<1-32> | *aa:nn*&<1-32>] [**internet** | **no-advertise** | **no-export** | **no-export-subconfed**] * • 拡張コミュニティリストを設定する: **ip community-list** { *adv-comm-list-num* | **advanced** *adv-comm-list-name* } { **deny** | **permit** } *regular-expression*	—

12.7 拡張コミュニティリストの設定

I. 拡張コミュニティリストの設定

番号で識別された拡張コミュニティリストとして複数のアイテムを定義することができます。アイテム間の関係は論理和です。つまり、ルートは、定義されたアイテムのうちの 1 つにマッチする場合、拡張コミュニティリストをパスします。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. 拡張コミュニティリストを設定する	**ip extcommunity-list** *ext-comm-list-number* { **deny** | **permit** } { **rt** *route-target* }&<1-32>	デフォルト：設定なし

12.8 ルーティングポリシーの設定

12.8.1 ルーティングポリシーの作成

I. ルーティングポリシーの作成

ルーティングポリシーが 1 つ以上のノードを持つ場合、少なくとも 1 つのノードは **permit** で構成される必要があります。どのノードにもマッチしないルーティング情報はルーティングポリシーをパスすることができません。ルーティングポリシーのすべてのノードが **deny** で設定された場合、どのルーティング情報も、ルーティングポリシーをパスすることができません。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. ルーティングポリシーとノードを作成し、routing policy node view に移行する	**route-policy** *route-policy-name* { **deny** | **permit** } **node** *node-number*	—

12.8.2 if-match の設定

I. if-match の設定

if-match を指定しないあるいは複数の **if-match** をルーティングポリシーに設定することができます。もし **permit** モードで **if-match** が指定されない場合、すべてのルーティング情報はパスすることができます。もし **deny** モードで **if-match** が指定されない場合、すべてのルーティング情報はパスすることができません。

II. 制限とガイドライン

if-match を設定するとき、以下の制限とガイドラインに従ってください。

- ルーティングポリシーノードの **if-match** は、論理積の関係にあります。つまり、ルーティング情報は、**apply** が実行される前にすべての **if-match** を満たす必要があります。もし **if-match** が最大長を超えるとき、複数の **if-match** が作成されます。これらは論理和の関係にあります。ルーティング情報は 1 つのみ必要です。
- ノードの **if-match** が IPv6 ACL のみを使用する場合、すべての IPv4 ルートはノードと一致します。 ノードの **if-match** が IPv4 ACL のみを使用する場合、すべての IPv6 ルートはノードと一致します。
- **if-match** で使用される ACL が存在しない場合、常に一致します。指定された ACL のルールが一致しない場合、または一致ルールが非アクティブの場合、一致しません。
- **if-match** で使用されるプレフィックスリスト、コミュニティリスト、または拡張コミュニティリストが存在しない場合、は常に一致します。指定されたプレフィックスリスト、コミュニティリスト、または拡張コミュニティリストのルールが一致しない場合、一致しません。

III. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. routing policy node view に移行する	**route-policy** *route-policy-name* { **deny** | **permit** } **node** *node-number*	―
3. 宛先、ネクストホップ、送信元が指定された ACL あるいはプレフィックスリストにマッチするルートを定義する	• IPv4: **if-match ip** { **address** | **next-hop** | **route-source** } { **acl** *ipv4-acl-number* | **prefix-list** *prefix-list-name* } • IPv6: **if-match ipv6** { **address** | **next-hop** | **route-source** } { **acl** *ipv6-acl-number* | **prefix-list** *prefix-list-name* }	デフォルト：設定なし **if-match**によって参照される ACLが存在しない場合、プレフィックスリストはマッチしています。参照されるACL がマッチしていないあるいはアクティブ状態でない場合、プレフィックスリストはマッチしていません。 **if-match**に指定するACLに、VPN ACLを指定することができません。
4. ルートを定義する	• 指定されたコストを持つルートにマッチするルートを定義する: **if-match cost** *value* • 指定された出力インタフェースにマッチするルートを定義する: **if-match interface** { *interface-type interface-number* }&<1-16> • 指定されたルートタイプを持つルートにマッチするルートを定義する: **if-match route-type** { **external-type1** | **external-type1or2** | **external-type2** | **internal** | **nssa-external-type1** | **nssa-external-type1or2** | **nssa-external-type2** }* • 指定されたタグを持つ IGPルートにマッチするルートを定義する: **if-match tag** *tag-value*	デフォルト：設定なし

12.8.3 apply の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. routing policy node view に移行する	**route-policy** *route-policy-name* { **deny** | **permit** } **node** *node-number*	―

操作	コマンド	補足
3. ルートのコストとコストタイプを設定する	• ルートのコストを設定する: **apply cost** [**+** | **-**] value • ルートのコストタイプを設定する: **apply cost-type** { **internal** | **type-1** | **type-2** }	デフォルト：設定なし
4. ルートのネクストホップを設定する	• IPv4: **apply ip-address next-hop** *ip-address* [**public** | **vpn-instance** *vpn-instance-name*] • IPv6: **apply ipv6 next-hop** *ipv6-address*	デフォルト：設定なし **apply ip-address next-hop** コマンドと **apply ipv6 next-hop** コマンドは、それぞれ、IPv4とIPv6の再配信ルートには適用できません。
5. ルーティングプロトコルの優先度を設定する	**apply preference** *preference*	デフォルト：設定なし
6. OSPF ルートのタグを設定する	**apply tag** *value*	デフォルト：設定なし

12.9 ルーティングポリシーの表示と維持

すべての view で **display** コマンドを実行でき、user view で **reset** コマンドを実行できます。

操作	コマンド
IPv4 プレフィックスリストの統計情報を表示する	**display ip prefix-list** [**name** *prefix-list-name*]
IPv6 プレフィックスリストの統計情報を表示する	**display ipv6 prefix-list** [**name** *prefix-list-name*]
ルーティングポリシー情報を表示する	**display route-policy** [**name** *route-policy-name*]
IPv4 プレフィックスリストの統計情報を削除する	**reset ip prefix-list** [*prefix-list-name*]
IPv6 プレフィックスリストの統計情報を削除する	**reset ipv6 prefix-list** [*prefix-list-name*]

12.10 ルーティングポリシーの設定例

12.10.1 スタティックルートを RIP に再配信するためのルーティングポリシーの適用例

I. ネットワーク要件

図 12-1に示すように、Switch A は、 RIP を使用して Switch B とルーティング情報を交換します。

Switch A で、3 つのスタティックルートを設定します。ルーティングポリシーを使用して、ネットワーク 20.1.1.1/32 および 40.1.1.1/32 を再配信し、ネットワーク 30.1.1.1/32 をブロックするように Switch B を設定します。

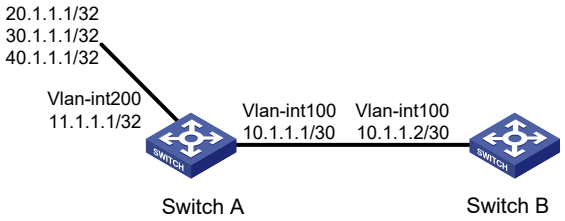


図 12-1 ネットワーク図

II. 設定手順

1)　Switch A を設定します。

インタフェース VLAN-interface 100 および VLAN-interface 200 用の IP アドレスを設定します。

```
<SwitchA> system-view
[SwitchA] interface vlan-interface 100
[SwitchA-vlan-interface100] ip address 10.1.1.1 30
[SwitchA-vlan-interface100] quit
[SwitchA] interface vlan-interface 200
[SwitchA-vlan-interface200] ip address 11.1.1.1 32
[SwitchA-vlan-interface200] quit
```

インタフェース VLAN-interface 100 で RIP を有効にします。

```
[SwitchA] interface vlan-interface 100
[SwitchA-vlan-interface100] rip 1 enable
[SwitchA-vlan-interface100] quit
```

3 つのスタティックルートを設定し、3 つのルートのネクストホップを 11.1.1.2 に設定します。

```
[SwitchA] ip route-static 20.1.1.1 32 11.1.1.2
[SwitchA] ip route-static 30.1.1.1 32 11.1.1.2
[SwitchA] ip route-static 40.1.1.1 32 11.1.1.2
```

ルーティングポリシーを設定します。

```
[SwitchA] ip prefix-list a index 10 permit 30.1.1.1 32
[SwitchA] route-policy static2rip deny node 0
[SwitchA-route-policy-static2rip-0] if-match ip address prefix-list a
[SwitchA-route-policy-static2rip-0] quit
```

```
[SwitchA] route-policy static2rip permit node 10
[SwitchA-route-policy-static2rip-10] quit
```

RIP を有効にし、ルーティングポリシー**static2rip** を適用して、再配信されたスタティックルートをフィルタリングします。

```
[SwitchA] rip
[SwitchA-rip-1] import-route static route-policy static2rip
```

2) Switch B を設定します。

インタフェース VLAN-interface 100 用の IP アドレスを設定します

```
<SwitchB> system-view
[SwitchB] interface vlan-interface 100
[SwitchB-vlan-interface100] ip address 10.1.1.2 30
```

RIP を有効にします。

```
[SwitchB] rip
[SwitchB-rip-1] quit
```

インタフェースで RIP を有効にします。

```
[SwitchB] interface vlan-interface 100
[SwitchB-vlan-interface100] rip 1 enable
[SwitchB-vlan-interface100] quit
```

III. 設定の確認

Switch B のルーティングテーブル情報を表示します。

```
<NEC>display ip routing-table
Destinations : 14       Routes : 14
Destination/Mask   Proto   Pre Cost        NextHop         Interface
0.0.0.0/32         Direct  0   0           127.0.0.1       InLoop0
10.1.1.0/30        Direct  0   0           10.1.1.2        Vlan100
10.1.1.0/32        Direct  0   0           10.1.1.2        Vlan100
10.1.1.2/32        Direct  0   0           127.0.0.1       InLoop0
10.1.1.3/32        Direct  0   0           10.1.1.2        Vlan100
20.0.0.0/8         RIP     100 1           10.1.1.1        Vlan100
40.0.0.0/8         RIP     100 1           10.1.1.1        Vlan100
127.0.0.0/8        Direct  0   0           127.0.0.1       InLoop0
127.0.0.0/32       Direct  0   0           127.0.0.1       InLoop0
127.0.0.1/32       Direct  0   0           127.0.0.1       InLoop0
127.255.255.255/32 Direct  0   0           127.0.0.1       InLoop0
224.0.0.0/4        Direct  0   0           0.0.0.0         NULL0
224.0.0.0/24       Direct  0   0           0.0.0.0         NULL0
255.255.255.255/32 Direct  0   0           127.0.0.1       InLoop0
```

12.10.2 IPv6 ルートの再配信ルートへのルーティングポリシーの設定例

I. ネットワーク要件

図 12-2に示すように設定します。

- Switch A と Switch B で RIPng を有効にします。
- Switch A に、3 つのスタティックルートを設定します。
- 再配信するスタティックルートに、ルート 20::0/32 と 40::0/32 を許可し、ルート 30::0/32 を許可しないようにしたルーティングポリシーを適用します。

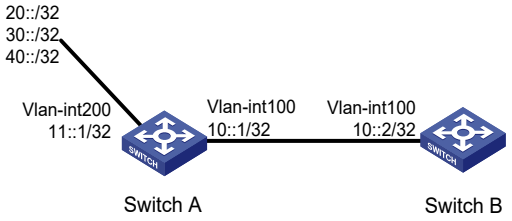


図 12-2 ネットワーク図

II. 設定手順

1)　Switch A を設定します。

VLAN インタフェース 100 と VLAN インタフェース 200 に IPv6 アドレスを設定します。

```
<SwitchA> system-view
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] ipv6 address 10::1 32
[SwitchA-Vlan-interface100] quit
[SwitchA] interface vlan-interface 200
[SwitchA-Vlan-interface200] ipv6 address 11::1 32
[SwitchA-Vlan-interface200] quit
```

VLAN インタフェース 100 で RIPng を有効にします。

```
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] ripng 1 enable
[SwitchA-Vlan-interface100] quit
```

ネクストホップが 11::2 の 3 つのスタティックルートを設定し、スタティックルートがアクティブであることを確認します。

```
[SwitchA] ipv6 route-static 20:: 32 11::2
[SwitchA] ipv6 route-static 30:: 32 11::2
[SwitchA] ipv6 route-static 40:: 32 11::2
```

ルーティングポリシーを設定します。

```
[SwitchA] ipv6 prefix-list a index 10 permit 30:: 32
[SwitchA] route-policy static2ripng deny node 0
[SwitchA-route-policy-static2ripng-0] if-match ipv6 address prefix-list a
[SwitchA-route-policy-static2ripng-0] quit
```

```
[SwitchA] route-policy static2ripng permit node 10
[SwitchA-route-policy-static2ripng-10] quit
```

RIPng を有効にし、再配信するスタティックルートへのルーティングポリシーを適用します。

```
[SwitchA] ripng
[SwitchA-ripng-1] import-route static route-policy static2ripng
```

2)　Switch B を設定します。

VLAN インタフェース 100 に IPv6 アドレスを設定します。

```
<SwitchB> system-view
[SwitchB] interface vlan-interface 100
[SwitchB-Vlan-interface100] ipv6 address 10::2 32
```

RIPng を有効にします。

```
[SwitchB] ripng
[SwitchB-ripng-1] quit
```

VLAN インタフェース 100 で RIPng を有効にします。

```
[SwitchB] interface vlan-interface 100
[SwitchB-Vlan-interface100] ripng 1 enable
[SwitchB-Vlan-interface100] quit
```

III. 設定の確認

Switch B で RIPng ルーティングテーブルを表示します。

```
[SwitchB] display ripng 1 route
   Route Flags: A - Aging, S - Suppressed, G - Garbage-collect
 ----------------------------------------------------------------

 Peer FE80::7D58:0:CA03:1 on Vlan-interface 100
 Destination 20::/32,
     via FE80::7D58:0:CA03:1, cost 1, tag 0, A, 8 secs
 Destination 40::/32,
     via FE80::7D58:0:CA03:1, cost 1, tag 0, A, 3 secs
 Local route
 Destination 10::/32,
     via ::, cost 0, tag 0, DOF
```

QX-S5100G シリーズ Ethernet スイッチ

オペレーションマニュアル

6. マルチキャスト

本マニュアルは以下に示す章で構成されています。

01-マルチキャストの概要
02-IGMP スヌーピング
03-マルチキャスト VLAN
04-MLD スヌーピング
05-IPv6 マルチキャスト VLAN

目次

このセクションのページは **6-x-x** です。

1 章 マルチキャストの概要 1-1
1.1 マルチキャストの導入 1-1
1.1.1 情報通信技術 1-1
1.1.2 マルチキャストの機能 1-3
1.1.3 マルチキャストの一般的な表記方法 1-4
1.1.4 マルチキャストの利点とアプリケーション 1-4
1.2 マルチキャストモデル 1-5
1.3 マルチキャストアーキテクチャ 1-6
1.3.1 マルチキャストアドレス 1-6
1.3.2 マルチキャストプロトコル 1-10
1.4 マルチキャストパケットの転送メカニズム 1-13

1章 マルチキャストの概要

1.1 マルチキャストの導入

ユニキャストおよびブロードキャストと共存する技術として、マルチキャスト技術はポイントツーマルチポイントデータ送信の問題を効果的に対処します。ネットワーク上で効率の高いポイントツーマルチポイントデータ送信を行うことで、マルチキャストはネットワーク帯域幅を大きく節約し、ネットワーク負荷を低減します。

マルチキャスト技術により、ネットワークオペレータは新しい付加価値のあるサービスを容易に提供することが可能となります。たとえば、Web キャスティング、Web TV、遠隔学習、遠隔医療、Web ラジオ、リアルタイムビデオカンファレンスなどの他に、帯域幅や時間が重要な情報サービスです。

1.1.1 情報通信技術

情報通信技術はユニキャスト、ブロードキャスト、マルチキャストを含みます。

I. ユニキャスト

ユニキャストでは、情報を必要とする各ホスト（Receiver）へ情報送信元（Source）から情報のコピーが個別に送信されます。

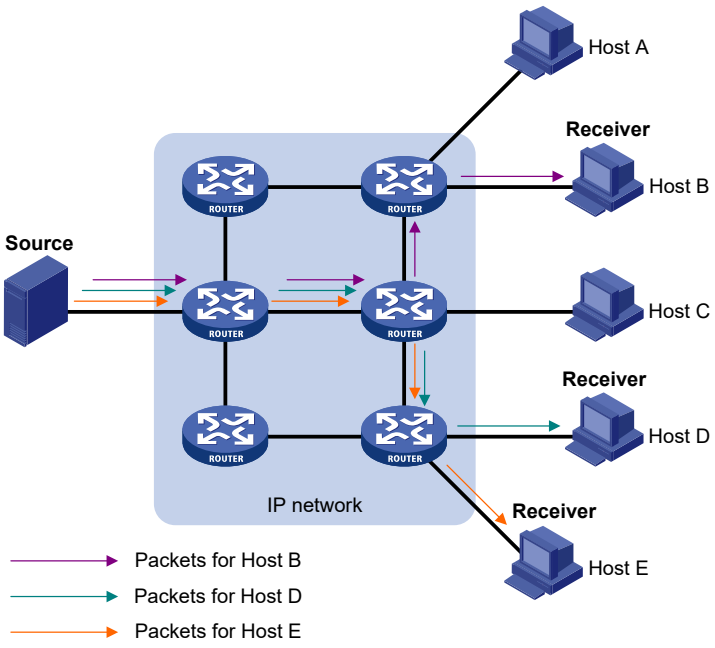


図 1-1 ユニキャスト通信

0において、Host B と Host D と Host E は情報を必要とします。個別の通信チャネルは情報送信元から各ホストに対して確立する必要があります。

ユニキャスト通信では、ネットワーク上のトラフィックは情報を必要とするホストの数に比例します。非常に多くのユーザが情報を必要とする場合、情報送信元は各ユーザに同じ情報のコピーを送信する必要があります。これは情報送信元とネットワーク帯域幅に相当な負荷をかけることになります。

ユニキャスト通信は情報のバッチ送信には適していません。

II. ブロードキャスト

ブロードキャストでは、情報を必要としていないホストがあったとしても、情報送信元からネットワーク上のすべてのホストに情報が送信されます。

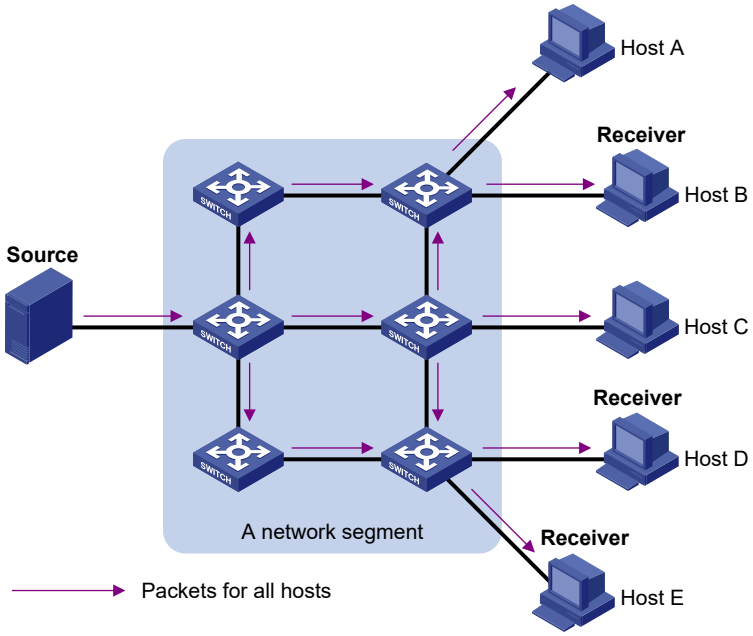


図 1-2 ブロードキャスト通信

図 1-2に示すように、Host B と Host D と Host E は情報を必要とします。情報が同一ネットワーク上にブロードキャストされた場合、Host A と Host C も情報を受信してしまいます。これにより、情報セキュリティの問題に加えて、同一ネットワーク上でトラフィックフラッディングも発生してしまいます。

特定のホストにデータを送信する場合、ブロードキャストは効率的ではありません。ブロードキャストの送信は多くのネットワークリソースを浪費します。

III. マルチキャスト

マルチキャストはネットワークリソースの消費を最小限に抑えてポイントツーマルチポイント送信を実現することができます。ネットワーク上のいくつかのホストがマルチキャスト情報を必要とした場合、情報の送信者あるいはマルチキャスト送信元は情報のコピー

を 1 つだけ送信します。マルチキャストルーティングプロトコルによってマルチキャスト配信ツリーが構成され、ツリーが分岐するノードでのみパケットがコピーされます。

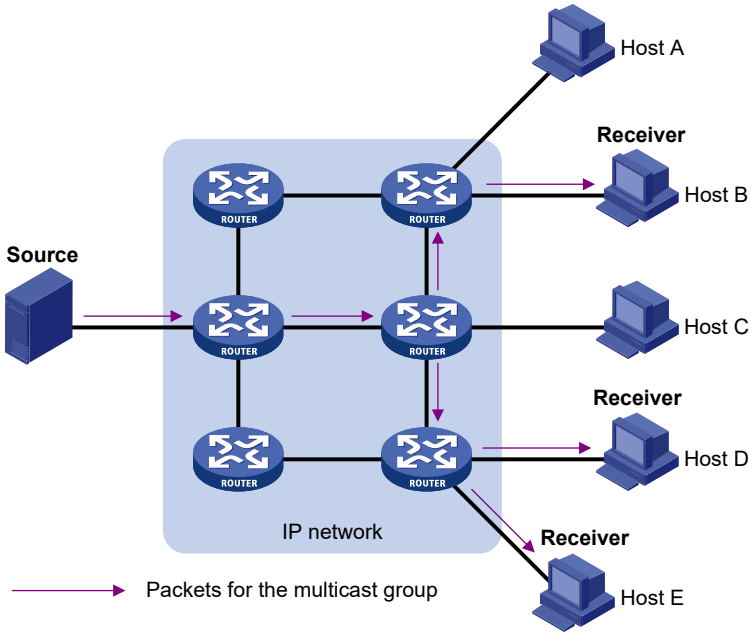


図 1-3 マルチキャスト通信

マルチキャスト送信元（Source）は情報のコピーを 1 つだけマルチキャストグループへ送信します。情報の受信者である Host B、Host D、Host E は、マルチキャストグループに参加する必要があります。ネットワーク上のルータはグループメンバの配置にもとづいて情報を複製して転送します。最終的に、情報は Host B と Host D と Host E に正確に送信されます。

要約すると、マルチキャストの利点を以下に示します。

- **ユニキャストからの利点** － ユニキャストに対しては、マルチキャストトラフィックは送信元から可能な限り遠いノードに流れてから複製、配信されるため、ホストの数が増加した場合でも送信元とネットワークの負荷を増やすことはありません。
- **ブロードキャストからの利点** － ブロードキャストに対しては、必要としている受信者だけにマルチキャストデータが送信されるので、マルチキャストは合理的にネットワーク帯域幅を使用し、ネットワークセキュリティを強化します。さらに、ブロードキャストの配信は同一ネットワークに限定されますが、マルチキャストの配信は同一ネットワークに限定されません。

1.1.2 マルチキャストの機能

- マルチキャストグループは IP マルチキャストアドレスによって識別されて配置されるマルチキャストレシーバです。ホストはマルチキャストグループ宛に送信されたマルチキャストデータを受信できるようになる前に、マルチキャストグループのメンバになるためにマルチキャストグループに参加します。通常、マルチキャストソースはマルチキャストグループに参加する必要はありません。
- マルチキャストソースは情報の送信者です。マルチキャストソースは同時に複数のマルチキャストグループにデータを送信することができます、そして、複数のマルチキ

ャストソースは同時に同一のマルチキャストグループにデータを送信することができます。

- グループメンバは動的です。ホストは、いつでもマルチキャストグループに参加あるいは離脱することができます。マルチキャストグループは、地理的な制約を受けません。
- レイヤ 3 マルチキャストをサポートするルータまたはレイヤ 3 スイッチは、マルチキャストルータまたはレイヤ 3 マルチキャスト装置と呼ばれます。マルチキャストルーティング機能の提供に加えて、マルチキャストルータはグループメンバに所属しているスタブサブネットのマルチキャストグループメンバを管理することもできます。マルチキャストルータ自身は、マルチキャストグループメンバになることができます。

マルチキャストの概念をより良く理解するために、マルチキャスト配信を TV 番組の配信に例えることができます。

表 1-1 TV 番組の配信とマルチキャスト通信の比較

TV 番組の配信	マルチキャスト配信
TV 局がチャンネルを介して TV 番組を放送します。	マルチキャストソースがマルチキャストグループにマルチキャストデータを送信します。
ユーザが TV をチャンネルに合わせます。	レシーバがマルチキャストグループに参加します。
チャンネルを介して TV 局から放送される TV 番組の視聴をユーザが開始します。	ソースからマルチキャストグループに送信されたマルチキャストデータをレシーバが受信し始めます。
ユーザが TV の電源を切るか、他のチャンネルに合わせます。	レシーバがマルチキャストグループから離脱するか、他のグループに参加します。

1.1.3 マルチキャストの一般的な表記方法

マルチキャストでは一般的に 2 つの表記法が使用されます。

- **(*, G)** － RPT（rendezvous point tree）または、あらゆるマルチキャストソースがマルチキャストグループ G へ送信したマルチキャストパケットを表します。（*）はあらゆるマルチキャストソース、(G) は特定のマルチキャストグループを表します。
- **(S, G)** － SPT（shortest path tree）または、マルチキャストソース S がマルチキャストグループ G へ送信したマルチキャストパケットを表します。（S）は特定のマルチキャストソース、（G）は特定のマルチキャストグループを表します。

1.1.4 マルチキャストの利点とアプリケーション

I. マルチキャストの利点

- **効率の向上** － 情報送信元サーバとネットワーク装置の CPU 負荷を低減します。
- **最適なパフォーマンス** － 冗長なトラフィックを低減します。
- **配信アプリケーション** － 最小限のネットワークリソースで、ポイントツーマルチポイントアプリケーションを可能にします。

II. マルチキャストアプリケーション

- マルチメディアとストリーミングアプリケーションがあります。たとえば Web TV、Web ラジオ、リアルタイムビデオ/オーディオ会議などがあります。
- 通信教育や遠隔医療などの研修および協力運用の通信があります。
- データウェアハウスと財務アプリケーション（株価情報）があります。
- その他のポイントツーマルチポイントデータ配信アプリケーションがあります。

1.2 マルチキャストモデル

レシーバ（受信者）がマルチキャストソース（送信元）をどのように扱うかによって、ASM（any-source multicast）、SFM（source-filtered multicast）、SSM（source-specific multicast）の 3 つのマルチキャストモデルがあります。

I. ASM モデル

ASM モデルでは、すべてのマルチキャストソースはマルチキャストグループへ情報を送信できます。レシーバ（受信者）がグループアドレスによって識別されたマルチキャストグループに参加し、そのマルチキャストグループ宛てのマルチキャスト情報を取得することができます。このモデルでは、レシーバ（受信者）はあらかじめマルチキャストソースの位置を認識していません。

II. SFM モデル

SFM モデルは ASM モデルから派生しています。センダ（送信者）の観点からは、2 つのモデルは同じマルチキャストメンバシップのアーキテクチャです。

SFM モデルは ASM モデルの機能拡張版です。SFM モデルでは、上位レイヤソフトウェアが受信したマルチキャストの送信元アドレスをチェックし、指定した送信元からのマルチキャストトラフィックを許可または拒否します。これにより、レシーバ（受信者）は一部のマルチキャストソースからのだけマルチキャストデータを受信することができます。レシーバ（受信者）の観点からは、マルチキャストソース（送信元）がすべて有効というわけではありません。マルチキャストソースはフィルタされます。

III. SSM モデル

SSM モデルは、マルチキャストレシーバが、必要となるマルチキャストソースを指定することができる転送サービスを提供します。

SSM モデルと ASM モデルの根本的な違いは、SSM モデルではレシーバ（受信者）が何らかの方法でマルチキャストソースの位置を既に知っていることです。これは SSM モデルと ASM モデルの主な相違点です。さらに、SSM モデルでは ASM /SFM モデルの場合とは異なるマルチキャストアドレス範囲を使用します。レシーバと指定のマルチキャストソースの間に専用のマルチキャスト転送パスが確立されます。

1.3 マルチキャストアーキテクチャ

IP マルチキャストは以下の問題を解決します。

- マルチキャストソースはどこに情報を送信するべきか？（マルチキャストアドレッシング）
- ネットワーク上にはどんなレシーバ（受信者）が存在するか？（ホストレジストレーション）
- レシーバが受信する必要があるマルチキャストデータのマルチキャストソース（送信元）がどこにいるのか？（マルチキャストソースディスカバリ）
- 情報がどのようにしてレシーバ（受信者）に転送されるのか？（マルチキャストルーティング）

IP マルチキャストはエンドツーエンドサービスの 1 つです。マルチキャストアーキテクチャには以下の 4 つのパートがあります。

- **アドレッシングメカニズム** － マルチキャストソースはマルチキャストアドレスを介してレシーバのグループへ情報を送信します。
- **ホストレジストレーション** － レシーバホストはマルチキャストグループへの参加と離脱を動的に行うことができます。このメカニズムはグループメンバシップ管理の基礎になります。
- **マルチキャストルーティング** － マルチキャストソースからレシーバへマルチキャストデータを配信するために、マルチキャスト配信ツリー（ネットワーク上でのマルチキャストデータの転送パスツリー）が構築されます。
- **マルチキャストアプリケーション** － ビデオ会議などのマルチキャストアプリケーションをサポートするソフトウェアシステムを、マルチキャストソース（送信元）とレシーバホスト（受信者）にインストールする必要があります。そして、TCP/IP スタックはマルチキャストデータの送受信をサポートする必要があります。

1.3.1 マルチキャストアドレス

I. IP マルチキャストアドレス

- IPv4 マルチキャストアドレス

IANA（Internet Assigned Numbers Authority）は IPv4 マルチキャストにクラス D アドレス（224.0.0.0～239.255.255.255）を割り当てました。

表 1-2 クラス D アドレスブロックと説明

アドレスブロック	説明
224.0.0.0 ～ 224.0.0.255	予約されている永久的なグループアドレスです。IP アドレス 224.0.0.0 は予約されており、その他の IP アドレスはルーティングプロトコルによって、そしてトポロジ検索、プロトコルの維持管理などのために使用されることができます。一般的な永久グループアドレスの一覧は表 1-3 に示されています。このブロックアドレス宛のパケットは、IP ヘッダの TTL （Time to Live） 値に関わらず、ローカルサブネットを越えて転送されることはありません。

アドレスブロック	説明
224.0.1.0 ～ 238.255.255.255	グローバルスコープグループアドレスです。このブロックには2種類の指定グループアドレスがあります。 ● **232.0.0.0/8** － SSMグループアドレス ● **233.0.0.0/8** － Glopグループアドレス
239.0.0.0 ～ 239.255.255.255	管理上、範囲指定されたマルチキャストアドレスです。これらのアドレスはグローバルにではなくローカルに一意とみなされ、異なる組織が管理しているドメインで衝突を起こすことなく再利用できます。詳細はRFC2365を参照してください。

🕮 **メモ：**

“Glop”は、異なる自律システム （AS） 間でマルチキャストアドレスを割り当てるメカニズムです。233.0.0.0 の中間の 2 バイトに AS の数字を入力することで、その AS に 255 のマルチキャストアドレスが得られます。詳細については、RFC2770 を参照してください。

表 1-3 一般的な予約済みマルチキャストグループアドレス

アドレス	説明
224.0.0.1	ホストとルータを含む、サブネット上のすべてのシステムです。
224.0.0.2	サブネット上のすべてのマルチキャストルータです。
224.0.0.3	未割り当てです。
224.0.0.4	DVMRP（Distance Vector Multicast Routing Protocol）ルータです。
224.0.0.5	OSPF（Open Shortest Path First）ルータです。
224.0.0.6	OSPFのDRまたはバックアップDRです。
224.0.0.7	ST（Shared Tree）ルータです。
224.0.0.8	STホストです。
224.0.0.9	RIPv2（Routing Information Protocol version 2）ルータです。
224.0.0.11	モバイルエージェントです。
224.0.0.12	DHCP（Dynamic Host Configuration Protocol）サーバまたはリレーエージェントです。
224.0.0.13	すべてのPIM（Protocol Independent Multicast）ルータです。
224.0.0.14	RSVP（Resource Reservation Protocol）のカプセル化です。
224.0.0.15	すべてのCBT（Core-Based Tree）ルータです。
224.0.0.16	指定されたSBM（Subnetwork Bandwidth Management）です。
224.0.0.17	すべてのSBMです。
224.0.0.18	VRRP（Virtual Router Redundancy Protocol）です。

- IPv6 マルチキャストアドレス

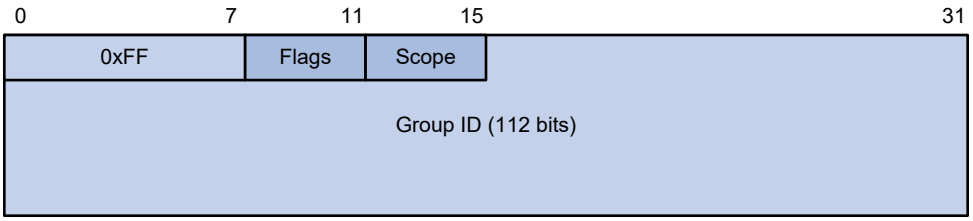


図 1-4 IPv6 マルチキャストフォーマット

以下に IPv6 マルチキャストアドレスのフィールドの説明を示します。

- **0xFF** － 8 ビットで 11111111 です。このアドレスが IPv6 マルチキャストアドレスであることを示します。
- **Flags** － 4 ビットのフラグフィールドです。

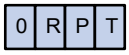


図 1-5 Flags フィールドフォーマット

表 1-4 フラグフィールドの説明

ビット	説明
0	予約済みです。常に0です。
R	● 0の場合、RPアドレスが埋め込まれていないIPv6マルチキャストアドレスであることを示します。 ● 1の場合、RPアドレスが埋め込まれているIPv6マルチキャストアドレスであることを示します。（PビットとTビットも1にセットされます）
P	● 0の場合、ユニキャストプレフィックスにもとづかないIPv6マルチキャストアドレスであることを示します。 ● 1の場合、ユニキャストプレフィックスにもとづくIPv6マルチキャストアドレスであることを示します。（Tビットも1にセットされます）
T	● 0の場合、IANAによって永続的に割り当てられた既知のIPv6マルチキャストアドレスであることを示します。 ● 1の場合、一時的あるいはダイナミックに使用される（非永続的な）マルチキャストアドレスであることを示します。

- **Scope** － 4 ビットの IPv6 マルチキャストアドレスの有効範囲を示すフィールドです。

表 1-5 Scope フィールドの値

値	意味
0、F	予約済み
1	インタフェースノードローカル
2	リンクローカル
3	サブネットローカル
4	アドミンローカル
5	サイトローカル

値	意味
6、7、9～D	未割り当て
8	組織ローカル
E	グローバル

- **Group ID** – 112 ビットで IPv6 マルチキャストグループを識別します。Scope フィールドが定義する範囲で IPv6 マルチキャストグループを一意に識別します。

II. イーサネットマルチキャスト MAC アドレス

- IPv4 マルチキャスト MAC アドレス

IANA によって定義されているように、IPv4 マルチキャスト MAC アドレスの上位 24 ビットは 0x01005E、25 ビット目は 0x0、および下位 23 ビットはマルチキャスト IPv4 アドレスの低位 23 ビットです。

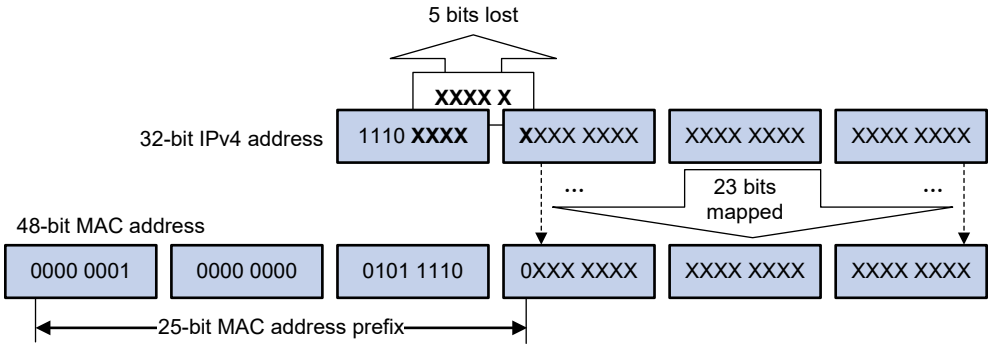


図 1-6 IPv4 アドレスと MAC アドレスのマッピング

IPv4 マルチキャストアドレスの上位 4 ビットは 1110 で固定です。IPv4 アドレスと MAC アドレスのマッピングで使用され、IPv4 マルチキャストアドレスの 5 ビットは失われます。その結果、32 個のマルチキャスト IPv4 アドレスは同じ MAC アドレスにマッピングされます。そのため、レイヤ 2 マルチキャスト転送においては、他の IPv4 マルチキャストグループに宛てたマルチキャストデータを受け取る場合があります。そのような冗長データは上位層によってフィルタする必要があります。

- IPv6 マルチキャスト MAC アドレス

IPv6 マルチキャスト MAC アドレスの上位 16 ビットは 0x3333 です。下位 32 ビットはマルチキャスト IPv6 アドレスの下位 32 ビットにマッピングされます。これは IPv4 アドレスから MAC アドレスのマッピングと同じように、IPv6 から MAC アドレスのマッピングが重複する問題があります。

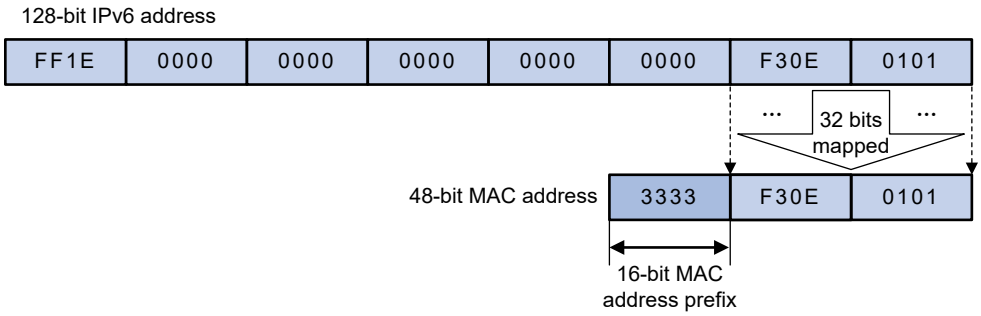


図 1-7 IPv6 アドレスと MAC アドレスのマッピング例

1.3.2 マルチキャストプロトコル

マルチキャストプロトコルは以下のカテゴリに分けられます。

- レイヤ 3、レイヤ 2 マルチキャストプロトコル
  - □ ネットワークレイヤで動作する IP マルチキャストのレイヤ 3 マルチキャスト

    レイヤ 3 マルチキャストプロトコル － IGMP、MLD、PIM、IPv6 PIM、MSDP、MBGP、IPv6 MBGP
  - □ データリンクレイヤで動作する IP マルチキャストのレイヤ 2 マルチキャスト

    レイヤ 2 マルチキャストプロトコル － IGMP snooping、MLD snooping、PIM snooping、IPv6 PIM snooping、マルチキャスト VLAN、IPv6 マルチキャスト VLAN
- IPv4、IPv6 マルチキャストプロトコル
  - □ **IPv4 ネットワーク** － IGMP snooping、PIM snooping、マルチキャスト VLAN、IGMP、PIM、MSDP、MBGP
  - □ **IPv6 ネットワーク** － MLD snooping、IPv6 PIM snooping、IPv6 マルチキャスト VLAN、MLD、IPv6 PIM、IPv6 MBGP

この章ではレイヤ 2、レイヤ 3 マルチキャストプロトコルの一般的なアプリケーションと機能について記載します。レイヤ 2 マルチキャストプロトコルに関する詳細は、関連する章を参照してください。

I. レイヤ 3 マルチキャストプロトコル

レイヤ 3 マルチキャストプロトコルには、マルチキャストグループ管理プロトコルやマルチキャストルーティングプロトコルがあります。

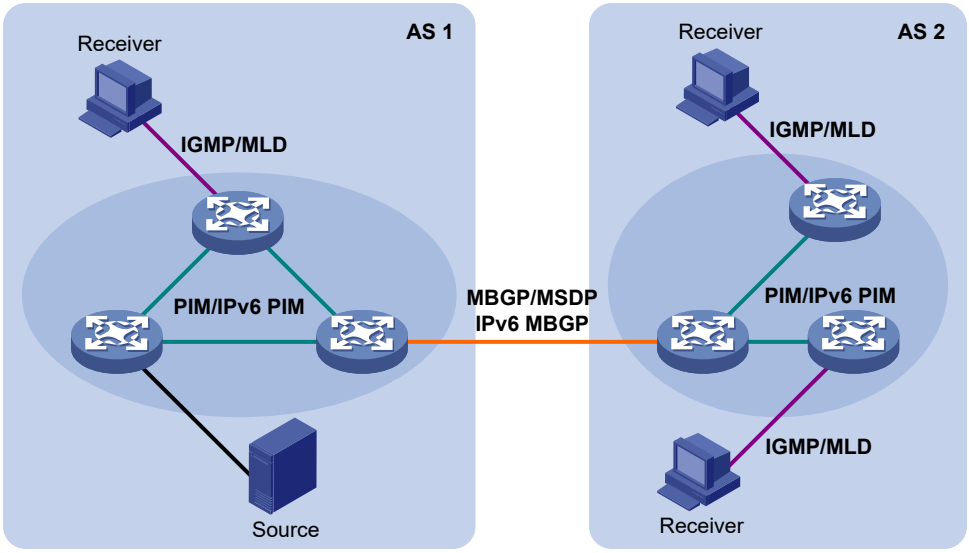


図 1-8 レイヤ 3 マルチキャストプロトコルの位置

- マルチキャストグループ管理プロトコル

通常は、IGMP（internet group management protocol）、MLD（multicast listener discovery protocol）はマルチキャストグループ管理プロトコルです。通常、これらのプロトコルは、ホストとレイヤ 3 マルチキャスト装置の間でグループメンバシップを確立して維持するメカニズムを定義します。

- マルチキャストルーティングプロトコル

マルチキャストルーティングプロトコルはレイヤ 3 マルチキャスト装置上で動作し、マルチキャストルートを確立して維持します。そして、マルチキャストパケットを正確に効率よく転送します。マルチキャストルートは、データソースから複数のレシーバまでループのないデータ転送パス（マルチキャスト配信ツリーとして知られます。）を構成します。

ASM モデルでは、マルチキャストルートはドメイン内ルートとドメイン間ルートがあります。

- □ マルチキャストデータをレシーバに配信するために、ドメイン内マルチキャストルーティングプロトコルを使用してマルチキャストソースの発見、AS 内マルチキャスト配信ツリーの構築を行います。さまざまな成熟したドメイン内マルチキャストルーティングプロトコルの中でも、PIM（protocol independent multicast）はよく使用されています。PIM にはスパースモード（PIM-SM）があります。
- □ ドメイン間マルチキャストルーティングプロトコルは 2 つの AS 間でマルチキャストの情報を発見するのに使われます。このプロトコルには、MSDP（Multicast Source Discovery Protocol）、MBGP が含まれます。MSDP は異なる AS 間でマルチキャスト送信元情報を送信します。MBGP は異なる AS 間でマルチキャストルーティング情報を交換するため、MP-BGP を拡張したものです。

SSM モデルでは、マルチキャストルートはドメイン間ルートおよびドメイン内ルートに分割されません。レシーバはマルチキャストソースの位置を知っているため、マルチキャスト情報の転送には PIM-SM によって確立されたチャネルで十分です。

II. レイヤ 2 マルチキャストプロトコル

レイヤ 2 マルチキャストプロトコルには、IGMP Snooping、MLD Snooping、PIM Snooping、IPv6 PIM Snooping、マルチキャスト VLAN、IPv6 マルチキャスト VLAN があります。

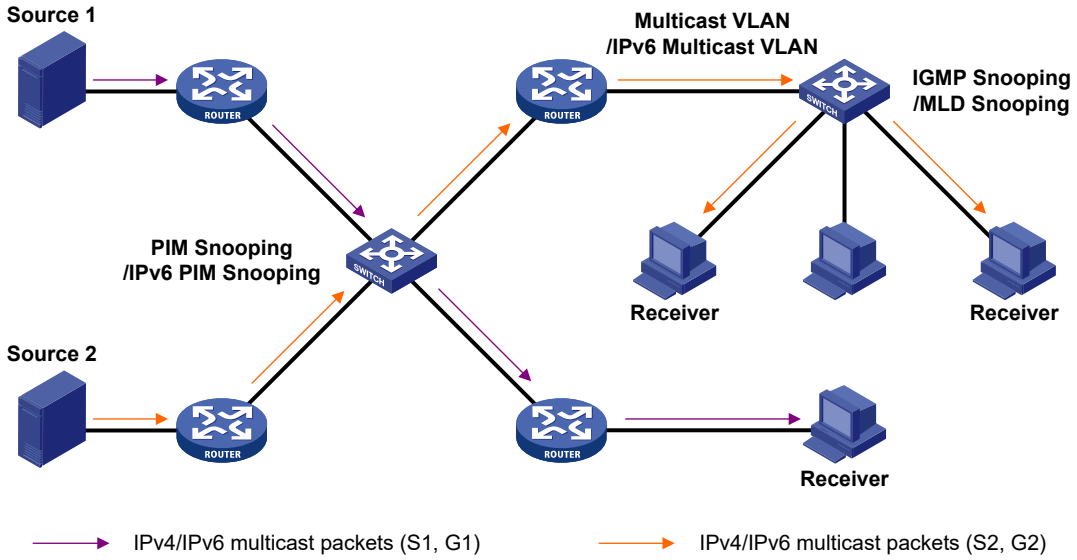


図 1-9 レイヤ 2 マルチキャストプロトコルの位置

- IGMP snooping、MLD snooping

マルチキャストの転送効率を改良するため PIM Snooping および IPv6 PIM Snooping はレイヤ 2 装置で動作するマルチキャスト構成メカニズムです。ホストとレイヤ 3 マルチキャスト装置の間で交換される IGMP または MLD メッセージをモニタ、解析することによって、マルチキャストグループを管理、制御します。このメカニズムはレイヤ 2 ネットワークでマルチキャストデータのフラッディングを制御するのに効率的です。

- PIM snooping、IPv6 PIM snooping

PIM Snooping および IPv6 PIM Snooping はレイヤ 2 装置で動作します。受信した PIM メッセージを解析するため、PIM snooping や IPv6 PIM snooping を動作させます。PIM snooping ルーティングエントリや IPv6 PIM snooping ルーティングエントリに、指定したマルチキャストデータに関連するポートのみを追加します。これによって、マルチキャストデータは、関連するポートに対してのみ転送します。

- マルチキャスト VLAN、IPv6 マルチキャスト VLAN

異なる VLAN に同一グループのマルチキャストレシーバが存在するところで、マルチキャストネットワークのレイヤ 2 装置でマルチキャスト VLAN、IPv6 マルチキャスト VLAN が動作します。これらのプロトコルでは、レイヤ 3 マルチキャスト装置はレイヤ 2 装置のマルチキャスト VLAN または IPv6 マルチキャスト VLAN へマルチキャストデータのコピーを 1 つだけ送信します。これにより、レイヤ 3 装置上のネットワーク帯域幅の浪費や余分な負荷を回避します。

1.4 マルチキャストパケットの転送メカニズム

マルチキャストモデルでは、マルチキャストグループのマルチキャストレシーバは通常、ネットワークの異なるエリアに存在します。これらのマルチキャストレシーバは同じマルチキャストグループアドレスによって識別されます。ネットワーク上の異なる位置に存在するレシーバにマルチキャストパケットを配信するため、宛先アドレスとして IP パケットのマルチキャストデータをマルチキャストグループアドレスにカプセル化します。通常は転送パス上のマルチキャストルータが 1 つの受信インタフェースで受信したマルチキャストパケットを複数の送信インタフェースに転送します。ユニキャストモデルと比較して、マルチキャストモデルは以下でユニキャストより複雑になっています。

- ネットワークにおいてマルチキャストパケットの転送を確実にするために、マルチキャストの転送に異なるルーティングテーブルが使用されます。ユニキャストルーティングテーブル、マルチキャストのルーティングテーブル（たとえば、MBGP ルーティングテーブル）、スタティックマルチキャストルーティングテーブルが含まれます。
- 異なるピアから発信され、同じ装置の異なるインタフェースで受信された同一マルチキャスト情報を処理するため、各マルチキャストパケットの RPF チェックを実行します。RPF チェックの結果によって、パケットの転送または破棄が決定されます。RPF チェックメカニズムは、マルチキャスト転送を実行するほとんどのマルチキャストルーティングプロトコルの基礎になっています。

目次

このセクションのページは**6-x-x** です。

2章 IGMPスヌーピング 2-1
2.1 概要 2-1
2.1.1 IGMP snoopingのポート 2-1
2.1.2 IGMP snoopingの動作 2-3
2.1.3 IGMP snoopingプロキシー機能 2-5
2.2 プロトコルと標準 2-6
2.3 IGMP snooping設定作業リスト 2-6
2.4 IGMP snoopingの基本機能の設定 2-7
2.4.1 IGMP snoopingの有効化 2-7
2.4.2 IGMP snoopingのバージョンの設定 2-8
2.4.3 IGMP snooping転送エントリの最大数の設定 2-8
2.4.4 スタティックマルチキャストMACアドレスエントリの設定 2-9
2.4.5 IGMP last member クエリ間隔の設定 2-9
2.5 IGMP snoopingポート機能の設定 2-10
2.5.1 ダイナミックポートのエージングタイマの設定 2-10
2.5.2 スタティックポートの設定 2-11
2.5.3 シミュレーティッドメンバホストの設定 2-12
2.5.4 fast-leave処理の有効化 2-12
2.6 IGMP snooping クエリの設定 2-13
2.6.1 設定要件 2-13
2.6.2 IGMP snoopingクエリアの有効化 2-14
2.6.3 IGMP クエリとresponseのパラメータの設定 2-14
2.7 IGMP snooping プロキシー機能の有効化 2-15
2.8 IGMPメッセージのパラメータの設定 2-15
2.8.1 設定要件 2-15
2.8.2 IGMPメッセージの送信元IPアドレスの設定 2-16
2.8.3 IGMPメッセージの802.1p優先度の設定 2-17
2.9 IGMP snooping ポリシーの設定 2-18
2.9.1 マルチキャストグループポリシーの設定 2-18
2.9.2 マルチキャストソースポートフィルタの設定 2-19
2.9.3 未知のマルチキャストデータ廃棄機能の有効化 2-19
2.9.4 IGMP report抑制機能の有効化 2-20
2.9.5 ポートで参加可能なマルチキャストグループの最大数の設定 2-20
2.9.6 マルチキャストグループ置き換え機能の有効化 2-21
2.10 送信するIGMPプロトコルパケットのDSCPの設定 2-21
2.11 IGMP snoopingの表示と維持 2-22
2.12 IGMP snooping設定例 2-23
2.12.1 グループポリシーとシミュレーティッドメンバホストの設定例 2-23
2.12.2 スタティックポートの設定例 2-25
2.12.3 IGMP snooping クエリアの設定例 2-29
2.12.4 IGMP snoopingプロキシー機能の設定例 2-32
2.13 IGMP snoopingのトラブルシューティング 2-34
2.13.1 レイヤ2マルチキャスト転送ができない 2-34
2.13.2 マルチキャストグループポリシーが動作しない 2-35

2章 IGMP スヌーピング

2.1 概要

IGMP snooping はマルチキャスト転送時のネットワークへの負荷を軽減するためのメカニズムです。

図 2-1に示すように、IGMP snooping を有効にしない場合、マルチキャストパケットはすべてのポートにフラッディングされます。レイヤ 2 装置で IGMP snooping を有効にすると、既知のマルチキャストグループからのマルチキャストパケットは、Receiver へのみ転送されます。IGMP snooping を有効にすることで、不要なマルチキャストトラフィックのフラッディングを抑止し、ネットワークを効率的に利用することができます。

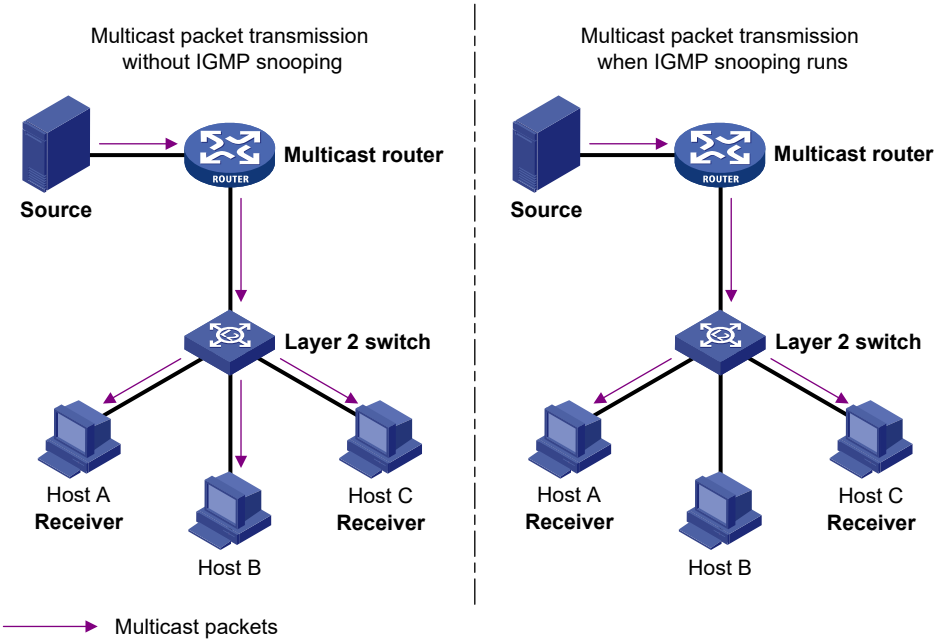


図 2-1 IGMP snooping を有効にする前と有効にした後のマルチキャストパケットの転送

2.1.1 IGMP snooping のポート

図 2-2に示すように、IGMP snooping は Switch A と Switch B で動作し、Host A と Host C がマルチキャストグループのホストとするレシーバです。IGMP snooping のポートはメンバポートとルータポートに分類されます。

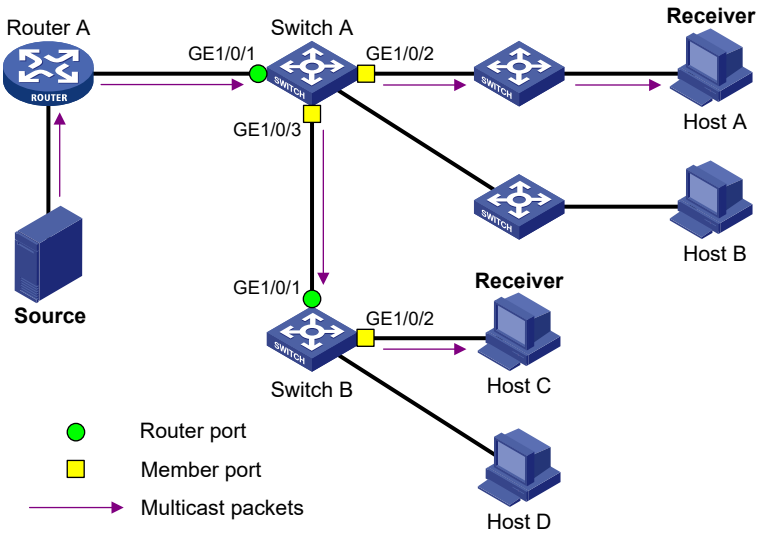


図 2-2 IGMP snooping 関連ポート

I. ルータポート

IGMP snooping のレイヤ 2 装置で、レイヤ 3 マルチキャストへのポートはルータポートと呼ばれます。図 2-2では、Switch A の GigabitEthernet 1/0/1 と Switch B の GigabitEthernet 1/0/1 がルータポートです。

ルータポートは以下のタイプがあります。

- **ダイナミックルータポート**－ポートで 0.0.0.0 以外の送信元アドレスの IGMP general クエリを受信する、あるいは PIM Hello メッセージを受信した場合、ダイナミックルータポートリストにポートを追加します。同時にポートのタイマを開始します。タイマが満了する前にメッセージを受信しない場合、ポートはダイナミックルータポートリストからポートを削除します。
- **スタティックルータポート**－ポートがルータポートとしてスタティックに設定された場合、スタティックルータポートリストにポートを追加します。スタティックルータポートはエージアウトしません。手動でのみ削除することができます。

IGMP snooping のルータポートをレイヤ 3 インタフェースのルーテッドインタフェースと混同しないでください。IGMP snooping のルータポートはレイヤ 2 インタフェースです。

II. メンバポート

IGMP snooping のレイヤ 2 装置で、マルチキャストレシーバへのポートはメンバポートと呼ばれます。図 2-2では、Switch A の GigabitEthernet 1/0/2 と GigabitEthernet 1/0/3、Switch B の GigabitEthernet 1/0/2 がメンバポートです。

メンバポートは以下のタイプがあります。

- **ダイナミックメンバポート**－ポートが IGMP report をした場合、出力インタフェースとして関連づけられたダイナミック IGMP snooping 転送エントリに追加されます。同時にポートのタイマを開始します。タイマが満了する前にメッセージを受信しない場合、ポートはダイナミック転送エントリからからポートを削除します。

- **スタティックメンバポート**－ポートがメンバポートとしてスタティックに設定された場合、出力インタフェースとして関連づけられたスタティック IGMP snooping 転送エントリに追加されます。スタティックメンバポートはエージアウトしません。手動でのみ削除することができます。

特に指定しない限り、この章でのルータポートとメンバポートは、スタティックルータポート、ダイナミックルータポートと、スタティックメンバポート、ダイナミックメンバポートを含みます。

2.1.2 IGMP snooping の動作

この章のポートはダイナミックポートです。スタティックポートの設定、削除方法については、オペレーションマニュアルのセクション 6 *マルチキャスト”IGMP スヌーピング”の”スタティックポートの設定”*を参照してください。

IGMP メッセージのタイプは、general クエリ、IGMP report、leave message を含みます。IGMP snooping が有効なレイヤ 2 装置は、受信した IGMP メッセージによってそれぞれ異なる動作をします。

I. General クエリ

IGMP クエリアは、アクティブなマルチキャストグループメンバが存在するかどうかを調べるために、ローカルサブネット上のすべてのホストとルータへ IGMP general クエリを定期的に送信します。

IGMP クエリアから IGMP general クエリを受信すると、装置はメッセージを受信したポートと同じ VLAN に属する、受信したポート以外のすべてのポートへ IGMP general クエリを転送します。受信ポートに対しては以下を実施します。

- 受信ポートがルータポートリストに存在するルータポートの場合、装置はこのルータポートのエージングタイマを再起動します。
- 受信ポートがルータポートリストに存在しない場合、装置はその受信ポートをルータポートリストに追加し、このルータポートのエージングタイマを開始します。

II. IGMP report

ホストは以下の目的により IGMP report を IGMP クエリアへ送信します。

- ホストがマルチキャストグループメンバである場合、IGMP クエリに応答します。
- マルチキャストグループ membership を適用します。

IGMP report を受信すると、装置は VLAN 内のすべてのルータポートからそれを転送し、報告されたマルチキャストグループのアドレスを解決します。そして、転送テーブルを検索します。

- 報告されたグループの転送テーブルエントリが存在しない場合、装置はエントリを作成して、受信したポートを転送エントリにダイナミックメンバポートとして追加します。そして、そのポートでメンバポートエージングタイマを起動します。
- 報告されたグループの転送テーブルエントリは存在するが、そのグループの発信ポートリストにポートが含まれていない場合、装置はポートをダイナミックメンバポートとして転送エントリに追加します。そのポートのメンバポートエージングタイマを起動します。

- 報告されたグループの転送テーブルエントリが存在し、転送エントリに受信ポートが含まれている場合、装置はそのポートのメンバポートエージングタイマをリセットします。

IGMP snooping が有効な装置でマルチキャストグループポリシーの設定がある際、ユーザがマルチキャストプログラムを要求したとき、ユーザのホストは IGMP report を初期化します。この IGMP report を受信した後、装置は IGMP report のマルチキャストグループアドレスを解決し、IGMP report の ACL によるフィルタリングを実行します。ACL のフィルタリングにパスした場合、出力インタフェースとして受信したポートの IGMP snooping 転送エントリを作成し、転送エントリにポートを追加します。パスしない場合、装置は IGMP report を廃棄します。ユーザはマルチキャストグループに加入できず、マルチキャストプログラムを要求することができないことを示します。

装置は IGMP report の抑制を行わないため、非ルータポートを通して IGMP report の転送を行いません。

III. Leave message

IGMPv1 ホストがマルチキャストグループを離脱する場合、ホストは IGMP leave メッセージを送信しません。レシーバホストに接続されているポートのエージングタイマが終了するまで、装置はホストに対応するメンバポートの転送エントリを転送テーブルから削除しません。この場合、ポートのマルチキャストグループのエージングタイマが終了したときのみ関連する転送エントリの出力インタフェースリストからポートを削除します。

IGMPv2 ホストあるいは IGMPv3 ホストがマルチキャストグループを離脱する場合、マルチキャストルータに IGMP leave メッセージを送信します。

装置がダイナミックメンバポートで IGMP leave メッセージを受信した場合、そのグループの転送テーブルエントリが存在するかどうかを確認します。

- 転送テーブルエントリが存在しない場合、装置は IGMP leave メッセージを破棄します。
- 転送テーブルエントリが存在するが転送エントリに受信ポートがない場合、装置は IGMP leave メッセージを破棄します。
- 転送テーブルエントリが存在し、受信ポートが転送エントリの出力インタフェースのみでない場合、以下の処理を行います。
  - □ IGMP leave メッセージを廃棄します。
  - □ グループに受信ポートに接続されたアクティブなレシーバがあるかどうかを確認するため、IGMP group-specific クエリを送信します。
  - □ 受信ポートのエージングタイマを IGMP last member クエリ間隔の 2 倍に設定します。
- 転送テーブルエントリが存在し、受信ポートが転送エントリの出力インタフェースのみである場合、以下の処理を行います。
  - □ VLAN のすべてのルータポートに IGMP leave メッセージを転送します。
  - □ グループに受信ポートに接続されたアクティブなレシーバがあるかどうかを確認するため、IGMP group-specific クエリを送信します。
  - □ 受信ポートのエージングタイマを IGMP last member クエリ間隔の 2 倍に設定します。

ホストから IGMP leave メッセージを受信したのち、IGMP クエリアはメッセージからマルチキャストグループのアドレスを解決します。そして leave メッセージを受信したポートからマルチキャストグループに IGMP group-specific クエリを送信します。

IGMP group-specific クエリを受信すると、装置は VLAN 内のすべてのルータポートとマルチキャストグループのすべてのメンバポートから IGMP group-specific クエリを転送します。直接接続されたレシーバから IGMP レポートの応答を待ちます。leave メッセージを受信したダイナミックメンバポートのため、装置は以下のアクションを実行します。

- メンバポートのエージングタイマが切れる前に、装置はそのポートのエージングタイマを再起動します。
- 装置はエージングタイマが終了すると、マルチキャストグループの転送テーブルエントリからポートを削除します。

2.1.3 IGMP snooping プロキシー機能

図 2-3に示すように、上流装置で受信される IGMP report メッセージ、IGMP leave メッセージの数を削減する場合、エッジ装置で IGMP snooping プロキシー機能を有効にします。IGMP snooping プロキシー機能を有効にした場合、IGMP report メッセージ、IGMP leave メッセージを Router A に送信するため、上流の IGMP snooping クエリアのエッジ装置はホストとして動作します。

エッジ装置でホスト IGMP report の抑制メカニズムは適用しません。

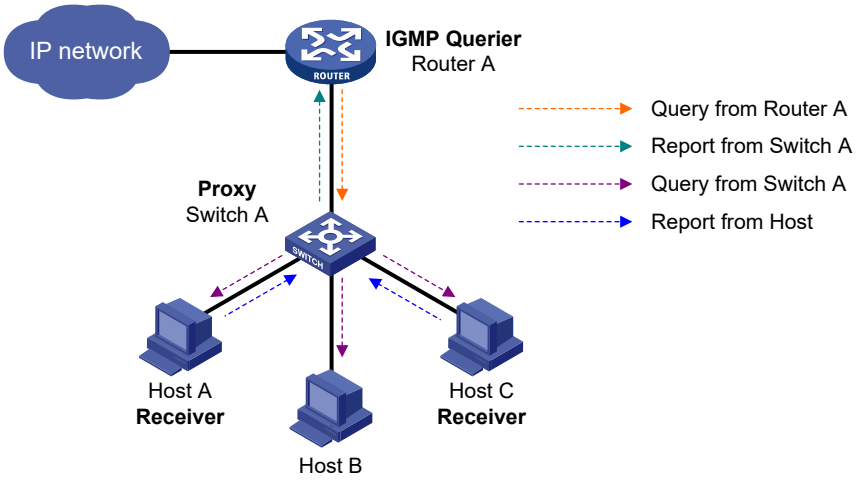


図 2-3 IGMP snooping プロキシー機能

IGMP snooping プロキシー機能が有効な装置は異なる IGMP メッセージを処理します。

- General クエリ

IGMP general クエリを受信したのち、装置は受信ポートを除く VLAN のすべてのポートにクエリを転送します。装置はローカルメンバシップ情報をもとにして IGMP report を作成し、すべてのルータポートに送信します。

- Group-specific クエリあるいは group-and-source-specific クエリ

IGMP group-specific クエリ あるいは IGMP group-and-source-specific クエリを受信したのち、装置は受信ポートを除く VLAN のすべてのポートにクエリを転送します。転送エントリにメンバポートがある場合、装置は VLAN のすべてのルータポートに report を送信します。

- Report

ホストから IGMP report を受信したのち、装置は以下のように一致するエントリを転送テーブルから検索します。

- □ エントリが一致し、転送エントリに受信ポートを含んでいる場合、装置はポートのエージングタイマをリセットします。
- □ エントリが一致するが、転送エントリに受信ポートが含まれない場合、装置は出力インタフェースリストに受信ポートを追加します。そして受信ポートをダイナミックメンバポートとしてマーキングします。ポートのエージングタイマを開始します。
- □ エントリが一致しない場合、装置は出力インタフェースを受信ポートとして転送エントリを作成します。受信ポートをダイナミックメンバポートとしてマーキングします。ポートのエージングタイマを開始します。そしてすべてのルータポートに report を送信します。

- Leave メッセージ

ポートで IGMP leave メッセージを受信したのち、装置は受信ポートを通して IGMP group-specific クエリを送信します。last メンバポートが転送エントリから削除されたときのみすべてのルータポートに IGMP leave メッセージを送信します。

2.2 プロトコルと標準

RFC 4541, *Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches*

2.3 IGMP snooping設定作業リスト

作業リスト
IGMP snoopingの基本機能の設定 ● （必須設定項目）IGMP snoopingの有効化 ● （オプション設定項目）IGMP snoopingのバージョンの設定 ● （オプション設定項目）IGMP snooping転送エントリの最大数の設定 ● （オプション設定項目）スタティックマルチキャストアドレスエントリの設定 ● （オプション設定項目）IGMP last member クエリ間隔の設定
IGMP snoopingポート機能の設定 ● （オプション設定項目）ダイナミックポートのエージングタイマの設定 ● （オプション設定項目）スタティックポートの設定 ● （オプション設定項目）シミュレーティッドメンバホストの設定 ● （オプション設定項目）fast-leave処理の有効化
IGMP snooping クエリの設定 ● （オプション設定項目）IGMP snoopingクエリアの有効化 ● （オプション設定項目）IGMP クエリとresponseのパラメータの設定
（オプション設定項目）IGMP snooping プロキシー機能の有効化
IGMPメッセージパラメータの設定 ● （オプション設定項目）IGMPメッセージの送信元IPアドレスの設定 ● （オプション設定項目）IGMPメッセージの802.1p優先度の設定

作業リスト
IGMP snooping ポリシーの設定 • （オプション設定項目）マルチキャストグループポリシーの設定 • （オプション設定項目）マルチキャストソースポートフィルタの設定 • （オプション設定項目）未知のマルチキャストデータ廃棄機能の有効化 • （オプション設定項目）IGMP report抑制機能の有効化 • （オプション設定項目）ポートで参加可能なマルチキャストグループの最大数の設定 • （オプション設定項目）マルチキャストグループ置き換え機能の有効化
（オプション設定項目）送信するIGMPプロトコルパケットのDSCPの設定

IGMP snooping において、アグリゲートインタフェース上での設定は、そのメンバポートの設定に干渉しないし、アグリゲーション計算にも参加しません。アグリゲートグループのメンバポートでの設定は、アグリゲートグループから離脱するまで有効になりません。

2.4 IGMP snoopingの基本機能の設定

IGMP snooping の基本機能の設定をする前に、以下の作業を完了させてください。

- 対応する VLAN を設定してください。
- IGMP snooping のバージョンを定義してください。
- IGMP snooping 転送エントリの最大数を定義してください。
- IGMP last member クエリの間隔を定義してください。

2.4.1 IGMP snooping の有効化

IGMP snooping を有効にするとき、以下のガイドラインに従ってください。

- VLAN で IGMP snooping を有効にする前に、グローバルで有効にしてください。
- VLAN 用の IGMP snooping は、VLAN のメンバポートでのみ動作します。

以下に IGMP snooping の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. IGMP snooping をグローバルで有効にし、IGMP-snooping view に移行する	**igmp-snooping**	デフォルト：無効
3. system view に戻る	**quit**	ー
4. VLAN view に移行する	**vlan** *vlan-id*	ー
5. VLAN で IGMP snooping を有効にする	**igmp-snooping enable**	デフォルト：無効

2.4.2 IGMP snooping のバージョンの設定

IGMP snooping のバージョン異なると、IGMP メッセージの異なるバージョンを処理することができます。

- IGMPv2 snooping は IGMPv1 と IGMPv2 のメッセージを処理することができますが、IGMPv3 メッセージは処理することはできず、VLAN 上にフラッディングされてしまいます。
- IGMPv3 snooping は IGMPv1、IGMPv2、IGMPv3 メッセージを処理することができます。

IGMPv3 snooping を IGMPv2 snooping に変更する場合、装置は以下のことを行います。

- ダイナミックに追加されたすべての IGMP snooping 転送エントリを削除します。
- IGMPv3 snooping スタティック（* , G）の転送エントリは維持します。
- IGMPv3 snooping スタティック（S , G）の転送エントリは削除します。IGMP snooping が IGMPv3 snooping に切り替わったとき復元されます。

スタティック IGMP snooping 転送エントリの詳細については、オペレーションマニュアルのセクション 6 *マルチキャスト*”*IGMP スヌーピング*”の”*スタティックポートの設定*”を参照してください。

以下に IGMP snooping のバージョンの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． VLAN view に移行する	**vlan** *vlan-id*	―
3． IGMP snooping のバージョンを指定する	**igmp-snooping version** *version-number*	デフォルト：2

2.4.3 IGMP snooping 転送エントリの最大数の設定

IGMP snooping 転送テーブルの最大エントリ数をグローバルに設定できます。この最大エントリ数はダイナミックエントリ、スタティックを含みます。装置の転送エントリ数が上限に達すると、装置は、いくつかのエントリがタイムアウトするか、手動で削除されるまで、転送エントリを生成することができません。新しいエントリを作成するため、手動でエントリを削除することを推奨します。

以下に IGMP snooping 転送エントリの最大数の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． IGMP-snooping view に移行する	**igmp-snooping**	―
3． IGMP snooping 転送エントリの最大数を設定する	**entry-limit** *limit*	デフォルト：4294967295

2.4.4 スタティックマルチキャスト MAC アドレスエントリの設定

レイヤ 2 マルチキャストにおいて、マルチキャスト MAC アドレスエントリは IGMP snooping などのレイヤ 2 マルチキャストプロトコルによってダイナミックに作成することができます。またマルチキャスト MAC アドレスと、マルチキャストデータの宛先ポートを制御するポートを関連づけることでスタティックマルチキャスト MAC アドレスエントリを手動で設定することができます。

I. 設定の制限とガイドライン

スタティックマルチキャスト MAC アドレスエントリを設定する場合、以下の設定の制限とガイドラインに従ってください。

- 設定する前に IP マルチキャストルーティングを有効にする必要はありません。
- スタティックマルチキャスト MAC アドレスエントリを設定するとき、使用していないマルチキャスト MAC アドレスを指定してください。マルチキャスト MAC アドレスは最上位オクテットの最下位ビット（LSB）が 1 です。
- system view で指定したインタフェース、あるいは interface view で現在のインタフェースにスタティックマルチキャスト MAC アドレスエントリを設定することができます。

II. system view でのスタティックマルチキャスト MAC アドレスエントリの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. スタティックマルチキャスト MAC アドレスエントリを設定する	**mac-address multicast** *mac-address* **interface** *interface-list* **vlan** *vlan-id*	デフォルト：設定なし 詳細はコマンドマニュアルのセクション6 *マルチキャスト“MACアドレステーブル”*を参照してください。

III. interface view でのスタティックマルチキャスト MAC アドレスエントリの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Layer 2 Ethernet interface view あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	―
3. スタティックマルチキャスト MAC アドレスエントリを設定する	**mac-address multicast** *mac-address* **vlan** *vlan-id*	デフォルト：設定なし

2.4.5 IGMP last member クエリ間隔の設定

グループの IGMP group-specific クエリを受信すると、レシーバホストは参加した各マルチキャストグループのタイマを起動します。このタイマは、0 から最大応答時間（ホストは、受信した IGMP クエリの Max Response Time フィールドから最大応答時間の値を取得します）の範囲でランダムな値に初期化されます。タイマ値が経過して 0 になったときに、ホストは対応するマルチキャストグループに IGMP report を送信します。

IGMP クエリの最大応答時間を適切に設定すると、ホストは速やかにクエリに応答できます。また、対応するタイマの期限が多数のホストで同時に切れたときに同時に送信する report によってネットワーク上で発生する IGMP トラフィックのバーストを回避することもできます。

I. 設定の制限とガイドライン

IGMP last member クエリの間隔を設定する場合、以下の制限とガイドラインに従ってください。

- fast-leave 処理が有効なポートから IGMP leave メッセージを受信した場合、装置は IGMP group-specific クエリを送信しません。
- IGMP-snooping view のすべての VLAN、あるいは VLAN view の VLAN でグローバルに IGMP last member クエリの間隔を設定することができます。VLAN で行った設定はグローバルで行った設定よりも優先されます。

II. グローバルでの IGMP last member クエリの間隔の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. IGMP-snooping view に移行する	**igmp-snooping**	―
3. IGMP last-member クエリの送信間隔を設定する	**last-member-query-interval** *interval*	デフォルト：1秒

III. グローバルでの IGMP last member クエリの間隔の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. VLAN view に移行する	**vlan** *vlan-id*	―
3. IGMP last-member クエリの送信間隔を設定する	**igmp-snooping last-member-query-interval** *interval*	デフォルト：1秒

2.5 IGMP snoopingポート機能の設定

IGMP snooping ポート機能の設定をする前に、以下の作業を完了させてください。

- VLAN で IGMP snooping を有効にしてください。
- ダイナミックルータポートのエージングタイマを定義してください。
- ダイナミックメンバポートのエージングタイマを定義してください。
- マルチキャストグループとマルチキャスト送信元アドレスを定義してください。

2.5.1 ダイナミックポートのエージングタイマの設定

ダイナミックポートのエージングタイマを設定するとき、以下のガイドラインに従ってください。

- マルチキャストグループメンバシップが頻繁に変更される場合は、メンバポートのエージングタイマに比較的小さな値を設定します。マルチキャストグループメンバシップがほとんど変更されない場合は、メンバポートのエージングタイマに比較的大きな値を設定します。
- ダイナミックルータポートが PIMv2 hello メッセージを受信した場合、ダイナミックポートのエージングタイマの時間は、hello メッセージの時間で指定されません。この場合、**router-aging-time** コマンドあるいは **igmp-snooping router-aging-time** コマンドはポートで適用されません。
- ダイナミックポートのエージングタイマの設定は、VLAN view の現在の VLAN あるいは IGMP-snooping view のすべての VLAN のどちらかに設定することができます。もし VLAN view と IGMP-snooping view の両方に設定がある場合、VLAN view の設定が適用されます。

I. グローバルでのダイナミックポートのエージングタイマの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. IGMP-snooping view に移行する	**igmp-snooping**	―
3. グローバルでのダイナミックルータポートのエージングタイマを設定する	**router-aging-time** *seconds*	デフォルト：260秒
4. グローバルでのダイナミックメンバポートのエージングタイマを設定する	**host-aging-time** *seconds*	デフォルト：260秒

II. VLAN でのダイナミックポートのエージングタイマの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. VLAN view に移行する	**vlan** *vlan-id*	―
3. VLAN でのダイナミックルータポートのエージングタイマを設定する	**igmp-snooping router-aging-time** *seconds*	デフォルト：260秒
4. VLAN でのダイナミックメンバポートのエージングタイマを設定する	**igmp-snooping host-aging-time** *seconds*	デフォルト：260秒

2.5.2 スタティックポートの設定

以下のタイプのスタティックポートを設定することができます。

- **スタティックメンバポート**－マルチキャストグループのスタティックメンバポートを設定するとき、ポートに接続されるすべてのホストはグループのマルチキャストデータを受信することができます。

  設定を完了した、あるいは取り消したとき、ポートは IGMP report や leave メッセージを送信しません。スタティックメンバポートは IGMP クエリに応答しません。

- **スタティックルータポート**－マルチキャストグループのスタティックルータポートを設定するとき、ポートで受信されたグループのすべてのマルチキャストデータは転送されます。

以下にスタティックポートの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	－
2. Layer 2 Ethernet interface view あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	－
3. ポートをスタティックポートに設定する	• ポートをスタティックメンバポートに設定する：**igmp-snooping static-group** *group-address* [**source-ip** *source-address*] **vlan** *vlan-id* • ポートをスタティックルータポートに設定する：**igmp-snooping static-router-port vlan** *vlan-id*	デフォルト：設定なし

2.5.3 シミュレーティッドメンバホストの設定

ポートでシミュレーティッドメンバホストを設定したとき、以下の方法により独立したホストと同等になります。

- 設定が完了したとき、unsolicited IGMP report を送信します。
- IGMP report として IGMP general クエリに応答します。
- 設定を削除したとき、IGMP leave メッセージを送信します。

シミュレーティッドホストの IGMP のバージョンと IGMP snooping バージョンが同一であることを確認してください。スタティックメンバポートと異なり、シミュレーティッドメンバホストとして設定されたポートはダイナミックメンバポートと同様にエージアウトします。

以下にシミュレーティッドメンバホストの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	－
2. Layer 2 Ethernet interface view あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	－
3. ポートをシミュレーティッドメンバホストとして設定する	**igmp-snooping host-join** *group-address* [**source-ip** *source-address*] **vlan** *vlan-id*	デフォルト：設定なし

2.5.4 fast-leave 処理の有効化

ポートが leave メッセージを受信するとき、装置は fast-leave 処理機能によって、IGMP leave メッセージを迅速に転送エントリからポートを削除することができます。

I. 設定の制限とガイドライン

IGMP snooping fast-leave 処理機能を設定するとき、以下の設定の制限とガイドラインに従ってください。

- 複数のホストが接続しているポートでは fast-leave 処理機能を有効にしないでください。そうでないと同じマルチキャストグループにあるポートに接続された他のレシーバのホストはマルチキャストデータを受信することができません。
- IGMP snooping fast-leave 処理機能は、ポートあるいはグローバルのどちらかに設定することができます。もしポートとグローバルの両方に設定がある場合、ポートの設定が適用されます。

II. グローバルでの IGMP snooping fast-leave 処理機能の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. IGMP-snooping view に移行する	**igmp-snooping**	―
3. グローバルで IGMP snooping fast-leave 処理機能を設定する	**fast-leave** [**vlan** *vlan-list*]	デフォルト：無効

III. ポートでの IGMP snooping fast-leave 処理機能の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Layer 2 Ethernet interface view あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	―
3. ポートで IGMP snooping fast-leave 処理機能を設定する	**igmp-snooping fast-leave** [**vlan** *vlan-list*]	デフォルト：無効

2.6 IGMP snooping クエリの設定

この項では IGMP snooping クエリの設定方法について記載します。

2.6.1 設定要件

IGMP snooping クエリを設定する前に、以下の作業を完了してください。

- VLAN で IGMP snooping を有効にしてください。
- IGMP general クエリの送信間隔を定義してください。
- IGMP last-member クエリの送信間隔を定義してください。
- IGMP general クエリの最大応答時間を定義してください。

2.6.2 IGMP snooping クエリアの有効化

この機能は、データリンクレイヤでマルチキャスト転送エントリを確立し、維持するために、装置が IGMP general クエリを定期的に送信します。レイヤ 3 マルチキャスト装置がないネットワークで IGMP snooping クエリアを設定することができます。

IGMP snooping クエリアを有効にするとき、IGMP が動作するマルチキャストネットワークで IGMP snooping クエリアを有効にしないでください。IGMP Snooping クエリアは IGMP クエリアの選択に関与しませんが、小さい送信元 IP アドレスで IGMP general クエリを送信するので IGMP クエリアの選択に影響を与える可能性があります。

以下に VLAN で IGMP snooping クエリアを有効にする設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． VLAN view に移行する	**vlan** *vlan-id*	―
3． IGMP snooping クエリアを有効にする	**igmp-snooping querier**	デフォルト：無効

2.6.3 IGMP クエリと response のパラメータの設定

⚠ **注意：**

IGMP general クエリ間隔は IGMP general クエリの最大応答時間よりも大きいことを確認してください。そうしないとマルチキャストグループメンバが誤って削除されてしまう可能性があります。

VLAN ベースのネットワークの実際の状況にもとづいて、IGMP general クエリ の送信間隔 を調整することができます。

IGMP クエリ（general クエリ または group-specific クエリ）を受信すると、レシーバホストは参加した各マルチキャストグループの report delay タイマを起動します。このタイマは、0 から最大応答時間（ホストは、受信した IGMP クエリの Max Response Time フィールドから最大応答時間の値を取得します）の範囲でランダムな値に初期化されます。タイマ値が経過して 0 になったときに、ホストは対応するマルチキャストグループに IGMP report を送信します。

IGMP クエリの最大応答時間を適切に設定すると、ホストは速やかにクエリに応答できます。また、対応するタイマの期限が多数のホストで同時に切れたときに同時に送信する report によってネットワーク上で発生する IGMP トラフィックのバーストを回避することもできます。

IGMP クエリと応答のパラメータは、VLAN view で現在の view あるは IGMP-snooping view ですべての VLAN で設定できます。もし VLAN view と IGMP-snooping view の 2 つの設定がある場合、VLAN view で設定された設定が適用されます。

I. グローバルでの IGMP クエリと response のパラメータの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． IGMP-snooping view に移行する	**igmp-snooping**	―
3． IGMP general クエリの最大応答時間を設定する	**max-response-time** *seconds*	デフォルト：10秒

II. VLAN での IGMP クエリと response のパラメータの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． VLAN view に移行する	**vlan** *vlan-id*	―
3． IGMP general クエリの送信間隔を設定する	**igmp-snooping query-interval** *interval*	デフォルト：125秒
4． IGMP general クエリの最大応答時間を設定する	**igmp-snooping max-response-time** *seconds*	デフォルト：10秒

2.7 IGMP snooping プロキシー機能の有効化

VLAN で IGMP snooping プロキシー機能を有効にする前に、VLAN で IGMP snooping 機能を有効にしてください。

以下に VLAN で IGMP snooping プロキシー機能を有効にする設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． VLAN view に移行する	**vlan** *vlan-id*	―
3． IGMP snooping プロキシー機能を有効にする	**igmp-snooping proxy enable**	デフォルト：無効

2.8 IGMPメッセージのパラメータの設定

この章では IGMP メッセージのパラメータの設定について記載します。

2.8.1 設定要件

VLAN で IGMP メッセージのパラメータを設定する前に、以下の作業を完了してください。

- VLAN で IGMP snooping を有効にしてください。
- IGMP general クエリの送信元 IP アドレスを定義してください。
- IGMP group-specific クエリの送信元 IP アドレスを定義してください。
- IGMP report の送信元 IP アドレスを定義してください。

- IGMP leave message の送信元 IP アドレスを定義してください。
- IGMP メッセージの 802.1p 優先度を定義してください。

2.8.2 IGMP メッセージの送信元 IP アドレスの設定

送信元 IP アドレスが 0.0.0.0 である IGMP クエリをポートで受信すると、装置はそのポートをダイナミックルータポートとして設定しません。これによって、マルチキャスト転送エントリがデータリンクレイヤで正しく作成されずに、最終的にマルチキャストトラフィック転送エラーが発生する可能性があります。

この問題を防ぐため、IGMP snooping クエリアとして動作する装置によって送信された IGMP クエリの送信元 IP アドレスとしてオール 0 以外の IP アドレスを設定することができます。IGMP クエリの送信元アドレスを変更するとサブネット内の IGMP クエリアの選定に影響する可能性があります。

シミュレーティッドメンバホストあるいは IGMP snooping のプロキシーによって IGMP report あるいは IGMP leave message の送信元 IP アドレスを変更することができます。

以下に VLAN での IGMP メッセージの送信元 IP アドレスの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． VLAN view に移行する	**vlan** *vlan-id*	―
3． IGMP general クエリの送信元 IP アドレスを設定する	**igmp-snooping general-query source-ip** *ip-address*	デフォルト : 現在のVLANインタフェースのIPアドレスです。 現在のVLANインタフェースにIPアドレスがない場合、0.0.0.0です。
4． IGMP group-specific クエリの送信元 IP アドレスを設定する	**igmp-snooping special-query source-ip** *ip-address*	デフォルト : 以下のいずれかとなります。 ● VLANのIGMP snoopingクエリアがIGMP general クエリを受信したとき、IGMP group-specific クエリの送信元IPアドレスはIGMP general クエリの送信元IPアドレスです。 ● VLANのIGMP snoopingクエリアがIGMP general クエリを受信していない場合、IGMP group-specific クエリの送信元IPアドレスは現在のVLANインタフェースのIPアドレスです。 ● VLANのIGMP snoopingクエリアがIGMP general クエリを受信しておらず、現在のVLANインタフェースにIPアドレスが設定されていない場合、送信元IPアドレスは0.0.0.0です。

操作	コマンド	補足
5. IGMP reports の送信元 IP アドレスを設定する	**igmp-snooping report source-ip** *ip-address*	デフォルト : 現在のVLANインタフェースのIPアドレスです。 現在のVLANインタフェースにIPアドレスがない場合、0.0.0.0です。
6. IGMP leave メッセージの送信元 IP アドレスを設定する	**igmp-snooping leave source-ip** *ip-address*	デフォルト : 現在のVLANインタフェースのIPアドレスです。 現在のVLANインタフェースにIPアドレスがない場合、0.0.0.0です。

2.8.3 IGMP メッセージの 802.1p 優先度の設定

装置の出力ポートで混雑が発生すると、802.1p 優先度が高い順から IGMP メッセージを転送します。装置によって作成あるいは転送される IGMP メッセージに高い 802.1p 優先度を割り当てることができます。

IGMP-snooping view のすべての VLAN あるいは VLAN view の現在の VLAN で IGMP メッセージの優先度を設定することができます。VLAN view での設定は IGMP-snooping view での設定よりも優先されます。

I. グローバルでの IGMP メッセージの 802.1p 優先度の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. IGMP-snooping view に移行する	**igmp-snooping**	ー
3. IGMP メッセージの 802.1p 優先度を設定する	**dot1p-priority** *priority*	デフォルト：設定なし 装置によって作成されるIGMPメッセージの優先度は0です。IGMPメッセージを転送する場合、優先度は変更しません。

II. VLAN での IGMP メッセージの 802.1p 優先度の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. VLAN view に移行する	**vlan** *vlan-id*	ー
3. IGMP メッセージの 802.1p 優先度を設定する	**igmp-snooping dot1p-priority** *priority*	デフォルト：設定なし 装置によって作成されるIGMPメッセージの優先度は0です。IGMPメッセージを転送する場合、優先度は変更しません。

2.9 IGMP snooping ポリシーの設定

IGMP snooping ポリシーの設定をする前に、以下の作業を完了させてください。

- VLAN で IGMP snooping を有効にしてください。
- マルチキャストグループポリシーに使用する ACL を定義してください。
- ポートが追加できるマルチキャストグループの最大数を定義してください。

2.9.1 マルチキャストグループポリシーの設定

マルチキャストグループを指定するACLとオプションのソースにもとづいてIGMP reportをフィルタします。受信ホストが加入するマルチキャストグループを管理するために使用されます。

I. 設定の制限とガイドライン

マルチキャストグループポリシーの設定を行うとき、以下の設定の制限とガイドラインに従ってください。

- この設定はポートがダイナミックに追加するマルチキャストグループに適用されます。
- マルチキャストグループポリシーは、ポートあるいはグローバルのどちらかに設定することができます。もしポートとグローバルの両方に設定がある場合、ポートの設定が適用されます。

II. グローバルでのマルチキャストグループポリシーの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. IGMP-snooping view に移行する	**igmp-snooping**	—
3. グローバルでマルチキャストグループポリシーを設定する	**group-policy** *ipv4-acl-number* [**vlan** *vlan-list*]	デフォルト：設定なし

III. ポートでのマルチキャストグループポリシーの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. Layer 2 Ethernet interface view あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	—
3. ポートでマルチキャストグループポリシーを設定する	**igmp-snooping group-policy** *ipv4-acl-number* [**vlan** *vlan-list*]	デフォルト：設定なし

2.9.2 マルチキャストソースポートフィルタの設定

この機能はすべてのマルチキャストデータパケットを廃棄し、マルチキャストプロトコルパケットを許可します。マルチキャストレシーバに接続するポートに設定します。

IGMP-snooping view で指定したポートあるいは interface view の現在のポートでマルチキャストソースポートフィルタを有効にすることができます。これらの設定は同じ優先度を持ちます。

I. グローバルでのマルチキャストソースポートフィルタの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. IGMP-snooping view に移行する	**igmp-snooping**	―
3. マルチキャストソースポートフィルタを有効にする	**source-deny port** *interface-list*	デフォルト：無効

II. ポートでのマルチキャストソースポートフィルタの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Layer 2 Ethernet interface view に移行する	**interface** *interface-type interface-number*	―
3. マルチキャストソースポートフィルタを有効にする	**igmp-snooping source-deny**	デフォルト：無効

2.9.3 未知のマルチキャストデータ廃棄機能の有効化

この機能はすべての未知のマルチキャストデータを廃棄します。未知のマルチキャストデータとは、IGMP snooping 転送テーブルにエントリが存在しないマルチキャストデータのことです。装置にルータポートがない場合、未知のマルチキャストデータを廃棄します。

この機能はすべての未知のマルチキャストデータを廃棄します。この機能を無効にした場合、装置は未知のマルチキャストパケットをデータが存在する VLAN にフラッディングします。

以下に未知のマルチキャストデータ廃棄機能の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. VLAN view に移行する	**vlan** *vlan-id*	―
3. 未知のマルチキャストデータ廃棄機能を有効にする	**igmp-snooping drop-unknown**	デフォルト：無効 未知のマルチキャストデータはフラッディングします。

2.9.4 IGMP report 抑制機能の有効化

この機能はマルチキャストグループ用に、直接接続されているレイヤ 3 装置に最初の IGMP report のみを転送します。以降の同じマルチキャストグループからの IGMP report を廃棄します。

以下に IGMP report 抑制機能を有効にする設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． IGMP-snooping view に移行する	**igmp-snooping**	―
3． IGMP report 抑制機能を有効にする	**report-aggregation**	デフォルト：有効

2.9.5 ポートで参加可能なマルチキャストグループの最大数の設定

ポートトラフィックを調整するため、ポートで参加可能なマルチキャストグループの最大数を設定することができます。

I. 設定の制限とガイドライン

ポートで参加可能なマルチキャストグループの最大数を設定するとき、以下の設定の制限とガイドラインに従ってください。

- この設定はダイナミックにマルチキャストグループに加入されたポートのみ適用します。
- ポートが参加したマルチキャストグループの数が設定されている最大数に達したときは、そのポートに残るすべての転送エントリを IGMP snooping 転送テーブルから削除します。このポートに接続されたホストは、最大数になる前に、再度マルチキャストグループに参加することができます。

II. 設定手順

以下にポートで参加可能なマルチキャストグループの最大数の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． Layer 2 Ethernet interface view あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	―
3． ポートで参加可能なマルチキャストグループの最大数を設定する	**igmp-snooping group-limit** *limit* [**vlan** *vlan-list*]	デフォルト：4294967295

2.9.6 マルチキャストグループ置き換え機能の有効化

この機能は、グループのメンバ数が上限を超えたとき、装置が既存のマルチキャストグループを新規に追加されたマルチキャストグループに置き換える機能です。この機能は一般的にチャンネルスイッチアプリケーションで使われます。この機能が無効の場合、装置は新しいグループの IGMP report を廃棄し、ユーザが新しいチャンネルに変更することができません。

I. 設定の制限とガイドライン

マルチキャストグループ置き換え機能を有効にしたとき、以下の設定の制限とガイドラインに従ってください。

- この設定はダイナミックにマルチキャストグループに加入されたポートのみ適用します。
- マルチキャストグループ置き換え機能は、インタフェースあるいはグローバルのどちらかに設定することができます。もしインタフェースとグローバルの両方に設定がある場合、インタフェースの設定が適用されます。

II. グローバルでのマルチキャストグループ置き換え機能の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. IGMP-snooping view に移行する	**igmp-snooping**	―
3. グローバルでマルチキャストグループ置き換え機能を有効にする	**overflow-replace** [**vlan** *vlan-list*]	デフォルト：無効

III. ポートでのマルチキャストグループ置き換え機能の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Layer 2 Ethernet interface view あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	―
3. ポートでマルチキャストグループ置き換え機能を有効にする	**igmp-snooping overflow-replace** [**vlan** *vlan-list*]	デフォルト：無効

2.10 送信するIGMPプロトコルパケットのDSCPの設定

I. 送信する IGMP プロトコルパケットの DSCP

DSCP はパケットのプライオリティを決定し、パケットを転送する優先度を決定します。DSCP の値が大きいほど優先度は高くなります。

II. 設定手順

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． IGMP-snooping view に移行する	**igmp-snooping**	―
3． 送信する IGMP プロトコルパケットの DSCP を設定する	**dscp** *dscp-value*	デフォルト：48

2.11 IGMP snoopingの表示と維持

すべての view で **display** コマンドを実行でき、user view で **reset** コマンドを実行できます。

操作	コマンド
IGMP snoopingステータスを表示する	**display igmp-snooping** [**global** | **vlan** *vlan-id*]
ダイナミックIGMP snooping転送エントリの情報を表示する	**display igmp-snooping group** [*group-address* | *source-address*] * [**vlan** *vlan-id*] [**verbose**] [**slot** *slot-number*]
スタティックIGMP snooping転送エントリの情報を表示する	**display igmp-snooping static-group** [*group-address* | *source-address*] * [**vlan** *vlan-id*] [**verbose**] [**slot** *slot-number*]
ダイナミックルータポートの情報を表示する	**display igmp-snooping router-port** [**vlan** *vlan-id*] [**slot** *slot-number*]
スタティックルータポートの情報を表示する	**display igmp-snooping static-router-port** [**vlan** *vlan-id*] [**slot** *slot-number*]
IGMP snoopingによって学習されたIGMPメッセージの統計情報を表示する	**display igmp-snooping statistics**
レイヤ2 IPマルチキャストグループの情報を表示する	**display l2-multicast ip** [**group** *group-address* | **source** *source-address*] * [**vlan** *vlan-id*] [**slot** *slot-number*]
レイヤ2 IPマルチキャストグループエントリの情報を表示する	**display l2-multicast ip forwarding** [**group** *group-address* | **source** *source-address*] * [**vlan** *vlan-id*] [**slot** *slot-number*]
レイヤ2 MACマルチキャストグループの情報を表示する	**display l2-multicast mac** [*mac-address*] [**vlan** *vlan-id*] [**slot** *slot-number*]
レイヤ2 MACマルチキャストグループエントリの情報を表示する	**display l2-multicast mac forwarding** [*mac-address*] [**vlan** *vlan-id*] [**slot** *slot-number*]
スタティックマルチキャストMACアドレスエントリを表示する	**display mac-address** [*mac-address* [**vlan** *vlan-id*] | [**multicast**] [**vlan** *vlan-id*] [**count**]]
指定されたマルチキャストグループのダイナミックIGMP snooping転送エントリを削除する	**reset igmp-snooping group** { *group-address* [*source-address*] | **all** } [**vlan** *vlan-id*]
ダイナミックルータポートを削除する	**reset igmp-snooping router-port** { **all** | **vlan** *vlan-id*]
IGMP snoopingによって学習されたIGMPメッセージの統計情報を削除する	**reset igmp-snooping statistics**

2.12 IGMP snooping設定例

2.12.1 グループポリシーとシミュレーティッドメンバホストの設定例

I. ネットワーク要件

本設定例では、Switch A が QX-S5100G シリーズに該当します。

別途、IPv4 マルチキャストルーティングに対応した Router A が必要です。

図 2-4に示すように、Router A は IGMPv2 を動作させ、IGMP クエリアとして機能します。Switch A は IGMPv2 snooping を動作させます。

グローバルポリシーとシミュレーティッドメンバホストを以下のように設定します。

- Host A と Host B がマルチキャストグループ 224.1.1.1 のマルチキャストデータのみ受信します。Host A と Host B がマルチキャストデータの受信に失敗しても、マルチキャストデータは連続して Switch A の GigabitEthernet1/0/3 と GigabitEthernet1/0/4 を通して転送することができます。
- Switch A は VLAN100 でフラッディングしないように未知のマルチキャストデータを廃棄します。

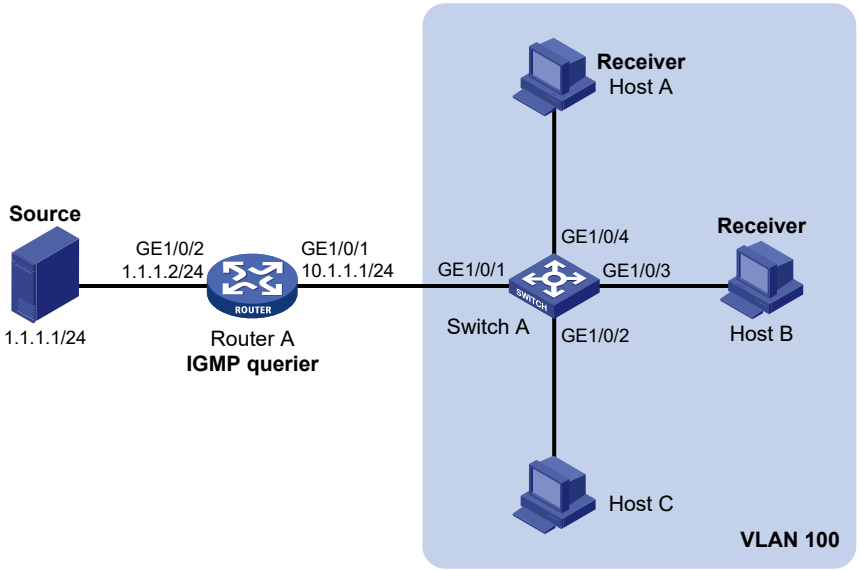


図 2-4 ネットワーク図

II. 設定手順

1) 図 2-4に対応する各インタフェースに IP アドレスとサブネットマスクを割り当てます。（詳細は省略します）
2) Router A を設定します。

IP マルチキャストルーティングを有効にします。

```
<RouterA> system-view
```

```
[RouterA] multicast routing
[RouterA-mrib] quit
```

GigabitEthernet 1/0/1 で IGMP を有効にします。

```
[RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] igmp enable
[RouterA-GigabitEthernet1/0/1] quit
```

GigabitEthernet 1/0/2 で PIM-SM を有効にします。

```
[RouterA] interface gigabitethernet 1/0/2
[RouterA-GigabitEthernet1/0/2] pim sm
[RouterA-GigabitEthernet1/0/2] quit
```

3)　Switch A を設定します。

グローバルで IGMP snooping を有効にします。

```
<SwitchA> system-view
[SwitchA] igmp-snooping
[SwitchA-igmp-snooping] quit
```

VLAN 100 を作成し、この VLAN に GigabitEthernet 1/0/1～GigabitEthernet 1/0/4 を割り当てます。

```
[SwitchA] vlan 100
[SwitchA-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/4
```

VLAN100 で IGMP snooping を有効にし、未知のマルチキャストデータ廃棄機能を有効にします。

```
[SwitchA-vlan100] igmp-snooping enable
[SwitchA-vlan100] igmp-snooping drop-unknown
[SwitchA-vlan100] quit
```

VLAN 100 にマルチキャストグループ 224.1.1.1 だけが参加できるように、マルチキャストグループポリシーを設定します。

```
[SwitchA] acl basic 2001
[SwitchA-acl-ipv4-basic-2001] rule permit source 224.1.1.1 0
[SwitchA-acl-ipv4-basic-2001] quit
[SwitchA] igmp-snooping
[SwitchA-igmp-snooping] group-policy 2001 vlan 100
[SwitchA-igmp-snooping] quit
```

マルチキャストグループ 224.1.1.1 のシミュレーティッドメンバホストとして GigabitEthernet 1/0/3、GigabitEthernet 1/0/4 を設定します。

```
[SwitchA] interface gigabitethernet 1/0/3
```

```
[SwitchA-GigabitEthernet1/0/3] igmp-snooping host-join 224.1.1.1 vlan 100
[SwitchA-GigabitEthernet1/0/3] quit
[SwitchA] interface gigabitethernet 1/0/4
[SwitchA-GigabitEthernet1/0/4] igmp-snooping host-join 224.1.1.1 vlan 100
[SwitchA-GigabitEthernet1/0/4] quit
```

III. 設定の確認

Host A と Host B がマルチキャストグループ 224.1.1.1、224.2.2.2 に加入するため IGMP report を受信します。（詳細は省略します）

Switch A で VLAN 100 のダイナミック IGMP snooping 転送エントリの情報を表示します。

```
[SwitchA] display igmp-snooping group vlan 100
Total 1 entries.

VLAN 100: Total 1 entries.
  (0.0.0.0, 224.1.1.1)
    Host ports (2 in total):
      GE1/0/3                                 (00:03:23)
      GE1/0/4                                 (00:04:10)
```

出力は、以下を示します。

- Switch A のメンバポート GigabitEthernet 1/0/4、GigabitEthernet 1/0/3 を通して、Host A と Host B がマルチキャストグループ 224.1.1.1 に加入しています。
- Host A と Host B がマルチキャストグループ 224.2.2.2 に加入できないことを示しています。マルチキャストグループのポリシーが適用されていることを示します。

2.12.2 スタティックポートの設定例

I. ネットワーク要件

本設定例では、Switch A、Switch B、 Switch C が QX-S5100G シリーズに該当し、Switch A へスタティックルータポートの設定をします。

別途、IPv4 マルチキャストルーティングに対応した Router A が必要です。

図 2-5に示すようなネットワークを設定します。

- Router A は IGMPv2 を動作させ、IGMP クエリアとして機能し、Switch A、Switch B、Switch C は IGMPv2 snooping を動作させます。
- Host A と Host C はマルチキャストグループ 224.1.1.1 の永久的なレシーバです。

以下の要件に適用するためスタティックポートを設定します。

- マルチキャストトラフィック送信の信頼性を強化するために、Switch C の GigabitEthernet 1/0/3 と GigabitEthernet 1/0/5 をマルチキャストグループ 224.1.1.1 のスタティックメンバポートとして設定します。
- ネットワークで STP が実行されていると仮定します。データループを回避するために、Switch A から Switch C への転送パスは通常状態ではブロックされます。マルチキャストトラフィックは Switch A—Switch B—Switch C のパスを経由して、Switch C

に接続されているレシーバに転送されます。Switch A—Switch B—Switch C のパスがブロックされた場合に、Switch A—Switch C のパスを経由してマルチキャストトラフィックがほとんど途切れずにレシーバへと転送できるように、Switch A の GigabitEthernet 1/0/3 にスタティックルータポートを設定します。STP の詳細は、オペレーションマニュアルのセクション 3 *アクセス”STP”* を参照してください。

メモ：

スタティックルータポートが設定されていない場合、Switch A—Switch B－Switch C のパスがブロックされたのち、マルチキャストの転送が中断されます。新しいパスでマルチキャストパケットを転送する前に、少なくとも 1 回以上の IGMP クエリと IGMP 応答の交換が必要です。

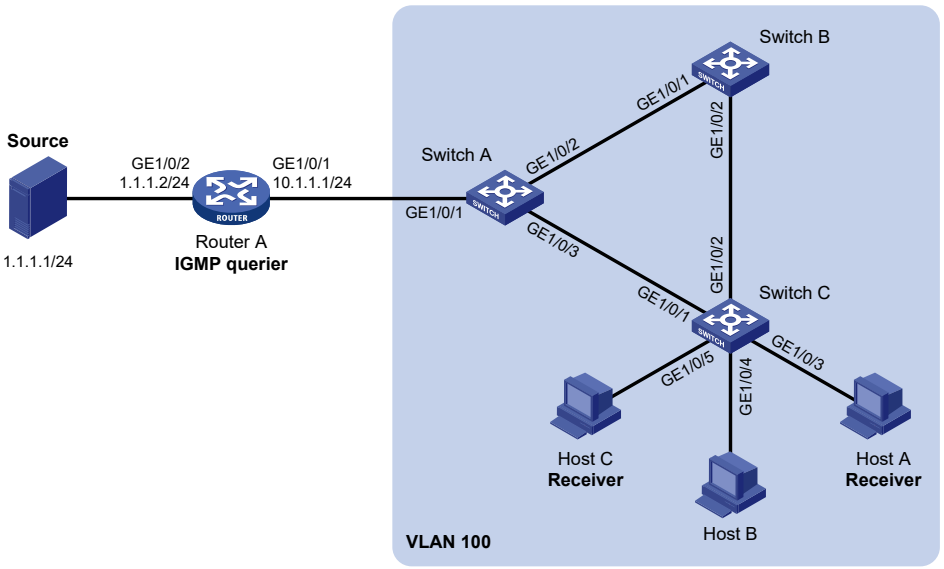


図 2-5 ネットワーク図

II. 設定手順

1) 図 2-5に対応する各インタフェースに IP アドレスとサブネットマスクを割り当てます。（詳細は省略します）
2) Router A を設定します。

IP マルチキャストルーティングを有効にします。

```
<RouterA> system-view
[RouterA] multicast routing
[RouterA-mrib] quit
```

GigabitEthernet 1/0/1 で IGMP を有効にします。

```
[RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] igmp enable
```

```
[RouterA-GigabitEthernet1/0/1] quit
```

GigabitEthernet 1/0/2 で PIM-SM を有効にします。

```
[RouterA] interface gigabitethernet 1/0/2
[RouterA-GigabitEthernet1/0/2] pim sm
[RouterA-GigabitEthernet1/0/2] quit
```

3)　Switch A を設定します。

グローバルに IGMP snooping を有効にします。

```
<SwitchA> system-view
[SwitchA] igmp-snooping
[SwitchA-igmp-snooping] quit
```

VLAN 100 を作成し、この VLAN に GigabitEthernet 1/0/1～GigabitEthernet 1/0/3 を割り当てます。

```
[SwitchA] vlan 100
[SwitchA-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/3
```

VLAN 100 で IGMP snooping を有効にします。

```
[SwitchA-vlan100] igmp-snooping enable
[SwitchA-vlan100] quit
```

スタティックルータポートとして、GigabitEthernet 1/0/3 を設定します。

```
[SwitchA] interface gigabitethernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] igmp-snooping static-router-port vlan 100
[SwitchA-GigabitEthernet1/0/3] quit
```

4)　Switch B を設定します。

グローバルに IGMP snooping を有効にします。

```
<SwitchB> system-view
[SwitchB] igmp-snooping
[SwitchB-igmp-snooping] quit
```

VLAN 100 を作成し、この VLAN に GigabitEthernet 1/0/1～GigabitEthernet 1/0/2 を割り当てます。

```
[SwitchB] vlan 100
[SwitchB-vlan100] port gigabitethernet 1/0/1 gigabitethernet 1/0/2
```

VLAN 100 で IGMP snooping を有効にします。

```
[SwitchB-vlan100] igmp-snooping enable
[SwitchB-vlan100] quit
```

5)　Switch C を設定します。

グローバルに IGMP snooping を有効にします。

```
<SwitchC> system-view
[SwitchC] igmp-snooping
[SwitchC-igmp-snooping] quit
```

VLAN 100 を作成し、この VLAN に GigabitEthernet 1/0/1～GigabitEthernet 1/0/5 を割り当てます。

```
[SwitchC] vlan 100
[SwitchC-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/5
```

VLAN100 で IGMP snooping を有効にします。

```
[SwitchC-vlan100] igmp-snooping enable
[SwitchC-vlan100] quit
```

マルチキャストグループ 224.1.1.1 のスタティックメンバポートとして GigabitEthernet 1/0/3、GigabitEthernet 1/0/5 を設定します。

```
[SwitchC] interface gigabitethernet 1/0/3
[SwitchC-GigabitEthernet1/0/3] igmp-snooping static-group 224.1.1.1 vlan 100
[SwitchC-GigabitEthernet1/0/3] quit
[SwitchC] interface gigabitethernet 1/0/5
[SwitchC-GigabitEthernet1/0/5] igmp-snooping static-group 224.1.1.1 vlan 100
[SwitchC-GigabitEthernet1/0/5] quit
```

III. 設定の確認

Switch A で VLAN 100 のスタティックルータポートの情報を表示します。

```
[SwitchA] display igmp-snooping static-router-port vlan 100
VLAN 100:
  Router ports (1 in total):
    GE1/0/3
```

出力は、Switch A の GigabitEthernet 1/0/3 がスタティックルータポートになっていることを示します。

Switch C で VLAN 100 のスタティック IGMP snooping 転送エントリの情報を表示します。

```
[SwitchC] display igmp-snooping static-group vlan 100
Total 1 entries.

VLAN 100: Total 1 entries.
  (0.0.0.0, 224.1.1.1)
    Host ports (2 in total):
      GE1/0/3
      GE1/0/5
```

出力は、Switch C の GigabitEthernet 1/0/3 と GigabitEthernet 1/0/5 がマルチキャストグループ 224.1.1.1 のスタティックメンバポートになっていることを示します。

2.12.3 IGMP snooping クエリアの設定例

I. ネットワーク要件

本設定例では、Switch A、Switch B、Switch C、Switch D が QX-S5100G シリーズに該当し、Switch A へ IGMP snooping クエリアの設定をします。

図 2-6に示すようなネットワークを設定します。

- ネットワークはレイヤ 2 のみのネットワークです。
- Source 1、Source 2 はそれぞれマルチキャストグループ 224.1.1.1、225.1.1.1 にマルチキャストデータを送信します。
- Host A、Host C はマルチキャストグループ 224.1.1.1 のレシーバで、Host B、Host D はマルチキャストグループ 225.1.1.1 のレシーバです。
- すべてのレシーバホストは IGMPv2 が動作し、すべての装置は IGMPv2 snooping が動作します。Switch A（マルチキャストソースにもっとも近い）は IGMP snooping クエリアとして動作します。

以下の要件に適合するように Switch を設定します。

- VLAN で未知のパケットをフラッディングしないように、すべての Switch で未知のマルチキャストパケットの廃棄機能を有効にします。
- レイヤ 2 転送エントリを確立するため、オール 0 以外の IP アドレスとして IGMP クエリの送信元 IP アドレスを設定します。

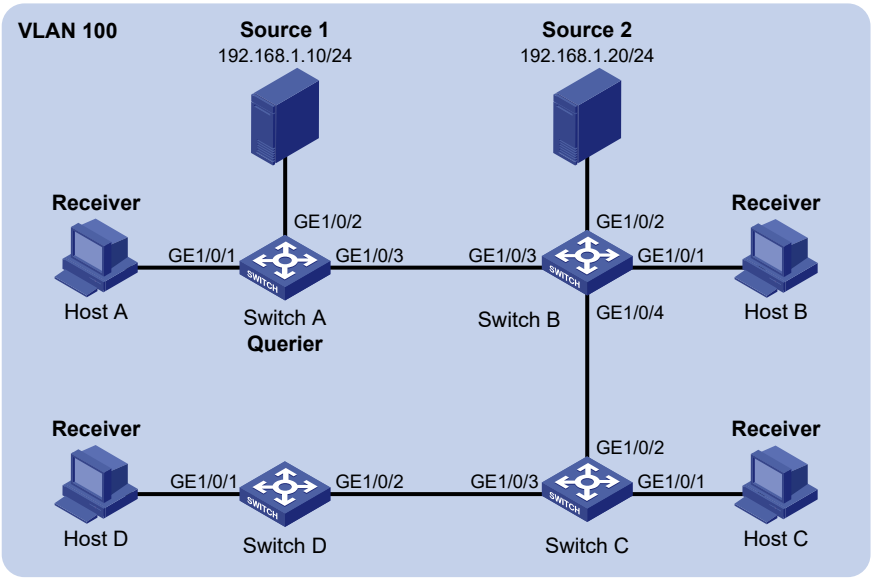


図 2-6 ネットワーク図

II. 設定手順

1)　Switch A を設定します。

グローバルに IGMP snooping を有効にします。

```
<SwitchA> system-view
[SwitchA] igmp-snooping
```

```
[SwitchA-igmp-snooping] quit
```

VLAN 100 を作成し、この VLAN に GigabitEthernet 1/0/1～GigabitEthernet 1/0/3 を割り当てます。

```
[SwitchA] vlan 100
[SwitchA-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/3
```

VLAN 100 で IGMP Snooping を有効にし、未知のマルチキャストデータ廃棄機能を有効にします。

```
[SwitchA-vlan100] igmp-snooping enable
[SwitchA-vlan100] igmp-snooping drop-unknown
```

VLAN 100 で IGMP Snooping クエリア機能を有効にします。

```
[SwitchA-vlan100] igmp-snooping querier
[SwitchA-vlan100] quit
```

VLAN 100 で IGMP general クエリの送信元 IP アドレスを 192.168.1.1 に設定します。

```
[SwitchA-vlan100] igmp-snooping general-query source-ip 192.168.1.1
```

VLAN 100 で IGMP group-specific クエリの送信元 IP アドレスを 192.168.1.1 に設定します。

```
[SwitchA-vlan100] igmp-snooping special-query source-ip 192.168.1.1
[SwitchA-vlan100] quit
```

2)　Switch B を設定します。

グローバルに IGMP snooping を有効にします。

```
<SwitchB> system-view
[SwitchB] igmp-snooping
[SwitchB-igmp-snooping] quit
```

VLAN 100 を作成し、この VLAN に GigabitEthernet 1/0/1～GigabitEthernet 1/0/4 を割り当てます。

```
[SwitchB] vlan 100
[SwitchB-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/4
```

VLAN 100 で IGMP Snooping を有効にし、未知のマルチキャストデータ廃棄機能を有効にします。

```
[SwitchB-vlan100] igmp-snooping enable
[SwitchB-vlan100] igmp-snooping drop-unknown
[SwitchB-vlan100] quit
```

3)　Switch C を設定します。

グローバルに IGMP snooping を有効にします。

```
<SwitchC> system-view
```

```
[SwitchC] igmp-snooping
[SwitchC-igmp-snooping] quit
```

VLAN 100 を作成し、この VLAN に GigabitEthernet 1/0/1～GigabitEthernet 1/0/3 を割り当てます。

```
[SwitchC] vlan 100
[SwitchC-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/3
```

VLAN 100 で IGMP Snooping を有効にし、未知のマルチキャストデータ廃棄機能を有効にします。

```
[SwitchC-vlan100] igmp-snooping enable
[SwitchC-vlan100] igmp-snooping drop-unknown
[SwitchC-vlan100] quit
```

4)　Switch D を設定します。

グローバルに IGMP snooping を有効にします。

```
<SwitchD> system-view
[SwitchD] igmp-snooping
[SwitchD-igmp-snooping] quit
```

VLAN 100 を作成し、この VLAN に GigabitEthernet 1/0/1～GigabitEthernet 1/0/2 を割り当てます。

```
[SwitchD] vlan 100
[SwitchD-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/2
```

VLAN 100 で IGMP Snooping を有効にし、未知のマルチキャストデータ廃棄機能を有効にします。

```
[SwitchD-vlan100] igmp-snooping enable
[SwitchD-vlan100] igmp-snooping drop-unknown
[SwitchD-vlan100] quit
```

III. 設定の確認

Switch B で IGMP snooping を通して学習した IGMP メッセージと PIMv2 メッセージの統計情報を表示します。

```
[SwitchB] display igmp-snooping statistics
Received IGMP general queries:  3
Received IGMPv1 reports:  0
Received IGMPv2 reports:  12
Received IGMP leaves:  0
Received IGMPv2 specific queries:  0
Sent     IGMPv2 specific queries:  0
Received IGMPv3 reports:  0
Received IGMPv3 reports with right and wrong records:  0
Received IGMPv3 specific queries:  0
Received IGMPv3 specific sg queries:  0
Sent     IGMPv3 specific queries:  0
```

```
Sent     IGMPv3 specific sg queries:  0
Received PIMv2 hello:  0
Received error IGMP messages:  0
```

出力は、Switch A が IGMP snooping クエリアとして動作したのち、Switch A を除くすべての Switch が IGMP general クエリを受信することができます。

2.12.4 IGMP snooping プロキシー機能の設定例

I. ネットワーク要件

本設定例では、Switch A が QX-S5100G シリーズに該当します。

別途、IPv4 マルチキャストルーティングに対応した Router A が必要です。

図 2-7に示すように、Router A は IGMPv2 を動作させ、IGMP クエリアとして動作します。Switch A は IGMPv2 snooping を動作させます。Switch A が以下の動作を行うため、IGMP snooping プロキシー機能の設定を行います。

- IGMP report、IGMP leave メッセージを Router A に転送します。
- Router A に送信された IGMP クエリに応答し、下流のホストにクエリを転送します。

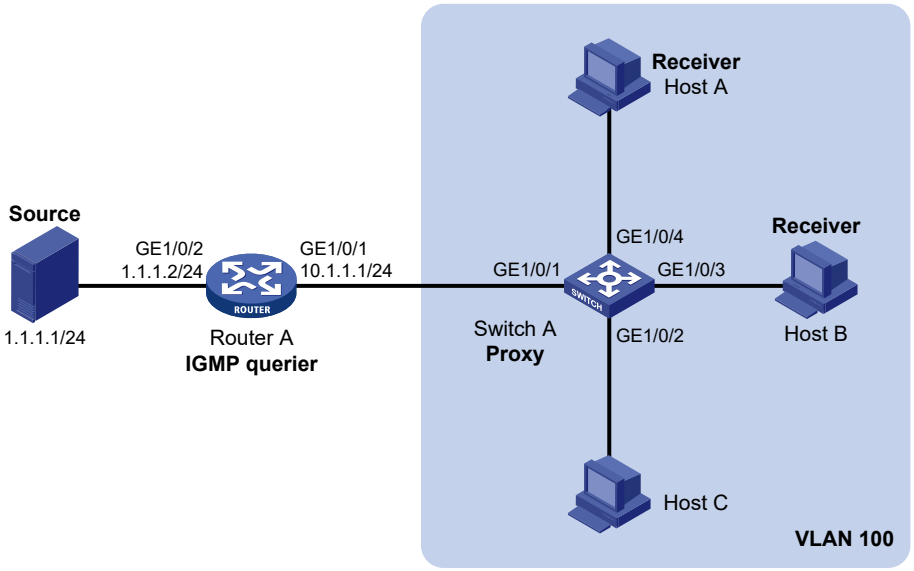


図 2-7 ネットワーク図

II. 設定手順

1) 図 2-7に対応する各インタフェースに IP アドレスとサブネットマスクを割り当てます。（詳細は省略します）
2) Router A を設定します。

IP マルチキャストルーティングを有効にします。

```
<RouterA> system-view
[RouterA] multicast routing
```

```
[RouterA-mrib] quit
```

GigabitEthernet 1/0/1 で IGMP を有効にし、PIM-SM を有効にします。

```
[RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] igmp enable
[RouterA-GigabitEthernet1/0/1] pim sm
[RouterA-GigabitEthernet1/0/1] quit
```

GigabitEthernet 1/0/2 で PIM-SM を有効にします。

```
[RouterA] interface gigabitethernet 1/0/2
[RouterA-GigabitEthernet1/0/2] pim sm
[RouterA-GigabitEthernet1/0/2] quit
```

3)　Switch A を設定します。

グローバルに IGMP snooping を有効にします。

```
<SwitchA> system-view
[SwitchA] igmp-snooping
[SwitchA-igmp-snooping] quit
```

VLAN 100 を作成し、この VLAN に GigabitEthernet 1/0/1～GigabitEthernet 1/0/4 を割り当てます。

```
[SwitchA] vlan 100
[SwitchA-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/4
```

VLAN 100 で IGMP snooping、IGMP snooping プロキシー機能を有効にします。

```
[SwitchA-vlan100] igmp-snooping enable
[SwitchA-vlan100] igmp-snooping proxy enable
[SwitchA-vlan100] quit
```

III. 設定の確認

Host A と Host B からマルチキャストグループ 224.1.1.1 に加入するため、IGMP report を送信します。（詳細は省略します。）

Switch A でダイナミック IGMP snooping グループエントリの情報を表示します。

```
[SwitchA] display igmp-snooping group
 Total 1 entries.

VLAN 100: Total 1 entries.
  (0.0.0.0, 224.1.1.1)
    Host ports (2 in total):
      GE1/0/3                                  (00:04:00)
      GE1/0/4                                  (00:04:04)
```

出力は、Switch C の GigabitEthernet 1/0/3 と GigabitEthernet 1/0/4 がマルチキャストグループ 224.1.1.1 のメンバポートになっていることを示します。Host A と Host B はグループのマルチキャストデータを受信することができます。

Router A の IGMP グループエントリの情報を表示します。

```
[RouterA] display igmp group
IGMP groups in total: 1
 GigabitEthernet1/0/1(10.1.1.1):
  IGMP groups reported in total: 1
   Group address   Last reporter   Uptime      Expires
   224.1.1.1       0.0.0.0         00:00:31    00:02:03
```

Host A からマルチキャストグループ 224.1.1.1 からさあ駆除するため、IGMP leave メッセージを送信します。（詳細は省略します。）

Switch A で IGMP snooping グループメンバシップの情報を表示します。

```
[SwitchA] display igmp-snooping group
Total 1 entries.

VLAN 100: Total 1 entries.
  (0.0.0.0, 224.1.1.1)
    Host ports (1 in total):
      GE1/0/3                                  ( 00:01:23 )
```

出力では、GigabitEthernet 1/0/4（Host A に接続されています）はマルチキャストグループ 224.1.1.1 のエントリから削除されていることを示します。

2.13 IGMP snoopingのトラブルシューティング

2.13.1 レイヤ 2 マルチキャスト転送ができない

I. 症状

装置でレイヤ 2 マルチキャスト転送ができません。

II. 分析

IGMP snooping が有効になっていません。

III. 解決策

1) IGMP snooping 情報を表示するため **display igmp-snooping** コマンドを使用します。
2) IGMP snooping が有効になっていない場合、グローバルで **igmp-snooping** コマンドを使用して IGMP snooping を有効にし、VLAN view で **igmp-snooping enable** コマンドを使用して IGMP snooping を有効にしてください。
3) グローバルで IGMP snooping が有効で、対応する VLAN で IGMP snooping が無効になっている場合、対応する VLAN の VLAN view 上で **igmp-snooping enable** コマンドを使用して IGMP snooping を有効にしてください。
4) 問題が解決しない場合、NEC に問い合わせてください。

2.13.2 マルチキャストグループポリシーが動作しない

I. 症状

マルチキャストポリシーによって許可されていないマルチキャストグループから、ホストがマルチキャストデータを受信できません。

II. 分析

- ACL ルールの設定が間違っています。
- マルチキャストグループポリシーが正しく適用されていません 。
- 未知のマルチキャストデータ廃棄機能が無効で、マルチキャストデータがフラッディングしています。

III. 解決策

1) **display acl** コマンドで ACL ルールの設定を確認してください。実行するマルチキャストグループポリシーに ACL ルールが一致していることを確認してください。
2) **display this** コマンドを IGMP snooping view または対応するポートの interface view で使用して、マルチキャストグループポリシーが正しく適用されているかどうかを確認してください。適用されていない場合、**group-policy** または **igmp-snooping group-policy** コマンドでマルチキャストグループポリシーを正しく適用してください。
3) **display igmp-snooping** コマンドを使用して、未知のマルチキャストデータ廃棄機能が有効になっているかどうか確認してください。有効になっていない場合、**igmp-snooping drop-unknown** コマンドを使用して未知のマルチキャストデータ廃棄機能を有効にしてください。
4) 問題が解決しない場合、NEC に問い合わせてください。

目次

このセクションのページは **6-x-x** です。

3 章 マルチキャスト VLAN 3-1
3.1 概要 3-1
3.2 マルチキャスト VLAN 設定作業リスト 3-3
3.3 サブ VLAN ベースマルチキャスト VLAN の設定 3-3
3.3.1 設定要件 3-4
3.3.2 設定の制限とガイドライン 3-4
3.3.3 設定手順 3-4
3.4 ポートベースマルチキャスト VLAN の設定 3-4
3.4.1 設定要件 3-4
3.4.2 ユーザポートの属性の設定 3-5
3.4.3 マルチキャスト VLAN のユーザポートの割り当て 3-5
3.5 マルチキャスト VLAN の転送エントリの最大数の設定 3-6
3.6 マルチキャスト VLAN の表示と維持 3-6
3.7 マルチキャスト VLAN 設定例 3-7
3.7.1 サブ VLAN ベースマルチキャスト VLAN の設定例 3-7
3.7.2 ポートベースマルチキャスト VLAN の設定例 3-10

3章 マルチキャスト VLAN

3.1 概要

図 3-1に示すとおり、3つの VLAN のホスト A、ホスト B、ホスト C は同じマルチキャストグループに所属しています。レイヤ 3 装置（Switch A）がグループのマルチキャストデータを受信するとき、レイヤ 2 装置（Switch B）のユーザ VLAN 毎にマルチキャストトラフィックをコピーします。この結果、ネットワークの帯域を浪費するだけでなく、レイヤ 3 装置にも負荷をかけてしまいます。

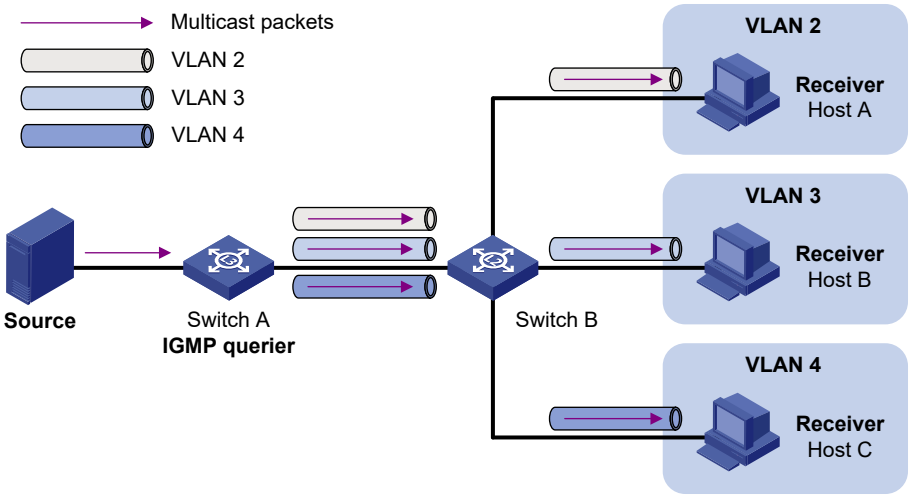


図 3-1 マルチキャスト VLAN を使用しないマルチキャストの転送

Switch B でマルチキャスト VLAN を設定した後、Switch A は Switch B のマルチキャスト VLAN にマルチキャストデータを 1 つのコピーのみを送信します。この方法はネットワークの帯域を節約し、レイヤ 3 装置の負荷を軽減します。

マルチキャスト VLAN はサブ VLAN ベースマルチキャストとポートベースマルチキャスト VLAN があります。

I. サブ VLAN ベースマルチキャスト VLAN

図 3-2にサブ VLAN ベースマルチキャスト VLAN を示します。

- ホスト A、ホスト B、ホスト Cはそれぞれ VLAN 2、VLAN 3、VLAN 4 に属します。
- Switch B において、VLAN10 をマルチキャスト VLAN に設定します。
- VLAN 2、VLAN 3、VLAN 4 は VLAN 10 のサブ VLAN です。
- マルチキャスト VLAN とマルチキャスト VLAN のサブ VLAN 上で IGMP Snooping を有効にします。

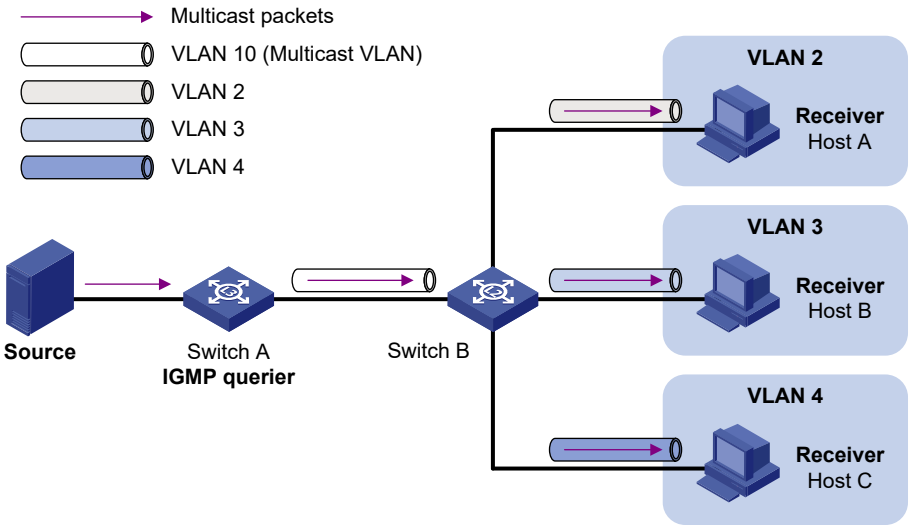


図 3-2 サブ VLAN ベースマルチキャスト VLAN

設定後、IGMP Snooping はマルチキャスト VLAN のルータポートとサブ VLAN のメンバポートを管理します。Switch A がマルチキャストソースからマルチキャストデータを受信するとき、Switch B のマルチキャスト VLAN に 1 つのマルチキャストデータのみを送信します。そして、Switch B はマルチキャスト VLAN のサブ VLAN へ分けられたコピーを送信します。

II. ポートベースマルチキャスト VLAN

図 3-3にポートベースベースマルチキャスト VLAN を示します。

- ホスト A、ホスト B、ホスト C はそれぞれ VLAN 2、VLAN 3、VLAN 4 に属します。
- Switch B において、VLAN10 はマルチキャスト VLAN です。すべてのユーザポートはハイブリッドポートで VLAN 10 に割り当てられています。
- マルチキャスト VLAN とすべてのユーザ VLAN 上で IGMP Snooping を有効します。

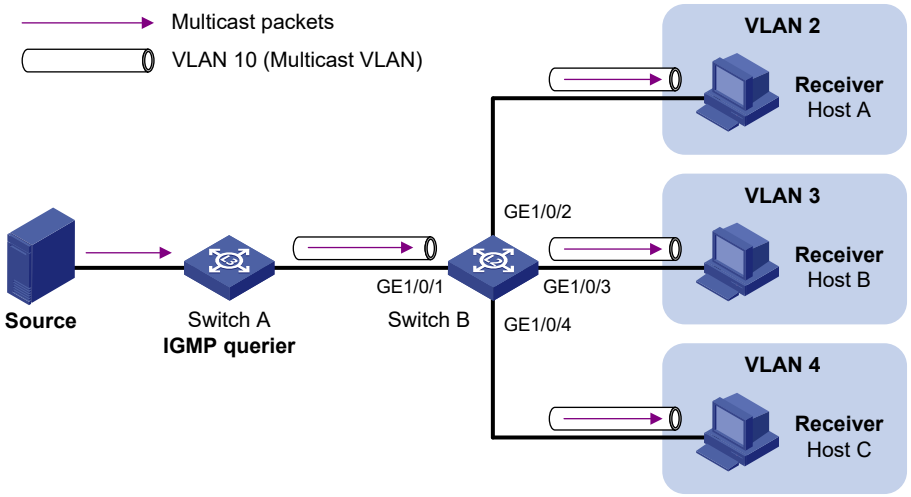


図 3-3 ポートベースベースマルチキャスト VLAN

IGMP Snooping はマルチキャスト VLAN のルータポートとメンバポートを管理します。Switch B がユーザポートで IGMP メッセージを受信すると、メッセージにマルチキャスト VLAN のタグをつけて IGMP クエリアへ送信します。Switch B でマルチキャストデータの 1 つコピーのみをマルチキャスト VLAN に送信します。そして、Switch B はマルチキャスト VLAN の各ユーザポートに分けられたコピーを送信します。

3.2 マルチキャストVLAN設定作業リスト

作業リスト
(必須設定項目)以下の作業の1つを実行します。 • サブVLANベースマルチキャストVLANの設定 • ポートベースマルチキャストVLANの設定 　• ユーザポートの属性の設定 　• マルチキャストVLANのユーザポートの割り当て
(オプション設定項目) マルチキャストVLAN転送エントリの最大数の設定

サブ VLAN ベースマルチキャスト VLAN とポートベースマルチキャスト VLAN の両方をデバイスに設定する場合、ポートベースマルチキャスト VLAN が優先されます。

3.3 サブVLANベースマルチキャストVLANの設定

サブ VLAN ベースマルチキャスト VLAN を設定するため、マルチキャスト VLAN として VLAN を設定し、マルチキャスト VLAN に受信ホストが含まれるようにサブ VLAN を設定する必要があります。

3.3.1 設定要件

サブ VLAN ベースマルチキャスト VLAN の設定をする前に、以下の作業を完了させてください。

- 必要な VLAN を作成します。
- マルチキャスト VLAN に設定する VLAN とサブ VLAN で IGMP Snooping を有効にします。

3.3.2 設定の制限とガイドライン

サブ VLAN ベースマルチキャスト VLAN の設定を行うとき、以下の設定の制限とガイドラインに従ってください。

- マルチキャスト VLAN に指定される VLAN が事前に作成されている必要があります。
- マルチキャスト VLAN のサブ VLAN に指定される VLAN は事前に作成されている必要があります。他のマルチキャスト VLAN のサブ VLAN であってはいけません。
- 装置のマルチキャスト VLAN の総数は、装置がサポートする最大数を超えてはいけません。
- マルチキャスト VLAN とマルチキャスト VLAN のサブ VLAN の両方でトランクポートがないことを確認してください。

3.3.3 設定手順

以下にサブ VLAN ベースマルチキャスト VLAN を設定する方法を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. 指定した VLAN をマルチキャスト VLAN に設定し、multicast VLAN view へ移行する	**multicast-vlan** *vlan-id*	デフォルト：設定なし
3. ポートをマルチキャスト VLAN に割り当てる	**subvlan** *vlan-list*	デフォルト：設定なし

3.4 ポートベースマルチキャストVLANの設定

マルチキャスト VLAN の設定は、イーサネットポートあるいはレイヤ 2 アグリゲートインタフェースにのみ、割り当てることができます。

3.4.1 設定要件

ポートベースマルチキャスト VLAN を設定するため、以下の作業を完了させてください。

- 必要な VLAN を作成します。
- マルチキャスト VLAN に設定する VLAN で IGMP snooping を有効にします。

- 受信ホストを含むすべての VLAN で IGMP Snooping を有効にします。

3.4.2 ユーザポートの属性の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. interface view に移行する	**interface** *interface-type interface-number*	ー
3. ポートリンクタイプをハイブリッドに設定する	**port link-type hybrid**	デフォルト：アクセス 詳細はコマンドマニュアルのセクション3 *アクセス" VLAN"* を参照してください。
4. ユーザポートが属している VLAN に現在のユーザポートの PVID を指定する	**port hybrid pvid vlan** *vlan-id*	デフォルト：ハイブリッドポートのPVIDはVLAN 1です。 詳細はコマンドマニュアルのセクション3 *アクセス" VLAN"* を参照してください。
5. 指定した VLAN のパケットの通過を許可し、出力の際に untag パケットにする	**port hybrid vlan** *vlan-id-list* **untagged**	デフォルト：VLAN1のみ許可 詳細はコマンドマニュアルのセクション3 *アクセス" VLAN"* を参照してください。

3.4.3 マルチキャスト VLAN のユーザポートの割り当て

ユーザポートをマルチキャスト VLAN に割り当てる場合、multicast VLAN view で設定する方法と、interface view で設定する方法のどちらかで行うことができます。どちらの設定の優先度は同一です。

I. 設定の制限とガイドライン

マルチキャスト VLAN ポートの設定を行うとき、以下の設定の制限とガイドラインに従ってください。

- マルチキャスト VLAN に指定される VLAN が事前に作成されている必要があります。
- ポートは 1 つのマルチキャスト VLAN にのみ属することができます。

II. 設定手順

以下に multicast VLAN view でマルチキャスト VLAN にポートを割り当てる設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. VLAN をマルチキャスト VLAN に設定し、multicast VLAN view へ移行する	**multicast-vlan** *vlan-id*	デフォルト：設定なし

操作	コマンド	補足
3. ポートをマルチキャスト VLAN に割り当てる	**port** *interface-list*	デフォルト：マルチキャスト VLANはユーザポートを持っていません。

以下に interface view でマルチキャスト VLAN にポートを割り当てる設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. VLAN をマルチキャスト VLAN に設定し、multicast VLAN view へ移行する	**multicast-vlan** *vlan-id*	デフォルト：設定なし
3. system view に戻る	**quit**	―
4. interface view に移行する	**interface** *interface-type interface-number*	―
5. 現在のポートをマルチキャスト VLAN ポートに設定する	**port multicast-vlan** *vlan-id*	デフォルト：マルチキャスト VLANには属していません。

3.5 マルチキャストVLANの転送エントリの最大数の設定

装置でマルチキャスト VLAN の IGMP Snooping 転送テーブルのエントリの最大数を設定できます。マルチキャスト VLAN の転送エントリ数がしきい値に達すると、いくつかのエントリがタイムアウトするか、手動で削除するまで、装置は転送エントリを作成しません。

設定時に、マルチキャスト VLAN の IGMP Snooping 転送テーブルの既存のエントリ数が上限より大きかった場合、システムは自動で既存のエントリを削除したり、新しいエントリを作成したりしません。手動でエントリを削除することを推奨します。

以下にマルチキャスト VLAN の転送エントリの最大数を設定する方法を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. マルチキャスト VLAN の転送エントリの最大数を設定する	**multicast-vlan entry-limit** *limit*	デフォルト：2000

3.6 マルチキャストVLANの表示と維持

すべての view で **display** コマンドを実行し、user view で **reset** コマンドを実行できます。

操作	コマンド
マルチキャストVLANの情報を表示する	**display multicast-vlan** [*vlan-id*]
マルチキャストVLANのマルチキャストグループの情報を表示する	**display multicast-vlan group** [*source-address* | *group-address* | **slot** *slot-number* | **verbose** | **vlan** *vlan-id*] *
マルチキャスト転送テーブルの情報を表示する	**display multicast-vlan forwarding-table** [*group-address* [**mask** { *mask-length* | *mask* }] | *source-address* [**mask** { *mask-length* | *mask* }] | **slot** *slot-number* | **subvlan** *vlan-id* | **vlan** *vlan-id*] *

操作	コマンド
マルチキャストVLANのマルチキャストグループを削除する	**reset multicast-vlan group** [*source-address* [**mask** { *mask-length* | *mask* }] | *group-address* [**mask** { *mask-length* | *mask* }] | **vlan** *vlan-id*] *

3.7 マルチキャストVLAN設定例

3.7.1 サブ VLAN ベースマルチキャスト VLAN の設定例

I. ネットワーク要件

図 3-4に示すように設定します。

- レイヤ 3 装置の Switch A で IGMPv2 が動作します。Switch A は IGMP クエリアです。レイヤ 2 装置の Switch B で IGMPv2 Snooping が動作します。
- マルチキャストソースはマルチキャストデータをマルチキャストグループ 224.1.1.1 へ送信します。ホスト A、ホスト B、ホスト C はマルチキャストグループのレシーバです。ホストはそれぞれ VLAN 2 から VLAN 4 に属しています。

Switch B でサブ VLAN ベースマルチキャスト VLAN を以下の要件に適用するように設定します。

- Switch A がマルチキャスト VLAN を通じてマルチキャストデータを Switch B へ送信します。
- Switch B が異なるユーザ VLAN に属するレシーバへマルチキャストデータを転送します。

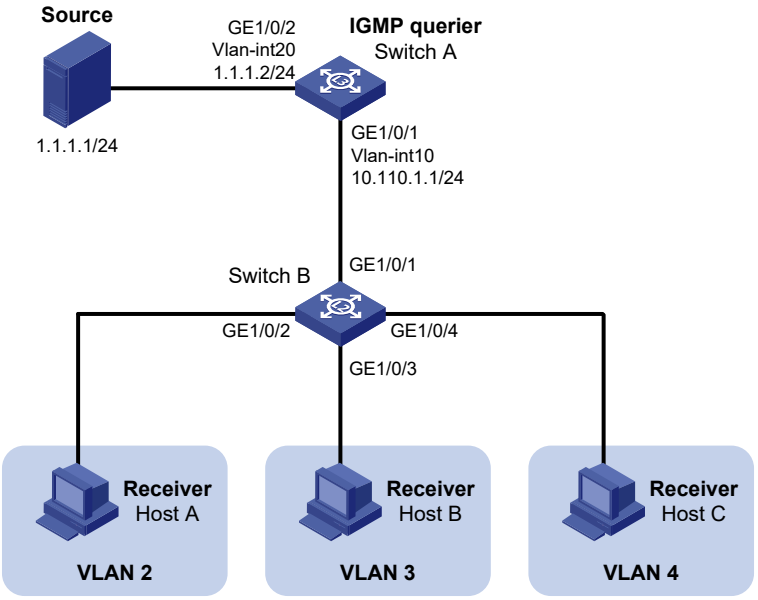


図 3-4 ネットワーク図

II. 設定手順

1)　Switch A の設定

IP マルチキャストルーティングを有効にします。

```
<SwitchA> system-view
[SwitchA] multicast routing
[SwitchA-mrib] quit
```

VLAN 20 を作成し、GigabitEthernet 1/0/2 を VLAN に割り当てます。

```
[SwitchA] vlan 20
[SwitchA-vlan20] port gigabitethernet 1/0/2
[SwitchA-vlan20] quit
```

VLAN インタフェース 20 に IP アドレスを設定し、PIM-SM を有効にします。

```
[SwitchA] interface vlan-interface 20
[SwitchA-Vlan-interface20] ip address 1.1.1.2 24
[SwitchA-Vlan-interface20] pim sm
[SwitchA-Vlan-interface20] quit
```

VLAN 10 を作成します。

```
[SwitchA] vlan 10
[SwitchA-vlan10] quit
```

ハイブリッドポートとして GigabitEthernet 1/0/1 を設定し、VLAN 10 からのパケットにタグをつけます。

```
[SwitchA] interface gigabitethernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] port link-type hybrid
[SwitchA-GigabitEthernet1/0/1] port hybrid vlan 10 tagged
[SwitchA-GigabitEthernet1/0/1] quit
```

VLAN インタフェース 10 に IP アドレスを設定し、IGMP を有効にします。

```
[SwitchA] interface vlan-interface 10
[SwitchA-Vlan-interface10] ip address 10.110.1.1 24
[SwitchA-Vlan-interface10] igmp enable
[SwitchA-Vlan-interface10] quit
```

2)　Switch B の設定

IGMP Snooping を有効にします。

```
<SwitchB> system-view
[SwitchB] igmp-snooping
[SwitchB-igmp-snooping] quit
```

VLAN 2 を作成し、GigabitEthernet 1/0/2 を VLAN に割り当て、IGMP Snooping を有効にします。

```
[SwitchB] vlan 2
[SwitchB-vlan2] port gigabitethernet 1/0/2
[SwitchB-vlan2] igmp-snooping enable
[SwitchB-vlan2] quit
```

VLAN 3 を作成し、GigabitEthernet 1/0/3 を VLAN に割り当て、IGMP Snooping を有効にします。

```
[SwitchB] vlan 3
[SwitchB-vlan3] port gigabitethernet 1/0/3
[SwitchB-vlan3] igmp-snooping enable
[SwitchB-vlan3] quit
```

VLAN 4 を作成し、GigabitEthernet11/0/4 を VLAN に割り当て、IGMP Snooping を有効にします。

```
[SwitchB] vlan 4
[SwitchB-vlan4] port gigabitethernet 1/0/4
[SwitchB-vlan4] igmp-snooping enable
[SwitchB-vlan4] quit
```

VLAN10 を作成し、IGMP Snooping を有効にします。

```
[SwitchB] vlan 10
[SwitchB-vlan10] igmp-snooping enable
[SwitchB-vlan10] quit
```

#ハイブリッドポートとして GigabitEthernet 1/0/1 を設定し、VLAN 10 からのパケットにタグをつけます。

```
[SwitchB] interface gigabitethernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] port link-type hybrid
[SwitchB-GigabitEthernet1/0/1] port hybrid vlan 10 tagged
[SwitchB-GigabitEthernet1/0/1] quit
```

マルチキャスト VLAN として VLAN 10 を設定し、サブ VLAN として VLAN 2～VLAN 4 を設定します。

```
[SwitchB] multicast-vlan 10
[SwitchB-mvlan-10] subvlan 2 to 4
[SwitchB-mvlan-10] quit
```

III. 設定の確認

Switch B ですべてのマルチキャスト VLAN の情報を表示します。

```
[SwitchB] display multicast-vlan
Total 1 multicast VLANs.

Multicast VLAN 10:
  Sub-VLAN list(3 in total):
     2-4
  Port list(0 in total):
```

Switch B でマルチキャスト VLAN のマルチキャストグループの情報を表示します。

```
[SwitchB] display multicast-vlan group
Total 1 entries.

Multicast VLAN 10: Total 1 entries.
  (0.0.0.0, 224.1.1.1)
    Sub-VLANs (3 in total):
      VLAN 2
      VLAN 3
      VLAN 4
```

出力では次のことを示します。マルチキャストグループ 224.1.1.1 がマルチキャスト VLAN 10 に属しています。マルチキャスト VLAN 10 はサブ VLAN 2～サブ VLAN 4 があります。Switch B は VLAN 10 のマルチキャストデータを VLAN 2～VLAN 4 にコピーしています。

3.7.2 ポートベースマルチキャスト VLAN の設定例

I. ネットワーク要件

図 3-5に示すように設定します。

- Switch A で IGMPv2 が動作します。Switch A は IGMP クエリアです。Switch B で IGMPv2 Snooping が動作します。
- マルチキャストソースはマルチキャストデータをマルチキャストグループ 224.1.1.1 に送信します。ホスト A、ホスト B、ホスト C はマルチキャストグループのレシーバです。ホストはそれぞれ VLAN2 から VLAN4 に属しています。

Switch B でポートベースマルチキャスト VLAN を以下の要件に適用するように設定します。

- Switch A はマルチキャスト VLAN を通じてマルチキャストデータを Switch B へ送信します。
- Switch B が異なるユーザ VLAN に属するレシーバへマルチキャストデータを転送します。

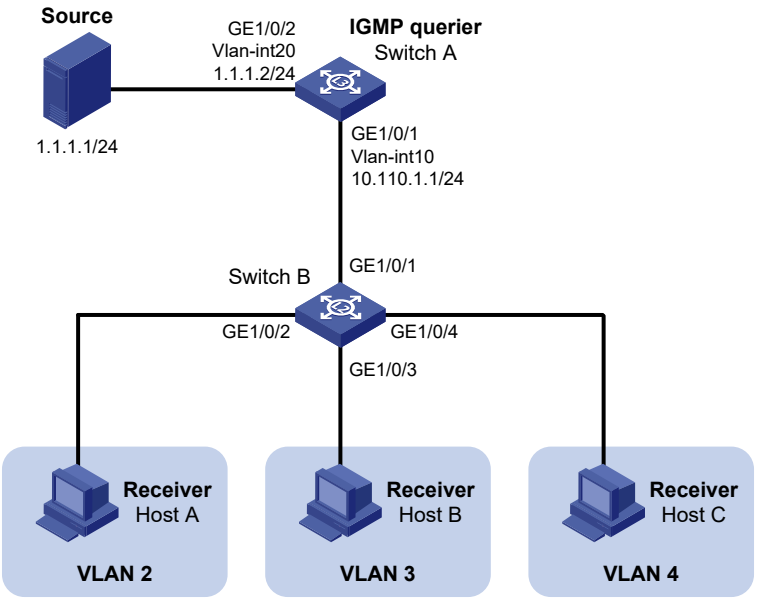


図 3-5 ネットワーク図

II. 設定例

1)　Switch A の設定

IP マルチキャストルーティングを有効にします。

```
<SwitchA> system-view
[SwitchA] multicast routing
[SwitchA-mrib] quit
```

VLAN 20 を作成し、GigabitEthernet 1/0/2 を VLAN に割り当てます。

```
[SwitchA] vlan 20
[SwitchA-vlan20] port gigabitethernet 1/0/2
[SwitchA-vlan20] quit
```

VLAN インタフェース 20 に IP アドレスを設定し、PIM-SM を有効にします。

```
[SwitchA] interface vlan-interface 20
[SwitchA-Vlan-interface20] ip address 1.1.1.2 24
[SwitchA-Vlan-interface20] pim sm
[SwitchA-Vlan-interface20] quit
```

VLAN 10 を作成し、GigabitEthernet 1/0/1 を割り当てます。

```
[SwitchA] vlan 10
[SwitchA-vlan10] port gigabitethernet 1/0/1
[SwitchA-vlan10] quit
```

VLAN インタフェース 10 に IP アドレスを設定し、インタフェースで IGMP を有効にします。

```
[SwitchA] interface vlan-interface 10
[SwitchA-Vlan-interface10] ip address 10.110.1.1 24
[SwitchA-Vlan-interface10] igmp enable
[SwitchA-Vlan-interface10] quit
```

2)　Switch B の設定

グローバルに IGMP Snooping を有効にします。

```
<SwitchB> system-view
[SwitchB] igmp-snooping
[SwitchB-igmp-snooping] quit
```

VLAN 10 を作成し、GigabitEthernet 1/0/1 を VLAN に割り当て、IGMP Snooping を有効にします。

```
[SwitchB] vlan 10
[SwitchB-vlan10] port gigabitethernet 1/0/1
[SwitchB-vlan10] igmp-snooping enable
[SwitchB-vlan10] quit
```

VLAN 2 を作成し、IGMP Snooping を有効にします。

```
[SwitchB] vlan 2
[SwitchB-vlan2] igmp-snooping enable
[SwitchB-vlan2] quit
```

VLAN 3 を作成し、IGMP Snooping を有効にします。

```
[SwitchB] vlan 3
[SwitchB-vlan3] igmp-snooping enable
[SwitchB-vlan3] quit
```

VLAN 4 を作成し、IGMP Snooping を有効にします。

```
[SwitchB] vlan 4
[SwitchB-vlan4] igmp-snooping enable
[SwitchB-vlan4] quit
```

#ハイブリッドポートとして GigabitEthernet 1/0/2 を設定し、ハイブリッドポートの PVID を 2 に設定します。

```
[SwitchB] interface gigabitethernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] port link-type hybrid
[SwitchB-GigabitEthernet1/0/2] port hybrid pvid vlan 2
```

VLAN 2、VLAN 10 に GigabitEthernet 1/0/2 を割り当て、VLAN 2、VLAN 10 からのパケットからタグを外します。

```
[SwitchB-GigabitEthernet1/0/2] port hybrid vlan 2 untagged
[SwitchB-GigabitEthernet1/0/2] port hybrid vlan 10 untagged
[SwitchB-GigabitEthernet1/0/2] quit
```

ハイブリッドポートとして GigabitEthernet 1/0/3 を設定し、ハイブリッドポートの PVID を 3 に設定します。

```
[SwitchB] interface gigabitethernet 1/0/3
[SwitchB-GigabitEthernet1/0/3] port link-type hybrid
[SwitchB-GigabitEthernet1/0/3] port hybrid pvid vlan 3
```

VLAN 3、VLAN 10 に GigabitEthernet 1/0/3 を割り当て、VLAN 3、VLAN 10 からのパケットからタグを外します。

```
[SwitchB-GigabitEthernet1/0/3] port hybrid vlan 3 untagged
[SwitchB-GigabitEthernet1/0/3] port hybrid vlan 10 untagged
[SwitchB-GigabitEthernet1/0/3] quit
```

ハイブリッドポートとして GigabitEthernet 1/0/4 を設定し、ハイブリッドポートの PVID を 4 に設定します。

```
[SwitchB] interface gigabitethernet 1/0/4
[SwitchB-GigabitEthernet1/0/4] port link-type hybrid
[SwitchB-GigabitEthernet1/0/4] port hybrid pvid vlan 4
```

VLAN 4、VLAN 10 に GigabitEthernet 1/0/4 を割り当て、VLAN 4、VLAN 10 からのパケットからタグを外します。

```
[SwitchB-GigabitEthernet1/0/4] port hybrid vlan 4 untagged
[SwitchB-GigabitEthernet1/0/4] port hybrid vlan 10 untagged
[SwitchB-GigabitEthernet1/0/4] quit
```

マルチキャスト VLAN として VLAN 10 を設定します。

```
[SwitchB] multicast-vlan 10
```

GigabitEthernet 1/0/2 と GigabitEthernet 1/0/3 に VLAN10 を割り当てます。

```
[SwitchB-mvlan-10] port gigabitethernet 1/0/2 to gigabitethernet 1/0/3
[SwitchB-mvlan-10] quit
```

GigabitEthernet 1/0/4 に VLAN10 を割り当てます。

```
[SwitchB] interface gigabitethernet 1/0/4
[SwitchB-GigabitEthernet1/0/4] port multicast-vlan 10
[SwitchB-GigabitEthernet1/0/4] quit
```

III. 設定の確認

Switch B のマルチキャスト VLAN の情報を表示します。

```
[SwitchB] display multicast-vlan
Total 1 multicast VLANs.

Multicast VLAN 10:
  Sub-VLAN list(0 in total):
  Port list(0 in total):
    GE1/0/2
    GE1/0/3
    GE1/0/4
```

Switch B でダイナミックマルチキャストグループの IGMP Snooping 転送エントリを表示します。

```
[SwitchB] display igmp-snooping group
Total 1 entries.

VLAN 10: Total 1 entries.
  (0.0.0.0, 224.1.1.1)
    Host slots (0 in total):
    Host ports (3 in total):
      GE1/0/2         (00:03:23)
      GE1/0/3         (00:04:07)
      GE1/0/4         (00:04:16)
```

出力では、IGMP Snooping が VLAN10 のユーザポートを維持していることを示します。Switch B はユーザポートを通して VLAN 10 のマルチキャストデータを転送します。

目次

このセクションのページは**6-x-x** です。

4章 MLDスヌーピング 4-1
4.1 概要 4-1
4.1.1 MLD snoopingのポート 4-1
4.1.2 MLD snoopingの動作 4-3
4.1.3 MLD snoopingプロキシー機能 4-5
4.2 プロトコルと標準 4-6
4.3 MLD snooping設定作業リスト 4-6
4.4 MLD snoopingの基本機能の設定 4-7
4.4.1 MLD snoopingの有効化 4-7
4.4.2 MLD snoopingのバージョンの設定 4-8
4.4.3 MLD snooping転送エントリの最大数の設定 4-9
4.4.4 MLD last listener クエリ間隔の設定 4-9
4.5 MLD snoopingのポート機能の設定 4-10
4.5.1 ダイナミックポートのエージングタイマの設定 4-10
4.5.2 スタティックポートの設定 4-11
4.5.3 シミュレーティッドメンバホストのポート設定 4-12
4.5.4 fast-leave処理の有効化 4-12
4.6 MLD snoopingクエリアの設定 4-13
4.6.1 設定要件 4-13
4.6.2 MLD snoopingクエリアの有効化 4-13
4.6.3 MLD general クエリとresponseのパラメータの設定 4-14
4.7 MLDメッセージのパラメータの設定 4-15
4.7.1 設定要件 4-15
4.7.2 MLDメッセージの送信元IPv6アドレスの設定 4-15
4.7.3 MLDメッセージの802.1p優先度の設定 4-17
4.8 MLD snoopingポリシーの設定 4-17
4.8.1 IPv6マルチキャストグループポリシーの設定 4-17
4.8.2 IPv6マルチキャストソースポートフィルタの有効化 4-18
4.8.3 未知のIPv6マルチキャストデータ廃棄機能の有効化 4-19
4.8.4 MLD report抑制機能の有効化 4-19
4.8.5 ポートのIPv6マルチキャストグループの最大数の設定 4-20
4.8.6 IPv6マルチキャストグループ置き換え機能の有効化 4-20
4.9 送信MLDプロトコルパケットのDSCP値の設定 4-21
4.10 MLD snoopingの表示と維持 4-22
4.11 MLD snooping設定例 4-22
4.11.1 IPv6グループポリシーとシミュレーティッドメンバホスト設定例 4-22
4.11.2 スタティックポート設定例 4-25
4.11.3 MLD snoopingクエリア設定例 4-29
4.12 MLD snoopingのトラブルシューティング 4-31
4.12.1 レイヤ2マルチキャスト転送ができない 4-31
4.12.2 IPv6マルチキャストグループポリシーが動作しない 4-32

4章 MLD スヌーピング

4.1 概要

MLD snooping は IPv6 マルチキャスト転送時のネットワークへの負荷を軽減するためのメカニズムです。

図 4-1に示すように MLD snooping を有効にしない場合、IPv6 マルチキャストパケットはすべてのホストにフラッディングされます。MLD snooping を有効にする場合、装置は既知の IPv6 マルチキャストグループからのマルチキャストパケットを Receiver のみに転送します。MLD snooping を有効にすることで、不要なマルチキャストトラフィックのフラッディングを抑止し、ネットワークを効率的に利用することができます。

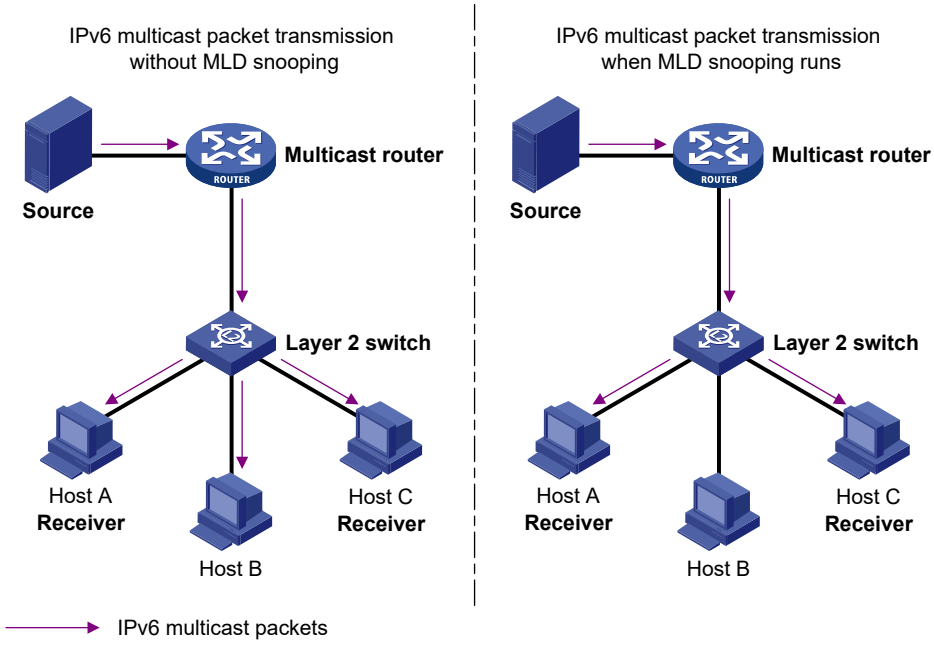


図 4-1 MLD snooping が無効な場合と有効にした場合のマルチキャストパケットの転送処理

4.1.1 MLD snooping のポート

図 4-2に示すように、MLD snooping は Switch A と Switch B で動作します。Host A と Host C は IPv6 マルチキャストグループ内のレシーバホストです。MLD snooping のポートはメンバポートとルータポートに分類されます。

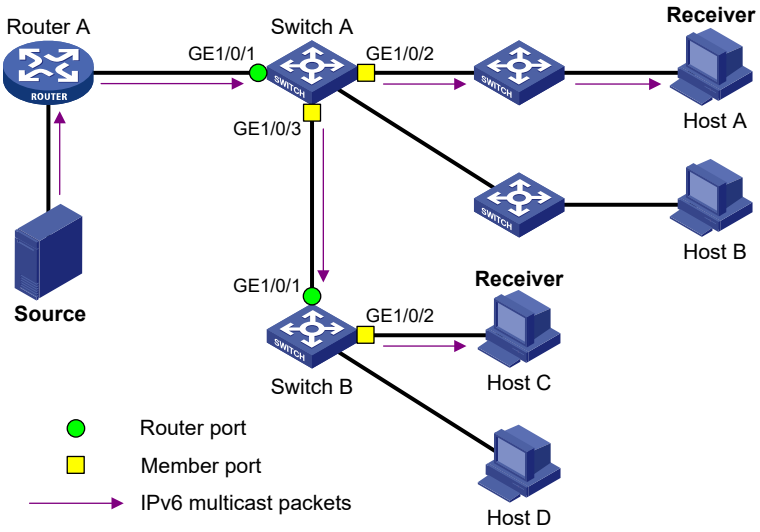


図 4-2 MLD snooping 関連ポート

I. ルータポート

MLD snooping のレイヤ 2 装置で、レイヤ 3 マルチキャストへのポートはルータポートと呼ばれます。図 4-2では、Switch A の GigabitEthernet 1/0/1 と Switch B の GigabitEthernet 1/0/1 がルータポートです。

ルータポートは以下のタイプがあります。

- **ダイナミックルータポート**－ポートで 0::0 以外の送信元アドレスの MLD general クエリを受信する、あるいは IPv6 PIM Hello メッセージを受信した場合、ダイナミックルータポートリストにポートを追加します。同時にポートのタイマを開始します。タイマが満了する前にメッセージを受信しない場合、ポートはダイナミックルータポートリストからポートを削除します。
- **スタティックルータポート**－ポートがルータポートとしてスタティックに設定された場合、スタティックルータポートリストにポートを追加します。スタティックルータポートはエージアウトしません。手動でのみ削除することができます。

MLD snooping のルータポートをレイヤ 3 インタフェースのルーテッドインタフェースと混同しないでください。MLD snooping のルータポートはレイヤ 2 インタフェースです。

II. メンバポート

MLD snooping のレイヤ 2 装置で、マルチキャストレシーバへのポートはメンバポートと呼ばれます。図 4-2では、Switch A の GigabitEthernet 1/0/2 と GigabitEthernet 1/0/3、Switch B の GigabitEthernet 1/0/2 がメンバポートです。

メンバポートは以下のタイプがあります。

- **ダイナミックメンバポート**－ポートが MLD report をした場合、出力インタフェースとして関連づけられたダイナミック MLD snooping 転送エントリに追加されます。同時にポートのタイマを開始します。タイマが満了する前にメッセージを受信しない場合、ポートはダイナミック転送エントリからからポートを削除します。

- **スタティックメンバポート**－ポートがメンバポートとしてスタティックに設定された場合、出力インタフェースとして関連づけられたスタティック MLD snooping 転送エントリに追加されます。スタティックメンバポートはエージアウトしません。手動でのみ削除することができます。

特に指定しない限り、この章でのルータポートとメンバポートは、スタティックルータポート、ダイナミックルータポートと、スタティックメンバポート、ダイナミックメンバポートを含みます。

4.1.2 MLD snooping の動作

この章のポートはダイナミックポートです。スタティックポートの設定、削除方法については、オペレーションマニュアルのセクション 6 *マルチキャスト*”*MLD スヌーピング*”の”*スタティックポートの設定*”を参照してください。

MLD メッセージのタイプは、general クエリ、MLD report、done メッセージを含みます。MLD snooping が有効なレイヤ 2 装置は、受信した MLD メッセージによってそれぞれ異なる動作をします。

I. General クエリ

MLD クエリアは、IPv6 マルチキャストグループメンバが存在するかどうかを調べるために、ローカルサブネット上のすべてのホストとルータへ MLD general クエリを定期的に送信します。

MLD general クエリを受信すると、装置は受信したポート以外の VLAN 内のすべてのポートへクエリメッセージを転送します。装置は以下のアクションの 1 つを実行します。

- 受信ポートがルータポートリストに存在するルータポートの場合、装置はこのルータポートのエージングタイマを再起動します。
- 受信ポートがルータポートリストに存在しない場合、装置はその受信ポートをルータポートリストに追加し、このルータポートのエージングタイマを開始します。

II. MLD report

ホストは以下の目的により MLD report を MLD クエリアへ送信します。

- ホストが IPv6 マルチキャストグループメンバである場合、クエリに応答します。
- IPv6 マルチキャスト membership を適用します。

ホストから MLD report を受信すると、装置は VLAN 内のすべてのルータポートから report を転送します。報告された IPv6 マルチキャストグループの IPv6 アドレスを解決します。エントリに一致するかどうか転送テーブルを検索します。

- 転送テーブルエントリが存在しない場合、装置は、グループ用に出力インタフェースが受信したポートの転送エントリを追加します。受信したポートはダイナミックメンバポートとして設定し、ポートのエージングタイマを起動します。
- 報告されたグループの転送テーブルエントリは存在するが、そのグループの発信ポートリストにポートが含まれていない場合、装置はポートをダイナミックメンバポートとして転送エントリに追加し、そのポートのメンバポートエージングタイマを起動します。

- 報告されたグループの転送テーブルエントリが存在し、転送エントリに受信ポートが含まれている、つまりこの受信ポートが既にメンバポートである場合、装置はそのポートのメンバポートエージングタイマを再起動します。

MLD snooping が有効な装置で IPv6 マルチキャストグループポリシーの設定がある状況で、ユーザが IPv6 マルチキャストプログラムをリクエストしたとき、ユーザのホストは MLD report を初期化します。このレポートを受信した後、装置はレポートの IPv6 マルチキャストグループアドレスを解決し、ポートの ACL フィルタリングを実行します。MLD report が ACL フィルタリングにパスした場合、装置は出力インタフェースが受信ポートの IPv6 マルチキャストグループの MLD snooping 転送エントリを作成します。MLD report が ACL フィルタリングにパスしない場合、装置は MLD report メッセージを廃棄します。レシーバが IPv6 マルチキャストグループに加入できず、ユーザはグループアドレス解決を行うことができません。

装置は、MLD report 抑制メカニズムによって MLD report を非ルータポートから転送することはありません。

III. Done メッセージ

ホストが IPv6 マルチキャストグループを離脱する場合、ホストは IPv6 マルチキャストルータに MLD done メッセージを送信します。装置がダイナミックメンバポートで MLD done メッセージを受信したとき、装置は最初にメッセージの IPv6 マルチキャストグループアドレスに一致する転送エントリが存在するかどうかを確認します。

- 転送テーブルエントリが存在しない場合、装置は MLD done メッセージを廃棄します。
- 転送テーブルエントリにマッチするが、受信ポートが転送エントリに含まれていない場合、装置は MLD done メッセージを廃棄します。
- 転送テーブルエントリが存在し、受信ポートが転送エントリの出力インタフェースのみでない場合、以下の処理を行います。
  - MLD done メッセージを廃棄します。
  - グループに受信ポートに接続されたアクティブなレシーバがあるかどうかを確認するため、MLD multicast-address-specific クエリを送信します
  - 受信ポートのエージングタイマを MLD last member クエリ間隔の 2 倍に設定します。
- 転送テーブルエントリが存在し、受信ポートが転送エントリの出力インタフェースのみである場合、以下の処理を行います。
  - VLAN のすべてのルータポートに MLD done メッセージを転送します。
  - グループに受信ポートに接続されたアクティブなレシーバがあるかどうかを確認するため、MLD multicast-address-specific クエリを送信します。
  - 受信ポートのエージングタイマを MLD last member クエリ間隔の 2 倍に設定します。

ホストから MLD done メッセージを受信したのち、MLD クエリアはメッセージから IPv6 マルチキャストグループのアドレスを解決します。そして MLD done メッセージを受信したポートから IPv6 マルチキャストグループに MLD multicast-address-specific クエリを送信します。

MLD multicast-address-specific クエリを受信したのち、装置は VLAN のすべてのルータポートと IPv6 マルチキャストグループのすべてのメンバポートにクエリを転送します。直接接続されているホストから MLD report の応答を待ちます。done メッセージを受信したダイナミックメンバポートは以下のアクションの 1 つを実行します。

- メンバポートのエージングタイマが満了する前にポートが MLD クエリを受信した場合、装置はポートのエージングタイマをリセットします。
- エージングタイマが満了しても MLD report を受信しない場合、装置は IPv6 マルチキャストグループの転送エントリからポートを削除します。

4.1.3 MLD snooping プロキシー機能

図 4-3に示すように、上流装置で受信される MLD report メッセージ、MLD done メッセージの数を削減する場合、エッジ装置で MLD snooping プロキシー機能を有効にします。MLD snooping プロキシー機能を有効にした場合、MLD report メッセージ、MLD done メッセージを Router A に送信するため、上流の MLD snooping クエリアのエッジ装置はホストとして動作します。エッジ装置でホスト MLD report の抑制メカニズムは適用しません。

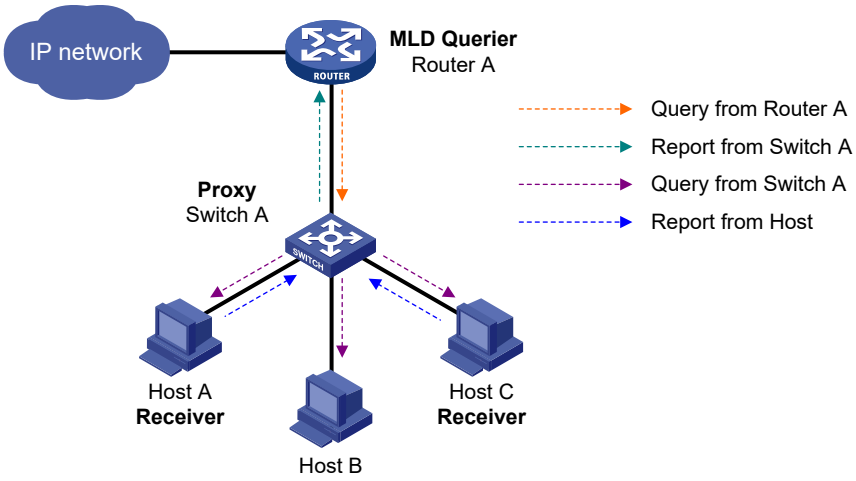


図 4-3 MLD snooping プロキシー機能

MLD snooping プロキシー機能が有効な装置は異なる MLD メッセージを処理します。

- General クエリ

MLD general クエリを受信したのち、装置は受信ポートを除く VLAN のすべてのポートにクエリを転送します。装置はローカルメンバシップ情報をもとにして MLD report を作成し、すべてのルータポートに送信します。

- Group-specific クエリあるいは group-and-source-specific クエリ

MLD group-specific クエリ あるいは MLD group-and-source-specific クエリを受信したのち、装置は受信ポートを除く VLAN のすべてのポートにクエリを転送します。転送エントリにメンバポートがある場合、装置は VLAN のすべてのルータポートに report を送信します。

- Report

ホストから MLD report を受信したのち、装置は以下のように一致するエントリを転送テーブルから検索します。

  - エントリが一致し、転送エントリに受信ポートを含んでいる場合、装置はポートのエージングタイマをリセットします。

- □ エントリが一致するが、転送エントリに受信ポートが含まれない場合、装置は出力インタフェースリストに受信ポートを追加します。そして受信ポートをダイナミックメンバポートとしてマーキングします。ポートのエージングタイマを開始します。
- □ エントリが一致しない場合、装置は出力インタフェースを受信ポートとして転送エントリを作成します。受信ポートをダイナミックメンバポートとしてマーキングします。ポートのエージングタイマを開始します。そしてすべてのルータポートに report を送信します。

- Done メッセージ

ポートで MLD done メッセージを受信したのち、装置は受信ポートを通して MLD multicast-address-specific を送信します。last メンバポートが転送エントリから削除されたときのみすべてのルータポートに MLD done メッセージを送信します。

4.2 プロトコルと標準

RFC 4541, *Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches*

4.3 MLD snooping設定作業リスト

作業リスト
MLD snoopingの基本機能の設定： ● （必須設定項目） MLD snoopingの有効化 ● （オプション設定項目） MLD snoopingのバージョンの設定 ● （オプション設定項目） MLD snooping転送エントリの最大数の設定 ● （オプション設定項目）MLD last listener クエリ間隔の設定
MLD snoopingのポート機能の設定： ● （オプション設定項目） ダイナミックポートのエージングタイマの設定 ● （オプション設定項目） スタティックポートの設定 ● （オプション設定項目） シミュレーティッドメンバホストのポート設定 ● （オプション設定項目） fast-leave処理の有効化
MLD snoopingクエリアの設定： ● （オプション設定項目） MLD snoopingクエリアの有効化 ● （オプション設定項目） MLD クエリとresponseのパラメータの設定
MLDメッセージのパラメータの設定： ● （オプション設定項目） MLDメッセージの送信元IPv6アドレスの設定 ● （オプション設定項目） MLDメッセージの802.1p優先度の設定

作業リスト
MLD snoopingポリシーの設定： • （オプション設定項目） IPv6マルチキャストグループポリシーの設定 • （オプション設定項目） IPv6マルチキャストソースポートフィルタの有効化 • （オプション設定項目） 未知のIPv6マルチキャストデータ廃棄機能の有効化 • （オプション設定項目） MLD report 抑制機能の有効化 • （オプション設定項目） ポートのIPv6マルチキャストグループの最大数の設定 • （オプション設定項目） IPv6マルチキャストグループ置き換え機能の有効化
（オプション設定項目）送信MLDプロトコルパケットのDSCP値の設定

レイヤ 2 アグリゲートインタフェースで設定された MLD snooping の設定は、メンバポートの設定に影響しません。また、アグリゲーションの計算にも参加しません。アグリゲートグループのメンバポートでの設定は、アグリゲートグループから離脱するまで有効になりません。

4.4 MLD snoopingの基本機能の設定

MLD snooping の基本機能の設定をする前に、以下の作業を完了させてください。

- 対応する VLAN を設定してください。
- MLD snooping のバージョンを定義してください。
- MLD last-member クエリの間隔を定義してください。
- MLD クエリの最大応答時間を定義してください。

4.4.1 MLD snooping の有効化

MLD snooping を有効にするとき、以下のガイドラインに従ってください。

- VLAN で MLD snooping を有効にする前に、グローバルで有効にしてください。
- VLAN 用の MLD snooping は、VLAN のメンバポートでのみ動作します。
- MLD snooping は MLD-snooping view あるいは VLAN view のどちらかで設定することができます。MLD-snooping view での設定と VLAN view での設定は同じ優先度を持ちます。

I. MLD-snooping view での VLAN の MLD snooping の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. MLD snooping をグローバルで有効にし、MLD-snooping view に移行する	**mld-snooping**	デフォルト：無効
3. 指定した VLAN で MLD snooping を有効にする	**enable vlan** *vlan-list*	デフォルト：無効

II. VLAN view での VLAN の MLD snooping の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． MLD snooping をグローバルで有効にし、MLD-snooping view に移行する	**mld-snooping**	デフォルト：無効
3． system view に戻る	**quit**	―
4． VLAN view に移行する	**vlan** *vlan-id*	―
5． VLAN での MLD snooping を有効にする	**mld-snooping enable**	デフォルト：無効

4.4.2 MLD snooping のバージョンの設定

MLD snooping のバージョンが異なると、異なるバージョンの MLD メッセージの処理を行います。

- MLDv1 snooping は MLDv1 を処理することができますが、MLDv2 メッセージは処理することはできず、VLAN 上にフラッディングされてしまいます。
- MLDv2 snooping は MLDv1 および MLDv2 メッセージを処理することができます。

MLDv2 snooping を MLDv1 snooping に変更する場合、装置は以下のことを行います。

- ダイナミックに作成されたすべての MLD snooping 転送エントリを削除します。
- MLDv2 snooping スタティック（* , G）の転送エントリは維持します。
- MLDv2 snooping スタティック（S , G）の転送エントリは削除します。MLD snooping が MLDv2 snooping に切り替わったとき復元されます。

スタティック MLD snooping 転送エントリの詳細については、オペレーションマニュアルのセクション 6 *マルチキャスト”MLD スヌーピング”の”スタティックポートの設定”* を参照してください。

MLD snooping のバージョンは MLD-snooping view あるいは VLAN view のどちらかで設定することができます。MLD-snooping view での設定と VLAN view での設定は同じ優先度を持ちます。

以下に MLD-snooping view での MLD snooping のバージョンの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． MLD snooping をグローバルで有効にし、MLD-snooping view に移行する.	**mld-snooping**	―
3． 指定した VLAN で MLD snooping のバージョンを指定する	**version** *version-number* **vlan** *vlan-list*	デフォルト：1

以下に VLAN view での MLD snooping のバージョンの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―

操作	コマンド	補足
2． VLAN view に移行する	**vlan** *vlan-id*	―
3． VLAN で MLD snooping のバージョンを指定する	**mld-snooping version** *version-number*	デフォルト：1

4.4.3 MLD snooping 転送エントリの最大数の設定

MLD snooping 転送エントリの最大数を変更することができます。転送エントリはダイナミックエントリとスタティックエントリの両方が含まれます。装置の転送エントリ数が上限に達すると、装置は、いくつかのエントリがタイムアウトするか、手動で削除されるまで、転送エントリを作成することができません。この場合、手動でエントリを削除することを推奨します。

以下に MLD snooping 転送エントリの最大数の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． MLD-snooping view に移行する	**mld-snooping**	―
3． MLD snooping 転送エントリの最大数を設定する	**entry-limit** *limit*	デフォルト：4294967295

4.4.4 MLD last listener クエリ間隔の設定

IPv6 マルチキャストグループの MLD multicast-address-specific クエリを受信すると、レシーバホストは参加した各 IPv6 マルチキャストグループのタイマを起動します。このタイマは、0 から最大応答時間の範囲でランダムな値に初期化されます。タイマ値が経過して 0 になったときに、ホストは対応する IPv6 マルチキャストグループに MLD report を送信します。

MLD last listener クエリ間隔は、MLD multicast-address-specific クエリの配信された最大応答時間を定義します。MLD last listener クエリの時間を適切に設定すると、ホストは速やかに MLD multicast-address-specific クエリに応答できます。また、対応するタイマの期限が多数のホストで同時に切れたときに同時に送信する report によってネットワーク上で発生する MLD report トラフィックのバーストを回避することもできます。

I. 設定の制限とガイドライン

MLD last listener クエリ間隔を設定する場合、以下の制限とガイドラインに従ってください。

- fast-leave 処理が有効なポートから MLD done メッセージを受信した場合、装置は MLD multicast-address-specific クエリを送信しません。
- MLD-snooping view のすべての VLAN、あるいは VLAN view の VLAN でグローバルに MLD last listener クエリの間隔を設定することができます。VLAN で行った設定はグローバルで行った設定よりも優先されます。

II. グローバルでの MLD クエリと response のパラメータの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． MLD-snooping view に移行する	**mld-snooping**	―
3． MLD last listener クエリ間隔を設定する	**last-listener-query-interval** *interval*	デフォルト：1秒

III. VLAN での MLD クエリと response のパラメータの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． MLD-snooping view に移行する	**mld-snooping**	―
3． MLD last listener クエリ間隔を設定する	**mld-snooping** **last-listener-query-interval** *interval*	デフォルト：1秒

4.5 MLD snoopingのポート機能の設定

MLD snooping のポート機能の設定をする前に、以下の作業を完了させてください。

- VLAN で MLD snooping を有効にしてください。
- ダイナミックルータポートのエージングタイマを定義してください。
- ダイナミックメンバポートのエージングタイマを定義してください。
- IPv6 マルチキャストグループと IPv6 マルチキャストソースのアドレスを定義してください。

4.5.1 ダイナミックポートのエージングタイマの設定

ダイナミックポートのエージングタイマを設定するとき、以下の制限とガイドラインに従ってください。

- IPv6 マルチキャストグループメンバシップが頻繁に変更される場合は、メンバポートのエージングタイマに比較的小さな値を設定します。IPv6 マルチキャストグループメンバシップがほとんど変更されない場合は、メンバポートのエージングタイマに比較的大きな値を設定します。
- ダイナミックルータポートが IPv6 PIMv2 hello メッセージを受信した場合、ダイナミックポートのエージングタイマの時間は、hello メッセージで指定された時間となります。**mld-snooping router-aging-time** コマンドの設定は適用されません。
- 装置が開始した MLD multicast-address-specific クエリによってダイナミックメンバポートのエージングタイマの調整を行います。ダイナミックメンバポートがクエリを受信した場合、エージングタイマは MLD last listener クエリ間隔の 2 倍に設定されます。
- ダイナミックポートのエージングタイマの設定は、VLAN view あるいは MLD-snooping view のどちらかに設定することができます。もし VLAN view と MLD-snooping view の両方に設定がある場合、VLAN view の設定が適用されます。

I. グローバルでのダイナミックポートのエージングタイマの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. MLD-snooping view に移行する	**mld-snooping**	―
3. グローバルでのダイナミックルータポートのエージングタイマを設定する	**router-aging-time** *seconds*	デフォルト：260秒
4. グローバルでのダイナミックメンバポートのエージングタイマを設定する	**host-aging-time** *seconds*	デフォルト：260秒

II. VLAN でのダイナミックポートのエージングタイマの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. VLAN view に移行する	**vlan** *vlan-id*	―
3. VLAN でのダイナミックルータポートのエージングタイマを設定する	**mld-snooping router-aging-time** *seconds*	デフォルト：260秒
4. VLAN でのダイナミックメンバポートのエージングタイマを設定する	**mld-snooping host-aging-time** *seconds*	デフォルト：260秒

4.5.2 スタティックポートの設定

以下のタイプのスタティックポートを設定することができます。

- **スタティックメンバポート**－IPv6 マルチキャストグループのスタティックメンバポートとしてポートを設定するとき、ポートに所属されたすべてのホストはグループの IPv6 マルチキャストデータを受信します。

  スタティックメンバポートは MLD クエリに応答しません。設定あるいは設定を取り消すとき、ポートは unsolicited MLD report や done メッセージを送信しません。
- **スタティックルータポート**－IPv6 マルチキャストグループのスタティックルータポートとしてポートを設定するとき、ポートで受信されたグループのすべての IPv6 マルチキャストデータは転送されます。

以下にスタティックポートの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Ethernet interface view あるいは aggregate interface view に移行する.	**interface** *interface-type interface-number*	―

操作	コマンド	補足
3. ポートをスタティックポートに設定する	• ポートをスタティックメンバポートに設定する：**mld-snooping static-group** *ipv6-group-address* [**source-ip** *ipv6-source-address*] **vlan** *vlan-id* • ポートをスタティックルータポートに設定する：**mld-snooping static-router-port vlan** *vlan-id*	デフォルト：設定なし

4.5.3 シミュレーティッドメンバホストのポート設定

ポートがシミュレーティッドメンバホストとして設定されるとき、以下に示す独立したホストと同等になります。

- 設定が完了したとき、unsolicited MLD report を送信します。
- MLD report の MLD general クエリに応答します。
- 設定を削除したとき、MLD done メッセージを送信します。

この操作を実行するとき、シミュレーティッドホストの MLD バージョンと MLD snooping バージョンが同一であることを確認してください。スタティックメンバポートと異なり、シミュレーティッドメンバホストとして設定されたポートはダイナミックメンバポートと同様にエージアウトします。

以下にシミュレーティッドメンバホストの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. Layer 2 Ethernet interface view あるいは aggregate interface view に移行する.	**interface** *interface-type interface-number*	—
3. シミュレーティッドメンバホストとしてポートを設定する	**mld-snooping host-join** *ipv6-group-address* [**source-ip** *ipv6-source-address*] **vlan** *vlan-id*	デフォルト：設定なし

4.5.4 fast-leave 処理の有効化

fast-leave 処理を有効にすることで、ポートが done メッセージを受信すると、IPv6 マルチキャストグループの転送エントリからポートをすぐに取り除くことができます。

I. 設定の制限とガイドライン

fast-leave 処理を有効にするとき、以下の制限とガイドラインに従ってください。

- VLAN に所属した複数のレシーバホストが接続されているポートでは有効にしないでください。そうでなければ同じ IPv6 マルチキャストグループにあるポートに接続された他のレシーバのホストは IPv6 マルチキャストデータを受信することができません。

- interface view での現在のポート、あるいはグローバルでのすべてのポートで fast-leave 処理を有効にすることができます。もし interface view と MLD-snooping view の両方に設定がある場合、interface view の設定が適用されます。

II. グローバルでの fast-leave 処理の有効化

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. MLD-snooping view に移行する	**mld-snooping**	―
3. グローバルで fast-leave 処理を有効にする	**fast-leave** [**vlan** *vlan-list*]	デフォルト：無効

III. ポートでの fast-leave 処理の有効化

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Ethernet interface view あるいは aggregate interface view に移行する.	**interface** *interface-type interface-number*	―
3. ポートで fast-leave 処理を有効にする	**mld-snooping fast-leave** [**vlan** *vlan-list*]	デフォルト：無効

4.6 MLD snoopingクエリアの設定

この項では MLD snooping クエリアを設定する方法を記載します。

4.6.1 設定要件

VLAN の MLD snooping クエリアを設定する前に、以下の作業を完了してください。

- VLAN で MLD snooping を有効にしてください。
- MLD general クエリの間隔を定義してください。
- MLD general クエリの最大応答時間を定義してください。

4.6.2 MLD snooping クエリアの有効化

データリンクレイヤで IPv6 マルチキャスト転送エントリを確立、維持するため、この機能を有効にすることで、装置が MLD general クエリを定期的に送信します。レイヤ 3 マルチキャスト装置を使用しないでネットワークで MLD snooping クエリアを設定することができます。

MLD が動作する IPv6 マルチキャストネットワークで MLD snooping クエリアを有効にしないでください。MLD snooping クエリアは、MLD クエリアの選択に参加しません。しか

し小さい送信元 IPv6 アドレスで MLD general クエリを送信する場合、MLD クエリアの選択に影響する可能性があります。

以下に VLAN で MLD snooping クエリアを有効にする設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． VLAN view に移行する	**vlan** *vlan-id*	―
3． MLD snooping クエリアを有効にする	**mld-snooping querier**	デフォルト：無効

4.6.3 MLD general クエリと response のパラメータの設定

注意：

MLD general クエリの間隔は、MLD general クエリの最大応答時間よりも大きいことを確認してください。そうでないと IPv6 マルチキャストグループメンバが誤って削除される可能性があります。

MLD general クエリの間隔を実際のネットワークの状況にもとづいて変更することができます。

レシーバホストが MLD general クエリを受信したとき、レシーバホストはレシーバホストが加入した各 IPv6 マルチキャストグループのタイマを開始します。このタイマは、0 から MLD クエリメッセージ内にアドバタイズされた最大応答時間の範囲でランダムな値に初期化されます。タイマ値が経過して 0 になったとき、ホストは IPv6 マルチキャストグループに MLD report を送信します。

MLD クエリの最大応答時間を適切に設定すると、ホストは速やかにクエリに応答できます。また、対応するタイマの期限が多数のホストで同時に切れたときに同時に送信する report によってネットワーク上で発生する MLD トラフィックのバーストを回避することもできます。

MLD クエリと応答のパラメータは、VLAN view で現在の view あるは MLD-snooping view ですべての VLAN で設定できます。もし VLAN view と MLD-snooping view の 2 つの設定がある場合、VLAN view で設定された設定が適用されます。

I. グローバルでの MLD クエリと response のパラメータの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． MLD-snooping view に移行する	**mld-snooping**	―
3． MLD general クエリの最大応答時間を設定する	**max-response-time** *seconds*	デフォルト：10秒

II. VLAN での MLD クエリと response のパラメータの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． VLAN view に移行する	**vlan** *vlan-id*	―
3． MLD general クエリの送信間隔を設定する	**mld-snooping query-interval** *interval*	デフォルト：125秒
4． MLD general クエリの最大応答時間を設定する	**mld-snooping max-response-time** *seconds*	デフォルト：10秒

4.7 MLDメッセージのパラメータの設定

この章では MLD メッセージのパラメータの設定方法について記載します。

4.7.1 設定要件

VLAN で MLD メッセージのパラメータを設定する前に、以下の作業を完了してください。

- VLAN で MLD snooping を有効にしてください。
- MLD general クエリの送信元 IPv6 アドレスを定義してください。
- MLD multicast-address-specific クエリの送信元 IPv6 アドレスを定義してください。
- MLD report の送信元 IPv6 アドレスを定義してください。
- MLD done メッセージの送信元 IPv6 アドレスを定義してください。
- MLD メッセージの 802.1p 優先度を定義してください。

4.7.2 MLD メッセージの送信元 IPv6 アドレスの設定

MLD snooping クエリアによって送信された MLD クエリの送信元 IPv6 アドレスを変更することができます。MLD クエリの送信元アドレスを変更するとサブネット内の MLD クエリアの選択に影響する可能性があります。

シミュレーティッドメンバホストによって MLD report あるいは MLD done メッセージの送信元 IPv6 アドレスを変更することができます。

以下に VLAN の MLD メッセージの送信元 IPv6 アドレスの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． VLAN view に移行する	**vlan** *vlan-id*	―

操作	コマンド	補足
3. MLD general クエリの送信元 IPv6 アドレスを設定する	**mld-snooping general-query source-ip** *ipv6-address*	デフォルト: 現在のVLANインタフェースのIPv6リンクローカルアドレスです。 現在のVLANインタフェースがIPv6リンクローカルアドレスを持っていない場合、送信元IPv6アドレスはFE80::02FF:FFFF:FE00:0001です。
4. MLD multicast-address-specific クエリの送信元 IPv6 アドレスを設定する	**mld-snooping special-query source-ip** *ipv6-address*	デフォルト：送信元IPv6アドレスは以下のいずれかとなります。 ● MLD snoopingクエリアがMLD general クエリを受信したとき、MLD multicast-address-specific クエリの送信元IPv6アドレスはMLD general クエリのIPv6アドレスです。 ● MLD snoopingクエリアがMLD general クエリを受信しないとき、送信元IPv6アドレスは現在のVLANインタフェースのIPv6リンクローカルアドレスです。 ● 現在のVLANインタフェースにIPv6リンクローカルアドレスが設定されていない場合、送信元IPv6アドレスはFE80::02FF:FFFF:FE00:0001です。
5. MLD report の送信元 IPv6 アドレスを設定する	**mld-snooping report source-ip** *ipv6-address*	デフォルト： 現在のVLANインタフェースのIPv6リンクローカルアドレスです。現在のVLANインタフェースがIPv6リンクローカルアドレスを持っていない場合、送信元IPv6アドレスはFE80::02FF:FFFF:FE00:0001です。
6. MLD done メッセージの送信元 IPv6 アドレスを設定する	**mld-snooping done source-ip** *ipv6-address*	デフォルト： 現在のVLANインタフェースのIPv6リンクローカルアドレスです。現在のVLANインタフェースがIPv6リンクローカルアドレスを持っていない場合、送信元IPv6アドレスはFE80::02FF:FFFF:FE00:0001です。

4.7.3 MLD メッセージの 802.1p 優先度の設定

装置の出力ポートで混雑が発生したとき、高い 802.1p 優先度から低い 802.1p 優先度の順番で、MLD メッセージを転送します。装置で作成あるいは転送された MLD メッセージに高い 802.1p 優先度を割り当てることができます。

MLD メッセージの 802.1p 優先度は、MLD-snooping view ですべての VLAN あるいは VLAN view で現在の VLAN で設定できます。もし VLAN view と MLD-snooping view の 2 つの設定がある場合、VLAN view で設定された設定が適用されます。

I. グローバルでの MLD メッセージの 802.1p 優先度の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. MLD-snooping view に移行する	**mld-snooping**	―
3. MLD メッセージの 802.1p 優先度を設定する	**dot1p-priority** *priority*	デフォルト：MLDメッセージの802.1p優先度はデフォルトで設定されていません。装置によって作成されるMLDメッセージの優先度は0です。

II. VLAN での MLD メッセージの 802.1p 優先度の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. VLAN view に移行する	**vlan** *vlan-id*	―
3. MLD メッセージの 802.1p 優先度を設定する	**mld-snooping dot1p-priority** *priority*	デフォルト：MLDメッセージの802.1p優先度はデフォルトで設定されていません。装置によって作成されるMLDメッセージの優先度は0です。

4.8 MLD snoopingポリシーの設定

MLD snooping ポリシーを設定する前に、以下の作業を完了してください。

- VLAN で MLD snooping を有効にしてください。
- IPv6 マルチキャストグループポリシーとして使用される ACL を定義してください。
- ポートが加入できる IPv6 マルチキャストグループの最大数を定義してください。

4.8.1 IPv6 マルチキャストグループポリシーの設定

この機能は IPv6 マルチキャストグループとオプションソースを指定した ACL をもとにして MLD report をフィルタする装置を有効にします。レシーバホストが加入できる IPv6 マルチキャストグループを管理することに使用されます。

I. 設定の制限とガイドライン

IPv6 マルチキャストグループポリシーを設定するときに、以下の設定の制限とガイドラインに従ってください。

- 設定はダイナミックにポートが加入する IPv6 マルチキャストグループにのみ適用されます。
- IPv6 マルチキャストポリシーの設定は MLD-snooping view ですべてのポート、あるいは interface view で現在のポートで行うことができます。もし interface view と MLD-snooping view の 2 つの設定がある場合、interface view で設定された設定が適用されます。

II. グローバルでの IPv6 マルチキャストグループポリシーの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. MLD-snooping view に移行する	**mld-snooping**	―
3. グローバルで IPv6 マルチキャストグループポリシーを設定する	**group-policy** *ipv6-acl-number* [**vlan** *vlan-list*]	デフォルト：設定なし

III. ポートでの IPv6 マルチキャストグループポリシーの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Ethernet interface view あるいは aggregate interface view に移行する.	**interface** *interface-type interface-number*	―
3. ポートで IPv6 マルチキャストグループポリシーを設定する	**mld-snooping group-policy** *ipv6-acl-number* [**vlan** *vlan-list*]	デフォルト：設定なし

4.8.2 IPv6 マルチキャストソースポートフィルタの有効化

この機能は、すべての IPv6 マルチキャストデータパケットの廃棄および IPv6 マルチプロトコルパケットの許可を、装置で設定することができます。IPv6 マルチキャストレシーバに接続されたポートのみ機能を有効にすることができます。

MLD-snooping view で指定されたポートあるいは interface view で現在のポートの IPv6 マルチキャストソースポートフィルタリングを有効にすることができます。MLD-snooping view での設定と interface view での設定の優先度は同一です。

I. グローバルでの IPv6 マルチキャストソースポートフィルタリングの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―

操作	コマンド	補足
2． MLD-snooping view に移行する	**mld-snooping**	―
3． IPv6 マルチキャストソースポートフィルタリングを有効にする	**source-deny port** *interface-list*	デフォルト：無効

II. ポートでの IPv6 マルチキャストソースポートフィルタリングの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． interface view に移行する	**interface** *interface-type interface-number*	―
3． IPv6 マルチキャストソースポートフィルタリングを有効にする	**mld-snooping source-deny**	デフォルト：無効

4.8.3 未知の IPv6 マルチキャストデータ廃棄機能の有効化

未知の IPv6 マルチキャストデータとは、MLD snooping 転送テーブルにエントリが存在しない IPv6 マルチキャストデータのことです。この機能はすべての未知の IPv6 マルチキャストデータを廃棄します。

もしこの機能が無効である場合、未知の IPv6 マルチキャストデータが所属している VLAN にフラッディングされます。

以下に未知の IPv6 マルチキャストデータ廃棄機能の有効化の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． VLAN view に移行する	**vlan** *vlan-id*	―
3． 未知の IPv6 マルチキャストデータ廃棄機能を有効にする	**mld-snooping drop-unknown**	デフォルト：無効 未知のIPv6マルチキャストデータはフラッディングします。

4.8.4 MLD report 抑制機能の有効化

この機能を有効にすることで、装置は直接接続されたレイヤ 3 装置に IPv6 マルチキャストグループの最初の MLD report のみ転送します。同じクエリ間隔内の同じグループの他の MLD report は廃棄されます。

以下に MLD report 抑制機能の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． MLD-snooping view に移行する	**mld-snooping**	―

操作	コマンド	補足
3． MLD report 抑制を有効にする	**report-aggregation**	デフォルト：有効

4.8.5 ポートの IPv6 マルチキャストグループの最大数の設定

ポートのトラフィックを調整するため、ポートでの IPv6 マルチキャストグループの最大数を設定することができます。

I. 設定の制限とガイドライン

ポートの IPv6 マルチキャストグループの最大数を設定するとき、以下の設定の制限とガイドラインに従ってください。

- この設定はダイナミックに IPv6 マルチキャストグループに加入されたポートのみ適用します。
- ポートが参加した IPv6 マルチキャストグループの数が設定されている上限に達したとき、そのポートに残るすべての転送エントリを MLD snooping 転送テーブルから削除します。このポートに接続されたレシーバホストは、上限になる前に、再度 IPv6 マルチキャストグループに参加することができます。

II. 設定手順

以下にポートの IPv6 マルチキャストグループの最大数の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． Ethernet interface view あるいは aggregate interface view に移行する.	**interface** *interface-type interface-number*	—
3． ポートの IPv6 マルチキャストグループの最大数を設定する	**mld-snooping group-limit** *limit* [**vlan** *vlan-list*]	デフォルト：4294967295

4.8.6 IPv6 マルチキャストグループ置き換え機能の有効化

この機能を有効にすることで、装置で IPv6 マルチキャストグループが上限を超えたとき、装置が存在する IPv6 マルチキャストグループを新しく追加されたグループに置き換えることができます。この機能は一般的にチャンネルスイッチングアプリケーションで使用されます。この機能が無効である場合、装置が新しいグループの MLD report を廃棄し、ユーザが新しいチャンネルに変更することができません。

I. 設定の制限とガイドライン

IPv6 マルチキャストグループ置き換え機能を有効にするとき、以下の設定の制限とガイドラインに従ってください。

- この設定はダイナミックに IPv6 マルチキャストグループに加入されたポートのみ適用します。
- IPv6 マルチキャストグループ置き換え機能は、ポートあるいはグローバルのどちらかに設定することができます。もしポートとグローバルの両方に設定がある場合、ポートの設定が適用されます。

II. グローバルでの IPv6 マルチキャストグループ置き換え機能の有効化の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. MLD-snooping view に移行する	**mld-snooping**	―
3. グローバルで IPv6 マルチキャストグループ置き換え機能を有効にする	**overflow-replace** [**vlan** *vlan-list*]	デフォルト：無効

III. ポートでの IPv6 マルチキャストグループ置き換え機能の有効化の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Ethernet interface view あるいは aggregate interface view に移行する.	**interface** *interface-type interface-number*	―
3. ポートで IPv6 マルチキャストグループ置き換え機能を有効にする	**mld-snooping overflow-replace** [**vlan** *vlan-list*]	デフォルト：無効

4.9 送信MLDプロトコルパケットのDSCP値の設定

I. 送信 MLD プロトコルパケットの DSCP 値

DSCP 値によって、パケット送信の優先順位が決まります。DSCP 値が大きいほど、優先度が高くなります。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. MLD-snooping view に移行する.	**mld-snooping**	―
3. 送信 MLD プロトコルパケットの DSCP 値を設定する	**dscp** *dscp-value*	デフォルト：48

4.10 MLD snoopingの表示と維持

すべての view で **display** コマンドを実行でき、user view で **reset** コマンドを実行できます。

操作	コマンド
レイヤ2IPv6マルチキャストグループの情報を表示する	**display ipv6 l2-multicast ip** [**group** *ipv6-group-address* | **source** *ipv6-source-address*] * [**vlan** *vlan-id*] [**slot** *slot-number*]
レイヤ2 IPv6マルチキャストグループエントリの情報を表示する	**display ipv6 l2-multicast ip forwarding** [**group** *ipv6-group-address* | **source** *ipv6-source-address*] * [**vlan** *vlan-id*] [**slot** *slot-number*]
レイヤ2 IPv6 MACマルチキャストグループの情報を表示する	**display ipv6 l2-multicast mac** [*mac-address*] [**vlan** *vlan-id*] [**slot** *slot-number*]
レイヤ2 IPv6 MACマルチキャストグループエントリの情報を表示する	**display ipv6 l2-multicast mac forwarding** [*mac-address*] [**vlan** *vlan-id*] [**slot** *slot-number*]
MLD snoopingのステータスを表示する	**display mld-snooping** [**global** | **vlan** *vlan-id*]
ダイナミックMLD snooping転送エントリの情報を表示する	**display mld-snooping group** [*ipv6-group-address* | *ipv6-source-address*] * [**vlan** *vlan-id*] [**verbose**] [**slot** *slot-number*]
スタティックMLD snooping転送エントリの情報を表示する	**display mld-snooping static-group** [*ipv6-group-address* | *ipv6-source-address*] * [**vlan** *vlan-id*] [**verbose**] [**slot** *slot-number*]
ダイナミックルータポートの情報を表示する	**display mld-snooping router-port** [**vlan** *vlan-id*] [**slot** *slot-number*]
スタティックルータポートの情報を表示する	**display mld-snooping static-router-port** [**vlan** *vlan-id*] [**slot** *slot-number*]
MLD snoopingによって学習されたMLDメッセージの統計情報を表示する	**display mld-snooping statistics**
IPv6マルチキャストグループのダイナミックMLD snooping転送エントリを削除する	**reset mld-snooping group** { *ipv6-group-address* [*ipv6-source-address*] | **all** } [**vlan** *vlan-id*]
ダイナミックルータポートを削除する	**reset mld-snooping router-port** { **all** | **vlan** *vlan-id* }
MLD snoopingによって学習されたMLDメッセージの統計情報を削除する	**reset mld-snooping statistics**

4.11 MLD snooping設定例

4.11.1 IPv6 グループポリシーとシミュレーティッドメンバホスト設定例

I. ネットワーク要件

本設定例では、Switch A が QX-S5100G シリーズに該当します。

別途、IPv4 マルチキャストルーティングに対応した Router A が必要です。

図 4-4に示すように Router A は MLDv1 を動作させ、MLD クエリアとして機能し、Switch A は MLDv1 snooping を動作させます。

以下が成り立つようにグループポリシーを設定します。

- Host A と Host B は宛先が IPv6 マルチキャストグループ FF1E::101 の IPv6 マルチキャストデータのみ受信します。
- VLAN100 でフラッディングしないように Switch A で未知の IPv6 マルチキャストデータ廃棄機能を有効にします。

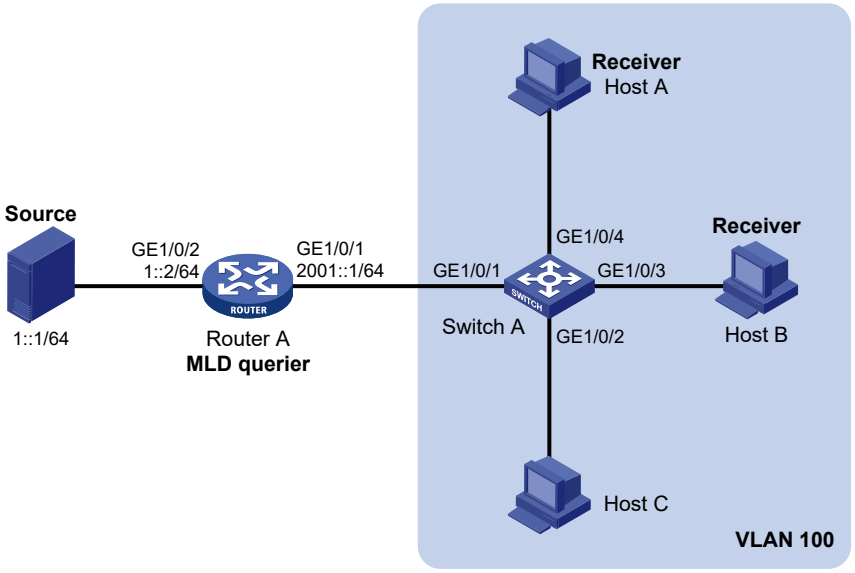


図 4-4 ネットワーク図

II. 設定手順

1) 図 4-4に対応する各インタフェースに IPv6 アドレスとプレフィックス長を割り当てます。（詳細は省略します）
2) Router A を設定します。

IPv6 マルチキャストルーティングを有効にします。

```
<RouterA> system-view
[RouterA] ipv6 multicast routing
[RouterA-mrib6] quit
```

GigabitEthernet 1/0/1 で MLD を有効にします。

```
[RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] mld enable
[RouterA-GigabitEthernet1/0/1] quit
```

GigabitEthernet 1/0/2 で IPv6 PIM-SM を有効にします。

```
[RouterA] interface gigabitethernet 1/0/2
```

```
[RouterA-GigabitEthernet1/0/2] ipv6 pim sm
[RouterA-GigabitEthernet1/0/2] quit
```

3)　Switch A を設定します。

グローバルで MLD snooping を有効にします。

```
<SwitchA> system-view
[SwitchA] mld-snooping
[SwitchA-mld-snooping] quit
```

VLAN 100 を作成し、この VLAN に GigabitEthernet 1/0/1～GigabitEthernet 1/0/4 を割り当てます。

```
[SwitchA] vlan 100
[SwitchA-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/4
```

VLAN100 で未知の IPv6 マルチキャストデータ廃棄機能を有効にします。

```
[SwitchA-vlan100] mld-snooping enable
[SwitchA-vlan100] mld-snooping drop-unknown
[SwitchA-vlan100] quit
```

VLAN 100 のホストが IPv6 マルチキャストグループ FF1E::101 のみ参加できるように、IPv6 マルチキャストグループポリシーを設定します。

```
[SwitchA] acl ipv6 basic 2001
[SwitchA-acl-ipv6-basic-2001] rule permit source ff1e::101 128
[SwitchA-acl-ipv6-basic-2001] quit
[SwitchA] mld-snooping
[SwitchA- mld-snooping] group-policy 2001 vlan 100
[SwitchA- mld-snooping] quit
```

IPv6 マルチキャストグループ FF1E::101 のシミュレーティッドメンバホストとして GigabitEthernet 1/0/3、GigabitEthernet 1/0/4 を設定します。

```
[SwitchA] interface gigabitethernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] mld-snooping host-join ff1e::101 vlan 100
[SwitchA-GigabitEthernet1/0/3] quit
[SwitchA] interface gigabitethernet 1/0/4
[SwitchA-GigabitEthernet1/0/4] mld-snooping host-join ff1e::101 vlan 100
[SwitchA-GigabitEthernet1/0/4] quit
```

III. 設定の確認

IPv6 マルチキャストグループ FF1E::101、FF1E::202 に加入するため Host A と Host B から MLD report を送信します。（詳細は省略します）

Switch A の VLAN 100 のダイナミック MLD snooping 転送エントリの情報を表示します。

```
[SwitchA] display mld-snooping group vlan 100
Total 1 entries.

VLAN 100: Total 1 entries.
  (::, FF1E::101)
    Host ports (2 in total):
      GE1/0/3                                 (00:03:23)
      GE1/0/4                                 (00:04:10)
```

出力は以下の情報を表示します。

- Host A と Host B は IPv6 マルチキャストグループ FF1E::101 に加入しています。（それぞれ Switch A の GigabitEthernet 1/0/4 と GigabitEthernet 1/0/3 のメンバポートを通して加入しています）
- Host A と Host B は IPv6 マルチキャストグループ FF1E::202 に加入できません。

4.11.2 スタティックルータポート設定例

I. ネットワーク要件

本設定例では、Switch A、Switch B、Switch C が QX-S5100G シリーズに該当し、Switch A と Switch C へ スタティックルータポートの設定をします。

別途、IPv4 マルチキャストルーティングに対応した Router A が必要です。

図 4-5に示すように設定します。

- Router A は MLDv1 を動作させ、MLD クエリアとして機能し、Switch A、Switch B、Switch C は MLDv1 snooping を動作させます。
- Host A と Host C は IPv6 マルチキャストグループ FF1E::101 の永久的なレシーバです。

スタティックポートを以下の要件に従って設定します。

- IPv6 マルチキャストトラフィック送信の信頼性を強化するために、Switch C の GigabitEthernet 1/0/3 と GigabitEthernet 1/0/5 を IPv6 マルチキャストグループ FF1E::101 のスタティックメンバポートとして設定します。
- ネットワークで STP が実行されていると仮定します。データループを回避するために、Switch A から Switch C への転送パスは通常状態ではブロックされます。IPv6 マルチキャストトラフィックは Switch A—Switch B—Switch C のパスを経由して、Switch C に接続されているレシーバに転送されます。Switch A—Switch B—Switch C のパスがブロックされた場合に、Switch A—Switch C のパスを経由して IPv6 マルチキャストトラフィックがほとんど途切れずにレシーバへと転送できるように、Switch A の GigabitEthernet 1/0/3 にスタティックルータポートを設定します。STP の詳細は、オペレーションマニュアルのセクション 3 *アクセス”STP”* を参照してください。

メモ：

スタティックルータポートが設定されていない場合、Switch A—Switch B－Switch C のパスがブロックされたのち、IPv6 マルチキャストの転送が中断されます。新しいパスで IPv6 マルチキャストパケットを転送する前に、少なくとも 1 回以上の MLD クエリ、MLD 応答の交換が必要です。

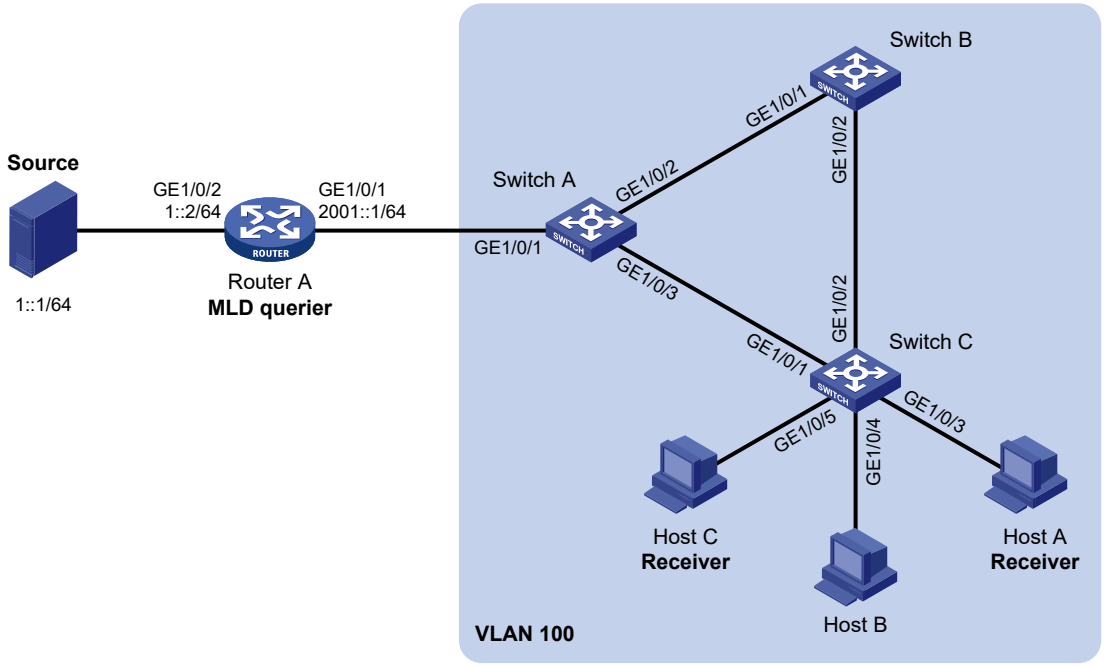


図 4-5 ネットワーク図

II. 設定手順

1) 図 4-5に対応する各インタフェースに IPv6 アドレスとプレフィックス長を割り当てます。（詳細は省略します）
2) Router A を設定します。

IPv6 マルチキャストルーティングを有効にします。

```
<RouterA> system-view
[RouterA] ipv6 multicast routing
[RouterA-mrib6] quit
```

GigabitEthernet 1/0/1 で MLD を有効にします。

```
[RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] mld enable
[RouterA-GigabitEthernet1/0/1] quit
```

GigabitEthernet 1/0/2 で IPv6 PIM-SM を有効にします。

```
[RouterA] interface gigabitethernet 1/0/2
[RouterA-GigabitEthernet1/0/2] ipv6 pim sm
[RouterA-GigabitEthernet1/0/2] quit
```

3)　Switch A を設定します。

グローバルで MLD snooping を有効にします。

```
<SwitchA> system-view
[SwitchA] mld-snooping
[SwitchA-mld-snooping] quit
```

VLAN 100 を作成し、この VLAN に GigabitEthernet 1/0/1～GigabitEthernet 1/0/3 を割り当てます。

```
[SwitchA] vlan 100
[SwitchA-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/3
```

VLAN 100 で MLD snooping を有効にします。

```
[SwitchA-vlan100] mld-snooping enable
[SwitchA-vlan100] quit
```

スタティックルータポートとして GigabitEthernet 1/0/3 を設定します。

```
[SwitchA] interface gigabitethernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] mld-snooping static-router-port vlan 100
[SwitchA-GigabitEthernet1/0/3] quit
```

4)　Switch B を設定します。

グローバルで MLD snooping を有効にします。

```
<SwitchB> system-view
[SwitchB] mld-snooping
[SwitchB-mld-snooping] quit
```

VLAN 100 を作成し、この VLAN に GigabitEthernet 1/0/1～GigabitEthernet 1/0/2 を割り当てます。

```
[SwitchB] vlan 100
[SwitchB-vlan100] port gigabitethernet 1/0/1 gigabitethernet 1/0/2
```

VLAN 100 で MLD snooping を有効にします。

```
[SwitchB-vlan100] mld-snooping enable
[SwitchB-vlan100] quit
```

5)　Switch C を設定します。

グローバルで MLD snooping を有効にします。

```
<SwitchC> system-view
[SwitchC] mld-snooping
```

```
[SwitchC-mld-snooping] quit
```

VLAN 100 を作成し、この VLAN に GigabitEthernet 1/0/1～GigabitEthernet 1/0/5 を割り当てます。

```
[SwitchC] vlan 100
[SwitchC-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/5
```

VLAN 100 で MLD snooping を有効にします。

```
[SwitchC-vlan100] mld-snooping enable
[SwitchC-vlan100] quit
```

IPv6 マルチキャストグループ FF1E::101 のスタティックメンバポートとして GigabitEthernet 1/0/3、GigabitEthernet 1/0/5 を設定します。

```
[SwitchC] interface gigabitethernet 1/0/3
[SwitchC-GigabitEthernet1/0/3] mld-snooping static-group ff1e::101 vlan 100
[SwitchC-GigabitEthernet1/0/3] quit
[SwitchC] interface gigabitethernet 1/0/5
[SwitchC-GigabitEthernet1/0/5] mld-snooping static-group ff1e::101 vlan 100
[SwitchC-GigabitEthernet1/0/5] quit
```

III. 設定の確認

Switch A で VLAN 100 のスタティックルータポートの情報を表示します。

```
[SwitchA] display mld-snooping static-router-port vlan 100
VLAN 100:
  Router ports (1 in total):
    GE1/0/3
```

出力は、Switch A の GigabitEthernet 1/0/3 がスタティックルータポートになっていることを示します。

Switch C で VLAN 100 のスタティック MLD snooping 転送エントリの情報を表示します。

```
[SwitchC] display mld-snooping static-group vlan 100
Total 1 entries).

VLAN 100: Total 1 entries).
  (::, FF1E::101)
    Host ports (2 in total):
      GE1/0/3
      GE1/0/5
```

出力は、Switch C の GigabitEthernet 1/0/3 と GigabitEthernet 1/0/5 が IPv6 マルチキャストグループ FF1E::101 のスタティックメンバポートになっていることを示します。

4.11.3 MLD snooping クエリア設定例

I. ネットワーク要件

図 4-6に示すように設定します。

- ネットワークはレイヤ 2 ネットワークです。
- Source1、Source2 はそれぞれ IPv6 マルチキャストグループ FF1E::101、FF1E::102 に IPv6 マルチキャストデータを送信します。
- Host A、Host C は IPv6 マルチキャストグループ FF1E::101 のレシーバです。Host B、Host D は IPv6 マルチキャストグループ FF1E::102 のレシーバです。
- すべてのレシーバホストで MLDv1 が動作し、すべての Switch で MLDv1 snooping が動作します。Switch A（IPv6 マルチキャストソースにもっとも近い Switch です）は MLD snooping クエリアとして動作します。
- VLAN に IPv6 パケットをフラッディングしないようにすべての Switch で未知の IPv6 マルチキャストデータ廃棄機能を有効にします。

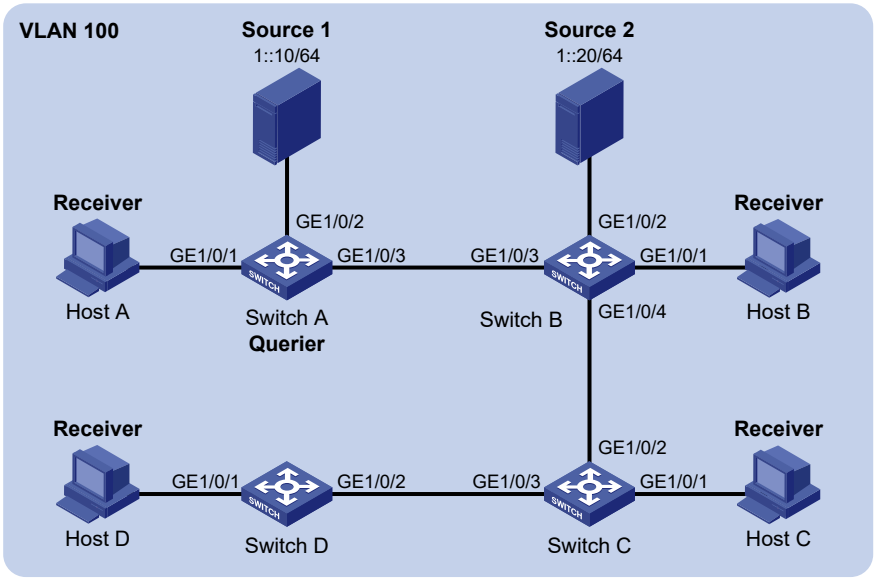


図 4-6 ネットワーク図

II. 設定手順

1)　Switch A を設定します。

グローバルで MLD snooping を有効にします。

```
<SwitchA> system-view
[SwitchA] mld-snooping
[SwitchA-mld-snooping] quit
```

VLAN 100 を作成し、この VLAN に GigabitEthernet 1/0/1～GigabitEthernet 1/0/3 を割り当てます。

```
[SwitchA] vlan 100
```

```
[SwitchA-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/3
```

VLAN 100 で MLD snooping を有効にし、未知の IPv6 マルチキャストデータ廃棄機能を有効にします。

```
[SwitchA-vlan100] mld-snooping enable
[SwitchA-vlan100] mld-snooping drop-unknown
```

VLAN 100 で MLD snooping クエリアを有効にします。

```
[SwitchA-vlan100] MLD-snooping querier
[SwitchA-vlan100] quit
```

2)　Switch B を設定します。

グローバルで MLD snooping を有効にします。

```
<SwitchB> system-view
[SwitchB] mld-snooping
[SwitchB-mld-snooping] quit
```

VLAN 100 を作成し、この VLAN に GigabitEthernet 1/0/1～GigabitEthernet 1/0/4 を割り当てます。

```
[SwitchB] vlan 100
[SwitchB-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/4
```

VLAN100 で MLD snooping を有効にし、未知の IPv6 マルチキャストデータ廃棄機能を有効にします。

```
[SwitchB-vlan100] mld-snooping enable
[SwitchB-vlan100] mld-snooping drop-unknown
[SwitchB-vlan100] quit
```

3)　Switch C を設定します。

グローバルで MLD snooping を有効にします。

```
<SwitchC> system-view
[SwitchC] mld-snooping
[SwitchC-mld-snooping] quit
```

VLAN 100 を作成し、この VLAN に GigabitEthernet 1/0/1～GigabitEthernet 1/0/3 を割り当てます。

```
[SwitchC] vlan 100
[SwitchC-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/3
```

VLAN 100 で MLD snooping を有効にし、未知の IPv6 マルチキャストデータ廃棄機能を有効にします。

```
[SwitchC-vlan100] mld-snooping enable
[SwitchC-vlan100] mld-snooping drop-unknown
[SwitchC-vlan100] quit
```

4)　Switch D を設定します。

グローバルで MLD snooping を有効にします。

```
<SwitchD> system-view
[SwitchD] mld-snooping
[SwitchD-mld-snooping] quit
```

VLAN 100 を作成し、この VLAN に GigabitEthernet 1/0/1～GigabitEthernet 1/0/2 を割り当てます。

```
[SwitchD] vlan 100
[SwitchD-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/2
```

VLAN 100 で MLD snooping を有効にし、未知の IPv6 マルチキャストデータ廃棄機能を有効にします。

```
[SwitchD-vlan100] mld-snooping enable
[SwitchD-vlan100] mld-snooping drop-unknown
[SwitchD-vlan100] quit
```

III. 設定の確認

Switch B の MLD snooping を通して学習した MLD メッセージ、IPv6 PIM hello メッセージの統計情報を表示します。

```
[SwitchB] display mld-snooping statistics
Received MLD general queries:  3
Received MLDv1 specific queries:  0
Received MLDv1 reports:  12
Received MLD dones:  0
Sent     MLDv1 specific queries:  0
Received MLDv2 reports:  0
Received MLDv2 reports with right and wrong records:  0
Received MLDv2 specific queries:  0
Received MLDv2 specific sg queries:  0
Sent     MLDv2 specific queries:  0
Sent     MLDv2 specific sg queries:  0
Received IPv6 PIM hello:  0
Received error MLD messages:  0
```

出力は、Switch A が MLD snooping クエリアとして動作した後、Switch A を除くすべての Switch が MLD general クエリを受信できることを示します。

4.12 MLD snoopingのトラブルシューティング

4.12.1 レイヤ 2 マルチキャスト転送ができない

I. 症状

MLD snooping を通してレイヤ 2 マルチキャスト転送ができません。

II. 分析

MLD snooping が有効になっていません。

III. 解決策

1) **display mld-snooping** コマンドを使用し、MLD snooping の情報を表示します。
2) MLD snooping が有効になっていない場合、system view でグローバルに **mld-snooping** コマンドを使用して MLD snooping を有効にしてください。VLAN view で **mld-snooping enable** コマンドを使用して MLD snooping を有効にしてください。
3) 対応する VLAN でのみ MLD snooping が無効になっている場合、対応する VLAN の VLAN view 上で **mld-snooping enable** コマンドを使用して MLD snooping を有効にしてください。
4) 問題が解決しない場合、NEC に問い合わせてください。

4.12.2 IPv6 マルチキャストグループポリシーが動作しない

I. 症状

ホストは IPv6 マルチキャストグループポリシーで許可されていない IPv6 マルチキャストグループから IPv6 マルチキャストデータを受信することができます。

II. 分析

- IPv6 ACL ルールの設定が間違っています。
- IPv6 マルチキャストグループポリシーが正しく適用されていません 。
- 未知の IPv6 マルチキャストデータ廃棄機能が無効で、IPv6 マルチキャストデータがフラッディングしています。

III. 解決策

1) **display acl ipv6** コマンドで IPv6 ACL ルールの設定を確認してください。実行する IPv6 マルチキャストグループポリシーに IPv6 ACL ルールが一致していることを確認してください。
2) **display this** コマンドを MLD snooping view または対応する interface view で使用して、IPv6 マルチキャストグループポリシーが正しく適用されているかどうかを確認してください。適用されていない場合、**group-policy** コマンドまたは **mld-snooping group-policy** コマンドで IPv6 マルチキャストグループポリシーを正しく適用してください。
3) **display mld-snooping** コマンドを使用して、未知の IPv6 マルチキャストデータ廃棄機能が有効になっているかどうか確認してください。有効になっていない場合、**mld-snooping drop-unknown** コマンドを使用して未知の IPv6 マルチキャストデータ廃棄機能を有効にしてください。
4) 問題が解決しない場合、NEC に問い合わせてください。

目次

このセクションのページは**6-x-x** です。

5章 IPv6マルチキャストVLAN..... 5-1
5.1 概要 5-1
5.2 IPv6マルチキャストVLAN設定作業リスト 5-3
5.3 サブVLANベースIPv6マルチキャストVLANの設定 5-4
5.3.1 設定要件 5-4
5.3.2 設定の制限とガイドライン 5-4
5.3.3 設定手順 5-4
5.4 ポートベースIPv6マルチキャストVLANの設定 5-5
5.4.1 設定要件 5-5
5.4.2 ユーザポートの属性の設定 5-5
5.4.3 IPv6 マルチキャストVLANへのユーザポートの割り当て 5-5
5.5 IPv6マルチキャストVLAN転送エントリの最大数の設定 5-6
5.6 IPv6マルチキャストVLANの表示と維持 5-7
5.7 IPv6マルチキャストVLANの設定例 5-7
5.7.1 サブVLANベースIPv6マルチキャストVLANの設定例 5-7
5.7.2 ポートベースIPv6マルチキャストVLANの設定例 5-11

5章 IPv6 マルチキャスト VLAN

5.1 概要

図 5-1に示すとおり、ホスト A、ホスト B、ホスト C は異なる VLAN に属しており、同じ IPv6 マルチキャストグループに所属しています。

レイヤ 3 装置（Switch A）がグループの IPv6 マルチキャストデータを受信するとき、レイヤ 2 装置（Switch B）にデータのコピーを 3 回送信します。この結果、ネットワークの帯域を浪費するだけでなく、レイヤ 3 装置にも負荷をかけてしまいます。

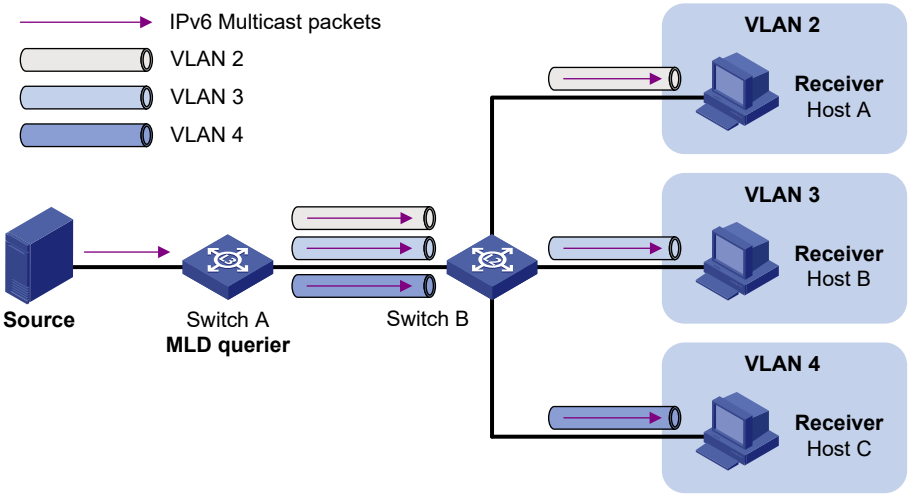


図 5-1 IPv6 マルチキャスト VLAN を使用しないマルチキャストの転送

Switch B で IPv6 マルチキャスト VLAN 機能を設定したのち、Switch A は Switch B の IPv6 マルチキャスト VLAN に IPv6 マルチキャストデータを 1 回コピーして送信します。これによりネットワークの帯域を節約し、レイヤ 3 装置の負荷を軽減します。

IPv6 マルチキャスト VLAN はサブ VLAN ベース IPv6 マルチキャスト VLAN とポートベース IPv6 マルチキャスト VLAN があります。

I. サブ VLAN ベース IPv6 マルチキャスト VLAN

図 5-2では以下のように設定されています。

- ホスト A、ホスト B、ホスト C はそれぞれ VLAN 2、VLAN 3、VLAN 4 に属します。
- Switch B で VLAN10 は IPv6 マルチキャスト VLAN です。

  VLAN2～VLAN4 は VLAN10 のサブ VLAN です。

  MLD snooping がマルチキャスト VLAN とサブ VLAN で有効になっています。

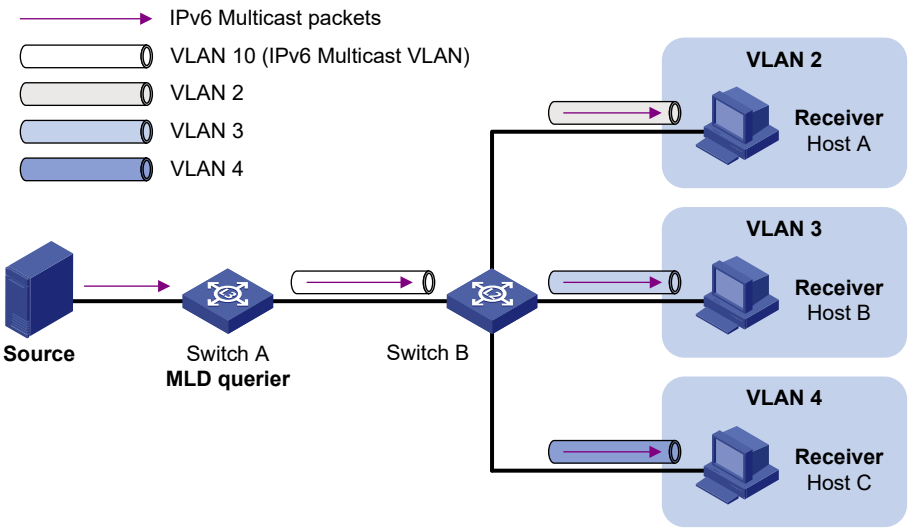


図 5-2 サブ VLAN ベース IPv6 マルチキャスト VLAN

MLD Snooping は IPv6 マルチキャスト VLAN のルータポートとサブ VLAN のメンバポートを管理します。Switch A がマルチキャストソースから IPv6 マルチキャストデータを受信するとき、Switch B で IPv6 マルチキャスト VLAN に IPv6 マルチキャストデータを 1 回のみコピーして送信します。そして、Switch B は IPv6 マルチキャスト VLAN のサブ VLAN へ分割されたコピーを送信します。

II. ポートベース IPv6 マルチキャスト VLAN

図 5-3では以下のように設定されています。

- ホスト A、ホスト B、ホスト C はそれぞれ VLAN 2、VLAN 3、VLAN 4 に属します。
- Switch B で VLAN10 は IPv6 マルチキャスト VLAN です。

  すべてのユーザポートはハイブリッドポートで VLAN10 に割り当てられています。

  IPv6 マルチキャスト VLAN と VLAN2 から VLAN4 で MLD snooping が有効です。

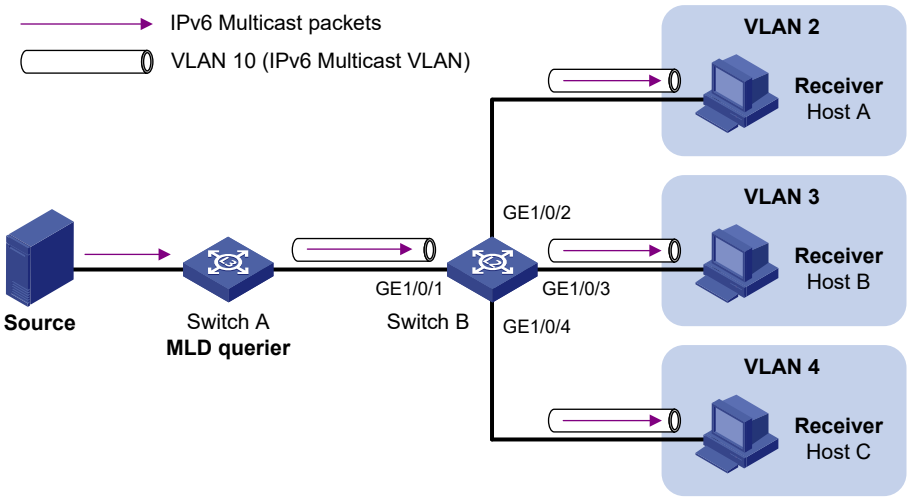


図 5-3 ポートベース IPv6 マルチキャスト VLAN

MLD Snooping は IPv6 マルチキャスト VLAN のルータポートとメンバポートを管理します。Switch A がマルチキャストソースから IPv6 マルチキャストデータを受信するとき、IPv6 マルチキャスト VLAN ID のタグをメッセージにタグづけし、MLD クエリアに送信します。

Switch A がマルチキャストソースから IPv6 マルチキャストデータを受信するとき、Switch B の IPv6 マルチキャスト VLAN にマルチキャストデータを 1 回のみコピーして送信します。そして、Switch B は IPv6 マルチキャスト VLAN のユーザポートへ分割されたコピーを送信します。

5.2 IPv6マルチキャストVLAN設定作業リスト

作業リスト
(必須設定項目)以下の作業の1つを実行します。 • サブVLANベースIPv6マルチキャストVLANの設定 • ポートベースIPv6マルチキャストVLANの設定 　• ユーザポートの属性の設定 　• IPv6マルチキャストVLANへのユーザポートの割り当て
(オプション設定項目) IPv6マルチキャストVLAN転送エントリの最大数の設定

サブ VLAN ベース IPv6 マルチキャスト VLAN とポートベース IPv6 マルチキャスト VLAN の両方を装置に設定する場合、ポートベース IPv6 マルチキャスト VLAN が適用されます。

5.3 サブVLANベースIPv6マルチキャストVLANの設定

IPv6 マルチキャスト VLAN として最初に VLAN を設定する必要があります。そして IPv6 マルチキャスト VLAN にマルチキャストレシーバが含まれるようにサブ VLAN を設定する必要があります。

5.3.1 設定要件

サブ VLAN ベース IPv6 マルチキャスト VLAN の設定をする前に、以下の作業を完了させてください。

- 必要な VLAN を作成します。
- IPv6 マルチキャスト VLAN に設定する VLAN とサブ VLAN で MLD Snooping を有効にします。

5.3.2 設定の制限とガイドライン

サブ VLAN ベース IPv6 マルチキャスト VLAN の設定を行うとき、以下の設定の制限とガイドラインに従ってください。

- IPv6 マルチキャスト VLAN に指定される VLAN が事前に作成されている必要があります。
- IPv6 マルチキャスト VLAN のサブ VLAN に指定される VLAN は事前に作成されている必要があります。他の IPv6 マルチキャスト VLAN のサブ VLAN であってはいけません。
- IPv6 マルチキャスト VLAN の総数は、装置がサポートする最大数を超えてはいけません。
- IPv6 マルチキャスト VLAN と IPv6 マルチキャスト VLAN のサブ VLAN の両方でトランクポートがないことを確認してください。

5.3.3 設定手順

以下にサブ VLAN ベース IPv6 マルチキャスト VLAN を設定する方法を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． VLAN を IPv6 マルチキャスト VLAN として設定し、その view へ移行する	**ipv6 multicast-vlan** *vlan-id*	デフォルト：設定なし
3． サブ VLAN として指定した VLAN を IPv6 マルチキャスト VLAN に割り当てる	**subvlan** *vlan-list*	デフォルト：設定なし

5.4 ポートベースIPv6マルチキャストVLANの設定

IPv6 マルチキャスト VLAN の設定は、イーサネットポートあるいはレイヤ 2 アグリゲートインタフェースにのみ、割り当てることができます。

5.4.1 設定要件

ポートベース IPv6 マルチキャスト VLAN を設定するため、以下の作業を完了させてください。

- 必要な VLAN を作成します。
- IPv6 マルチキャスト VLAN に設定する VLAN で MLD snooping を有効にします。
- 受信ホストを含むすべての VLAN で MLD Snooping を有効にします。

5.4.2 ユーザポートの属性の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. interface view に移行する	**interface** *interface-type interface-number*	―
3. ポートリンクタイプをハイブリッドに設定する	**port link-type hybrid**	デフォルト：アクセス 詳細はコマンドマニュアルのセクション3 *アクセス” VLAN”* を参照してください。
4. ユーザポートが属している VLAN に現在のユーザポートの PVID を指定する	**port hybrid pvid vlan** *vlan-id*	デフォルト：ハイブリッドポートのPVIDはVLAN 1です。 詳細はコマンドマニュアルのセクション3 *アクセス” VLAN”* を参照してください。
5. IPv6 マルチキャスト VLAN を許可する現在のユーザポートを設定し、untag パケットを設定する	**port hybrid vlan** *vlan-id-list* **untagged**	デフォルト：VLAN1のみ許可 詳細はコマンドマニュアルのセクション3 *アクセス” VLAN”* を参照してください。

5.4.3 IPv6 マルチキャスト VLAN へのユーザポートの割り当て

IPv6マルチキャストVLANにユーザポートを割り当てる設定は、IPv6 multicast VLAN viewあるいは interface view のどちらかで行うことができます。

I. 設定の制限とガイドライン

IPv6 マルチキャスト VLAN ポートの設定を行うとき、以下の設定の制限とガイドラインに従ってください。

- IPv6 マルチキャスト VLAN に指定される VLAN が事前に作成されている必要があります。
- ポートは 1 つの IPv6 マルチキャスト VLAN にのみ属することができます。

II. IPv6 multicast VLAN view での IPv6 マルチキャスト VLAN へのポートの割り当て

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. IPv6 VLAN を IPv6 マルチキャスト VLAN として設定し、その view へ移行する	**ipv6 multicast-vlan** *vlan-id*	デフォルト：設定なし
3. IPv6 マルチキャスト VLAN にポートを割り当てる	**port** *interface-list*	デフォルト：IPv6マルチキャストVLANはユーザポートを持っていません。

III. interface view での IPv6 マルチキャスト VLAN へのポートの割り当て

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. IPv6 VLAN を IPv6 マルチキャスト VLAN として設定し、その view へ移行する	**ipv6 multicast-vlan** *vlan-id*	デフォルト：設定なし
3. system view に戻る	**quit**	ー
4. interface view に移行する	**interface** *interface-type interface-number*	ー
5. 現在のポートを IPv6 マルチキャスト VLAN ポートに割り当てる	**ipv6 port multicast-vlan** *vlan-id*	デフォルト : ユーザポートは IPv6マルチキャストVLANに属していません。

5.5 IPv6マルチキャストVLAN転送エントリの最大数の設定

装置で IPv6 マルチキャスト VLAN の転送エントリの最大数を設定することができます。IPv6 マルチキャスト VLAN の転送エントリ数が上限に達すると、いくつかのエントリがタイムアウトするか手動で削除されるまで、装置は IPv6 マルチキャスト VLAN 転送エントリを生成しません。

エントリ数の総数が設定した上限を超過している場合、システムは自動で既存のエントリを削除しません。削除あるいは、新しいエントリを生成しません。手動で超過したエントリを削除することを推奨します。

以下に IPv6 マルチキャスト VLAN の転送エントリの最大数を設定する方法を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. IPv6 マルチキャスト VLAN の転送エントリの最大数を設定する	**ipv6 multicast-vlan entry-limit** *limit*	デフォルト：500

5.6 IPv6マルチキャストVLANの表示と維持

すべての view で **display** コマンドを実行し、user view で **reset** コマンドを実行できます。

操作	コマンド
IPv6マルチキャストVLANの情報を表示する	**display ipv6 multicast-vlan** [*vlan-id*]
IPv6マルチキャストVLANのIPv6マルチキャストグループの情報を表示する	**display ipv6 multicast-vlan group** [*ipv6-source-address* | *ipv6-group-address* | **slot** *slot-number* | **verbose** | **vlan** *vlan-id*] *
IPv6マルチキャスト転送テーブルの情報を表示する	**display ipv6 multicast-vlan forwarding-table** [*ipv6-source-address* [*prefix-length*] | *ipv6-group-address* [*prefix-length*] | **slot** *slot-number* | **subvlan** *vlan-id* | **vlan** *vlan-id*] *
IPv6マルチキャストVLAN内のIPv6マルチキャストグループを削除する	**reset ipv6 multicast-vlan group** [*ipv6-group-address* [*prefix-length*] | *ipv6-source-address* [*prefix-length*] | **vlan** *vlan-id*] *

5.7 IPv6マルチキャストVLANの設定例

5.7.1 サブ VLAN ベース IPv6 マルチキャスト VLAN の設定例

I. ネットワーク要件

本設定例では、Switch B が QX-S5100G シリーズに該当します。

別途、IPv4 マルチキャストルーティングに対応した Switch A が必要です。

図 5-4に示すように設定します。

- レイヤ 3 装置の Switch A で MLDv1 が動作します。Switch A は MLD クエリアです。レイヤ 2 装置の Switch B で MLDv1 Snooping が動作します。
- IPv6 マルチキャストソースは IPv6 マルチキャストデータを IPv6 マルチキャストグループ 224.1.1.1 へ送信します。Host A、Host B、Host C はレシーバです。ホストはそれぞれ VLAN 2～VLAN 4 に所属しています。

以下ができるように Switch B でサブ VLAN ベース IPv6 マルチキャスト VLAN を設定します。

- Switch A は IPv6 マルチキャスト VLAN を通じて IPv6 マルチキャストデータを Switch B へ送信します。
- Switch B は異なるユーザ VLAN に属するレシーバへ IPv6 マルチキャストデータを転送します。

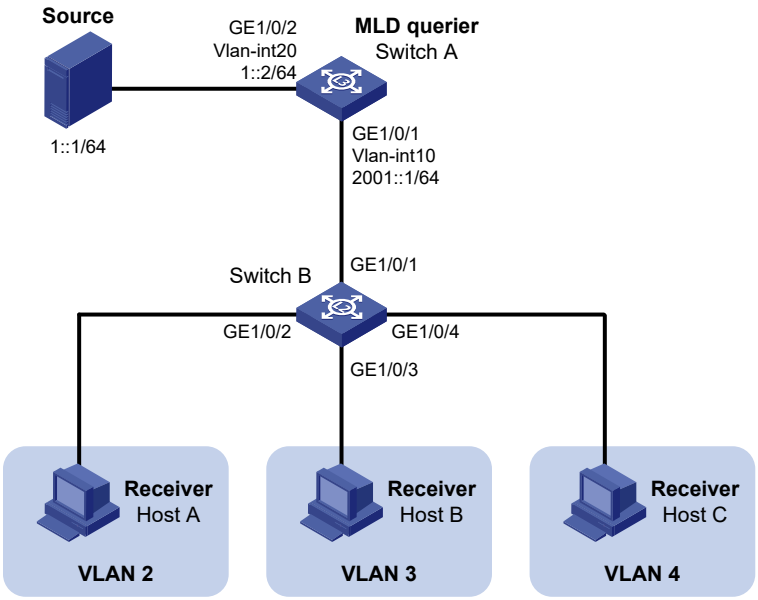


図 5-4 ネットワーク図

II. 設定手順

1)　Switch A を設定します。

グローバルに IPv6 マルチキャストルーティングを有効にします。

```
<SwitchA> system-view
[SwitchA] ipv6 multicast routing
[SwitchA-mrib6] quit
```

VLAN 20 を作成し、GigabitEthernet 1/0/2 を VLAN に割り当てます。

```
[SwitchA] vlan 20
[SwitchA-vlan20] port gigabitethernet 1/0/2
[SwitchA-vlan20] quit
```

VLAN インタフェース 20 に IPv6 アドレスを設定し、IPv6 PIM-SM を有効にします。

```
[SwitchA] interface vlan-interface 20
[SwitchA-Vlan-interface20] ipv6 address 1::2 64
[SwitchA-Vlan-interface20] ipv6 pim sm
[SwitchA-Vlan-interface20] quit
```

VLAN 10 を作成します。

```
[SwitchA] vlan 10
[SwitchA-vlan10] quit
```

ハイブリッドポートとして GigabitEthernet 1/0/1 を設定し、VLAN 10 からのパケットにタグをつけます。

```
[SwitchA] interface gigabitethernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] port link-type hybrid
[SwitchA-GigabitEthernet1/0/1] port hybrid vlan 10 tagged
[SwitchA-GigabitEthernet1/0/1] quit
```

VLAN インタフェース 10 に IPv6 アドレスを設定し、MLD を有効にします。

```
[SwitchA] interface vlan-interface 10
[SwitchA-Vlan-interface10] ipv6 address 2001::1 64
[SwitchA-Vlan-interface10] mld enable
[SwitchA-Vlan-interface10] quit
```

2)　Switch B を設定します。

グローバルに MLD snooping を有効にします。

```
<SwitchB> system-view
[SwitchB] mld-snooping
[SwitchB-mld-snooping] quit
```

VLAN 2 を作成し、GigabitEthernet 1/0/2 を VLAN に割り当て、MLD Snooping を有効にします。

```
[SwitchB] vlan 2
[SwitchB-vlan2] port gigabitethernet 1/0/2
[SwitchB-vlan2] mld-snooping enable
[SwitchB-vlan2] quit
```

VLAN 3 を作成し、GigabitEthernet 1/0/3 を VLAN に割り当て、MLD Snooping を有効にします。

```
[SwitchB] vlan 3
[SwitchB-vlan3] port gigabitethernet 1/0/3
[SwitchB-vlan3] mld-snooping enable
[SwitchB-vlan3] quit
```

VLAN 4 を作成し、GigabitEthernet 1/0/4 を VLAN に割り当て、MLD Snooping を有効にします。

```
[SwitchB] vlan 4
[SwitchB-vlan4] port gigabitethernet 1/0/4
[SwitchB-vlan4] mld-snooping enable
[SwitchB-vlan4] quit
```

VLAN 10 を作成し、VLAN で MLD Snooping を有効にします。

```
[SwitchB] vlan 10
[SwitchB-vlan10] mld-snooping enable
```

```
[SwitchB-vlan10] quit
```

ハイブリッドポートとして GigabitEthernet 1/0/1 を設定し、VLAN 10 からのパケットにタグをつけます。

```
[SwitchB] interface gigabitethernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] port link-type hybrid
[SwitchB-GigabitEthernet1/0/1] port hybrid vlan 10 tagged
[SwitchB-GigabitEthernet1/0/1] quit
```

IPv6 マルチキャスト VLAN として VLAN 10 を設定し、サブ VLAN として VLAN 2～VLAN 4 を設定します。

```
[SwitchB] ipv6 multicast-vlan 10
[SwitchB-ipv6-mvlan-10] subvlan 2 to 4
[SwitchB-ipv6-mvlan-10] quit
```

III. 設定の確認

Switch B ですべての IPv6 マルチキャスト VLAN の情報を表示します。

```
[SwitchB] display ipv6 multicast-vlan
Total 1 IPv6 multicast VLANs.

IPv6 multicast VLAN 10:
  Sub-VLAN list(3 in total):
     2-4
  Port list(0 in total):
```

Switch B で IPv6 マルチキャスト VLAN の IPv6 マルチキャストグループの情報を表示します。

```
[SwitchB] display ipv6 multicast-vlan group
Total 1 entries.

IPv6 multicast VLAN 10: Total 1 entries.
  (::, FF1E::101)
    Sub-VLANs (3 in total):
      VLAN 2
      VLAN 3
      VLAN 4
```

出力では次のことを示します。IPv6 マルチキャストグループ FF1E::101 が IPv6 マルチキャスト VLAN 10 に属しています。IPv6 マルチキャスト VLAN 10 はサブ VLAN2～サブ VLAN4 があります。Switch B は VLAN 10 の IPv6 マルチキャストデータを VLAN 2～VLAN 4 にコピーしています。

5.7.2 ポートベース IPv6 マルチキャスト VLAN の設定例

I. ネットワーク要件

II. 本設定例では、Switch B が QX-S5100G シリーズに該当します。

III. 別途、IPv4 マルチキャストルーティングに対応した Switch A が必要です。

図 5-5に示すように設定します。

- Switch A で MLDv1 が動作します。Switch A は MLD クエリアです。Switch B で MLDv1 Snooping が動作します。
- IPv6 マルチキャストソースは IPv6 マルチキャストデータを IPv6 マルチキャストグループ 224.1.1.1 へ送信します。Host A、Host B、Host C は IPv6 マルチキャストグループのレシーバです。ホストはそれぞれ VLAN 2～VLAN 4 に所属しています。

以下ができるように Switch B でポートベース IPv6 マルチキャスト VLAN を設定します。

- Switch A は IPv6 マルチキャスト VLAN を通じて IPv6 マルチキャストデータを Switch B へ送信します。
- Switch B は異なるユーザ VLAN に属するレシーバへ IPv6 マルチキャストデータを転送します。

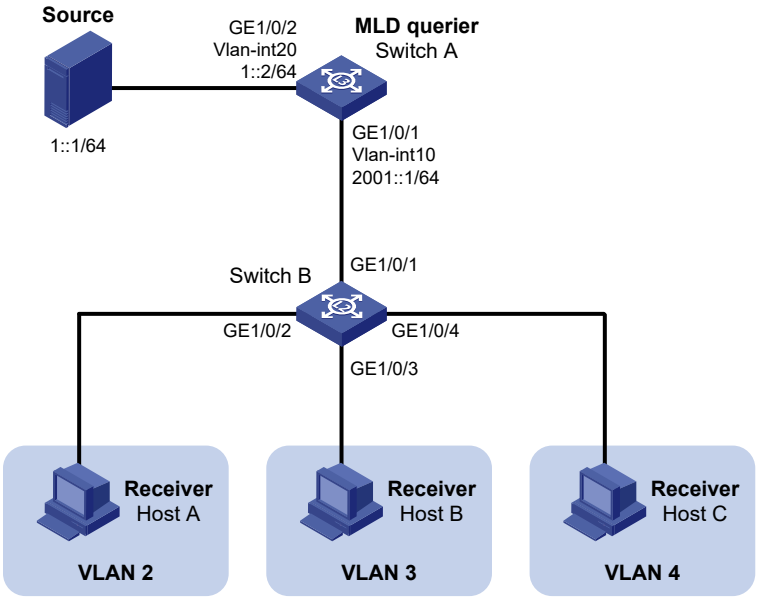


図 5-5 ネットワーク図

IV. 設定手順

1)　Switch A を設定します。

グローバルに IPv6 マルチキャストルーティングを有効にします。

```
<SwitchA> system-view
```

```
[SwitchA] ipv6 multicast routing
[SwitchA-mrib6] quit
```

VLAN 20 を作成し、GigabitEthernet 1/0/2 を VLAN に割り当てます。

```
[SwitchA] vlan 20
[SwitchA-vlan20] port gigabitethernet 1/0/2
[SwitchA-vlan20] quit
```

VLAN インタフェース 20 に IPv6 アドレスを設定し、IPv6 PIM-SM を有効にします。

```
[SwitchA] interface vlan-interface 20
[SwitchA-Vlan-interface20] ipv6 address 1::2 64
[SwitchA-Vlan-interface20] ipv6 pim sm
[SwitchA-Vlan-interface20] quit
```

VLAN10 を作成し、GigabitEthernet 1/0/1 を VLAN に割り当てます。

```
[SwitchA] vlan 10
[SwitchA-vlan10] port gigabitethernet 1/0/1
[SwitchA-vlan10] quit
```

VLAN インタフェース 10 に IPv6 アドレスを設定し、MLD を有効にします。

```
[SwitchA] interface vlan-interface 10
[SwitchA-Vlan-interface10] ipv6 address 2001::1 64
[SwitchA-Vlan-interface10] mld enable
[SwitchA-Vlan-interface10] quit
```

2)　Switch B を設定します。

グローバルに MLD Snooping を有効にします。

```
<SwitchB> system-view
[SwitchB] mld-snooping
[SwitchB-mld-snooping] quit
```

VLAN 10 を作成し、GigabitEthernet 1/0/1 を VLAN に割り当て、MLD Snooping を有効にします。

```
[SwitchB] vlan 10
[SwitchB-vlan10] port gigabitethernet 1/0/1
[SwitchB-vlan10] mld-snooping enable
[SwitchB-vlan10] quit
```

VLAN 2 を作成し、MLD Snooping を有効にします。

```
[SwitchB] vlan 2
[SwitchB-vlan2] mld-snooping enable
```

```
[SwitchB-vlan2] quit
```

VLAN 3 を作成し、MLD Snooping を有効にします。

```
[SwitchB] vlan 3
[SwitchB-vlan3] mld-snooping enable
[SwitchB-vlan3] quit
```

VLAN 4 を作成し、MLD Snooping を有効にします。

```
[SwitchB] vlan 4
[SwitchB-vlan4] mld-snooping enable
[SwitchB-vlan4] quit
```

ハイブリッドポートとして GigabitEthernet 1/0/2 を設定し、ハイブリッドポートの PVID を 2 に設定します。

```
[SwitchB] interface gigabitethernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] port link-type hybrid
[SwitchB-GigabitEthernet1/0/2] port hybrid pvid vlan 2
```

VLAN 2、VLAN 10 に GigabitEthernet 1/0/2 を割り当て、VLAN 2、VLAN 10 からのパケットからタグを外します。

```
[SwitchB-GigabitEthernet1/0/2] port hybrid vlan 2 untagged
[SwitchB-GigabitEthernet1/0/2] port hybrid vlan 10 untagged
[SwitchB-GigabitEthernet1/0/2] quit
```

ハイブリッドポートとして GigabitEthernet 1/0/3 を設定し、ハイブリッドポートの PVID を 3 に設定します。

```
[SwitchB] interface gigabitethernet 1/0/3
[SwitchB-GigabitEthernet1/0/3] port link-type hybrid
[SwitchB-GigabitEthernet1/0/3] port hybrid pvid vlan 3
```

VLAN 3、VLAN 10 に GigabitEthernet 1/0/3 を割り当て、VLAN 3、VLAN 10 からのパケットからタグを外します。

```
[SwitchB-GigabitEthernet1/0/3] port hybrid vlan 3 untagged
[SwitchB-GigabitEthernet1/0/3] port hybrid vlan 10 untagged
[SwitchB-GigabitEthernet1/0/3] quit
```

ハイブリッドポートとして GigabitEthernet 1/0/4 を設定し、ハイブリッドポートの PVID を 4 に設定します。

```
[SwitchB] interface gigabitethernet 1/0/4
[SwitchB-GigabitEthernet1/0/4] port link-type hybrid
[SwitchB-GigabitEthernet1/0/4] port hybrid pvid vlan 4
```

VLAN 4、VLAN 10 に GigabitEthernet 1/0/4 を割り当て、VLAN 4、VLAN 10 からのパケットからタグを外します。

```
[SwitchB-GigabitEthernet1/0/4] port hybrid vlan 4 untagged
[SwitchB-GigabitEthernet1/0/4] port hybrid vlan 10 untagged
[SwitchB-GigabitEthernet1/0/4] quit
```

IPv6 マルチキャスト VLAN として VLAN 10 を設定します。

```
[SwitchB] ipv6 multicast-vlan 10
```

GigabitEthernet 1/0/2 と GigabitEthernet 1/0/3 に VLAN 10 を割り当てます。

```
[SwitchB-ipv6-mvlan-10] port gigabitethernet 1/0/2 to gigabitethernet 1/0/3
[SwitchB-ipv6-mvlan-10] quit
```

GigabitEthernet 1/0/4 に VLAN 10 を割り当てます。

```
[SwitchB] interface gigabitethernet 1/0/4
[SwitchB-GigabitEthernet1/0/4] ipv6 port multicast-vlan 10
[SwitchB-GigabitEthernet1/0/4] quit
```

V. 設定の確認

Switch B の IPv6 マルチキャスト VLAN の情報を表示します。

```
[SwitchB] display ipv6 multicast-vlan
Total 1 IPv6 multicast VLANs.

IPv6 multicast VLAN 10:
  Sub-VLAN list(0 in total):
  Port list(0 in total):
    GE1/0/2
    GE1/0/3
    GE1/0/4
```

Switch B でダイナミックマルチキャストグループの MLD Snooping 転送エントリを表示します。

```
[SwitchB] display mld-snooping group
Total 1 entries.

VLAN 10: Total 1 entries.
  (::, FF1E::101)
    Host slots (0 in total):
    Host ports (3 in total):
      GE1/0/2          (00:03:23)
      GE1/0/3          (00:04:07)
      GE1/0/4          (00:04:16)
```

出力では、MLD Snooping が VLAN 10 のユーザポートを維持していることを示します。Switch B はユーザポートを通して VLAN 10 の IPv6 マルチキャストデータを転送します。

QX-S5100G シリーズ Ethernet スイッチ

オペレーションマニュアル

7.MCE

本マニュアルは以下に示す章で構成されています。

01-MCE

02-IPv6 MCE

目次

このセクションのページは **7-x-x** です。

1 章 MCE 1-1
1.1 MCE の概要 1-1
1.2 MCE 設定作業リスト 1-2
1.3 VPN インスタンスの設定 1-2
1.3.1 VPN インスタンスの作成 1-2
1.3.2 VPN インスタンスとインタフェースの関連づけ 1-3
1.3.3 VPN インスタンスのルート関連属性の設定 1-3
1.4 MCE のルーティングの設定 1-4
1.4.1 MCE と VPN サイト間のルーティングの設定 1-4
1.5 MCE の表示と維持 1-6
1.6 MCE 設定例 1-7
1.6.1 PE に VPN ルートを通知するために OSPF を使用する MCE の設定例 1-7

1章 MCE

この章は MCE(Multi-VPN-Instance CE)の設定についてのみ記載します。ルーティングプロトコルについての詳細は、オペレーションマニュアルのセクション 5 *ルーティングプロトコル*を参照してください。

1.1 MCEの概要

MCE(Multi-VPN-Instance CE)は CE で複数の VPN インスタンスを作成することができます。VPN インスタンスは独立したルーティングテーブルと、サービスの隔離を行うアドレス空間があります。

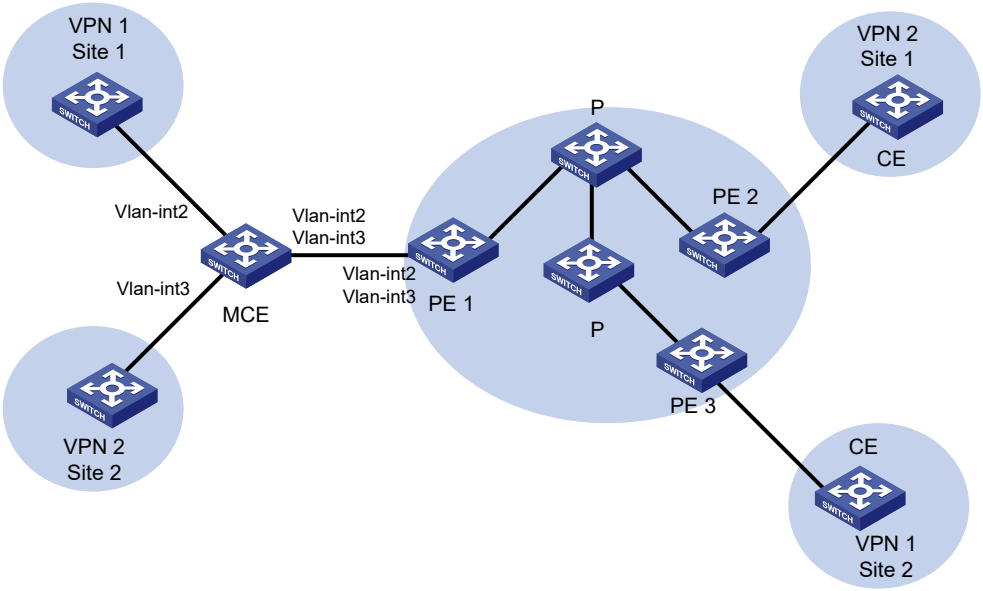


図 1-1 MCE のネットワーク図

図 1-1 に示すように、MCE は VPN サイトと PE1 のプライベートルートを交換し、VPN インスタンスに対応するルーティングテーブルにプライベートルートを追加します。

- **MCE と VPN サイト間のルート交換**－MCE 上で VPN インスタンス VPN1 と VPN インスタンス VPN2 を作成します。VLAN インタフェース 2 に VPN1 を割り当て、VLAN インタフェース 3 に VPN2 を割り当てます。MCE は受信する VLAN インタフェースに隣接する VPN インスタンスのルーティングテーブルに受信したルートを追加します。
- **MCE と PE 間のルート交換**－MCE は VLAN2、VLAN3 を許可するトランクのリンクを通して PE1 に接続します。PE1 で VPN インスタンス VPN1、VPN インスタンス VPN2 を作成し、VLAN インタフェース 2 を VPN1 に割り当て、VLAN インタフェース 3 を VPN2 に割り当てます。MCE と PE は受信したルートを受信 VLAN インタフ

ェースに隣接する VPN インスタンスのルーティングテーブルに受信ルートを追加します。

MCE と VPN サイト間および MCE と PE 間でスタティックルート、RIP、OSPF を設定することができます。

メモ:

プライベートネットワークの DHCP クライアントにダイナミック IP アドレスの割り当てを行うため、MCE に DHCP サーバあるいは DHCP リレーエージェントを設定することができます。DHCP サーバとして動作する MCE では、異なるプライベートネットワークに IP アドレスを重複することができません。

1.2 MCE設定作業リスト

作業リスト
VPNインスタンスの設定: 1. (必須設定項目) VPN インスタンスの作成 2. (必須設定項目) VPN インスタンスとインタフェースの関連づけ 3. (オプション設定項目) VPN インスタンスのルート関連属性の設定
MCEのルーティングの設定: ● (必須設定項目) MCEとVPNサイト間のルーティングの設定

1.3 VPNインスタンスの設定

VPN インスタンスを設定することによって、パブリックネットワークルートから VPN ルートを隔離し、ほかの VPN からも隔離します。VPN インスタンスの設定は、すべての MCE ネットワークで必要となります。

1.3.1 VPN インスタンスの作成

VPN インスタンスは VPN メンバーシップと関連したサイトのルーティングルールが集合したものです。VPN インスタンスは 1 つの VPN に対応しない可能性があります。

以下に VPN インスタンスの作成の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. VPN インスタンスを作成し、VPN instance view に移行する	**ip vpn-instance** *vpn-instance-name*	デフォルト：設定なし
3. VPN インスタンスの RD を設定する	**route-distinguisher** *route-distinguisher*	デフォルト：設定なし
4. (オプション設定項目) VPN インスタンスの記述を設定する	**description** *text*	デフォルト：設定なし

1.3.2 VPN インスタンスとインタフェースの関連づけ

VPN インスタンスの作成、設定をしたのち、VPN インスタンスをサイトおよび PE に接続する MCE インタフェースに関連づけます。

以下に VPN インスタンスとインタフェースの関連づけの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． interface view に移行する	**interface** *interface-type interface-number*	―
3． インタフェースを VPN インスタンスに関連づける	**ip binding vpn-instance** *vpn-instance-name*	デフォルト：設定なし **ip binding vpn-instance**コマンドは現在のインタフェースに設定されたIPアドレス設定を削除します。VPNインスタンスとインタフェースの関連づけをした後、再度IPアドレスを設定してください。

1.3.3 VPN インスタンスのルート関連属性の設定

以下に VPN インスタンスのルート関連属性の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． VPN instance view あるいは IPv4 VPN view に移行する	● VPN instance viewに移行する: **ip vpn-instance** *vpn-instance-name* ● IPv4 VPN viewに移行する: 1． **ip vpn-instance** *vpn-instance-name* 2． **address-family ipv4**	VPN instance viewでの設定はIPv6 VPNとIPv6 VPNの両方に適用されます。IPv4 VPNはVPN instance view での設定よりIPv4 VPN viewでの設定が優先されます。
3． VPN インスタンスを VPN ターゲットと関連づける	**vpn-target** *vpn-target*&<1-8> [**both** | **export-extcommunity** | **import-extcommunity**]	デフォルト：設定なし
4． VPN インスタンスの最大ルート数を設定する	**routing-table limit** *number* { *warn-threshold* | **simply-alert** }	デフォルト：制限なし VPNインスタンスの最大ルート数を設定すると、PEに再配信されてからのルートが過大となることを防止します。

操作	コマンド	補足
5. 受信ルートポリシーを設定する	**import route-policy** *route-policy*	デフォルト：すべてのルートが通信可能です。 ルーティングポリシーがすでに存在していることを確認してください。ルーティングポリシーの詳細は、オペレーションマニュアルのセクション5 *ルーティングプロトコル"ルーティングポリシー"*を参照してください。
6. 送信ルートポリシーを設定する	**export route-policy** *route-policy*	デフォルト：すべてのルートが通信可能です。 ルーティングポリシーがすでに存在していることを確認してください。ルーティングポリシーの詳細は、オペレーションマニュアルのセクション5 *ルーティングプロトコル"ルーティングポリシー"*を参照してください。

1.4 MCEのルーティングの設定

MCE はルート情報の隔離を行います。MCE ルーティング設定は以下があります。

- MCE-VPN サイトルーティング設定
- MCE-PE ルーティング設定

PE で以下のことを行ってください。

- ルート計算によるルート損失を避けるため、ルーティングループの検出を無効にしてください。
- システムリソースを削減するため、ルーティングプロトコルでルートの再配信を無効にしてください。

MCE のルーティングを設定する前に MCE で VPN インスタンスを設定し、VPN サイトと PE に接続されたインタフェースの VPN インスタンスを割り当ててください。

1.4.1 MCE と VPN サイト間のルーティングの設定

MCE と VPN サイト間でスタティックルート、RIP、OSPF を設定することができます。

I. MCE と VPN サイト間のスタティックルーティングの設定

MCE はスタティックルートによって VPN サイトに到達します。伝統的な CE のスタティックルートは、全体に影響します。従って VPN 間をまたぐアドレスをサポートしません。異なる VPN インスタンスが互いに隔離できるように、VPN インスタンスにスタティックルートを割り当てます。

以下に MCE-VPN サイト間のスタティックルートの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. VPN インスタンスにスタティックルートを設定する	**ip route-static vpn-instance** *s-vpn-instance-name dest-address* { *mask-length* | *mask* } { *interface-type interface-number* [*next-hop-address*] | *next-hop-address* [**public**] [**track** *track-entry-number*] | **vpn-instance** *d-vpn-instance-name next-hop-address* [**track** *track-entry-number*] } [**permanent**] [**preference** *preference-value*] [**tag** *tag-value*] [**description** *description-text*]	デフォルト：設定なし この設定はMCEで行ってください。VPNサイトでは通常のスタティックルートを設定してください。
3. (オプション設定項目) スタティックルートのデフォルト優先度を設定する	**ip route-static default-preference** *default-preference-value*	デフォルト：60

II. MCE と VPN サイト間の RIP の設定

RIP プロセスを、パブリックネットワークあるいは 1 つの VPN インスタンスのみ結びつけて使用することができます。どの VPN インスタンスにも結びつけられていない RIP プロセスは、パブリックネットワークに属していることとなります。

RIP プロセスを VPN インスタンスに関連づけることで、異なる VPN のルートを分離することができます。RIP の詳細は、オペレーションマニュアルのセクション 5 *ルーティングプロトコル "RIP"*を参照してください。

以下に MCE-VPN サイト間の RIP の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. VPN インスタンスの RIP プロセスを作成し、RIP view に移行する	**rip** [*process-id*] **vpn-instance** *vpn-instance-name*	この設定はMCEで行ってください。VPNサイトでは共通のRIPプロセスを作成してください。
3. 指定されたネットワークに接続されたインタフェースで RIP を有効にする	**network** *network-address*	デフォルト：無効
4. PE によって通知されたリモートサイトのルートを RIP に再配信する	**import-route** { **ospf** | **rip** } [*process-id* | **all-processes**] [**allow-direct** | **cost** *cost-value* | **route-policy** *route-policy-name* | **tag** *tag*]*	デフォルト：設定なし
5. (オプション設定項目) 再配信されたルートのデフォルトコストを設定する	**default cost** *cost*	デフォルト：0

III. MCE と VPN サイト間の OSPF の設定

OSPF プロセスを、パブリックネットワークあるいは 1 つの VPN インスタンスのみ結びつけて使用することができます。どのVPNインスタンスにも結びつけられていないOSPFプロセスは、パブリックネットワークに属していることとなります。

OSPF プロセスを VPN インスタンスに関連づけることで、異なる VPN のルートを分離することができます。OSPF の詳細は、オペレーションマニュアルのセクション 5 *ルーティングプロトコル "OSPF"*を参照してください。

以下に MCE-VPN サイト間の OSPF の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. VPN インスタンスの OSPF を作成し、OSPF view に移行する	**ospf** [*process-id* | **router-id** *router-id* | **vpn-instance** *vpn-instance-name*]*	この設定はMCEで行ってください。VPNサイトは通常のOSPFを設定してください。VPNインスタンスに設定されたOSPFプロセスはsystem viewで設定されたパブリックネットワークのルータIDを使用しません。そのためルータIDを設定する必要があります。OSPFプロセスは1つのVPNインスタンスのみ所属することができますが、1つのVPNインスタンスは複数のOSPFプロセスを使用することができます。
3. PE によって通知されたリモートサイトのルートを OSPF に再配信する	**import-route** *protocol* [*process-id* | **all-processes**] [**cost** *cost* | **route-policy** *route-policy-name* | **tag** *tag* | **type** *type*]*	デフォルト：設定なし
4. OSPF エリアを作成し、OSPF area view に移行する	**area** *area-id*	デフォルト：設定なし
5. 指定したネットワークエリアのインタフェースに OSPF を有効にする	**network** *ip-address wildcard-mask*	デフォルト：設定なし

1.5 MCEの表示と維持

すべての view で **display** コマンドが実行できます。

操作	コマンド
VPNインスタンスの情報を表示する	**display ip vpn-instance** [**instance-name** *vpn-instance-name*]

VPN インスタンスのルーティング情報の表示、ルーティングセッションの維持など、ほかの MCE に関するコマンドの表示、維持の詳細については、コマンドマニュアルのセクション 5 *ルーティングプロトコル*を参照してください。

1.6 MCE設定例

1.6.1 PE に VPN ルートを通知するために OSPF を使用する MCE の設定例

I. ネットワーク要件

図 1-2 に示すように、VPN2 は OSPF が動作します。異なる VPN からルートを隔離させ、OSPF を通して PE1 に VPN ルートを通知するように、MCE を設定します。

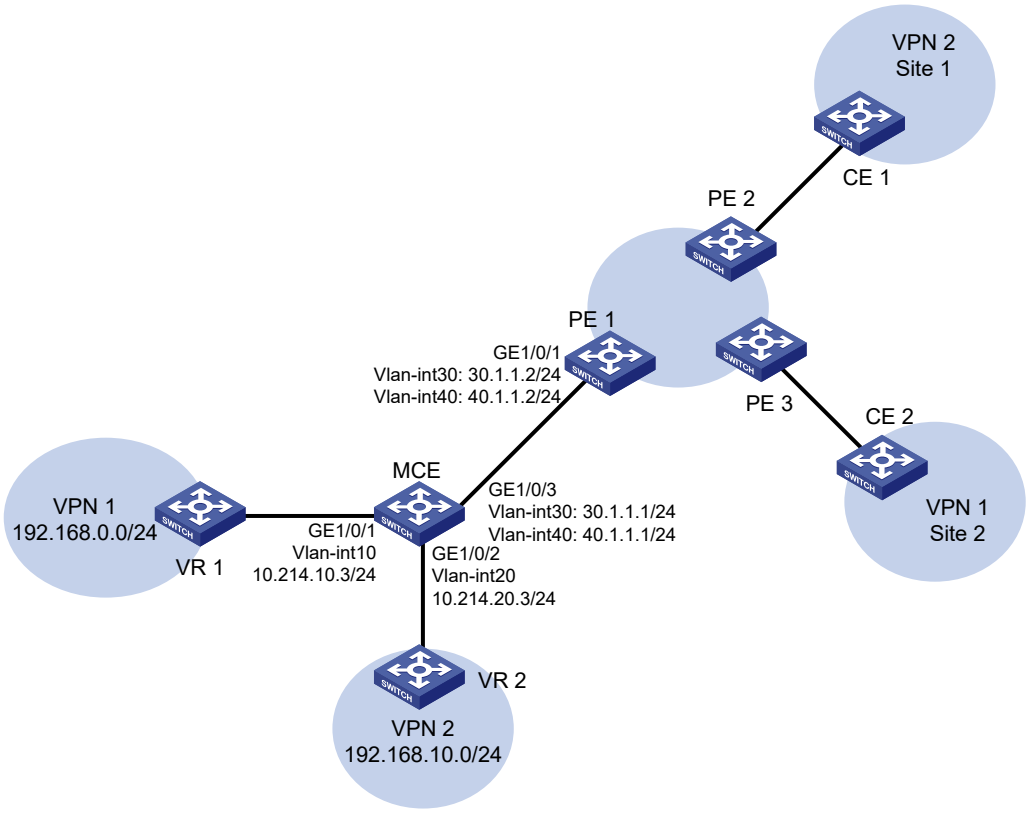


図 1-2 ネットワーク図

II. 設定手順

MCE のシステム名を MCE に設定し、VPN1、VPN2 のシステム名を VR1、VR2 に設定し、PE1 のシステム名を PE1 に設定します。

1)　MCE と PE 1 の VPN インスタンスを設定します。

MCE で VPN インスタンス **vpn1**、**vpn2** を設定し、RD、各 VPN インスタンスのルートターゲットを指定します。

```
<MCE> system-view
[MCE] ip vpn-instance  vpn1
```

```
[MCE-vpn-instance-vpn1] route-distinguisher 10:1
[MCE-vpn-instance-vpn1] vpn-target 10:1
[MCE-vpn-instance-vpn1] quit
[MCE] ip vpn-instance vpn2
[MCE-vpn-instance-vpn2] route-distinguisher 20:1
[MCE-vpn-instance-vpn2] vpn-target 20:1
[MCE-vpn-instance-vpn2] quit
```

VLAN10 を作成し、GigabitEthernet 1/0/1 に割り当てます。

```
[MCE] vlan 10
[MCE-vlan10] port gigabitethernet 1/0/1
[MCE-vlan10] quit
```

VLAN インタフェース 10 を作成し、VPN インスタンス **vpn1** に割り当てます。

```
[MCE] interface vlan-interface 10
[MCE-Vlan-interface10] ip binding vpn-instance vpn1
```

VLAN インタフェース 10 の IP アドレスを設定します。

```
[MCE-Vlan-interface10] ip address 10.214.10.3 24
[MCE-Vlan-interface10] quit
```

VLAN20 を作成し、GigabitEthernet 1/0/2 に割り当てます。

```
[MCE] vlan 20
[MCE-vlan20] port gigabitethernet 1/0/2
[MCE-vlan20] quit
```

VLAN インタフェース 20 を作成し、VPN インスタンス **vpn2** に割り当てます。

```
[MCE] interface vlan-interface 20
[MCE-Vlan-interface20] ip binding vpn-instance vpn2
```

VLAN インタフェース 20 の IP アドレスを設定します。

```
[MCE-Vlan-interface20] ip address 10.214.20.3 24
[MCE-Vlan-interface20] quit
```

PE1 で VPN インスタンス **vpn1**、VPN インスタンス **vpn2** を設定し、RD、各 VPN インスタンスのルートターゲットを指定します。

```
<PE1> system-view
[PE1] ip vpn-instance vpn1
[PE1-vpn-instance-vpn1] route-distinguisher 10:1
[PE1-vpn-instance-vpn1] vpn-target 10:1
[PE1-vpn-instance-vpn1] quit
```

```
[PE1] ip vpn-instance  vpn2
[PE1-vpn-instance-vpn2]  route-distinguisher  20:1
[PE1-vpn-instance-vpn2]  vpn-target  20:1
[PE1-vpn-instance-vpn2]  quit
```

2)　MCE と VPN サイト間のルーティングを設定します。

MCE は直接 VPN1 に接続し、VPN1 でルーティングプロトコルが無効であるため、スタティックルートを設定します。

VR1 で MCE に接続しているインタフェースに IP アドレス 10.214.10.2/24 を設定し、VPN1 に接続しているインタフェースに IP アドレス 192.168.0.1/24 を設定します。VLAN にポートを追加します。(詳細は省略します。)

VR1 でネクストホップ 10.214.10.3 としてデフォルトルートを設定します。

```
<VR1> system-view
[VR1] ip route-static 0.0.0.0 0.0.0.0 10.214.10.3
```

MCE でスタティックルート 192.168.0.0/24 を設定し、ネクストホップ 10.214.10.2 を指定し、VPN インスタンス **vpn1** にスタティックルートを割り当てます。

```
[MCE] ip route-static vpn-instance  vpn1  192.168.0.0  24 10.214.10.2
```

MCE で VPN インスタンス **vpn1** のルーティング情報を表示します。

```
[MCE] display ip routing-table  vpn-instance  vpn1

Destinations : 13        Routes : 13

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
0.0.0.0/32          Direct 0    0            127.0.0.1       InLoop0
10.214.10.0/24      Direct 0    0            10.214.10.3     Vlan10
10.214.10.0/32      Direct 0    0            10.214.10.3     Vlan10
10.214.10.3/32      Direct 0    0            127.0.0.1       InLoop0
10.214.10.255/32    Direct 0    0            10.214.10.3     Vlan10
127.0.0.0/8         Direct 0    0            127.0.0.1       InLoop0
127.0.0.0/32        Direct 0    0            127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0            127.0.0.1       InLoop0
127.255.255.255/32  Direct 0    0            127.0.0.1       InLoop0
192.168.0.0/24      Static 60   0            10.214.10.2     Vlan10
224.0.0.0/4         Direct 0    0            0.0.0.0         NULL0
224.0.0.0/24        Direct 0    0            0.0.0.0         NULL0
255.255.255.255/32  Direct 0    0            127.0.0.1       InLoop0
```

出力では MCE に VPN インスタンス **vpn1** のスタティックルートがあることを示しています。

VPN2 で OSPF を動作させ、OSPF プロセス 20 を作成し、MCE の VPN インスタンス **vpn2** に割り当てます。VPN インスタンス **vpn2** のルートを学習し、ルーティングテーブルに追加できるようにします。

```
[MCE] ospf 2 vpn-instance  vpn2
```

サブネット 10.214.20.0 を通知します。

```
[MCE-ospf-2]  area  0
[MCE-ospf-2-area-0.0.0.0]  network  10.214.20.0  0.0.0.255
[MCE-ospf-2-area-0.0.0.0]  quit
```

```
[MCE-ospf-2] quit
```

VR2 で MCE に接続されているインタフェースに IP アドレス 10.214.20.2/24 を割り当て、VPN2 に接続されているインタフェースに IP アドレス 192.168.10.1/24 を割り当てます。(詳細は省略します。)

OSPF プロセス 2 を設定し、サブネット 192.168.10.0、10.214.20.0 を通知します。

```
<VR2> system-view
[VR2] ospf 2
[VR2-ospf-2] area 0
[VR2-ospf-2-area-0.0.0.0] network 192.168.10.0 0.0.0.255
[VR2-ospf-2-area-0.0.0.0] network 10.214.20.0 0.0.0.255
[VR2-ospf-2-area-0.0.0.0] quit
[VR2-ospf-2] quit
```

MCE で VPN インスタンス **vpn2** のルーティング情報を表示します。

```
[MCE] display ip routing-table vpn-instance vpn2

Destinations : 13        Routes : 13

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
0.0.0.0/32          Direct 0    0            127.0.0.1       InLoop0
10.214.20.0/24      Direct 0    0            10.214.20.3     Vlan20
10.214.20.0/32      Direct 0    0            10.214.20.3     Vlan20
10.214.20.3/32      Direct 0    0            127.0.0.1       InLoop0
10.214.20.255/32    Direct 0    0            10.214.20.3     Vlan20
127.0.0.0/8         Direct 0    0            127.0.0.1       InLoop0
127.0.0.0/32        Direct 0    0            127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0            127.0.0.1       InLoop0
127.255.255.255/32  Direct 0    0            127.0.0.1       InLoop0
192.168.10.0/24     OSPF   10   2            10.214.20.2     Vlan20
224.0.0.0/4         Direct 0    0            0.0.0.0         NULL0
224.0.0.0/24        Direct 0    0            0.0.0.0         NULL0
255.255.255.255/32  Direct 0    0            127.0.0.1       InLoop0
```

出力で MCE は VPN2 のプライベートルートを学習していることを示します。MCE は 2 つの異なるルーティングテーブルに分けて VPN1 と VPN2 のルートを維持します。このようにして異なる VPN からのルートを隔離します。

3)　MCE と PE 1 間のルーティングを設定します。

MCE は PE の GigabitEthernet 1/0/1 に接続するため、GigabitEthernet 1/0/3 を使用します。2 つのポートはトランクポートとして設定し、VLAN タグ 30、40 のパケットの送信を許可するように設定します。

```
[MCE] interface gigabitethernet 1/0/3
[MCE-GigabitEthernet1/0/3] port link-type trunk
[MCE-GigabitEthernet1/0/3] port trunk permit vlan 30 40
[MCE-GigabitEthernet1/0/3] quit
```

PE で GigabitEthernet 1/0/1 を設定します。

```
[PE1] interface gigabitethernet 1/0/1
[PE1-GigabitEthernet1/0/1] port link-type trunk
```

```
[PE1-GigabitEthernet1/0/1] port trunk permit vlan 30 40
[PE1-GigabitEthernet1/0/1] quit
```

MCE で VLAN30、VLAN インタフェース 30 を作成し、VPN インスタンス **vpn1** に VLAN インタフェースを割り当て、IP アドレスを設定します。

```
[MCE] vlan 30
[MCE-vlan30] quit
[MCE] interface vlan-interface 30
[MCE-Vlan-interface30] ip binding vpn-instance vpn1
[MCE-Vlan-interface30] ip address 30.1.1.1 24
[MCE-Vlan-interface30] quit
```

MCE で VLAN40、VLAN インタフェース 40 を作成し、VPN インスタンス **vpn2** に VLAN インタフェースを割り当て、IP アドレスを設定します。

```
[MCE] vlan 40
[MCE-vlan40] quit
[MCE] interface vlan-interface 40
[MCE-Vlan-interface40] ip binding vpn-instance vpn2
[MCE-Vlan-interface40] ip address 40.1.1.1 24
[MCE-Vlan-interface40] quit
```

PE1 で VLAN30、VLAN インタフェース 30 を作成し、VPN インスタンス **vpn1** に VLAN インタフェースを割り当て、IP アドレスを設定します。

```
[PE1] vlan 30
[PE1-vlan30] quit
[PE1] interface vlan-interface 30
[PE1-Vlan-interface30] ip binding vpn-instance vpn1
[PE1-Vlan-interface30] ip address 30.1.1.2 24
[PE1-Vlan-interface30] quit
```

PE1 で VLAN40、VLAN インタフェース 40 を作成し、VPN インスタンス **vpn2** に VLAN インタフェースを割り当て、IP アドレスを設定します。

```
[PE1] vlan 40
[PE1-vlan40] quit
[PE1] interface vlan-interface 40
[PE1-Vlan-interface40] ip binding vpn-instance vpn2
[PE1-Vlan-interface40] ip address 40.1.1.2 24
[PE1-Vlan-interface40] quit
```

MCE 用としてループバックインタフェース 0 に IP アドレス 101.101.10.1 を設定し、PE1 用として IP アドレス 100.100.10.1 を設定します。MCE と PE1 のルータ ID としてループバックインタフェースの IP アドレスを指定します。(詳細は省略します。)

MCE で OSPF プロセス 10 を有効にし、VPN インスタンス **vpn1** に割り当てます。

```
[MCE] ospf 10 router-id 101.101.10.1 vpn-instance vpn1
```

OSPF ルーティングループ検出を無効にします。

```
[MCE-ospf-10] vpn-instance-capability simple
```

ドメイン ID を 10 に設定します。

```
[MCE-ospf-10] domain-id 10
```

MCE でエリア 0 のサブネット 30.1.1.0 を通知し、VPN1 のスタティックルートを再配信します。

```
[MCE-ospf-10] area 0
[MCE-ospf-10-area-0.0.0.0] network 30.1.1.0 0.0.0.255
[MCE-ospf-10-area-0.0.0.0] quit
[MCE-ospf-10] import-route static
```

PE1 で OSPF プロセス 10 を有効にし、VPN インスタンス **vpn1** に割り当てます。

```
[PE1] ospf 10 router-id 100.100.10.1 vpn-instance vpn1
```

ドメイン ID を 10 に設定します。

```
[PE1-ospf-10] domain-id 10
```

エリア 0 のサブネット 30.1.1.0 を通知します。

```
[PE1-ospf-10] area 0
[PE1-ospf-10-area-0.0.0.0] network 30.1.1.0 0.0.0.255
[PE1-ospf-10-area-0.0.0.0] quit
[PE1-ospf-10] quit
```

MCE と PE1 間で OSPF プロセス 20 を同様に設定し、VPN2 のルーティング情報を再配信します。(詳細は省略します。)

III. 設定の確認

PE1 で VPN1 のルーティングテーブルを表示します。出力は VPN1 のスタティックルートが PE1 の OSPF ルーティングテーブルに再配信されていることを示します。

```
[PE1] display ip routing-table vpn-instance vpn1

Destinations : 13        Routes : 13

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
0.0.0.0/32          Direct 0    0            127.0.0.1       InLoop0
30.1.1.0/24         Direct 0    0            30.1.1.2        Vlan30
30.1.1.0/32         Direct 0    0            30.1.1.2        Vlan30
30.1.1.2/32         Direct 0    0            127.0.0.1       InLoop0
30.1.1.255/32       Direct 0    0            30.1.1.2        Vlan30
127.0.0.0/8         Direct 0    0            127.0.0.1       InLoop0
```

```
127.0.0.0/32          Direct 0    0           127.0.0.1       InLoop0
127.0.0.1/32          Direct 0    0           127.0.0.1       InLoop0
127.255.255.255/32    Direct 0    0           127.0.0.1       InLoop0
192.168.0.0/24        OSPF   150  1           30.1.1.1        Vlan30
224.0.0.0/4           Direct 0    0           0.0.0.0         NULL0
224.0.0.0/24          Direct 0    0           0.0.0.0         NULL0
255.255.255.255/32    Direct 0    0           127.0.0.1       InLoop0
```

PE1 で VPN2 のルーティングテーブルを表示します。出力は VPN2 の OSPF プロセス 2 のルートが、PE1 の OSPF ルーティングテーブルに再配信されていることを示します。

```
[PE1] display ip routing-table vpn-instance vpn2

Destinations : 13        Routes : 13

Destination/Mask    Proto   Pre  Cost        NextHop         Interface
0.0.0.0/32          Direct  0    0           127.0.0.1       InLoop0
40.1.1.0/24         Direct  0    0           40.1.1.2        Vlan40
40.1.1.0/32         Direct  0    0           40.1.1.2        Vlan40
40.1.1.2/32         Direct  0    0           127.0.0.1       InLoop0
40.1.1.255/32       Direct  0    0           40.1.1.2        Vlan40
127.0.0.0/8         Direct  0    0           127.0.0.1       InLoop0
127.0.0.0/32        Direct  0    0           127.0.0.1       InLoop0
127.0.0.1/32        Direct  0    0           127.0.0.1       InLoop0
127.255.255.255/32  Direct  0    0           127.0.0.1       InLoop0
192.168.10.0/24     OSPF    150  1           40.1.1.1        Vlan40
224.0.0.0/4         Direct  0    0           0.0.0.0         NULL0
224.0.0.0/24        Direct  0    0           0.0.0.0         NULL0
255.255.255.255/32  Direct  0    0           127.0.0.1       InLoop0
```

2 つの VPN のルーティング情報が PE1 のルーティングテーブルに再配信されています。

目次

このセクションのページは **7-x-x** です。

2 章 IPv6 MCE 2-1
2.1 概要 2-1
2.2 IPv6 MCE 設定作業リスト 2-1
2.3 VPN インスタンスの設定 2-1
2.3.1 VPN インスタンスの作成 2-1
2.3.2 VPN インスタンスとインタフェースの関連づけ 2-2
2.3.3 VPN インスタンスのルート関連属性の設定 2-2
2.4 MCE のルーティングの設定 2-3
2.4.1 MCE と VPN サイト間のルーティングの設定 2-4
2.5 IPv6 MCE の表示と維持 2-5
2.6 IPv6 MCE 設定例 2-6

2章 IPv6 MCE

本章は IPv6 MCE について設定方法を説明します。

2.1 概要

MCE は VPN と接続された PE 間の IPv4 ルーティング情報を送信し、IPv4 パケットを転送します。

IPv6 MCE は VPN と接続された PE 間の IPv6 ルーティング情報を送信し、IPv6 パケットを転送します。基本的に、IPv6 MCE は IPv4 MCE と同様に動作します。詳細は、オペレーションマニュアルのセクション *7 MCE"MCE"*を参照してください。

2.2 IPv6 MCE設定作業リスト

作業リスト
VPNインスタンスの設定: 1. (必須設定項目) VPN インスタンスの作成 2. (必須設定項目) VPN インスタンスとインタフェースの関連づけ 3. (オプション設定項目) VPN インスタンスのルート関連属性の設定
MCEのルーティングの設定: ● (必須設定項目) MCEとVPNサイト間のルーティングの設定

2.3 VPNインスタンスの設定

VPN インスタンスを設定することによって、パブリックネットワークルートから VPN ルートを隔離し、ほかの VPN からも隔離します。VPN インスタンスの設定は、すべての MCE ネットワークで必要となります。

2.3.1 VPN インスタンスの作成

VPNインスタンスは VPNメンバーシップと関連したサイトのルーティングルールが集合したものです。VPN インスタンスは 1 つの VPN に対応しない可能性があります。

以下に VPN インスタンスの作成の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. VPN インスタンスを作成し、VPN instance view に移行する	**ip vpn-instance** *vpn-instance-name*	デフォルト：設定なし

操作	コマンド	補足
3. VPN インスタンスの RD を設定する	**route-distinguisher** *route-distinguisher*	デフォルト：設定なし
4. (オプション設定項目) VPN インスタンスの記述を設定する	**description** *text*	デフォルト：設定なし 特定のVPNとの関係などのVPNインスタンスに関連した情報を記載することを推奨します。
5. (オプション設定項目) VPN インスタンス ID を設定する	**vpn-id** *vpn-id*	デフォルト：設定なし

2.3.2 VPN インスタンスとインタフェースの関連づけ

VPN インスタンスの作成、設定をしたのち、VPN インスタンスをサイトおよび PE に接続する MCE インタフェースに関連づけます。

以下に VPN インスタンスとインタフェースの関連づけの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. interface view に移行する	**interface** *interface-type interface-number*	―
3. インタフェースを VPN インスタンスに関連づける	**ip binding vpn-instance** *vpn-instance-name*	デフォルト：設定なし **ip binding vpn-instance**コマンドはインタフェースに設定されたIPアドレス設定を削除します。VPNインスタンスとインタフェースの関連づけをした後、再度IPアドレスを設定してください。

2.3.3 VPN インスタンスのルート関連属性の設定

VPN ルートは PE によって管理され、通知されます。以下の手順で設定され、PE に通知されます。

1) CE から学習した VPN ルートを BGP に再配信するとき、拡張コミュニティ属性リストを VPN インスタンスと関連づけます。それは通常、CE に関連した VPN インスタンスのエクスポートルート属性リストです。
2) VPN インスタンスは受信および再配信するルートをルートターゲットの **import-extcommunity** に従って決定します。
3) VPN インスタンスはルートのターゲット属性の変更方法を、ルートターゲットの **export-extcommunity** に従って決定します。

以下に VPN インスタンスのルート関連属性の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―

操作	コマンド	補足
2. VPN instance view あるいは IPv6 VPN view に移行する	● VPN instance viewに移行する: **ip vpn-instance** *vpn-instance-name* ● IPv6 VPN viewに移行する: **address-family ipv6**	VPN instance viewでの設定はIPv4 VPNとIPv6 VPNの両方に適用されます。 IPv6 VPNはVPN instance view での設定よりIPv6 VPN viewでの設定が優先されます。
3. VPN ターゲットを設定する	**vpn-target** *vpn-target*&<1-8> [**both** | **export-extcommunity** | **import-extcommunity**]	デフォルト：設定なし
4. サポートされるアクティブルートの最大数を設定する	**routing-table limit** *number* { *warn-threshold* | **simply-alert** }	デフォルト：制限なし VPNインスタンスの最大アクティブルート数を設定すると、PEに再配信されてからのルートが過大となることを防止します。
5. 受信ルートポリシーを設定する	**import route-policy** *route-policy*	デフォルト：すべてのルートが通信可能です。 ルーティングポリシーがすでに存在していることを確認してください。そうでないと受信ルートをフィルタしません。 ルーティングポリシーの詳細は、オペレーションマニュアルのセクション5 *ルーティングプロトコル"ルーティングポリシー"*を参照してください。
6. 送信ルートポリシーを設定する	**export route-policy** *route-policy*	デフォルト：すべてのルートが通信可能です。 ルーティングポリシーがすでに存在していることを確認してください。そうでないと受信ルートをフィルタしません。 ルーティングポリシーの詳細は、オペレーションマニュアルのセクション5 *ルーティングプロトコル"ルーティングポリシー"*を参照してください。

2.4 MCEのルーティングの設定

MCE はルート情報の隔離を行います。MCE ルーティング設定は以下があります。

- MCE-VPN サイトルーティング設定
- MCE-PE ルーティング設定

MCE のルーティングを設定する前に以下の作業を行う必要があります。

- PE でルーティングループの検出を無効にしてください。
- システムリソースを削減するため、ルーティングプロトコルでルートの再配信を無効にしてください。

2.4.1 MCE と VPN サイト間のルーティングの設定

MCE と VPN サイト間でスタティックルート、RIPng、OSPFv3 を設定することができます。

I. MCE と VPN サイト間のスタティックルーティングの設定

MCE は IPv6 スタティックルートによって VPN サイトに到達します。伝統的な CE のスタティックルートは、全体に影響します。従って VPN 間をまたぐアドレスをサポートしません。異なる IPv6 VPN インスタンスが互いに隔離できるように、VPN インスタンスに IPv6 スタティックルートを割り当てます。

以下に MCE-VPN サイト間の IPv6 スタティックルートの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. IPv6 VPN インスタンスに IPv6 スタティックルートを設定する	**ipv6 route-static vpn-instance** *s-vpn-instance-name ipv6-address prefix-length* { *interface-type interface-number* [*next-hop-address*] | *nexthop-address* [**public**] | **vpn-instance** *d-vpn-instance-name nexthop-address* } [**permanent**] [**preference** *preference-value*] [**tag** *tag-value*] [**description** *description-text*]	デフォルト：設定なし この設定はMCEで行ってください。VPNサイトでは通常のIPv6スタティックルートを設定してください。
3. (オプション設定項目) IPv6 スタティックルートのデフォルト優先度を設定する	**ipv6 route-static default-preference** *default-preference-value*	デフォルト：60

II. MCE と VPN サイト間の RIPng の設定

RIPng プロセスを、パブリックネットワークあるいは 1 つの IPv6 VPN インスタンスのみ結びつけて使用することができます。どの IPv6 VPN インスタンスにも結びつけられていない RIPng プロセスは、パブリックネットワークに属していることとなります。

RIPng プロセスを IPv6 VPN インスタンスに関連づけることで、異なる IPv6 VPN のルートを分離することができます。RIPng の詳細は、オペレーションマニュアルのセクション 5 *ルーティングプロトコル*"*RIPng*"を参照してください。

以下に MCE-VPN サイト間の RIPng の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. VPN インスタンスの RIP プロセスを作成し、RIP view に移行する	**ripng** [*process-id*] **vpn-instance** *vpn-instance-name*	この設定はMCEで行ってください。VPNサイトでは通常のRIPngプロセスを設定してください。

操作	コマンド	補足
3. PE によって通知されたリモートサイトのルートを RIP に再配信する	**import-route** *protocol* [*process-id*] [**cost** *cost* | **route-policy** *route-policy-name* | **tag** *tag*] *	デフォルト：設定なし
4. system view に戻る	**quit**	―
5. interface view に移行する	**interface** *interface-type interface-number*	―
6. インタフェースで RIPng を有効にする	**ripng** *process-id* **enable**	デフォルト：無効

III. MCE と VPN サイト間の OSPFv3 の設定

OSPFv3 プロセスを、パブリックネットワークあるいは 1 つの IPv6 VPN インスタンスのみ結びつけて使用することができます。どの IPv6 VPN インスタンスにも結びつけられていない OSPFv3 プロセスは、パブリックネットワークに属していることとなります。

OSPFv3 プロセスを IPv6 VPN インスタンスに関連づけることで、異なる IPv6 VPN のルートを分離することができます。OSPFv3 の詳細は、オペレーションマニュアルのセクション 5 *ルーティングプロトコル* "*OSPFv3*"を参照してください。

以下に MCE-VPN サイト間の OSPFv3 の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. VPN インスタンスの OSPFv3 を作成し、OSPFv3 view に移行する	**ospfv3** [*process-id* | **vpn-instance** *vpn-instance-name*] *	この設定はMCEで行ってください。VPNサイトは通常のOSPFv3を設定してください。またVPNインスタンスを削除するには関連したすべてのOSPFv3プロセスを削除してください。
3. ルータ ID を設定する	**router-id** *router-id*	―
4. PE によって通知されたリモートサイトのルートを再配信する	**import-route** *protocol* [*process-id* | **all-processes**] [**cost** *cost* | **route-policy** *route-policy-name* | **type** *type*] *	デフォルト：設定なし
5. system view に戻る	**quit**	―
6. interface view に移行する	**interface** *interface-type interface-number*	―
7. インタフェースで OSPFv3 を有効にする	**ospfv3** *process-id* **area** *area-id* [**instance** *instance-id*]	デフォルト：無効

2.5 IPv6 MCEの表示と維持

すべての view で **display** コマンドが実行できます。

操作	コマンド
VPNインスタンスの情報を表示する	**display ip vpn-instance** [**instance-name** *vpn-instance-name*]

ルーティングテーブルの表示コマンドの詳細については、コマンドマニュアルのセクション 5 *ルーティングプロトコル*を参照してください。

2.6 IPv6 MCE設定例

I. ネットワーク要件

図 2-1に示すように、RIPng は VPN2 で動作します。異なる VPN からルートを隔離させ、OSPFv3 を通して PE1 に VPN ルートを通知するように、MCE を設定します。

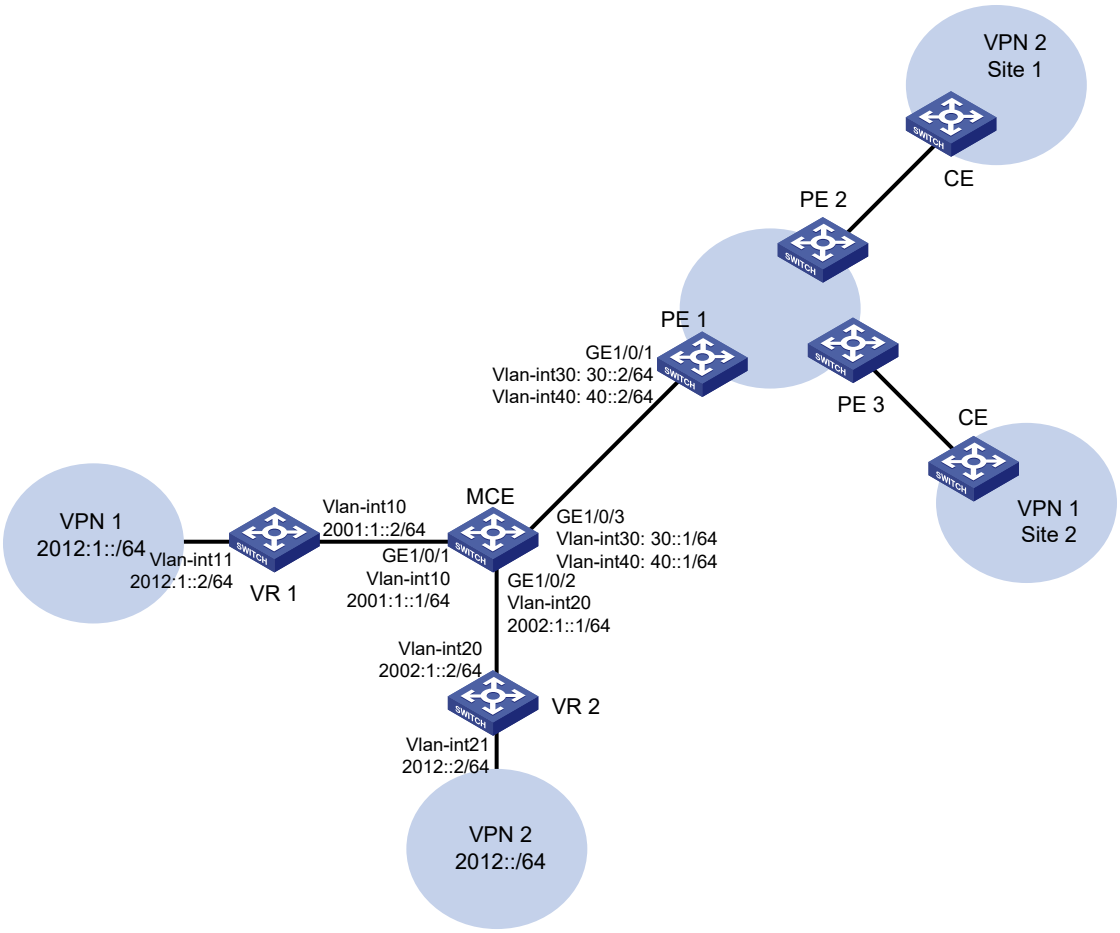


図 2-1 ネットワーク図

II. 設定手順

MCE のシステム名を MCE に設定し、VPN1、VPN2 のシステム名を VR1、VR2 に設定し、PE1 のシステム名を PE1 に設定します。

1)　MCE と PE 1 の VPN インスタンスを設定します。

MCE で VPN インスタンス **vpn1**、**vpn2** を設定し、RD、各 VPN インスタンスのルートターゲットを指定します。

```
<MCE> system-view
[MCE] ip vpn-instance  vpn1
[MCE-vpn-instance-vpn1]  route-distinguisher  10:1
[MCE-vpn-instance-vpn1]  vpn-target  10:1
[MCE-vpn-instance-vpn1]  quit
[MCE] ip vpn-instance  vpn2
[MCE-vpn-instance-vpn2]  route-distinguisher  20:1
```

```
[MCE-vpn-instance-vpn2] vpn-target 20:1
[MCE-vpn-instance-vpn2] quit
```

VLAN10 を作成し、GigabitEthernet 1/0/1 に割り当てます。VLAN インタフェース 10 を作成します。

```
[MCE] vlan 10
[MCE-vlan10] port gigabitethernet 1/0/1
[MCE-vlan10] quit
```

VLAN インタフェース 10 を VPN インスタンス **vpn1** に割り当てます。VLAN インタフェース 10 に IPv6 アドレスを設定します。

```
[MCE] interface vlan-interface 10
[MCE-Vlan-interface10] ip binding vpn-instance vpn1
[MCE-Vlan-interface10] ipv6 address 2001:1::1 64
[MCE-Vlan-interface10] quit
```

VLAN20 を作成し、GigabitEthernet 1/0/2 に割り当てます。

```
[MCE] vlan 20
[MCE-vlan20] port gigabitethernet 1/0/2
[MCE-vlan20] quit
```

VPN インスタンス **vpn2** に VLAN インタフェース 20 を割り当てます。

```
[MCE] interface vlan-interface 20
[MCE-Vlan-interface20] ip binding vpn-instance vpn2
```

VLAN インタフェース 20 に IPv6 アドレスを設定します。

```
[MCE-Vlan-interface20] ipv6 address 2002:1::1 64
[MCE-Vlan-interface20] quit
```

PE1 で VPN インスタンス **vpn1**、**vpn2** を設定し、RD、各 VPN インスタンスのルートターゲットを指定します。

```
<PE1> system-view
[PE1] ip vpn-instance vpn1
[PE1-vpn-instance-vpn1] route-distinguisher 30:1
[PE1-vpn-instance-vpn1] vpn-target 10:1
[PE1-vpn-instance-vpn1] quit
[PE1] ip vpn-instance vpn2
[PE1-vpn-instance-vpn2] route-distinguisher 40:1
[PE1-vpn-instance-vpn2] vpn-target 20:1
[PE1-vpn-instance-vpn2] quit
```

2)　MCE と VPN サイト間のルーティングを設定します。

MCE は直接 VPN1 に接続され、VPN1 でルーティングプロトコルが無効であるため、IPv6 スタティックルートを設定します。

VR1 で MCE に接続しているインタフェースに IPv6 アドレス 2001:1::2/64 を設定し、VPN1 に接続しているインタフェースに IPv6 アドレス 2012:1::2/64 を設定します。VLAN にポートを追加します。(詳細は省略します。)

VR1 でネクストホップ 2001:1::1 としてデフォルトルートを設定します。

```
<VR1> system-view
[VR1] ipv6 route-static :: 0 2001:1::1
```

MCE で IPv6 スタティックルート 2012:1::/64 を設定し、ネクストホップ 2001:1::2 を指定し、VPN インスタンス **vpn1** にスタティックルートを割り当てます。

```
[MCE] ipv6 route-static vpn-instance vpn1 2012:1:: 64 2001:1::2
```

VPN2 で RIPng を動作させます。MCE が VPN2 のルートを学習し、VPN インスタンス **vpn2** のルーティングテーブルにルートを追加できるように MCE で VPN インスタンス **vpn2** の RIPng プロセス 20 を設定します。

```
[MCE] ripng 20 vpn-instance vpn2
```

RIPng を通してサブネット 2002:1::/64 を通知します。

```
[MCE] interface vlan-interface 20
[MCE-Vlan-interface20] ripng 20 enable
[MCE-Vlan-interface20] quit
```

VR2 で MCE に接続されているインタフェースに IPv6 アドレス 2002:1::2/64 を割り当て、VPN2 に接続されているインタフェースに IPv6 アドレス 2012::2/64 を割り当てます。(詳細は省略します)

RIPng を設定し、サブネット 2012::/64、2002:1::/64 を通知します。

```
<VR2> system-view
[VR2] ripng 20
[VR2-ripng-20] quit
[VR2] interface vlan-interface 20
[VR2-Vlan-interface20] ripng 20 enable
[VR2-Vlan-interface20] quit
[VR2] interface vlan-interface 21
[VR2-Vlan-interface21] ripng 20 enable
[VR2-Vlan-interface21] quit
```

MCE で VPN インスタンス **vpn1** のルーティングテーブルを表示します。

```
[MCE] display ipv6 routing-table vpn-instance vpn1

Destinations : 6 Routes : 6

Destination: ::1/128                                Protocol  : Direct
NextHop    : ::1                                    Preference: 0
```

```
Interface  : InLoop0                                Cost      : 0

Destination: 2001:1::/64                            Protocol  : Direct
NextHop    : ::                                     Preference: 0
Interface  : Vlan10                                 Cost      : 0

Destination: 2001:1::1/128                          Protocol  : Direct
NextHop    : ::1                                    Preference: 0
Interface  : InLoop0                                Cost      : 0

Destination: 2012:1::/64                            Protocol  : Static
NextHop    : 2001:1::2                              Preference: 60
Interface  : Vlan10                                 Cost      : 0

Destination: FE80::/10                              Protocol  : Direct
NextHop    : ::                                     Preference: 0
Interface  : NULL0                                  Cost      : 0

Destination: FF00::/8                               Protocol  : Direct
NextHop    : ::                                     Preference: 0
Interface  : NULL0                                  Cost      : 0
```

MCE で VPN インスタンス **vpn2** のルーティングテーブルを表示します。

```
[MCE] display ipv6 routing-table vpn-instance vpn2

Destinations : 6 Routes : 6

Destination: ::1/128                                Protocol  : Direct
NextHop    : ::1                                    Preference: 0
Interface  : InLoop0                                Cost      : 0

Destination: 2002:1::/64                            Protocol  : Direct
NextHop    : ::                                     Preference: 0
Interface  : Vlan20                                 Cost      : 0

Destination: 2002:1::1/128                          Protocol  : Direct
NextHop    : ::1                                    Preference: 0
Interface  : InLoop0                                Cost      : 0

Destination: 2012::/64                              Protocol  : RIPng
NextHop    : FE80::20C:29FF:FE40:701                Preference: 100
Interface  : Vlan20                                 Cost      : 1

Destination: FE80::/10                              Protocol  : Direct
NextHop    : ::                                     Preference: 0
Interface  : NULL0                                  Cost      : 0

Destination: FF00::/8                               Protocol  : Direct
NextHop    : ::                                     Preference: 0
Interface  : NULL0                                  Cost      : 0
```

出力で MCE は VPN2 のプライベートルートを学習していることを示します。MCE は 2 つの異なるルーティングテーブルに分けて VPN1 と VPN2 のルートを維持します。このようにして異なる VPN からのルートを隔離します。

3)　MCE と PE 1 間のルーティングを設定します。

MCE で PE1 に接続されているポートをトランクポートに設定し、VLAN タグ 30、VLAN タグ 40 のパケットの送信を許可するように設定します。

```
[MCE] interface gigabitethernet 1/0/3
[MCE-GigabitEthernet1/0/3] port link-type trunk
[MCE-GigabitEthernet1/0/3] port trunk permit vlan 30 40
[MCE-GigabitEthernet1/0/3] quit
```

PE1 で MCE に接続されているポートをトランクポートに設定し、VLAN タグ 30、VLAN タグ 40 のパケットの送信を許可するように設定します。

```
[PE1] interface gigabitethernet 1/0/1
[PE1-GigabitEthernet1/0/1] port link-type trunk
[PE1-GigabitEthernet1/0/1] port trunk permit vlan 30 40
[PE1-GigabitEthernet1/0/1] quit
```

MCE で VLAN30、VLAN インタフェース 30 を作成し、VPN インスタンス **vpn1** に VLAN インタフェースを割り当てます。VLAN インタフェース 30 に IPv6 アドレスを設定します。

```
[MCE] vlan 30
[MCE-vlan30] quit
[MCE] interface vlan-interface 30
[MCE-Vlan-interface30] ip binding vpn-instance vpn1
[MCE-Vlan-interface30] ipv6 address 30::1 64
[MCE-Vlan-interface30] quit
```

MCE で VLAN40、VLAN インタフェース 40 を作成し、VPN インスタンス **vpn2** に VLAN インタフェースを割り当てます。VLAN インタフェース 40 に IPv6 アドレスを設定します。

```
[MCE] vlan 40
[MCE-vlan40] quit
[MCE] interface vlan-interface 40
[MCE-Vlan-interface40] ip binding vpn-instance vpn2
[MCE-Vlan-interface40] ipv6 address 40::1 64
[MCE-Vlan-interface40] quit
```

PE1 で VLAN30、VLAN インタフェース 30 を作成し、VPN インスタンス **vpn1** に VLAN インタフェースを割り当てます。VLAN インタフェース 30 に IPv6 アドレスを設定します。

```
[PE1] vlan 30
[PE1-vlan30] quit
[PE1] interface vlan-interface 30
[PE1-Vlan-interface30] ip binding vpn-instance vpn1
[PE1-Vlan-interface30] ipv6 address 30::2 64
[PE1-Vlan-interface30] quit
```

PE1 で VLAN40、VLAN インタフェース 40 を作成し、VPN インスタンス **vpn2** に VLAN インタフェースを割り当てます。VLAN インタフェース 40 に IPv6 アドレスを設定します。

```
[PE1] vlan 40
[PE1-vlan40] quit
[PE1] interface vlan-interface 40
[PE1-Vlan-interface40] ip binding vpn-instance vpn2
```

```
[PE1-Vlan-interface40] ipv6 address 40::2 64
[PE1-Vlan-interface40] quit
```

MCE 用としてループバックインタフェース 0に IP アドレス 101.101.10.1 を設定します。PE1 用として IP アドレス 100.100.10.1 を設定します。MCE と PE1 のルータ ID としてループバックインタフェースの IP アドレスを指定します。(詳細は省略します)

PE1 で OSPFv3 プロセス 10 を有効にし、VPN インスタンス **vpn1** に割り当てます。VPN インスタンス **vpn1** の IPv6 スタティックルートを再配信します。

```
[MCE] ospfv3 10 vpn-instance vpn1
[MCE-ospfv3-10] router-id 101.101.10.1
[MCE-ospfv3-10] import-route static
[MCE-ospfv3-10] quit
```

VLAN インタフェース 30 で OSPFv3 を有効にします。

```
[MCE] interface vlan-interface 30
[MCE-Vlan-interface30] ospfv3 10 area 0.0.0.0
[MCE-Vlan-interface30] quit
```

PE1 で OSPFv3 プロセス 10 を有効にし、VPN インスタンス **vpn1** に割り当てます。

```
[PE1] ospfv3 10 vpn-instance vpn1
[PE1-ospfv3-10] router-id 100.100.10.1
[PE1-ospfv3-10] quit
```

VLAN インタフェース 30 で OSPFv3 を有効にします。

```
[PE1] interface vlan-interface 30
[PE1-Vlan-interface30] ospfv3 10 area 0.0.0.0
[PE1-Vlan-interface30] quit
```

MCE と PE1 間で OSPFv3 プロセス 20 を同様に設定し、RIPNG プロセス 20 からの VPN2 のルーティング情報を MCE の OSPFv3 ルーティングテーブルに再配信します。(詳細は省略します。)

III. 設定の確認

PE1 で VPN インスタンス **vpn1** のルーティングテーブルを表示します。出力は VPN1 のプライベートルートが PE1 の OSPFv3 ルーティングテーブルに再配信されていることを示します。

```
[PE1] display ipv6 routing-table vpn-instance vpn1

Destinations : 6 Routes : 6

Destination: ::1/128                                Protocol  : Direct
NextHop    : ::1                                    Preference: 0
Interface  : InLoop0                                Cost      : 0

Destination: 30::/64                                Protocol  : Direct
NextHop    : ::                                     Preference: 0
```

```
Interface  : Vlan30                                  Cost      : 0

Destination: 30::2/128                               Protocol  : Direct
NextHop    : ::1                                     Preference: 0
Interface  : InLoop0                                 Cost      : 0

Destination: 2012:1::/64                             Protocol  : OSPFv3
NextHop    : FE80::202:FF:FE02:2                     Preference: 150
Interface  : Vlan30                                  Cost      : 1

Destination: FE80::/10                               Protocol  : Direct
NextHop    : ::                                      Preference: 0
Interface  : NULL0                                   Cost      : 0

Destination: FF00::/8                                Protocol  : Direct
NextHop    : ::                                      Preference: 0
Interface  : NULL0                                   Cost      : 0
```

VPN インスタンス **vpn2** のルーティングテーブルを表示します。出力は OSPFv3 を経由して VPN2 のプライベートルートが、PE1 のルーティングテーブルに再配信されていることを示します。

```
[PE1] display ipv6 routing-table vpn-instance vpn2

Destinations : 6 Routes : 6

Destination: ::1/128                                 Protocol  : Direct
NextHop    : ::1                                     Preference: 0
Interface  : InLoop0                                 Cost      : 0

Destination: 40::/64                                 Protocol  : Direct
NextHop    : ::                                      Preference: 0
Interface  : Vlan40                                  Cost      : 0

Destination: 40::2/128                               Protocol  : Direct
NextHop    : ::1                                     Preference: 0
Interface  : InLoop0                                 Cost      : 0

Destination: 2012::/64                               Protocol  : OSPFv3
NextHop    : FE80::200:FF:FE0F:5                     Preference: 150
Interface  : Vlan40                                  Cost      : 1

Destination: FE80::/10                               Protocol  : Direct
NextHop    : ::                                      Preference: 0
Interface  : NULL0                                   Cost      : 0

Destination: FF00::/8                                Protocol  : Direct
NextHop    : ::                                      Preference: 0
Interface  : NULL0                                   Cost      : 0
```

2 つの VPN のルーティング情報が PE1 のルーティングテーブルに再配信されています。

QX-S5100G シリーズ Ethernet スイッチ

オペレーションマニュアル

8.ACL and QoS

本マニュアルは以下に示す章で構成されています。

01-ACL
02-QoS の概要
03-QoS ポリシー
04-プライオリティマッピング
05-トラフィックポリシング、GTS、ラインレート
06-輻輳制御
07-トラフィックフィルタリング
08-プライオリティマーキング
09-ネスティング
10-トラフィックリダイレクティング
11-クラスベースアカウンティング
12-付録
13-データバッファ
14-タイムレンジ

目次

このセクションのページは**8-x-x** です。

1章 ACL 1-1
1.1 概要 1-1
1.1.1 ACLタイプ 1-1
1.1.2 ACLの番号づけと命名 1-2
1.1.3 走査順 1-2
1.1.4 ルールナンバリング 1-3
1.1.5 ACLでのフラグメントフィルタリング 1-4
1.2 制限とガイドライン：ACLの設定 1-4
1.3 設定作業リスト 1-5
1.4 標準ACLの設定 1-5
1.4.1 標準IPv4 ACLの設定 1-5
1.4.2 標準IPv6 ACLの設定 1-6
1.5 拡張ACLの設定 1-6
1.5.1 拡張IPv4 ACLの設定 1-6
1.5.2 拡張IPv6 ACLの設定 1-8
1.6 L2 ACLの設定 1-9
1.7 ACLのコピー 1-10
1.8 ACLへのパケットフィルタの設定 1-10
1.8.1 パケットフィルタリングのためのインタフェースへのACLの適用 1-11
1.8.2 VLANインタフェースでのパケットフィルタリングの適用範囲の設定 1-11
1.8.3 フィルタリングのログ作成と出力間隔の設定 1-12
1.9 ACLの表示と維持 1-12
1.10 ACL設定例 1-13
1.10.1 ネットワーク要件 1-13
1.10.2 設定手順 1-13
1.10.3 設定の確認 1-14

1章 ACL

1.1 概要

ACL（Access Control List）は、送信元 IP アドレス、宛先 IP アドレス、ポート番号などにマッチするルールの設定です。

ACL は QoS、セキュリティ、ルーティング、その他の機能でトラフィックの設定に使用でき、モジュールにおけるパケットの廃棄、転送を決定します。

⚠ **注意：**

ACL の処理には、設定されている view について「interface > vlan > global」の優先順位があります。ACL は、高優先の処理を実行すると低優先の処理を実行しません。つまり、interface に設定された ACL の処理が実行された場合、vlan や global に設定された ACL の処理は実行されません。

1.1.1 ACL タイプ

タイプ	ACL 番号	IP バージョン	マッチング基準
標準ACL	2000～2999	IPv4	送信元IPアドレス
		IPv6	送信元IPv6アドレス
拡張ACL	3000～3999	IPv4	送信元IPv4アドレス、宛先IPv4アドレス、パケットプライオリティ、プロトコル番号、その他のレイヤ3、またはレイヤ4のプロトコルヘッダ情報
		IPv6	送信元IPv6アドレス、宛先IPv6アドレス、パケットプライオリティ、プロトコル番号、その他のレイヤ3、またはレイヤ4のプロトコルヘッダ情報
L2 ACL	4000～4999	IPv4、IPv6	送信元MACアドレス、宛先MACアドレス、802.1pプライオリティ、リンクレイヤプロトコルタイプなどの、レイヤ2プロトコルヘッダフィールド

🕮 **メモ：**

ハードウェアベースの ACL（QoS, packet-filter など）は暗黙の permit となり、ソフトウェアベースの ACL（telnet, snmp など）は暗黙の deny になります。

1.1.2 ACL の番号づけと命名

各 ACL のタイプには、ACL 番号の固有な範囲があります。ACL を作成するとき、固有の ACL 番号あるいは名前を付ける必要があります。識別を簡略化するために ACL の名前を割り当てることができます。ACL を作成した後、設定した名前を変更、削除することもできません。

標準 IPv4 ACL と拡張 IPv4 ACL では、IPv4 で固有の ACL 番号と名前を使用する必要があります。

標準 IPv6 ACL と拡張 IPv6 ACL では、IPv6 で固有の ACL 番号と名前を使用する必要があります。

L2 ACL では、固有の ACL 番号と名前を使用する必要があります。

1.1.3 走査順

ACL のルールは指定された順序で探索されます。パケットが、あるルールにマッチした時点で探索動作を終了します。ACL が重複や矛盾したルールを含んでいる場合、探索結果や動作は探索順序に依存します。

IPv4 ACL の走査順には、以下の 2 つ方法があります。

- **config** : ルール ID を昇順で探索します。大きいルール ID よりも先に小さいルール ID にマッチします。この方法を使用する場合、ルールの内容と順序に注意してください。
- **auto** : depth-first により ACL の探索を行います。depth-first ルールでの走査順は、ACL のタイプによって表 1-1の定義に従って決定されます。

表 1-1 ACL の depth-first 走査順

ACL 種別	走査順
標準IPv4 ACL	1. 送信元 IPv4 アドレスのワイルドカードの 0 が多い順（0 が多いと IPv4 アドレスのワイルドカードの範囲が狭いことを示します。） 2. ルールが作成された順
拡張IPv4 ACL	1. プロトコルタイプが IP よりも高いレイヤかどうか 2. 送信元 IP アドレスのワイルドカードマスクの 0 が多い順 3. 宛先 IP アドレスのワイルドカードマスクの 0 が多い順 4. TCP/UDP のポート番号の範囲が小さい順 5. ルールが作成された順
標準IPv6 ACL	1. 送信元 IPv6 アドレスのプレフィックスの長い順（0 が多いと IPv6 アドレスのワイルドカードの範囲が狭いことを示します。） 2. ルーが作成された順
拡張IPv6 ACL	1. プロトコルタイプが IP よりも高いレイヤかどうか 2. 送信元 IPv6 アドレスのプレフィックスの長い順 3. 宛先 IPv6 アドレスのプレフィックスの長い順 4. TCP/UDP のポート番号の範囲が小さい順 5. ルールが作成された順
L2 ACL	1. 送信元 MAC アドレスのマスクの 1 が多い順（1 が多いと MAC アドレスが小さいことを示します。） 2. 宛先 MAC アドレスのマスクの 1 が多い順 3. ルールが作成された順

インバースマスク（inverse mask）と呼ばれるワイルドカードマスクは、10 進数表示のドット表示で表される 32 ビットバイナリです。ネットマスクの 0 は“一致する（do care）”ビットと表現され、1 は“無視する（don’t care）”ビットと表現されます。サブネットマスクの 0 と 1 を反転したものとは異なります。IP アドレスが“do care”ビットである場合、一致させ、“無視する（don’t care）”ビットである場合、無視されます。ワイルドマスクが 0.255.255.255、ネットマスクが 192.168.1.1 の場合、最初の 0 は”一致する（do care）"ビットで、２番目以降が“無視する（don’t care）”ビットであるため、192.0.0.0 のネットワークに一致する ACL となります。ワイルドカードマスクの 0 と 1 は非連続にすることができます。たとえば 0.255.0.255 は有効なワイルドマスクです。

1.1.4 ルールナンバリング

ACL ルールは手動ナンバリングあるいは自動ナンバリングを選択できます。本セクションでは自動ナンバリングの動作を説明します。

I. ルールナンバリングのステップ

作成したルールに ID を割り当てない場合、システムは ACL ルールにルール ID を自動的に割り当てます。ステップのナンバリングルールは、システムが自動的にルールの番号づけを行う増加分を設定します。たとえば、デフォルトの ACL ルールのナンバリングステップは 5 です。ルールに ID を割り当てない場合、ルールには 0、5、10、15･･･の順で自動的に番号が振られます。広いナンバリングのステップの場合、2 つのルールの間に、さらにルールを挿入することができます。

隣接したナンバリングルールより、ルールの間に隙間を導入することによって、新規にルールを挿入するように、ACL に柔軟性を持たせることができます。この機能は config-order ACL にとって重要です。config-order ACL の ACL ルールはルール ID の昇順でマッチされています。

II. 自動ルールナンバリングと再ナンバリング

システムは、現在の最大のステップ番号よりも大きなステップの最小倍数を新しく定義されたルールに割り当てます。これは 0 から始まります。

たとえば、ナンバリングのステップを 5 に設定し、ACL ルールに 0、5、9、10、12 を設定した場合、新しく定義されたルールには 15 が割り当てられます。ACL にルールが 1 つも定義されていない場合、最初に定義されるルールの番号は 0 です。

ルールのステップを変更したとき、ルールは再ナンバリングされ、0 から始まります。たとえば、ルールの番号 5、10、13、15 があるとします。ステップを 5 から 2 に変更すると、ルールの番号は 0、2、4、6 となります。

1.1.5 ACL でのフラグメントフィルタリング

通常のパケットフィルタリングはパケットの最初のフラグメントのみマッチし、後続のフラグメントはパスします。攻撃者はネットワークを攻撃するため、最初でないフラグメントを偽造することができます。

このリスクを防ぐため、以下の ACL を使用します。

- デフォルトで、最初のフラグメント以外のパケットを含むすべてのフラグメントをフィルタします。
- マッチ条件の変更を行います。たとえば、最初のフラグメント以外のパケットのみをフィルタします。

1.2 制限とガイドライン：ACLの設定

- ACL 番号が付いた ACL を作成する場合、以下のいずれかのコマンドを使用して ACL の view に移行することができます。
  - **acl** [**ipv6**] **number** *acl-number*
  - **acl** { [**ipv6**] { **advanced** | **basic** } | **mac** } *acl-number*
- **acl** [**ipv6**] **number** *acl-number* **name** *acl-name* コマンドを使用して ACL 番号が付いた ACL を作成する場合、以下のいずれかのコマンドを使用して ACL の view に移行することができます。
  - **acl** [**ipv6**] **name** *acl-name*（標準 ACL および拡張 ACL の場合のみ）
  - **acl** [**ipv6**] **number** *acl-number* [**name** *acl-name*]
  - **acl** { [**ipv6**] { **advanced** | **basic** } | **mac** } **name** *acl-name*
- **acl** { [**ipv6**] { **advanced** | **basic** } | **mac** } **name** *acl-name* コマンドを使用して ACL 名が付いた ACL を作成する場合、以下のコマンドを使用して ACL の view に移行することができます。
  - **acl** [**ipv6**] **name** *acl-name*（標準 ACL および拡張 ACL の場合のみ）
  - **acl** { [**ipv6**] { **advanced** | **basic** } | **mac** } **name** *acl-name*
- ACL ルールに一致基準が含まれている場合、または次の一致基準と機能に加えて機能が有効になっている場合、一致するパケットは低速転送によって転送されます。
  - 送信元および宛先 IP アドレス
  - 送信元および宛先ポート
  - トランスポートレイヤプロトコル
  - ICMP または ICMPv 6 メッセージタイプ、メッセージコード、およびメッセージ名
  - VPN インスタンス
  - ロギング
  - 時間範囲

1.3 設定作業リスト

作業リスト
（必須設定項目） 少なくとも1つの作業を行ってください。 ● 標準ACLの設定 　● 標準IPv4 ACLの設定 　● 標準IPv6 ACLの設定 ● 拡張ACLの設定 　● 拡張IPv4 ACLの設定 　● 拡張IPv6 ACLの設定 ● L2 ACLの設定
（オプション設定項目） ACLのコピー
（オプション設定項目） ACLへのパケットフィルタの設定

1.4 標準ACLの設定

この章では、IPv4 および IPv6 での標準 ACL の設定方法について説明します。

1.4.1 標準 IPv4 ACL の設定

標準 IPv4 ACL は送信元 IP アドレスにもとづいたパケットにのみマッチします。

以下に標準 IPv4 ACL の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． 標準 IPv4 ACL を作成し、その view に移行する	**acl basic** { *acl-number* | **name** *acl-name* } [**match-order** { **auto** | **config** }] **number**コマンドの場合： **acl number** *acl-number* [**match-order** { **auto** | **config** }]	デフォルト：設定なし 設定範囲は2000～2999です。 IPv4 ACLの番号を指定する場合、**acl basic** *acl-number*コマンドを使用した後でviewに移行することができます。 IPv4 ACLの名前を指定する場合、**acl basic name** *acl-name* コマンドを使用した後でviewに移行することができます。
3． （オプション設定項目）標準 IPv4 ACL の説明を設定する	**description** *text*	デフォルト：設定なし
4． （オプション設定項目）ルールの番号づけステップを設定する	**step** *step-value*	デフォルト：5
5． ルールを作成/修正する	**rule** [*rule-id*] { **deny** | **permit** } [**counting** | **fragment** | **logging** | **source** { *source-address source-wildcard* | **any** } | **time-range** *time-range-name*] *	デフォルト：設定なし **logging**キーワードはモジュール（パケットフィルタリングなど）がサポートしている場合のみ機能します。

操作	コマンド	補足
6. （オプション設定項目）ルールの説明を設定する	**rule** *rule-id* **comment** *text*	デフォルト：設定なし

1.4.2 標準 IPv6 ACL の設定

標準 IPv6 ACL は送信元 IP アドレスにもとづいたパケットにのみマッチします。

以下に標準 IPv6 ACL の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. 標準 IPv6 ACL を作成し、その view に移行する	**acl ipv6 basic** { *acl-number* | **name** *acl-name* } [**match-order** { **auto** | **config** }] **number**コマンドの場合： **acl ipv6 number** *acl-number* [**match-order** { **auto** | **config** }]	デフォルト：設定なし 設定範囲は2000～2999です。 IPv6 ACLの番号を指定する場合、**acl ipv6 basic** *acl-number*コマンドを使用した後でviewに移行することができます。 IPv6 ACLの名前を指定する場合、**acl ipv6 basic name** *acl-name*コマンドを使用した後でviewに移行することができます。
3. （オプション設定項目）標準 IPv6 ACL の説明を設定する	**description** *text*	デフォルト：設定なし
4. （オプション設定項目）ルールの番号付けステップを設定する	**step** *step-value*	デフォルト：5
5. ルールを作成/修正する	**rule** [*rule-id*] { **deny** | **permit** } [**counting** | **fragment** | **logging** | **routing** [**type** *routing-type*] | **source** { *source-address source-prefix* | *source-address*/*source-prefix* | **any** } | **time-range** *time-range-name*] *	デフォルト：設定なし **logging**キーワードはモジュール（たとえばパケットフィルタリング）がサポートしている場合のみ機能します。
6. （オプション設定項目）ルールの説明を設定する	**rule** *rule-id* **comment** *text*	デフォルト：設定なし

1.5 拡張ACLの設定

この章では、IPv4 および IPv6 での拡張 ACL の設定方法について説明します。

1.5.1 拡張 IPv4 ACL の設定

拡張 IPv4 ACL では、以下の情報にもとづいてマッチングを行うことができます。

- 送信元 IP アドレス
- 送信先 IP アドレス
- パケットのプライオリティ
- プロトコル番号
- TCP/UDP の送信元/送信先ポート番号、TCP フラグ、ICMP メッセージタイプ、ICMP メッセージコードなどの他のプロトコルヘッダ情報

標準 IPv4 ACL と比較すると、拡張 IPv4 ACL では柔軟で正確なフィルタリングを行うことができます。

以下に拡張 IPv4 ACL の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. 拡張 IPv4 ACL を作成し、その view に移行する	**acl advanced** { *acl-number* | **name** *acl-name* } [**match-order** { **auto** | **config** }] **number**コマンドの場合： **acl number** *acl-number* [**match-order** { **auto** | **config** }]	デフォルト：設定なし 設定範囲は3000～3999です。 IPv4 ACLの番号を指定する場合、**acl advanced** *acl-number*コマンドを使用した後でviewに移行することができます。 IPv4 ACLの名前を指定する場合、**acl advanced name** *acl-name*コマンドを使用した後でviewに移行することができます。
3. （オプション設定項目）拡張 IPv4 ACL の説明を設定する	**description** *text*	デフォルト：設定なし
4. （オプション設定項目）ルールの番号付けステップを設定する	**step** *step-value*	デフォルト：5
5. ルールを作成/修正する	**rule** [*rule-id*] { **deny** | **permit** } *protocol* [{ { **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn** *syn-value* | **urg** *urg-value* } * | **established** } | **counting** | **destination** { *dest-address dest-wildcard* | **any** } | **destination-port** *operator port1* [*port2*] | { **dscp** *dscp* | { **precedence** *precedence* | **tos** *tos* } * } | **fragment** | **icmp-type** { *icmp-type* [*icmp-code*] | *icmp-message* } | **logging** | **source** { *source-address source-wildcard* | **any** } | **source-port** *operator port1* [*port2*] | **time-range** *time-range-name*] *	デフォルト：設定なし **logging**キーワードはモジュール（たとえばパケットフィルタリング）がサポートしている場合のみ機能します。
6. （オプション設定項目）ルールの説明を設定する	**rule** *rule-id* **comment** *text*	デフォルト：設定なし

1.5.2 拡張 IPv6 ACL の設定

🕮 **ポイント：**

IPv6 アドレスのフィルタについて、destination の場合は、フィルタできるアドレスに条件があります。
inbound フィルタ の場合は、アドレスの先頭 1 バイトと末尾 2 バイトをフィルタします。
outbound フィルタの場合は、アドレスの先頭 1 バイトのみをフィルタします。
詳細はコマンドマニュアルのセクション 8 ACL and QoS ”rule (IPv6 advanced ACL view)”を参照してください。

拡張 IPv6ACL では、以下の情報にもとづいてマッチングを行うことができます。

- 送信元 IPv6 アドレス
- 送信先 IPv6 アドレス
- パケットのプライオリティ
- プロトコル番号
- TCP/UDP の送信元/送信先ポート番号、TCP フラグ、ICMP メッセージタイプ、ICMP メッセージコードなどの他のプロトコルヘッダ情報

標準 IPv6 ACL と比較すると、拡張 IPv6 ACL では柔軟で正確なフィルタリングを行うことができます。

以下に拡張 IPv6 ACL の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． 拡張 IPv6 ACL を作成し、その view に移行する	**acl ipv6 advanced** { *acl-number* | **name** *acl-name* } [**match-order** { **auto** | **config** }] **number**コマンドの場合： **acl ipv6 number** *acl-number* [**match-order** { **auto** | **config** }]	デフォルト：設定なし 設定範囲は3000～3999です。 IPv6 ACLの番号を指定する場合、**acl ipv6 advanced** *acl-number*コマンドを使用した後でviewに移行することができます。 IPv6 ACLの名前を指定する場合、**acl ipv6 advanced name** *acl-name* コマンドを使用した後でviewに移行することができます。
3． （オプション設定項目）拡張 IPv6 ACL の説明を設定する	**description** *text*	デフォルト：設定なし
4． （オプション設定項目）ルールの番号付けステップを設定する	**step** *step-value*	デフォルト：5

操作	コマンド	補足
5. ルールを作成/修正する	**rule** [*rule-id*] { **deny** | **permit** } *protocol* [{ { **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn** *syn-value* | **urg** *urg-value* } * | **established** } | **counting** | **destination** { *dest-address dest-prefix* | *dest-address/dest-prefix* | **any** } | **destination-port** *operator port1* [*port2*] | **dscp** *dscp* | **flow-label** *flow-label-value* | **fragment** | **icmp6-type** { *icmp6-type icmp6-code* | *icmp6-message* } | **logging** | **routing** [**type** *routing-type*] | **source** { *source-address source-prefix* | *source-address/source-prefix* | **any** } | **source-port** *operator port1* [*port2*] | **time-range** *time-range-name*] *	デフォルト：設定なし **logging**キーワードはモジュール（たとえばパケットフィルタリング）がサポートしている場合のみ機能します。
6. （オプション設定項目）ルールの説明を設定する	**rule** *rule-id* **comment** *text*	デフォルト：設定なし

1.6 L2 ACLの設定

イーサネットフレームのヘッダを使用した ACL は“L2 ACL”と呼ばれます。L2 ACL では以下のレイヤ 2 のプロトコルヘッダにもとづいてマッチングを行います。

- 送信元 MAC アドレス
- 送信先 MAC アドレス
- 802.1p 優先順位（VLAN プライオリティ）
- リンクレイヤのプロトコルタイプ
- カプセル化タイプ
- 内部送信元 MAC アドレス
- 内部宛先 MAC アドレス
- 内部リンクレイヤのプロトコルタイプ

以下に L2 ACL の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. L2 ACL を作成し、その view に移行する	**acl mac** { *acl-number* | **name** *acl-name* } [**match-order** { **auto** | **config** }] **number**コマンドの場合： **acl number** *acl-number* [**match-order** { **auto** | **config** }]	デフォルト：設定なし 設定範囲は4000～4999です。 L2 ACLの番号を指定する場合、**acl mac** *acl-number*コマンドを使用した後でviewに移行することができます。 L2 ACLの名前を指定する場合、**acl mac name** *acl-name* コマンドを使用した後でviewに移行することができます。
3. （オプション設定項目）L2 ACL の説明を設定する	**description** *text*	デフォルト：設定なし

操作	コマンド	補足
4．（オプション設定項目）ルールの番号付けステップを設定する	**step** *step-value*	デフォルト：5
5．ルールを作成/修正する	**rule** [*rule-id*] { **deny** | **permit** } [**cos** *dot1p* | **counting** | **dest-mac** *dest-address dest-mask* | { **lsap** *lsap-type lsap-type-mask* | **type** *protocol-type protocol-type-mask* } | **source-mac** *source-address source-mask* | **time-range** *time-range-name*] *	デフォルト：設定なし
6．（オプション設定項目）ルールの説明を設定する	**rule** *rule-id* **comment** *text*	デフォルト：設定なし

1.7 ACLのコピー

既存の ACL（送信元 ACL）をコピーして、ACL（宛先 ACL）を新しく作成することができます。新しい ACL（宛先 ACL）は送信元 ACL と同じタイプ、内容を持ちます。ただし同じ ACL 番号、ACL 名ではありません。

ACL のコピーを行うため、以下のことを確認してください。

- 送信元の ACL と宛先 ACL は同じタイプである必要があります。
- コピーを実行する前に、送信元の ACL が存在し、宛先 ACL は存在しないことを確認してください。

以下に ACL のコピーの設定を示します。

操作	コマンド
1．system view に移行する	**system-view**
2．既存の ACL をコピーし、新しく ACL を作成する	**acl** [**ipv6** | **mac**] **copy** { *source-acl-number* | **name** *source-acl-name* } **to** { *dest-acl-number* | **name** *dest-acl-name* }

1.8 ACLへのパケットフィルタの設定

この章では指定したインタフェースの受信、出力パケットをフィルタする手順を示します。

🕮 **メモ：**

パケットフィルタはイーサネットインタフェース、VLAN インタフェースで有効にすることが可能です。この章のインタフェースは VLAN インタフェース、レイヤ 3 Ethernet インタフェースを含むレイヤ 3 インタフェースを示します。

1.8.1 パケットフィルタリングのためのインタフェースへの ACL の適用

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． interface view に移行する	**interface** *interface-type interface-number*	―
3． パケットをフィルタするために ACL をインタフェースに適用する	**packet-filter** [**ipv6** | **mac**] { *acl-number* | **name** *acl-name* } { **inbound** | **outbound** } [**hardware-count**]	デフォルト：設定なし インタフェースに同一方向の設定は最大3つまで設定できます。標準ACL、拡張ACL、L2 ACLそれぞれ1つずつ設定することができます。 インタフェースで送信されるパケットをフィルタすることはできません。 VLANインタフェースでフィルタリングを設定した場合、別のVLANインタフェースに転送される場合にのみフィルタされます。

🕮 **メモ：**

VLAN インタフェースには同じ方向のパケットフィルタを設定できません。設定がある場合は、先に元の設定を削除してください。
同じ方向のパケットフィルタを設定してエラーが表示された場合は、**display packet-filter verbose** コマンドで正常に適用されていない ACL を確認できます。

1.8.2 VLAN インタフェースでのパケットフィルタリングの適用範囲の設定

I. このタスクについて

VLAN インタフェースでパケットフィルタリングを設定して、次のパケットをフィルタリングできます。

- VLAN インタフェースによってレイヤ 3 で転送されるパケット
- VLAN インタフェースによってレイヤ 3 で転送されたパケットと、VLAN インタフェースに関連付けられた物理ポートによってレイヤ 2 で転送されたパケットを含む、すべてのパケット

II. 設定手順

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． VLAN インタフェースを作成し、その view に移行する	**interface vlan-interface** *vlan-interface-id*	―

操作	コマンド	補足
3． VLAN インタフェースでパケットフィルタリングの適用範囲を指定する	**packet-filter filter** [**route** | **all**]	デフォルト : すべてのパケットをフィルタリングします。

1.8.3 フィルタリングのログ作成と出力間隔の設定

出力間隔を設定したのち、装置は information center にパケットフィルタリングのログを定期的に出力することができます。ログにはパケットにマッチする数、マッチした ACL ルールが含まれます。information center の詳細はオペレーションマニュアルのセクション 11 *システム管理*”*Information Center*”を参照してください。

以下にフィルタリングログの出力設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． フィルタリングのログ出力を設定し､出力間隔を設定する	**acl logging interval** *interval*	デフォルト：0分 0分を設定した場合、ログを出力しません。

1.9 ACLの表示と維持

すべての view で **display** コマンドを実行でき、user view で **reset** コマンドを実行できます。

操作	コマンド
ACLの設定とマッチした統計情報を表示する	**display acl** [**ipv6** | **mac**] { *acl-number* | **all** | **name** *acl-name* }
インタフェースに適用したACLが正常に動作したかどうかパケットフィルタの状態を表示する	**display packet-filter** { **interface** [*interface-type interface-number*] [**inbound** | **outbound**] | **interface** *vlan-interface vlan-interface-number* [**inbound** | **outbound**] [**slot** *slot-number*] }
パケットフィルタの統計情報を表示する	**display packet-filter statistics interface** *interface-type interface-number* { **inbound** | **outbound** } [[**ipv6** | **mac**] { *acl-number* | **name** *acl-name* }] [**brief**]
パケットフィルタの累積統計情報を表示する	**display packet-filter statistics sum** { **inbound** | **outbound** } [**ipv6** | **mac**] { *acl-number* | **name** *acl-name* } [**brief**]
パケットフィルタの詳細情報を表示する	**display packet-filter verbose interface** *interface-type interface-number* { **inbound** | **outbound** } [[**ipv6** | **mac**] { *acl-number* | **name** *acl-name* }] [**slot** *slot-number*]
QoSおよびACLリソースの使用率を表示する	**display qos-acl resource** [**slot** *slot-number*]
ACLの統計情報を削除する	**reset acl** [**ipv6** | **mac**] **counter** { *acl-number* | **all** | **name** *acl-name* }
パケットフィルタの累積統計を含む統計情報を削除する	**reset packet-filter statistics interface** [*interface-type interface-number*] { **inbound** | **outbound** } [[**ipv6** | **mac**] { *acl-number* | **name** *acl-name* }]

1.10 ACL設定例

1.10.1 ネットワーク要件

図 1-1のネットワークでは Device を介して各部門間が相互に通信します。ACL を以下のように設定します。

- 社長室（President's office）からの経理データベース(Financial database server)へのアクセスを常時許可します。
- 経理部門(Financial department)からの経理データベース(Financial database server)へのアクセス許可を平日 8:00～18:00 までに制限します。
- 上記 2 部門以外からの経理データベース(Financial database server)へのアクセスを常時拒否します。

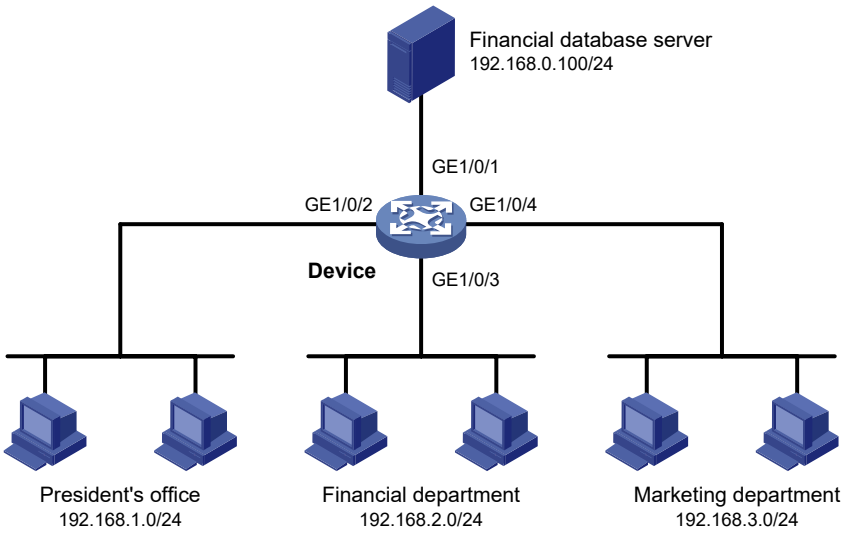


図 1-1 ネットワーク図

1.10.2 設定手順

勤務時間を平日 8:00～18:00 として設定します。

```
<Device> system-view
[Device] time-range work 08:0 to 18:00 working-day
```

拡張 IPv4 ACL 3000 を作成します。

```
[Device] acl advanced 3000
```

社長室から経理データベースサーバへのアクセスを許可するルールを作成します。

```
[Device-acl-ipv4-adv-3000] rule permit ip source 192.168.1.0 0.0.0.255 destination 192.168.0.100 0
```

経理部門から経理データベースサーバへの平日の勤務時間内でのアクセスを許可するルールを作成します。

```
[Device-acl-ipv4-adv-3000] rule permit ip source 192.168.2.0 0.0.0.255 destination 192.168.0.100 0 time-range work
```

他部門からの経理データベースサーバへのアクセスを拒否するルールを作成します。

```
[Device-acl-ipv4-adv-3000] rule deny ip source any destination 192.168.0.100 0
[Device-acl-ipv4-adv-3000] quit
```

GigabitEthernet 1/0/1 の出力パケットについて拡張 IPv4 ACL 3000 を適用します。

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] packet-filter 3000 outbound
[Device-GigabitEthernet1/0/1] quit
```

1.10.3 設定の確認

平日の勤務時間において、経理部門の PC から経理データベースサーバへ ping を実行します。（この例では、PC はすべて Windows 2000 以上を使用しています）

```
C:\> ping 192.168.0.100

Pinging 192.168.0.100 with 32 bytes of data:

Reply from 192.168.0.100: bytes=32 time=1ms TTL=255
Reply from 192.168.0.100: bytes=32 time<1ms TTL=255
Reply from 192.168.0.100: bytes=32 time<1ms TTL=255
Reply from 192.168.0.100: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.0.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

平日の勤務時間において、営業部門から経理データベースサーバへ ping を実行します。

```
C:\> ping 192.168.0.100

Pinging 192.168.0.100 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.0.100:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

平日の勤務時間中の Device で、拡張 IPv4 ACL 3000 の統計情報および設定情報を表示します。

```
[Device] display acl 3000
Advanced IPv4 ACL 3000, 3 rules,
ACL's step is 5
 rule 0 permit ip source 192.168.1.0 0.0.0.255 destination 192.168.0.100 0
 rule 5 permit ip source 192.168.2.0 0.0.0.255 destination 192.168.0.100 0
time-range work (Active)
 rule 10 deny ip destination 192.168.0.100 0
```

出力は、ルール 5 がアクティブであることを示します。

目次

このセクションのページは **8-x-x** です。

2 章 QoS の概要 2-1
2.1 QoS サービスモデル 2-1
2.1.1 ベストエフォートサービスモデル 2-1
2.1.2 IntServ モデル 2-1
2.1.3 DiffServ モデル 2-2
2.2 QoS 技術の概要 2-2
2.2.1 ネットワークの QoS 技術の展開 2-2
2.2.2 装置の QoS 処理フロー 2-3

2章 QoS の概要

QoS（Quality of Service）は、ネットワークトラフィックのフォワーディングプロセスで帯域幅、遅延、パケットロスに関与します。帯域の保証や、遅延、ジッタ、パケットロス率等の低減を行うことによって、QoS の向上ができます。

QoS でトラフィックの優先度付けを行い、各トラフィックに対するネットワークリソースの割り当てを考慮する必要があります。

本章では、QoS サービスモデルと広く使用される QoS の技術を紹介します。

2.1 QoSサービスモデル

この章では一般的な QoS サービスモデルについて説明します。

2.1.1 ベストエフォートサービスモデル

ベストエフォートモデルは、単独のサービスモデルです。最も簡単なサービスモデルです。ベストエフォートサービスモデルは、他のモデルに比べて信頼性は低くなり、遅延や信頼性などの保証はしません。

ベストエフォートサービスモデルは、インターネットでのデフォルトのモデルです。ほとんどのネットワークアプリケーションに適用され、FIFO（First In First Out）キューイングとして実装されます。

2.1.2 IntServ モデル

IntServ（integrated service）は、複数の多様な QoS 要件に適用できる多重サービスモデルです。このモデルは、各データフローに QoS を保証、識別することができ、きめ細かく差別化された QoS を提供します。

IntServ モデルでは、データを送信する前にアプリケーション上で、特定の種類のサービスを使用できるようにネットワークへ要求する必要があります。IntServの要求は、RSVP シグナリングによって行われます。RSVP は、送信元から宛先までの装置で動作し、データフローがあらかじめ要求/予約したリソースより多くのリソースを使わないよう、各アプリケーションフローをモニタします。

IntServは装置の高い処理能力が必要となります。IntServモデルはネットワークへの大量のデータトラフィックが、ストレージデバイスの処理能力に非常に大きな負担がかかります。したがって多くのデータフローが流れるコアインターネット網や何百万のフローが流れるネットワークなどの大規模のネットワークでは利用されず、IntServ モデルは中小規模のネットワークで利用されます。

2.1.3 DiffServ モデル

DiffServ（differentiated service）は、多様な QoS 要件を満たせる多重サービスモデルです。IntServ とは異なり、DiffServ はデータを送信する前に、アプリケーションからネットワークに信号に出す必要がありません。DiffServ は、実行や拡張が容易に行えます。

2.2 QoS技術の概要

QoS 技術には以下の機能があります。

- トラフィックの分類
- トラフィックポリシー
- トラフィックシェーピング
- レートリミット
- 輻輳管理
- 輻輳回避

このマニュアルに記載するすべての QoS 技術は、DiffServ モデルにもとづいています。

🕮 メモ：

QX-S5100G シリーズは輻輳回避をサポートしていません。

2.2.1 ネットワークの QoS 技術の展開

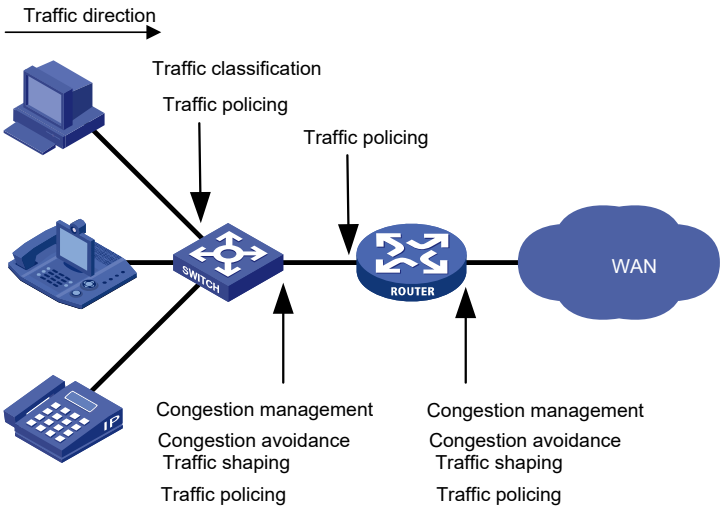


図 2-1 ネットワークの QoS 技術の位置

図 2-1に示すように、以下にトラフィックの分類、トラフィックシェーピング、トラフィックポリシー、輻輳管理、輻輳回避の主要な機能を実装します。

- **トラフィックの分類**－異なった特性、異なったクラスのパケットを組織化するために、ある評価基準を使用します。トラフィックの分類にもとづいて、差別化されたサービスを提供することができます。
- **トラフィックポリシー**－トラフィックが設定したしきい値を超えたとき、ネットワークリソースの過剰使用を防ぐため、フローの制限等の対策を施行できます。トラフィックポリシーは、ポートの入力トラフィック、出力トラフィックの双方向に適用できます。
- **トラフィックシェーピング**－下流の装置向けのトラフィックに適用することで、パケット廃棄と輻輳回避のため、トラフィック出力レートを調整できます。トラフィックシェーピングは、ポートの出力トラフィックに適用します。
- **輻輳管理**－パケットの輻輳が発生した際の転送順序を定義し、リソースのスケジューリングポリシーを提供します。輻輳管理は、ポートの出力トラフィックに適用します。
- **輻輳回避**－ネットワークリソースの使用状態をモニタし、パケットの輻輳が発生すると、パケットを廃棄してキューのトラフィック量を減らすことができます。輻輳回避は、ポートの出力トラフィックに適用します。

2.2.2 装置の QoS 処理フロー

図 2-2に示すように QoS モジュールはトラフィックの処理を行います。

1) トラフィックの分類処理は、後続の QoS アクションを行うため、トラフィックを識別し、分類します。
2) QoS モジュールはトラフィック処理プロセスフェーズとネットワークの状態に従い、分類されたトラフィックでさまざまな QoS アクションを行います。たとえば、以下の処理を行うように QoS モジュールを設定することができます。

- 入力トラフィックのトラフィックポリシー
- 出力トラフィックのトラフィックシェーピング
- 衝突が発生したときに衝突制御を行います。

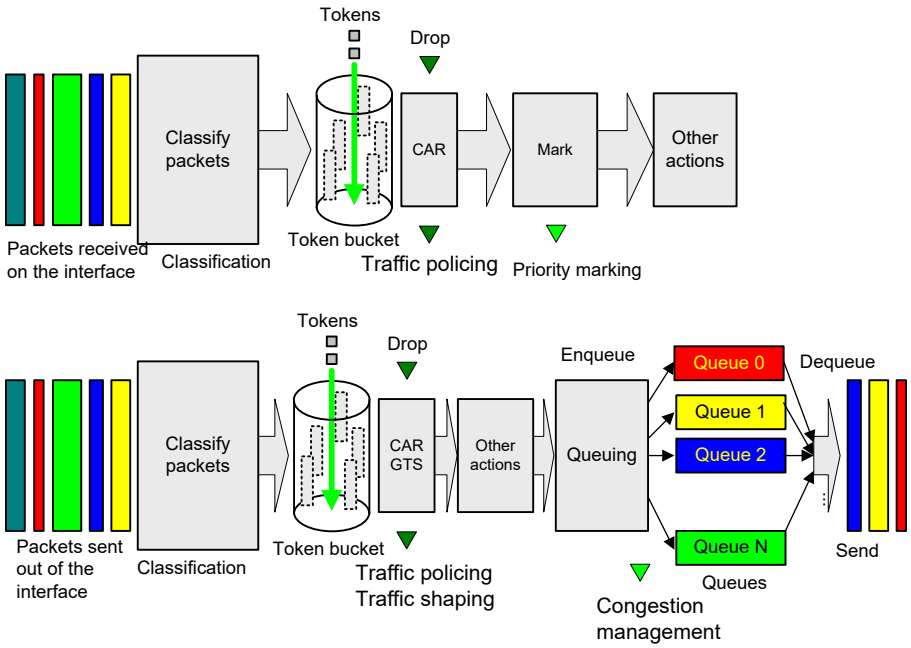


図 2-2 QoS 処理フロー

目次

このセクションのページは **8-x-x** です。

3 章 QoS ポリシー..... 3-1
3.1 非ポリシーベースのアプローチ..... 3-1
3.2 ポリシーベースのアプローチ..... 3-1
3.3 QoS ポリシーの設定手順..... 3-1
3.4 トラフィッククラスの定義..... 3-2
3.5 トラフィック動作の定義..... 3-2
3.6 QoS ポリシーの定義..... 3-3
3.7 QoS ポリシーの適用..... 3-3
3.7.1 インタフェースへの QoS ポリシーの適用..... 3-4
3.7.2 VLAN への QoS ポリシーの適用..... 3-4
3.7.3 グローバルへの QoS ポリシーの適用..... 3-4
3.7.4 QoS ポリシーのユーザプロファイルへの適用..... 3-5
3.8 QoS ポリシーの情報表示と維持..... 3-5

3章 QoS ポリシー

QoS 設定は、ポリシーベースあるいは非ポリシーベースの 2 つのアプローチが利用可能です。

3.1 非ポリシーベースのアプローチ

インタフェースに直接レートリミットを設定する等、QoS ポリシーを使用せずに QoS サービスパラメータを使用する設定を非ポリシーベースと呼びます。

3.2 ポリシーベースのアプローチ

QoS ポリシーによる QoS サービスパラメータを使用して設定する設定をポリシーベース MQC（Modular QoS Configuration）と呼びます。ポリシーベースは、トラフィックの異なるクラスに対応するため、トラフィックポリシーやほかの QoS アクションを定義します。

トラフィッククラスはトラフィックを特定するための条件を定義し、論理積（AND）または論理和（OR）の演算子（オペレータ）を使用します。

- オペレータが AND である場合、パケットはトラフィッククラスの一致条件すべてにマッチする必要があります。
- オペレータが OR である場合､パケットはトラフィッククラスの一致条件のいずれかにマッチします。

トラフィック動作（traffic behavior）でパケットの優先順位のマーキングとトラフィックのリダイレクト等の QoS アクションを定義します。

QoS ポリシーでトラフィッククラスとトラフィック動作を関連づけます。トラフィッククラスで定義した条件で特定されたトラフィックをトラフィック動作で定義した QoS アクションで処理させることができます。

3.3 QoSポリシーの設定手順

図 3-1に QoS ポリシーの設定手順を示します。

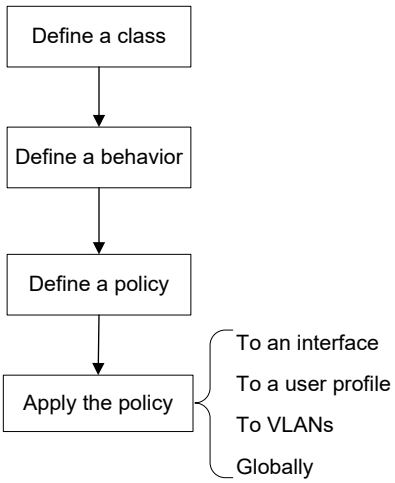


図 3-1 QoS ポリシーの設定手順

3.4 トラフィッククラスの定義

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. トラフィッククラスを作成し、traffic class view に移行する	**traffic classifier** *classifier-name* [**operator** { **and** | **or** }]	―
3. （オプション設定項目）トラフィッククラスの説明を設定する	**description** *text*	デフォルト：設定なし
4. 一致条件を設定する	**if-match** *match-criteria*	デフォルト：設定なし **if-match**コマンドの詳細はコマンドマニュアルのセクション8 *ACL and QoS*”*QoS*ポリシー”を参照してください。

3.5 トラフィック動作の定義

トラフィック動作でトラフィックフィルタリング、トラフィックポリシー、プライオリティマーキング等の QoS の動作を定義します。

以下にトラフィック動作の設定手順を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. トラフィック動作を作成し traffic behavior view に移行する	**traffic behavior** *behavior-name*	デフォルト：設定なし

操作	コマンド	補足
3. QoS の動作を定義する	トラフィックポリシー、トラフィックフィルタリング、プライオリティマーキング、クラスベースアカウンティングなどのトラフィック動作の目的に応じて、オペレーションマニュアルのセクション8 *ACL and QoS*を参照してください。	デフォルト：設定なし

3.6 QoSポリシーの定義

トラフィック動作を QoS ポリシーのトラフィッククラスに関連づけます。トラフィック動作は、クラスの一致条件にマッチしたパケットに実行されます。

トラフィッククラス定義のために QoS ポリシーによって ACL が参照された場合は、ACL のアクション（許可あるいは拒否）は無視されます。アクションはトラフィック動作に関連づけられたものが使われます。

クラスとトラフィック動作の関連づけ手順を以下に示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. QoS ポリシーを作成し、qos policy view に移行する	**qos policy** *policy-name*	デフォルト：設定なし
3. トラフィッククラスとトラフィック動作を関連づける	**classifier** *classifier-name* **behavior** *behavior-name* [**insert-before** *before-classifier-name*]	デフォルト：設定なし 複数、作成する場合、コマンドを繰り返してください。

3.7 QoSポリシーの適用

QoS ポリシーは以下の種類に適用できます。

- **インタフェース**－QoS ポリシーはインタフェースで送受信したトラフィックに適用します。
- **VLAN**－QoS ポリシーは VLAN のすべてのポートで送受信したトラフィックに適用します。
- **グローバル**－QoS ポリシーはすべてのポートで送受信したトラフィックに適用します。

QoS ポリシーを適用している場合、QoS ポリシーを適用した後でも QoS ポリシーのトラフィッククラス、トラフィック動作、トラフィッククラスとトラフィッククラスの関連づけの設定を修正できます。トラフィッククラスがトラフィックの分類の ACL を参照する場合、ACL を削除あるいは修正できます。（たとえば、ACL のルールへの追加、削除、修正です）

3.7.1 インタフェースへの QoS ポリシーの適用

1 つの QoS ポリシーを複数のインタフェースに適用できますが、インタフェースの 1 つの方向（インバウンド/アウトバウンド）に適用できる QoS ポリシーは 1 つのみです。

インタフェースの出力トラフィックに適用された QoS ポリシーはローカルパケットに適用されません。ローカルパケットは、装置の正常動作を維持するためのパケットです。一般的なローカルパケットはリンクのメンテナンスパケットやルーティング、LDP パケット、RSVP パケット、SSH パケットがあります。

以下にインタフェースへの QoS ポリシーの適用手順を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. interface view に移行する	**interface** *interface-type interface-number*	―
3. QoS ポリシーを適用する	**qos apply policy** *policy-name* { **inbound** | **outbound** }	デフォルト：設定なし

3.7.2 VLAN への QoS ポリシーの適用

QoS ポリシーを VLAN に対してトラフィック制御のために適用できます。

I. 設定の制限とガイドライン

QoS ポリシーを VLAN に適用するため、以下の設定の制限とガイドラインに従ってください。

- QoS ポリシーはダイナミック VLAN に適用できません。
- IRF スタックメンバ装置のハードウェアリソースが十分でない場合、VLAN で IRF スタックメンバ装置への QoS ポリシーの適用は失敗する可能性があります。システムは自動でほかの IRF スタックメンバ装置に適用されている設定から QoS ポリシーの設定に戻りません。整合させるためには **undo qos vlan-policy vlan** コマンドを使用して QoS ポリシーの設定を削除してください。

II. 設定手順

VLAN への QoS ポリシーの適用手順を以下に示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. QoS ポリシーを適用する	**qos vlan-policy** *policy-name* **vlan** *vlan-id-list* { **inbound** | **outbound** }	デフォルト：設定なし

3.7.3 グローバルへの QoS ポリシーの適用

すべてのポートのインバウンド/アウトバウンド方向に QoS ポリシーを適用できます。

IRF スタックメンバ装置のハードウェアリソースが十分でない場合、VLAN で IRF スタックメンバ装置への QoS ポリシーの適用は失敗する可能性があります。システムは自動で

ほかの IRF スタックメンバ装置に適用されている設定から QoS ポリシーの設定に戻りません。整合させるためには **undo qos vlan-policy vlan** コマンドを使用して QoS ポリシーの設定を削除してください。

グローバルへの QoS ポリシーの適用手順を以下に示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. QoS ポリシーを適用する	**qos apply policy** *policy-name* **global** { **inbound** | **outbound** }	デフォルト：設定なし

3.7.4 QoS ポリシーのユーザプロファイルへの適用

ユーザプロファイルが設定されている場合、ユーザに基づいてトラフィックポリシングを実行できます。ユーザが認証に成功すると、認証サーバはユーザに関連付けられたユーザプロファイルの名前を装置に送信します。ユーザプロファイルビューで設定された QoS ポリシーは、ユーザがオンラインになったときにだけ有効になります。

QoS ポリシーを複数のユーザプロファイルに適用できます。各ユーザプロファイルの一方向では、1 つのポリシーだけを適用できます。方向にすでに適用されている QoS ポリシーを変更するには、最初に適用されている QoS ポリシーを削除します。

ユーザプロファイルへの QoS ポリシーの適用手順を以下に示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. user profile view に移行する	**user-profile** *profile-name*	―
3. QoS ポリシーをユーザプロファイルに適用する	**qos apply policy** *policy-name* { **inbound** | **outbound** }	デフォルト：設定なし

パラメータ	説明
inbound	装置がユーザプロファイルから受信したトラフィックに QoS ポリシーを適用します。
outbound	装置からユーザプロファイルに送信されるトラフィックに QoS ポリシーを適用します。

3.8 QoSポリシーの情報表示と維持

すべての view で **display** コマンドを実行でき、user view で **reset** コマンドを実行できます。

操作	コマンド
トラフィッククラスの設定情報を表示する	**display traffic classifier user-defined** [*classifier-name*] [**slot** *slot-number*]

操作	コマンド
トラフィック動作についての情報を表示する	**display traffic behavior user-defined** [*behavior-name*] [**slot** *slot-number*]
QoSおよびACLリソースの使用率を表示する	**display qos-acl resource** [**slot** *slot-number*]
QoSポリシーの設定を表示する	**display qos policy user-defined** [*policy-name* [**classifier** *classifier-name*]] [**slot** *slot-number*]
指定したinterface、あるいはすべてのinterfaceのQoSポリシーの設定を表示する	**display qos policy interface** [*interface-type interface-number*] [**inbound** | **outbound**]
ユーザプロファイルに適用されたQoSポリシーについての情報を表示する	**display qos policy user-profile** [**name** *profile-name*] [**user-id** *user-id*] [**slot** *slot-number*] [**inbound** | **outbound**]
VLANに適用されたQoSポリシーについての情報を表示する	**display qos vlan-policy** { **name** *policy-name* | **vlan** [*vlan-id*] } [**slot** *slot-number*] [**inbound** | **outbound**]
グローバルに適用されたQoSポリシーについての情報を表示する	**display qos policy global** [**slot** *slot-number*] [**inbound** | **outbound**]
VLANに適用されたQoSポリシーの統計情報を削除する	**reset qos vlan-policy** [**vlan** *vlan-id*] [**inbound** | **outbound**]
グローバルに適用されたQoSポリシーの統計情報を削除トする	**reset qos policy global** [**inbound** | **outbound**]

目次

このセクションのページは **8-x-x** です。

4 章 プライオリティマッピング 4-1
4.1 概要 4-1
4.1.1 プライオリティの導入 4-1
4.1.2 プライオリティマッピング 4-1
4.2 プライオリティマッピングの設定作業リスト 4-2
4.3 プライオリティマッピングの設定 4-2
4.4 プライオリティマッピングのパケットプライオリティを信用するインタフェースの設定4-3
4.5 インタフェースのポートプライオリティの変更 4-3
4.6 プライオリティマッピングの表示と維持 4-4
4.7 プライオリティマッピングの設定例 4-4
4.7.1 トラステッドモードの設定例 4-4
4.7.2 プライオリティマッピングテーブルとプライオリティマーキングの設定例 4-5

4章 プライオリティマッピング

4.1 概要

パケットを受信すると、装置は以下のいずれかのプライオリティにもとづいて QoS プライオリティのパラメータをパケットに割り当てます。

- パケットに含まれているプライオリティのフィールドの値
- 入力ポートのポートプライオリティ

このプロセスはプライオリティマッピングと呼ばれます。このプロセスの間、装置はプライオリティマッピングのルールに従ってパケットのプライオリティを修正することができます。QoS プライオリティのパラメータはパケットのスケジュールプライオリティとフォワーディングプライオリティを決めます。

プライオリティマッピングはプライオリティマッピングテーブルに実装され、以下のプライオリティを決定します。

- 802.1p プライオリティ
- DSCP
- IP プレシーデンス
- ローカルプレシーデンス

4.1.1 プライオリティの導入

プライオリティは、ローカルプライオリティとパケットに含まれているプライオリティと、スケジューリング用にローカルに割り当てられるプライオリティがあります。

パケットに含まれているプライオリティは、802.1p プライオリティ、DSCP プレシーデンス、IP プレシーデンスがあります。パケットに含まれるプライオリティは、他の装置でも使用されるため、ネットワークに影響します。プライオリティの詳細はオペレーションマニュアルのセクション 8 *ACL and QoS*”*付録*”を参照してください。

ローカルプライオリティは装置内でのみ使用されるため、ネットワークに影響しません。ローカルプライオリティは、ローカルプレシーデンスと呼ばれ、キューのスケジューリング用に使用されます。ローカルプレシーデンスの値は出力キューに対応します。ローカルプレシーデンスの値が高いパケットが高い出力キューに割り当てられます。

4.1.2 プライオリティマッピング

装置はさまざまなプライオリティマッピングのタイプを提供します。プライオリティマッピングは、プライオリティマッピングテーブルを参照し、その後のパケットを処理するため、パケットに割り当てるプライオリティを決定します。

デフォルトのプライオリティマップ（オペレーションマニュアルのセクション 8 *ACL and QoS*”*付録*”の”*デフォルトプライオリティ*”を参照してください）はプライオリティマッピングに利用できます。デフォルトのマップは、ほとんどの場合において通常に使用す

ることができます。デフォルトのプライオリティマップでは要件を満たすことができない場合、必要に応じてプライオリティのマッピングを変更することができます。

4.2 プライオリティマッピングの設定作業リスト

以下の方法を使用してプライオリティマッピングを設定することができます。

プライオリティマッピングテーブル、ポートのプライオリティのトラステッドモード、ポートプライオリティを変更することによって、プライオリティマッピングを変更することができます。

- **プライオリティのトラステッドモードの設定**－プライオリティマッピングで運ばれた受信パケットのトラステッドプライオリティタイプ（たとえば、802.1p）を検索するために使用するプライオリティを設定することができます。システムはターゲットのプライオリティのタイプと値にトラステッドプライオリティの値をマッピングします。
- **ポートプライオリティの変更**－パケットのプライオリティを信用しない場合、受信パケットのポートプライオリティが使用されます。ポートのポートプライオリティを変更することによって、ポートで受信するパケットのプライオリティを変更します。

プライオリティマッピングを設定するには、以下の手順を実施してください。

作業リスト
（オプション設定項目）プライオリティマッピングの設定
（必須設定項目）いずれか1つを設定してください。 • プライオリティマッピングのパケットプライオリティを信用するインタフェースの設定 • インタフェースのポートプライオリティの変更

4.3 プライオリティマッピングの設定

装置は以下のタイプのプライオリティマッピングを提供します。

プライオリティマッピング	説明
dot1p-lp	802.1p-ローカルプライオリティマッピングテーブルです。
dscp-dot1p	DSCP-802.1pプライオリティマッピングテーブルです。
dscp-dscp	DSCP-DSCPプライオリティマッピングテーブルです。

以下にプライオリティマッピングの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	－
2. priority map view に移行する	**qos map-table** { **dot1p-lp** | **dscp-dot1p** | **dscp-dscp** }	－

操作	コマンド	補足
3. プライオリティマッピングを設定する	**import** *import-value-list* **export** *export-value*	デフォルト: デフォルトのプライオリティマップ 詳細は、オペレーションマニュアルのセクション8 *ACL and QoS" 付録"* を参照してください。 新規の設定は、既存に上書きします。

4.4 プライオリティマッピングのパケットプライオリティを信用するインタフェースの設定

インタフェースのプライオリティマッピングのパケットで運ばれた特定のプライオリティフィールドを信用するように装置を設定できます。

インタフェース上で信用できるパケットのプライオリティタイプを設定する場合は、以下の内で使用可能なキーワードを使用します。

- **dot1p**: マッピングのため受信したパケットの 802.1p プライオリティを使用します。
- **dscp**: マッピングのため受信した IP パケットの DSCP プレシーデンスを使用します。

プライオリティトラステッドモードの設定手順を以下に示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. interface view に移行する	**interface** *interface-type interface-number*	―
3. パケットプライオリティタイプの信用を設定する	**qos trust** { **dot1p** | **dscp** }	デフォルト：信用しない

4.5 インタフェースのポートプライオリティの変更

インタフェースがパケットのプライオリティを信用しない設定の場合、装置は受信したパケットのプライオリティパラメータセットを探すために、自身のポートプライオリティを使用します。ポートプライオリティを変更することで、異なるインタフェースで受信されたトラフィックに優先順位を付けることができます。

ポートプライオリティの変更手順を以下に示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. interface view に移行する	**interface** *interface-type interface-number*	―
3. ポートプライオリティを設定する	**qos priority** *priority-value*	デフォルト：0

4.6 プライオリティマッピングの表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
プライオリティマッピングの設定を表示する	**display qos map-table** [**dot1p-lp** | **dscp-dot1p** | **dscp-dscp**]
ポートに設定されているトラステッドプレシーデンスを表示する	**display qos trust interface** [*interface-type interface-number*]

4.7 プライオリティマッピングの設定例

4.7.1 トラステッドモードの設定例

I. ネットワーク要件

図 4-1に示すように設定します。

- Device A から Device C へのトラフィックの IP プレシーデンスは 3 です。
- Device B から Device C へのトラフィックの IP プレシーデンスは 1 です。

Device C の GigabitEthernet 1/0/3 でパケットが輻輳した場合、Device C は Device A からサーバへのパケットを優先します。

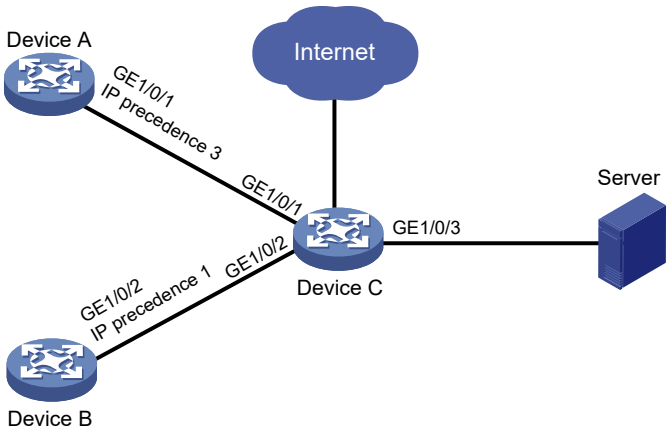


図 4-1 ネットワーク図

II. 設定手順

GigabitEthernet 1/0/1、GigabitEthernet 1/0/2 にポートプライオリティを設定します。GigabitEthernet 1/0/1 のプライオリティは GigabitEthernet 1/0/2 のプライオリティよりも高いことを確認してください。

```
<DeviceC> system-view
```

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] qos priority 3
[DeviceC-GigabitEthernet1/0/1] quit
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] qos priority 1
[DeviceC-GigabitEthernet1/0/2] quit
```

4.7.2 プライオリティマッピングテーブルとプライオリティマーキングの設定例

I. ネットワーク要件

図 4-2に示すように、プライオリティマッピングテーブルとプライオリティマーキングを設定します。

- 営業部は装置の GigabitEthernet 1/0/1 に接続し、営業部からのトラフィックの 802.1p プライオリティを 3 に設定します。
- 研究開発部は装置の GigabitEthernet 1/0/2 に接続し、研究開発部からのトラフィックの 802.1p プライオリティを 4 に設定します。
- 管理部は装置の GigabitEthernet 1/0/3 に接続し、管理部からのトラフィックの 802.1p プライオリティを 5 に設定します。

表 4-1に示すようにポートプライオリティ、802.1p-local プライオリティマッピングテーブル、プライオリティマーキングを設定します。

表 4-1 設定計画

トラフィック先	トラフィックプライオリティの順番	キューイング計画		
		送信元	送信キュー	キュープライオリティ
Public servers	研究開発部>管理部>営業部	研究開発部	6	High
		管理部	4	Medium
		営業部	2	Low
Internet	管理部>営業部>研究開発部	研究開発部	2	Low
		管理部	6	High
		営業部	4	Medium

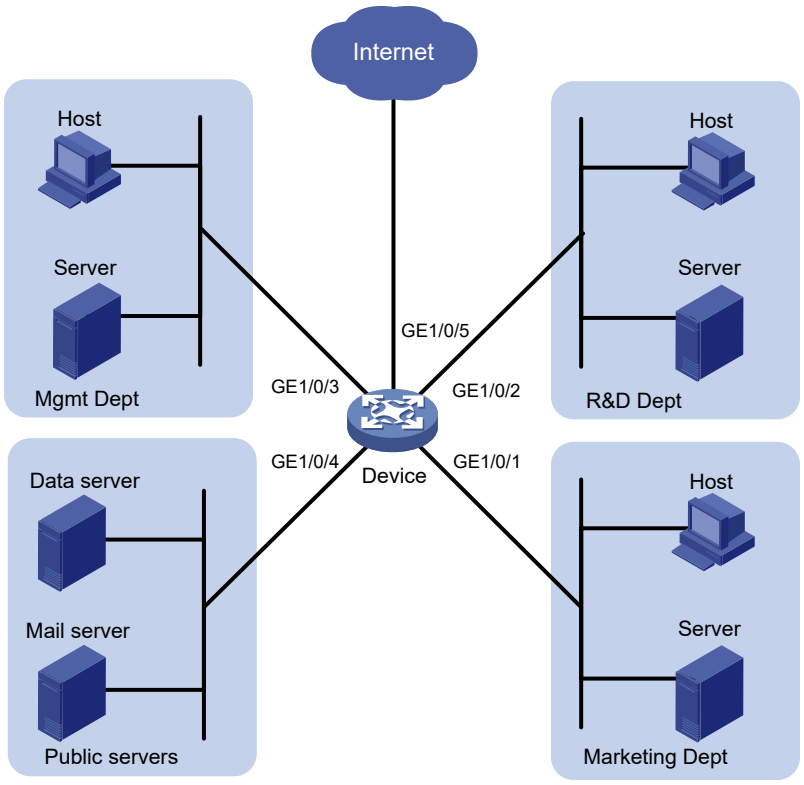


図 4-2 ネットワーク図

II. 設定手順

1)　ポートプライオリティを設定します。

GigabitEthernet 1/0/1 のポートプライオリティを 3 に設定します。

```
<Device> system-view
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] qos priority 3
[Device-GigabitEthernet1/0/1] quit
```

GigabitEthernet 1/0/2 のポートプライオリティを 4 に設定します。

```
[Device] interface gigabitethernet 1/0/2
[Device-GigabitEthernet1/0/2] qos priority 4
[Device-GigabitEthernet1/0/2] quit
```

GigabitEthernet 1/0/3 のポートプライオリティを 5 に設定します。

```
[Device] interface gigabitethernet 1/0/3
[Device-GigabitEthernet1/0/3] qos priority 5
[Device-GigabitEthernet1/0/3] quit
```

2) プライオリティマッピングテーブルを設定します。802.1p-ローカルプライオリティのマッピングテーブルを 802.1p プライオリティの値 3、4、5 をローカルプライオリティの 2、6、4 にマップします。

研究開発部、管理部、営業部は public server にアクセスするため、プライオリティを低くします。

```
[Device] qos map-table dot1p-lp
[Device-maptbl-dot1p-lp] import 3 export 2
[Device-maptbl-dot1p-lp] import 4 export 6
[Device-maptbl-dot1p-lp] import 5 export 4
[Device-maptbl-dot1p-lp] quit
```

3) プライオリティマーキングを設定します。

ACL 3000 を作成します。HTTP のトラフィックに一致するようにルールを設定します。

```
[Device] acl advance 3000
[Device-acl-adv-3000] rule permit tcp destination-port eq 80
[Device-acl-adv-3000] quit
```

トラフィッククラス **http** を作成し、ACL 3000 を一致条件に設定します。

```
[Device] traffic classifier http
[Device-classifier-http] if-match acl 3000
[Device-classifier-http] quit
```

トラフィック動作 **admin** を作成し、管理部向けのマーキングアクションを設定します。

```
[Device] traffic behavior admin
[Device-behavior-admin] remark dot1p 4
[Device-behavior-admin] quit
```

QoS ポリシー**admin** を作成し、トラフィッククラス **http** とトラフィック動作 **admin** を関連づけます。

```
[Device] qos policy admin
[Device-qospolicy-admin] classifier http behavior admin
[Device-qospolicy-admin] quit
```

GigabitEthernet 1/0/3 の入力トラフィックに QoS ポリシー**admin** を適用します。

```
[Device] interface gigabitethernet 1/0/3
[Device-GigabitEthernet1/0/3] qos apply policy admin inbound
```

トラフィック動作 **market** を作成し、営業部向けのマーキングアクションを設定します。

```
[Device] traffic behavior market
[Device-behavior-market] remark dot1p 5
[Device-behavior-market] quit
```

QoS ポリシー**market** を作成し、トラフィッククラス **http** とトラフィック動作 **admin** を関連づけます。

```
[Device] qos policy market
[Device-qospolicy-market] classifier http behavior market
[Device-qospolicy-market] quit
```

GigabitEthernet 1/0/1 の入力トラフィックに QoS ポリシー**market** を適用します。

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] qos apply policy market inbound
```

トラフィック動作 **rd** を作成し、研究開発部向けのマーキングアクションを設定します。

```
[Device] traffic behavior rd
[Device-behavior-rd] remark dot1p 3
[Device-behavior-rd] quit
```

QoS ポリシー**rd** を作成し、トラフィッククラス **http** とトラフィック動作 **rd** を関連づけます。

```
[Device] qos policy rd
[Device-qospolicy-rd] classifier http behavior rd
[Device-qospolicy-rd] quit
```

GigabitEthernet 1/0/2 の入力トラフィックに QoS ポリシー**rd** を適用します。

```
[Device] interface gigabitethernet 1/0/2
[Device-GigabitEthernet1/0/2] qos apply policy rd inbound
```

目次

このセクションのページは**8-x-x** です。

5章 トラフィックポリシング、GTS、ラインレート 5-1
5.1 概要 5-1
5.1.1 トラフィックレートの検証とトークンバケット 5-1
5.1.2 トラフィックポリシング 5-3
5.1.3 GTS 5-3
5.1.4 ラインレート 5-4
5.2 QoSポリシーを使用したトラフィックポリシングの設定 5-5
5.3 GTSの設定 5-6
5.4 インタフェースのラインレートの設定 5-6
5.5 トラフィックポリシング、GTS、ラインレートの表示と維持 5-7
5.6 トラフィックポリシング、GTS、ラインレートの設定例 5-7
5.6.1 ネットワーク要件 5-7
5.6.2 設定手順 5-8

5章　トラフィックポリシング、GTS、ラインレート

5.1 概要

トラフィックポリシングはネットワークリソース（帯域幅を含みます）の割り当てを手助けし、ネットワーク性能を向上させます。たとえば、特定のパケット転送に使用する帯域幅を制限し保証することで、バーストトラフィックに起因するネットワークの輻輳を回避することができます。

トラフィックポリシングと GTS（generic traffic shaping）やラインレート（レートリミット）は、特定のトラフィックが割り当てた帯域幅を上回る場合、リソースの使用量を制限します。 トラフィックレートを検証するには、トークンバケットを使用します。

5.1.1 トラフィックレートの検証とトークンバケット

I. トークンバケットの機能

トークンバケットは、トークンを保持するための一定の容量を持つ容器と見なすことができます。システムは、設定されたレートでトークンをバケットに入れます。トークンバケットが一杯になると、トークンがバケットからあふれます。

II. トークンバケットを使用したトラフィックレートの検証

トラフィックは、バケット内のトークンの数を見て検証します。バケット転送に対して、バケット内のトークンの数に余裕がある場合、以下のように対応します。

- トラフィックは仕様に対応します。（適合トラフィックと呼ばれます）
- 対応するトークンがバケットから取り外されます。

そうでない場合、トラフィックは仕様に対応しません。（余剰トラフィックと呼ばれます）

トークンバケットは以下の設定可能なパラメータがあります。

- トークンが許可されたトラフィック平均レートによってバケットに入るレートです。通常 CIR（Committed Information Rate）によって設定されます。
- バーストサイズあるいはトークンバケットの容量です。各バーストで許可された最大トラフィックサイズです。通常 CBS（Committed Burst Size）によって設定されます。設定されたバーストサイズは最大パケットサイズよりも大きくする必要があります。

各パケットが到着するたびに検証されます。

III. 複雑な検証

トークンバケットには、以下の設定可能なパラメータがあります。

より複雑な環境でトラフィックを評価し、より多くのポリシーの柔軟性を行うように 2 つのトークンバケット（バケット C、バケット E）を設定することができます。

- **1 レート 2 色**—1 つのトークンバケットと以下のパラメータを使用します。
  - **CIR**（Committed Information Rate）：バケット C に入るトークンのレートです。バケット C によって許可された平均転送レートを設定します。
  - **CBS**（Committed Burst Size）：バケット C のサイズです。バケット C が転送できるトラフィックの転送バーストを設定します。

  パケットが到達するとき、以下のルールに従います。

  - バケット C にパケットを転送するために十分なトークンがある場合、パケットは green に色分けされます。
  - そうでない場合、パケットは red に色分けされます。
- **1 レート 3 色**—2 つのトークンバケットと以下のパラメータを使用します。
  - **CIR**（Committed Information Rate）：バケット C に入るトークンのレートです。バケット C によって許可された平均転送レートを設定します。
  - **CBS**（Committed Burst Size）：バケット C のサイズです。バケット C が転送できるトラフィックの転送バーストを設定します。
  - **EBS**（Excess burst size）：バケット E のサイズからバケット C のサイズを引いたサイズです。バケット E が転送できるトラフィックの転送バーストを設定します。EBS は 0 にできません。バケット E のサイズは CBS と EBS の合計です。

  パケットが到達するとき、以下のルールに従います。

  - バケット C にパケットを転送するために十分なトークンがある場合、パケットは green に色分けされます。
  - バケット C にパケットを転送するために十分なトークンがないが、バケット E にパケットを転送するために十分なトークンがある場合、パケットは yellow に色分けされます。
  - バケット C、バケット E にパケットを転送するために十分なトークンがない場合、パケットは red に色分けされます。
- **2 レート 3 色**—2 つのトークンバケットと以下のパラメータを使用します。
  - **CIR**（Committed Information Rate）：バケット C に入るトークンのレートです。バケット C によって許可された平均転送レートを設定します。
  - **CBS**（Committed Burst Size）：バケット C のサイズです。バケット C が転送できるトラフィックの転送バーストを設定します。
  - **PIR**（Peak information rate）：バケット E に入るトークンのレートです。バケット E によって許可された平均転送レートを設定します。
  - **EBS**（Excess burst size）：バケット E のサイズです。バケット E が転送できるトラフィックの転送バーストを設定します。

  パケットが到達するとき、以下のルールに従います。

  - バケット C にパケットを転送するために十分なトークンがある場合、パケットは green に色分けされます。
  - バケット C にパケットを転送するために十分なトークンがないが、バケット E にパケットを転送するために十分なトークンがある場合、パケットは yellow に色分けされます。
  - バケット C、バケット E にパケットを転送するために十分なトークンがない場合、パケットは red に色分けされます。

5.1.2 トラフィックポリシング

トラフィックポリシングは、入出力トラフィックのポリシーをサポートすることができます。

一般的なトラフィックポリシングのアプリケーションは、ネットワークの特定のトラフィックを監視し、トラフィックを妥当な範囲内で制限します。別のアプリケーションは、ネットワークリソースが積極的に使用しないようにするため、余剰トラフィックの調整を行います。たとえば、HTTP パケットの帯域幅を全体の 50%未満に制限することができます。セッションのトラフィックが制限を超過すると、トラフィックポリシングはパケットの廃棄やパケットの DSCP をリセットすることができます。図 5-1にインタフェースの出力トラフィックのポリシングの例を示します。

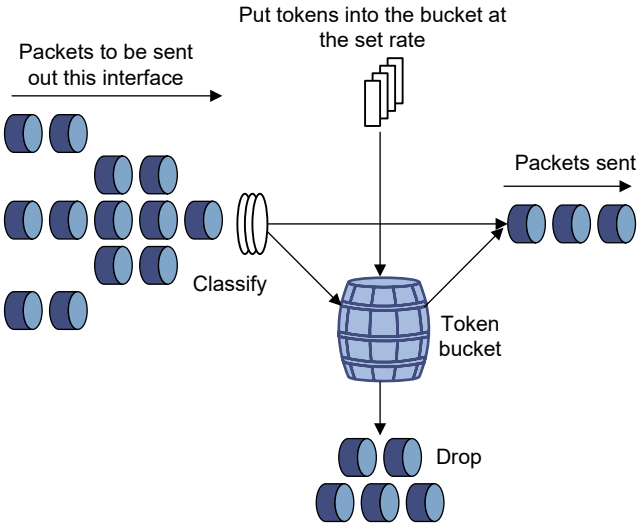


図 5-1 トラフィックポリシング

トラフィックポリシングは、ISP（Internet Service Provider）のネットワークのトラフィックの制限などに広く使用されます。トラフィックポリシングはトラフィックを分類し、検証結果にもとづいて、トラフィックを事前に定義されたトラフィック動作で処理します。トラフィック動作には以下があります。

- 適合トラフィックを転送します。
- 余剰トラフィックを破棄します。
- 検証結果が適合である場合、リマークした DSCP に従ってパケットを転送します。

5.1.3 GTS

GTS は、出力トラフィックのシェーピングをサポートします。GTS は、超過したトラフィックをバッファすることによって、送信トラフィックの転送レートを制限します。パケットロスを防ぐため、GTS を使用することで、装置のトラフィックの出力レートを、装置に接続されたトラフィックの入力レートに適合させます。

トラフィックポリシングと GTS の違いを以下に示します。

- 図 5-2に示すように、トラフィックポリシングで廃棄されたパケットはバッファや GTS のキューに残されています。十分なトークンがトークンバケットにある場合、バッファされたパケットが適切なレートで送信されます。
- GTS は追加で遅延が生じることがありますが、トラフィックポリシングはありません。

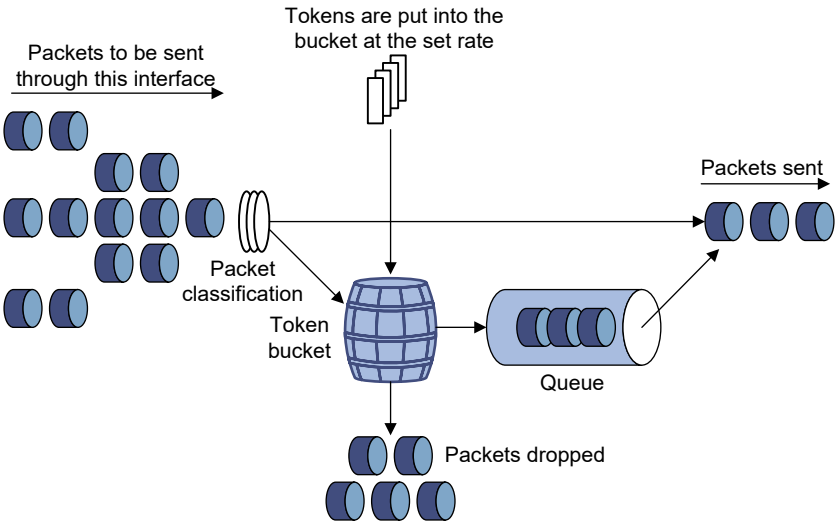


図 5-2 GTS

たとえば、図 5-3では、Device B は Device A からのパケットのトラフィックポリシングを行い、制限に超過したパケットを廃棄します。パケットロスを防ぐため、制限を超過しているパケットが Device A でキャッシュできるように Device A の出力インタフェースで GTS を実行します。一度リソースが解放されると、GTS はキャッシュされたパケットを取り出し、送信します。

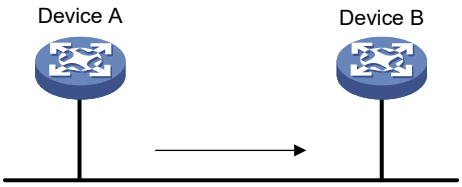


図 5-3 GTS アプリケーション

5.1.4 ラインレート

ラインレート（レートリミット）は、入出力トラフィックのレートを管理します。たとえば出力トラフィックについて説明します。

物理インタフェースのラインレートは、パケット（クリティカルパケットを除く）の最大転送レートを指定します。

ラインレートも、トラフィックを管理するためにトークンバケットを使用します。ラインレートがインタフェースで設定されるとき、トークンバケットはインタフェースを通してすべてのパケットが送信されます。もしトークンバケットに十分なトークンがある場合、

パケットを転送することができます。そうでなければ、パケットは輻輳制御のため QoS キューに入ります。このように物理インタフェースを通したトラフィックが管理されます。

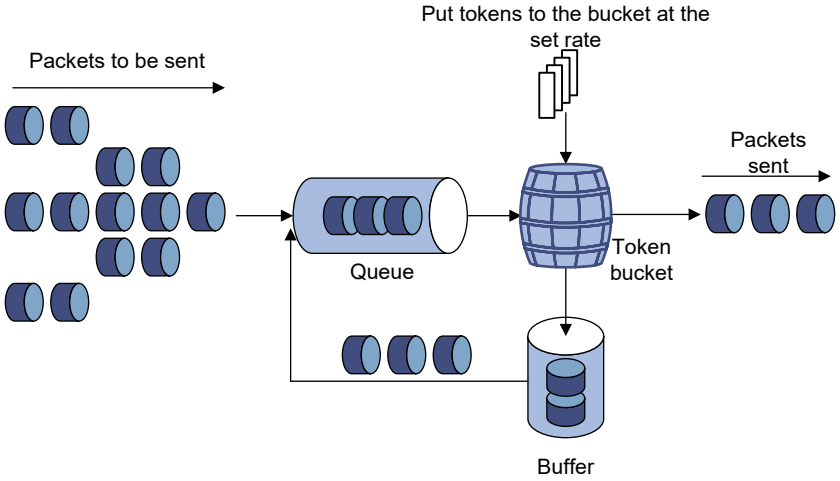


図 5-4 ラインレートの実装

トークンバケットメカニズムは、バーストデータを適応させるときに、トラフィックレートを制限します。十分なトークンが有効である場合、バーストトラフィックは転送されます。トークンが不十分である場合、効率的なトークンがトークバケットで作成されるまでパケットは転送できません。トラフィックレートを、トークン作成用のレートに制限します。

ラインレートは物理インタフェースのすべてのパケットの全レートを管理します。物理インタフェースの全トラフィックレートを管理するトラフィックポリシングよりも簡単に利用できます。

5.2 QoSポリシーを使用したトラフィックポリシングの設定

以下に QoS ポリシー（MQC アプローチ）を使用したトラフィックポリシングの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. トラフィッククラスを作成し traffic class view に移行する	**traffic classifier** *classifier-name* [**operator** { **and** | **or** }]	デフォルト：設定なし
3. 一致条件を設定する	**if-match** *match-criteria*	デフォルト：設定なし **if-match**コマンドの詳細はコマンドマニュアルのセクション8 *ACL and QoS*”*QoSポリシー*”を参照してください。
4. system view に戻る	**quit**	ー
5. トラフィック動作を作成し traffic behavior view に移行する	**traffic behavior** *behavior-name*	デフォルト：設定なし

操作	コマンド	補足
6. トラフィックポリシングアクションを設定する	**car cir** *committed-information-rate* [**cbs** *committed-burst-size* [**ebs** *excess-burst-size*]] [**green** *action* | **red** *action* | **yellow** *action*] * **car cir** *committed-information-rate* [**cbs** *committed-burst-size*] **pir** *peak-information-rate* [**ebs** *excess-burst-size*] [**green** *action* | **red** *action* | **yellow** *action*] *	どちらか一方の設定を行います。 デフォルト：設定なし
7. system view に戻る	**quit**	ー
8. QoS ポリシーを作成し QoS policy view に移行する	**qos policy** *policy-name*	デフォルト：設定なし
9. トラフィック行動とトラフィッククラスを関連づける	**classifier** *classifier-name* **behavior** *behavior-name*	デフォルト：設定なし
10. system view に戻る	**quit**	ー
11. QoS ポリシーを適用する	• インタフェースへ適用 • VLANへ適用 • グローバルに適用	必要とされる宛先の1つを選択してください。 デフォルト：設定なし
12. （オプション設定項目）トラフィックポリシングの設定を表示する	**display traffic behavior user-defined** [*behavior-name*]	すべてのviewで実行可能です。

5.3 GTSの設定

装置は、非 QoS ポリシー（MQC アプローチを使用しない）を使用して、キューベース GTS の設定をサポートします。キューベース GTS は GTS パラメータを特定のキューのパケットに設定します。

GTS の設定手順を以下に示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. interface view に移行する	**interface** *interface-type interface-number*	ー
3. キューに GTS を設定する	**qos gts queue** *queue-id* **cir** *committed-information-rate* [**cbs** *committed-burst-size*]	デフォルト：設定なし

5.4 インタフェースのラインレートの設定

物理インタフェースのラインレート（レートリミット）は、受信または送信パケットの最大レートで設定します。

ラインレートの設定手順を以下に示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． interface view に移行する	**interface** *interface-type interface-number*	―
3． ラインレートを設定する	**qos lr** { **inbound** | **outbound** } **cir** *committed-information-rate* [**cbs** *committed-burst-size*]	デフォルト：設定なし

5.5 トラフィックポリシング、GTS、ラインレートの表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
QoSとACLのリソース使用状況を表示する	**display qos-acl resource** [**slot** *slot-number*]
トラフィック動作の設定を表示する	**display traffic behavior user-defined** [*behavior-name*] [**slot** *slot-number*]
インタフェースのGTSの設定と統計情報を表示する	**display qos gts interface** [*interface-type interface-number*]
インタフェースのラインレートの設定と統計情報を表示する	**display qos lr interface** [*interface-type interface-number*]

5.6 トラフィックポリシング、GTS、ラインレートの設定例

5.6.1 ネットワーク要件

図 5-5に示すように設定します。

- Server、Host A、Host B は Device A、Device B を通してインタネットにアクセスできます。
- Server、Host A、Device A の GigabitEthernet 1/0/1 は同一ネットワークセグメントにあります。
- Host B、Device A の GigabitEthernet 1/0/2 は同一ネットワークセグメントにあります。

Server と Host A からのトラフィックを受信する Device A の GigabitEthernet 1/0/3 でトラフィックコントロールを設定します。

- Server からの入力トラフィックレートを 10240kbps に設定します。トラフィックレートが 10240kbps 以下である場合、トラフィックは正常に転送されます。トラフィックレートが 10240kbps を超過したとき、超過トラフィックに DSCP 値 0 をリマークし、トラフィックを転送します。
- Host A からの入力トラフィックレートを 2560kbps に設定します。トラフィックレートが 2560kbps 以下である場合、トラフィックは正常に転送されます。トラフィックレートが 2560kbps を超過したとき、余剰トラフィックを廃棄します。

Device B の GigabitEthernet 1/0/1 と GigabitEthernet 1/0/2 でトラフィックの管理を行います。以下の要件に従います。

- GigabitEthernet 1/0/1 からの入力トラフィックレートを 20480kbps に設定し、余剰トラフィックを廃棄します。
- GigabitEthernet 1/0/2 の出力トラフィックレートを 10240kbps に設定し、余剰トラフィックを廃棄します。

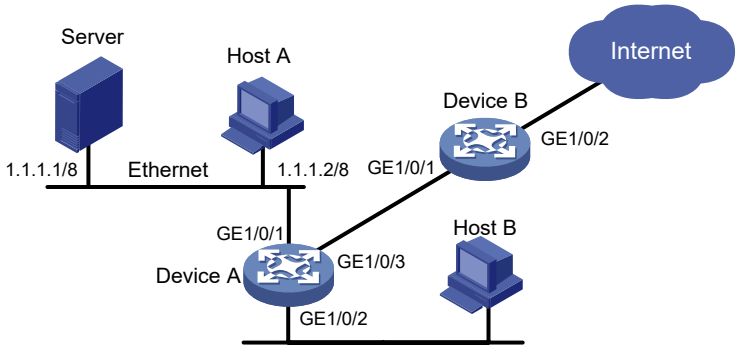


図 5-5 ネットワーク図

5.6.2 設定手順

1)　Device A を設定します。

Server と Host A からのトラフィックにマッチする ACL 2001、ACL 2002 をそれぞれ設定します。

```
[DeviceA] acl basic 2001
[DeviceA-acl-ipv4-basic-2001] rule permit source 1.1.1.1 0
[DeviceA-acl-ipv4-basic-2001] quit
[DeviceA] acl basic 2002
[DeviceA-acl-ipv4-basic-2002] rule permit source 1.1.1.2 0
[DeviceA-acl-ipv4-basic-2002] quit
```

トラフィッククラス **server** を作成し、一致条件に ACL 2001 を適用します。

```
[DeviceA] traffic classifier server
[DeviceA-classifier-server] if-match acl 2001
[DeviceA-classifier-server] quit
```

トラフィッククラス **host** を作成し、一致条件に ACL 2002 を適用します。

```
[DeviceA] traffic classifier host
[DeviceA-classifier-host] if-match acl 2002
[DeviceA-classifier-host] quit
```

トラフィック動作 **server** を作成します。トラフィックポリシーのアクションを設定します。CIR を 10240kbps に設定します。

```
[DeviceA] traffic behavior server
```

```
[DeviceA-behavior-server] car cir 10240 red remark-dscp-pass 0
[DeviceA-behavior-server] quit
```

トラフィック動作 **host** を作成し、トラフィックポリシーのアクションを設定します。CIR を 2560kbps に設定します。

```
[DeviceA] traffic behavior host
[DeviceA-behavior-host] car cir 2560
[DeviceA-behavior-host] quit
```

QoS ポリシー**car** を作成します。トラフィッククラス **server** をトラフィック動作 **server** に関連づけます。トラフィッククラス **host** をトラフィック動作 **host** に関連づけます。

```
[DeviceA] qos policy car
[DeviceA-qospolicy-car] classifier server behavior server
[DeviceA-qospolicy-car] classifier host behavior host
[DeviceA-qospolicy-car] quit
```

GigabitEthernet 1/0/1 のポートの入力トラフィックに QoS ポリシー**car** を適用します。

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] qos apply policy car inbound
```

2)　Device B を設定します。

HTTP パケットにマッチする拡張 ACL 3001 を設定します。

```
<DeviceB> system-view
[DeviceB] acl advanced 3001
[DeviceB-acl-adv-3001] rule permit tcp destination-port eq 80
[DeviceB-acl-adv-3001] quit
```

トラフィッククラス **http** を作成し、一致条件に ACL 3001 を適用します。

```
[DeviceB] traffic classifier http
[DeviceB-classifier-http] if-match acl 3001
[DeviceB-classifier-http] quit
```

トラフィッククラス **class** を作成し、すべてのパケットにマッチするように設定します。

```
[DeviceB] traffic classifier class
[DeviceB-classifier-class] if-match any
[DeviceB-classifier-class] quit
```

トラフィック動作 **car_inbound** を作成し、トラフィックポリシーのアクションを設定します。CIR を 20480kbps に設定します。

```
[DeviceB] traffic behavior car_inbound
[DeviceB-behavior-car_inbound] car cir 20480
[DeviceB-behavior-car_inbound] quit
```

トラフィック動作 **car_outbound** を作成し、トラフィックポリシーのアクションを設定します。CIR を 10240kbps に設定します。

```
[DeviceB] traffic behavior car_outbound
[DeviceB-behavior-car_outbound] car cir 10240
[DeviceB-behavior-car_outbound] quit
```

QoS ポリシー**car_inbound** を作成し、トラフィッククラス **class** と QoS ポリシーのトラフィック動作 **car_inbound** を関連づけます。

```
[DeviceB] qos policy car_inbound
[DeviceB-qospolicy-car_inbound] classifier class behavior car_inbound
[DeviceB-qospolicy-car_inbound] quit
```

QoS ポリシー**car_outbound** を作成し、トラフィッククラス **http** と QoS ポリシーのトラフィック動作 **car_outbound** を関連づけます。

```
[DeviceB] qos policy car_outbound
[DeviceB-qospolicy-car_outbound] classifier http behavior car_outbound
[DeviceB-qospolicy-car_outbound] quit
```

GigabitEthernet 1/0/1 のポートの入力トラフィックに QoS ポリシー**car_inbound** を適用します。

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] qos apply policy car_inbound inbound
```

GigabitEthernet 1/0/2 のポートの入力トラフィックに QoS ポリシー**car_outboun**d を適用します。

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] qos apply policy car_outbound outbound
```

目次

このセクションのページは **8-x-x** です。

6 章 輻輳制御 6-1
6.1 概要 6-1
6.1.1 SP キューイング 6-1
6.1.2 WRR キューイング 6-2
6.2 設定作業リスト 6-4
6.3 インタフェースのキューイングの設定 6-4
6.3.1 キューイングの設定の制限とガイドライン 6-4
6.3.2 SP キューイングの設定 6-4
6.3.3 WRR キューイングの設定 6-4
6.3.4 SP+WRR キューイングの設定 6-5
6.4 輻輳制御の表示と維持 6-6

6章 輻輳制御

6.1 概要

輻輳は、トラフィックサイズがリンクあるいはノードの処理容量を超えるとき、リンクあるいはノードで発生します。これは、統計的多重化ネットワークで起こる輻輳の典型的であり、その他にも、リンク障害、リソース不足、その他 様々な原因によって発生します。

図 6-1に 2 つの典型的な輻輳のシナリオを示します。

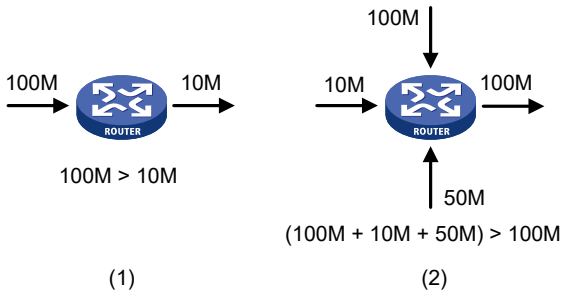


図 6-1 トラフィックの輻輳のシナリオ

輻輳は、以下のような悪影響をもたらします。

- パケット伝送の遅延およびジッタの増加
- ネットワークのスループットおよびリソースの使用効率の減少
- ネットワークリソース（特にメモリ）の枯渇やシステムの故障

輻輳は、スイッチネットワークとマルチユーザーアプリケーション環境では避けられません。ネットワークサービスのパフォーマンスを向上させるために、輻輳に対処する適切な措置の管理と制御を行う必要があります。

輻輳管理の鍵は、パケットを送信する順序を定めたポリシーのリソースを設定することです。

輻輳管理はポートを除外するトラフィックを区分けし、分類しするためにキューイングとスケジューリングアルゴリズムを使用します。

装置は以下のキューースケジューリングメカニズムをサポートします。

6.1.1 SP キューイング

SP キューイングは、輻輳が発生するときに応答遅延を減らすように、優先的なサービスが要求されるミッションクリティカルなアプリケーションのために設計されています。

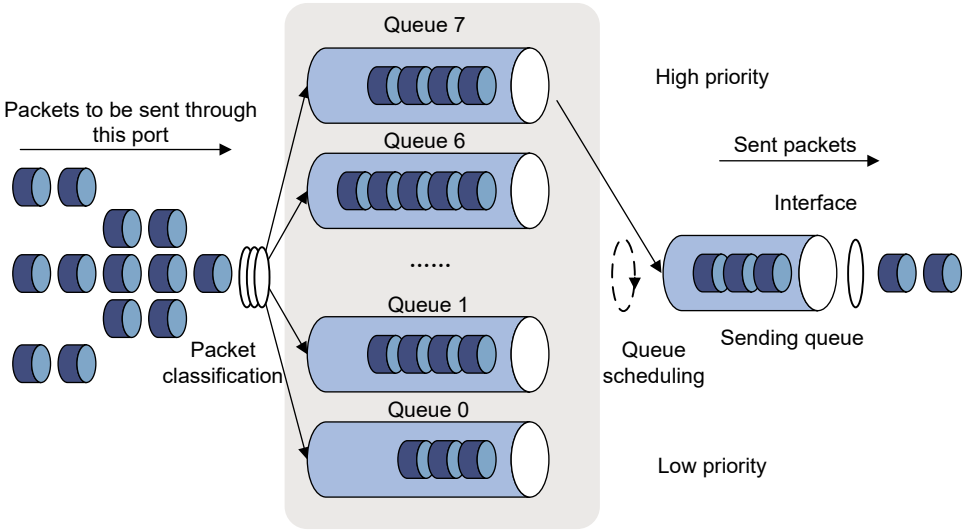


図 6-2 SP キューイング

図 6-2に示すように、SP キューイングはポートに 8 つにクラス分けしたキューを割り当てます。キューの番号 7 から 0 の順に優先順位は低くなります。

SP キューイングは、優先順位が高い方から低い方へ順番に従って 8 つのキューを厳格にスケジューリングします。最初にキューの中のもっとも優先順位が高いパケットを送信します。もっとも高いプライオリティのキューが空のとき、キューの中でその次に優先度の高いプライオリティのパケットが送信されます。ミッションクリティカルなパケットを高いプライオリティキューに割り当てることで、常に最初に処理されるようにし、一般サービスパケットは低いプライオリティに順番付けすることにより、高いプライオリティキューが空のときに送信するようになります。
SP キューの欠点は、より高い優先度のキューにパケットがある場合、低い優先度のキューのパケットは転送できないということです。これは、低い優先度トラフィックの通信停止を引き起こします。

6.1.2 WRR キューイング

図 6-3に示すように、WRR キュースケジューリングアルゴリズムは、あらゆるキューが特定のサービスタイムに割り当てられように、すべてのキューを順にスケジューリングします。

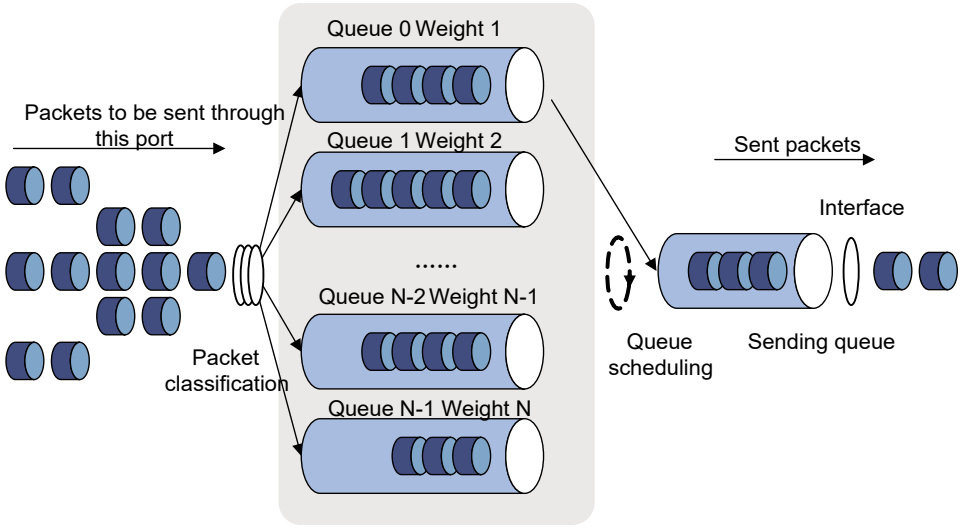


図 6-3 WRR キューイング

ポートに 8 つの出力キューがあると仮定します。WRR は、各キューへリソース割り当てを決めるため、w7、w6、w5、w4、w3、w2、w1、w0 と示される 8 つの重み付けを割り当てます。キューの重みづけはキューに割り当てられたリソースの割合を決定します。100Mbps のポートでは、重みづけの値を 50、30、10、10、50、30、10、10（それぞれ w7、w6、w5、w4、w3、w2、w1、w0 に対応します）に設定できます。このように、最低優先度のキューも、少なくとも 5Mbps（100Mbps ×（最低優先度の重み 10/重みづけの合計 200））の帯域幅が確保できます。こうして、低優先度のキューがなかなか転送されない可能性がある SP キューイングの欠点を回避できます。

キューが総当たりでスケジュールした場合、各キューのサービスタイムが固定されないという WRR キューイングの別の利点があります。キューが空きの場合、次のキューはすぐにスケジューリングされます。帯域幅のリソースを効率的に使用することができます。

WRR キューイングは以下のタイプがあります。

- **基本 WRR キューイング**– 複数のキューが含まれます。各キューの重みを設定することができます。WRR は総当たりでユーザ定義のパラメータにもとづいてキューをスケジュールすることができます。
- **グループベース WRR キューイング**– すべてのキューが WRR によってスケジューリングされます。出力キューを WRR プライオリティキューグループ 1、WRR プライオリティキューグループ 2 に分割することができます。総当たりのキュースケジューリングは最初にグループ 1 を実行します。グループ 1 が空きの場合、グループ 2 が実行されます。

グループベース WRR キューイングが有効なインタフェースでは、SP グループにキューを割り当てることができます。SP グループのキューは SP にスケジューリングされます。SP グループは WRR グループよりも高いプライオリティを持ちます。

🕮 **メモ：**

基本 WRR キューイングは現在のソフトウェアバージョンでサポートされていません。WRR プライオリティキューグループはグループ 1 のみサポートします。

6.2 設定作業リスト

作業リスト
（必須設定項目）インタフェースのキューイングの設定 ● SPキューイングの設定 ● WRRキューイングの設定 ● SP+WRRキューイングの設定

6.3 インタフェースのキューイングの設定

6.3.1 キューイングの設定の制限とガイドライン

ここでは、レイヤ 2 イーサネットインタフェースを「インタフェース」と呼びます。

キュースケジューリングテンプレートは、**display qos queue interface** コマンド出力のキューID、キュー名、グループ、および重みで設定されます。キュースケジューリングテンプレートは、インタフェースのキューパラメータ設定の一意の組み合わせに対応します。

6.3.2 SP キューイングの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. interface *view に移行する*	**interface** *interface-type interface-number*	―
3. SP キュースケジューリングアルゴリズムを設定する	**qos sp**	デフォルト: パケット単位の WRRキューイング

6.3.3 WRR キューイングの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. interface view に移行する	**interface** *interface-type interface-number*	―
3. パケット単位の WRR キューイングを有効にする	**qos wrr weight**	デフォルト: パケット単位の WRRキューイング
4. WRR グループにキューを割り当て、キューのスケジュールパラメータを設定する	**qos wrr** *queue-id* **group 1 weight** *schedule-value*	デフォルト : WRRが有効なすべてのキューはWRRグループ1にあります。キュー0～キュー7の重みは、それぞれ1、2、3、4、5、9、13、15です。

6.3.4 SP+WRR キューイングの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. interface view に移行する	**interface** *interface-type interface-number*	ー
3. パケット単位の WRR キューイングを有効にする	**qos wrr weight**	デフォルト: パケット単位の WRRキューイング
4. SP キュースケジュールグループにキューを割り当てる	**qos wrr** *queue-id* **group sp**	デフォルト : WRRキューが有効なポートはWRRグループ1です キューがインタフェースのトラフィックの負荷でもっとも低いプライオリティを持つ場合、SPグループのキューはスケジューリングされません。
5. WRR グループにキューを割り当て、キューのスケジュールパラメータを設定する	**qos wrr** *queue-id* **group 1 weight** *schedule-value*	デフォルト : WRRが有効なすべてのキューはWRRグループ1にあります。キュー0～キュー7の重みは、それぞれ1、2、3、4、5、9、13、15です。

I. 設定例

1) ネットワーク要件
   - □ GigabitEthernet 1/0/1 で SP+WRR キューイングを設定します。
   - □ GigabitEthernet 1/0/1 のキュー4、5、6、7 に SP グループを割り当てます。
   - □ GigabitEthernet 1/0/1 のキュー0、1、2、3 に WRR グループ 1 を割り当てます。それぞれ重みづけ 1、2、1、3 を設定します。

2) 設定手順

system view に移行します。

```
<Switch> system-view
```

GigabitEthernet11/0/1 に SP+WRR キューイングを設定します。

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] qos wrr weight
[Switch-GigabitEthernet1/0/1] qos wrr 4 group sp
[Switch-GigabitEthernet1/0/1] qos wrr 5 group sp
[Switch-GigabitEthernet1/0/1] qos wrr 6 group sp
[Switch-GigabitEthernet1/0/1] qos wrr 7 group sp
[Switch-GigabitEthernet1/0/1] qos wrr 0 group 1 weight 1
[Switch-GigabitEthernet1/0/1] qos wrr 1 group 1 weight 2
[Switch-GigabitEthernet1/0/1] qos wrr 2 group 1 weight 1
[Switch-GigabitEthernet1/0/1] qos wrr 3 group 1 weight 3
```

6.4 輻輳制御の表示と維持

すべての view で **display** コマンドが実行できます。

操作	コマンド
SPキューイングの情報を表示する	**display qos queue sp interface** [*interface-type interface-number*]
WRRキューイングの情報を表示する	**display qos queue wrr interface** [*interface-type interface-number*]
キューベースの出力トラフィックの統計情報を表示する	**display qos queue-statistics interface** [*interface-type interface-number*] **outbound**
インタフェースの統計情報を削除する	**reset counters interface** [*interface-type interface-number*]

目次

このセクションのページは **8-x-x** です。

7 章 トラフィックフィルタリング 7-1
7.1 設定手順 7-1
7.2 設定例 7-2
7.2.1 ネットワーク要件 7-2
7.2.2 設定手順 7-2

7章 トラフィックフィルタリング

トラフィックフィルタリングは、設定したアクションとクラスを組み合わせることにより受信/送信トラフィックをフィルタします。たとえば、ネットワークの状態にしたがって指定した送信元 IP アドレスのパケットをフィルタすることができます。

7.1 設定手順

以下にトラフィックフィルタリングの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. トラフィッククラスを作成し、traffic class view に移行する	**traffic classifier** *classifier-name* [**operator** { **and** | **or** }]	デフォルト：設定なし
3. マッチ条件を設定する	**if-match** *match-criteria*	デフォルト：設定なし
4. system view に戻る	**quit**	ー
5. トラフィック動作を作成し、traffic behavior view に移行する	**traffic behavior** *behavior-name*	デフォルト：設定なし
6. トラフィックフィルタリングアクションを設定する	**filter** { **deny** | **permit** }	デフォルト：設定なし
7. system view に戻る	**quit**	ー
8. QoS ポリシーを作成し、QoS policy view に移行する	**qos policy** *policy-name*	デフォルト：設定なし
9. トラフィッククラスと QoS ポリシーのトラフィック動作を関連づける	**classifier** *classifier-name* **behavior** *behavior-name*	デフォルト：設定なし
10. system view に戻る	**quit**	ー
11. QoS ポリシーを適用する	● VLANにQoSポリシーを適用する ● インタフェースにQoSポリシーを適用する ● グローバルにQoSポリシーを適用する	必要とされるアプリケーションの宛先の1つを選択してください。 デフォルト：設定なし
12. (オプション設定項目) トラフィックフィルタリングの設定を表示する	**display traffic behavior user-defined** [*behavior-name*]	すべてのviewで実行できます。

7.2 設定例

7.2.1 ネットワーク要件

図 7-1に示すように、GigabitEthernet 1/0/1 で受信し、送信元ポート番号 21 で、パケットをフィルタするためにトラフィックフィルタリングを設定します。

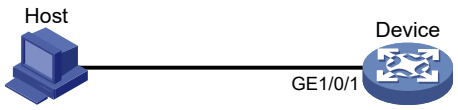


図 7-1 ネットワーク図

7.2.2 設定手順

拡張 ACL 3000 を作成し、送信元ポートが 21 のパケットにマッチするルールを設定します。

```
<Device> system-view
[Device] acl advanced 3000
[Device-acl-ipv4-adv-3000] rule 0 permit tcp source-port eq 21
[Device-acl-ipv4-adv-3000] quit
```

トラフィッククラス **classifier_1** を作成し、トラフィッククラスにマッチする条件として ACL 3000 を参照するように設定します。

```
[Device] traffic classifier classifier_1
[Device-classifier-classifier_1] if-match acl 3000
[Device-classifier-classifier_1] quit
```

#トラフィック動作 **behavior_1** を作成し、パケットを廃棄するトラフィックフィルタリングのアクションを設定します。

```
[Device] traffic behavior behavior_1
[Device-behavior-behavior_1] filter deny
[Device-behavior-behavior_1] quit
```

QoS ポリシー**policy** を作成し、トラフィッククラス **classifier_1** とトラフィック動作 **behavior_1** を関連づけます。

```
[Device] qos policy policy
[Device-qospolicy-policy] classifier classifier_1 behavior behavior_1
[Device-qospolicy-policy] quit
```

GigabitEthernet 1/0/1 の入力トラフィックに QoS ポリシー **policy** を適用します。

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] qos apply policy policy inbound
```

目次

このセクションのページは**8-x-x** です。

8章 プライオリティマーキング 8-1
8.1 概要 8-1
8.2 設定手順 8-1
8.3 プライオリティマーキングの設定例 8-3
8.3.1 ネットワーク要件 8-3
8.3.2 設定手順 8-3

8章 プライオリティマーキング

8.1 概要

プライオリティマーキングは、トラフィックのプライオリティを変更するためにパケットのプライオリティフィールドまたはフラグビットを設定します。たとえば、パケットを転送するプライオリティを変更する場合、トラフィッククラスの IP プレシーデンスまたは DSCP を設定するプライオリティマーキングを用います。

プライオリティマーキングを設定するために、パケットクラスのプライオリティフィールドあるいはフラグビットを以下のように設定します。

1)　トラフィック動作をプライオリティマーキングアクションに設定します。
2)　トラフィッククラスをトラフィック動作に関連づけます。

プライオリティマーキングの設定は、プライオリティマッピングと同時に設定することができます。詳細は、オペレーションマニュアルのセクション 8 *ACL and QoS*”*プライオリティマッピング*”を参照してください。

8.2 設定手順

以下にプライオリティマーキングの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． トラフィッククラスを作成し、traffic class view に移行する	**traffic classifier** *classifier-name* [**operator** { **and** | **or** }]	デフォルト：設定なし
3． マッチ条件を設定する	**if-match** *match-criteria*	デフォルト：設定なし **if-match**コマンドの詳細は、コマンドマニュアルのセクション8 *ACL and QoS*”*QoSポリシー*”を参照してください。
4． system view に戻る	**quit**	ー
5． トラフィック動作を作成し、traffic behavior view に移行する	**traffic behavior** *behavior-name*	デフォルト：設定なし

操作	コマンド	補足

6. プライオリティマーキングアクションを設定する	• DSCP値を設定する：**remark** [**green** | **red** | **yellow**] **dscp** *dscp-value*
	• 802.1pプライオリティを設定する、あるいは内部-外部タグのプライオリティのコピー機能を設定する：
	  • **remark** [**green** | **red** | **yellow**] **dot1p** *dot1p-value*
	  • **remark dot1p customer-dot1p-trust**
	• DSCP マーキングアクションを設定する：**remark** [**green** | **red** | **yellow**] **dscp** *dscp-value*
	• ローカルプレシーデンスを設定する：**remark local-precedence** *local-precedence-value*
	• 外部VLAN IDを設定する：**remark service-vlan-id** *vlan-id*
		1つ以上のいずれかのコマンドを設定します。
		デフォルト：設定なし

7. system view に戻る	**quit**	ー
8. QoS ポリシーを作成し、QoS policy view に移行する	**qos policy** *policy-name*	デフォルト：設定なし
9. トラフィッククラスにQoS ポリシーのトラフィック動作を関連付け得る	**classifier** *classifier-name* **behavior** *behavior-name*	デフォルト：設定なし
10. system view に戻る.	**quit**	ー
11. QoS ポリシーを適用する	• インタフェースにQoSポリシーを適用する • VLANにQoSポリシーを適用する • グローバルにQoSポリシーを適用する	必要とされるアプリケーションの宛先の1つを選択してください。 デフォルト：設定なし
12. （オプション設定項目）プライオリティマーキングの設定を表示する	**display traffic behavior user-defined** [*behavior-name*]	すべてのviewで実行できます。

🕮 **メモ：**

1 つの traffic behavior view で local-precedence と dot1p のリマークは併用できません。

8.3 プライオリティマーキングの設定例

8.3.1 ネットワーク要件

図 8-1に示すように、以下の要件を満足するようにプライオリティマーキングを設定します。

送信元	宛先	プライオリティ
Host A, B	Data server	High
Host A, B	Mail server	Medium
Host A, B	File server	Low

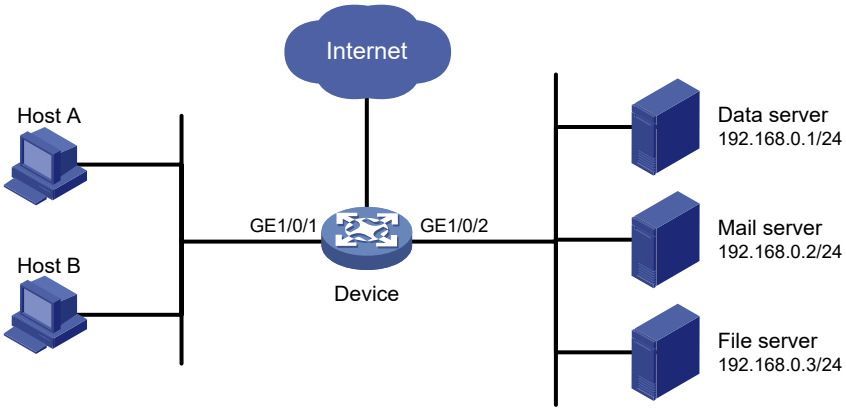


図 8-1 ネットワーク図

8.3.2 設定手順

拡張 ACL 3000 を作成し、宛先 IP アドレス 192.168.0.1 にパケットがマッチするルールを設定します。

```
<Device> system-view
[Device] acl advanced 3000
[Device-acl-ipv4-adv-3000] rule permit ip destination 192.168.0.1 0
[Device-acl-ipv4-adv-3000] quit
```

拡張 ACL 3001 を作成し、宛先 IP アドレス 192.168.0.2 にパケットがマッチするルールを設定します。

```
[Device] acl advanced 3001
[Device-acl-ipv4-adv-3001] rule permit ip destination 192.168.0.2 0
[Device-acl-ipv4-adv-3001] quit
```

拡張 ACL 3002 を作成し、宛先 IP アドレス 192.168.0.3 にパケットがマッチするルールを設定します。

```
[Device] acl advanced 3002
[Device-acl-ipv4-adv-3002] rule permit ip destination 192.168.0.3 0
[Device-acl-ipv4-adv-3002] quit
```

トラフィッククラス **classifier_dbserver** を作成し、トラフィッククラスのマッチ条件に ACL 3000 を適用します。

```
[Device] traffic classifier classifier_dbserver
[Device-classifier-classifier_dbserver] if-match acl 3000
[Device-classifier-classifier_dbserver] quit
```

トラフィッククラス **classifier_mserver** を作成し、トラフィッククラスのマッチ条件に ACL 3001 を適用します。

```
[Device] traffic classifier classifier_mserver
[Device-classifier-classifier_mserver] if-match acl 3001
[Device-classifier-classifier_mserver] quit
```

トラフィッククラス **classifier_fserver** を作成し、トラフィッククラスのマッチ条件に ACL 3002 を適用します。

```
[Device] traffic classifier classifier_fserver
[Device-classifier-classifier_fserver] if-match acl 3002
[Device-classifier-classifier_fserver] quit
```

トラフィック動作 **behavior_dbserver** を作成し、ローカルプレシーデンスの値を 4 としたアクションを設定します。

```
[Device] traffic behavior behavior_dbserver
[Device-behavior-behavior_dbserver] remark local-precedence 4
[Device-behavior-behavior_dbserver] quit
```

トラフィック動作 **behavior_mserver** を作成し、ローカルプレシーデンスの値を 3 としたアクションを設定します。

```
[Device] traffic behavior behavior_mserver
[Device-behavior-behavior_mserver] remark local-precedence 3
[Device-behavior-behavior_mserver] quit
```

トラフィック動作 **behavior_fserver** を作成し、ローカルプレシーデンスの値を 2 としたアクションを設定します。

```
[Device] traffic behavior behavior_fserver
[Device-behavior-behavior_fserver] remark local-precedence 2
[Device-behavior-behavior_fserver] quit
```

QoS ポリシー**policy_server** を作成し、トラフィッククラスを QoS ポリシーのトラフィック動作に関連づけます。

```
[Device] qos policy policy_server
```

```
[Device-qospolicy-policy_server] classifier classifier_dbserver behavior behavior_dbserver
[Device-qospolicy-policy_server] classifier classifier_mserver behavior behavior_mserver
[Device-qospolicy-policy_server] classifier classifier_fserver behavior behavior_fserver
[Device-qospolicy-policy_server] quit
```

GigabitEthernet 1/0/1 の入力トラフィックに QoS ポリシー**policy_server** を適用します。

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] qos apply policy policy_server inbound
[Device-GigabitEthernet1/0/1] quit
```

目次

このセクションのページは **8-x-x** です。

9 章 ネスティング 9-1
9.1 設定手順 9-1
9.2 設定例 9-2
9.2.1 ネットワーク要件 9-2
9.2.2 設定手順 9-3

9章 ネスティング

ネスティングはマッチするパケットに VLAN タグを追加します。対応する VLAN によって、VLAN タグ付けされているパケットを許可するようにします。たとえば、カスタマネットワークからサービスプロバイダネットワークのパケットに外部 VLAN タグを追加します。サービスプロバイダによって割り当てられた VLAN タグをパケットにつけることによってサービスプロバイダネットワークを通過できるようにします。

9.1 設定手順

以下にネスティングの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. トラフィッククラスを作成し、traffic class view に移行する	**traffic classifier** *classifier-name* [**operator** { **and** | **or** }]	デフォルト：設定なし
3. マッチ条件を設定する	**if-match** *match-criteria*	デフォルト：設定なし **if-match**コマンドの詳細はコマンドマニュアルのセクション8 *ACL and QoS*”*QoS*ポリシー”を参照してください。
4. system view に戻る	**quit**	―
5. トラフィック動作を作成し、traffic behavior view に移行する	**traffic behavior** *behavior-name*	デフォルト：設定なし
6. VLAN タグの追加アクションを設定する	**nest top-most vlan** *vlan-id*	デフォルト：設定なし
7. system view に戻る	**quit**	―
8. QoS ポリシーを作成し、QoS policy view に移行する	**qos policy** *policy-name*	デフォルト：設定なし
9. トラフィッククラスを QoS ポリシーのトラフィック動作に関連づける	**classifier** *classifier-name* **behavior** *behavior-name*	デフォルト：設定なし
10. system view に戻る	**quit**	―

操作	コマンド	補足
11．QoS ポリシーを適用する	• インタフェースにQoSポリシーを適用する • VLANにQoSポリシーを適用する • グローバルにQoSポリシーを適用する	必要とされるアプリケーションの宛先の1つを選択してください。 デフォルト：設定なし インタフェースでQinQが有効で、VLANタグを追加するアクションがVLAN IDの一致条件に関連づけられている場合、追加アクションは適用されない可能性があります。追加アクションを適用するため、インタフェースはVLANタグがつけられたパケットを許可する必要があります。

9.2 設定例

9.2.1 ネットワーク要件

図 9-1に示すように、VPN A の Site1 と Site2 は、company の 2 つの支社で、トラフィックを転送するのに、VLAN 5 を使用します。Site1 と Site2 は異なるエリアにあるため、2 つの Site はサービスプロバイダの VPN アクセスサービスを使用します。サービスプロバイダは 2 つの Site に VLAN 100 を割り当てます。

2 つの支社がサービスプロバイダネットワークを通して通信できるように、ネスティングを設定します。

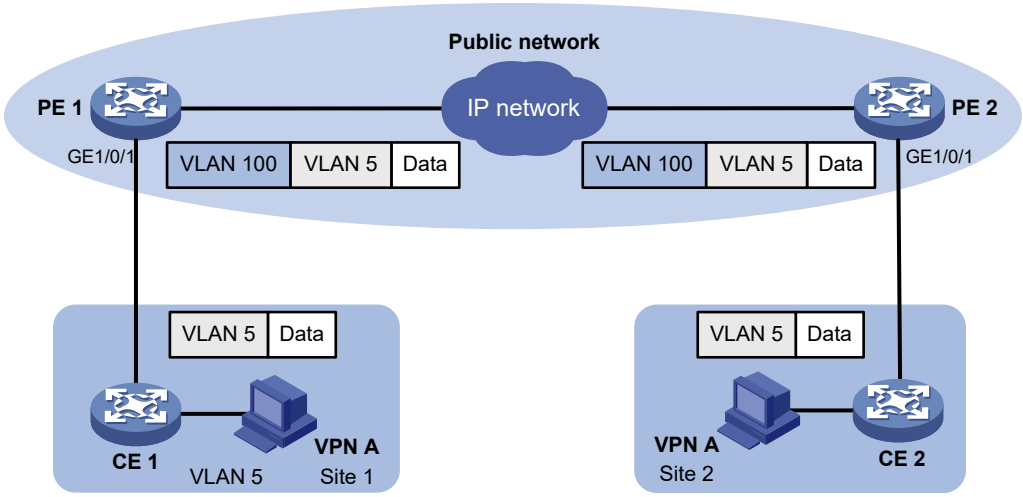


図 9-1 ネットワーク図

9.2.2 設定手順

1)　PE 1 を設定します。

VLAN ID 5 にトラフィックをマッチさせるクラス **test** を作成します。

```
<PE1> system-view
[PE1] traffic classifier test
[PE1-classifier-test] if-match service-vlan-id 5
[PE1-classifier-test] quit
```

トラフィック動作 **test** に外部 VLAN タグ 100 を追加するアクションを設定します。

```
[PE1] traffic behavior test
[PE1-behavior-test] nest top-most vlan 100
[PE1-behavior-test] quit
```

QoS ポリシー**test** を作成し、トラフィッククラス **test** と QoS ポリシーのトラフィック動作 **test** を関連づけます。

```
[PE1] qos policy test
[PE1-qospolicy-test] classifier test behavior test
[PE1-qospolicy-test] quit
```

ハイブリッドポートとして下流ポート GigabitEthernet 1/0/1 を設定し、タグ付けされていないメンバとして VLAN 100 にポートを割り当てます。

```
[PE1] interface gigabitethernet 1/0/1
[PE1-GigabitEthernet1/0/1] port link-type hybrid
[PE1-GigabitEthernet1/0/1] port hybrid vlan 100 untagged
```

QoS ポリシー**test** に下流ポート GigabitEthernet 1/0/1 の入力トラフィックを適用します。

```
[PE1-GigabitEthernet1/0/1] qos apply policy test inbound
[PE1-GigabitEthernet1/0/1] quit
```

トランクポートとして上流ポート GigabitEthernet 1/0/2 を設定し、VLAN 100 に割り当てます。

```
[PE1] interface gigabitethernet 1/0/2
[PE1-GigabitEthernet1/0/2] port link-type trunk
[PE1-GigabitEthernet1/0/2] port trunk permit vlan 100
[PE1-GigabitEthernet1/0/2] quit
```

2)　PE 2 を設定します。

PE1 の設定と同様に PE2 の設定を行います。

目次

このセクションのページは **8-x-x** です。

10 章 トラフィックリダイレクティング 10-1
10.1 設定手順 10-1
10.2 設定例 10-2
10.2.1 ネットワーク要件 10-2
10.2.2 設定手順 10-3

10章 トラフィックリダイレクティング

トラフィックリダイレクトは、指定した基準でパケットをリダイレクトさせます。CPU あるいはインタフェースへのリダイレクトアクションをサポートしています。

10.1 設定手順

以下にトラフィックリダイレクティングの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. トラフィッククラスを作成し、traffic class view に移行する	**traffic classifier** *classifier-name* [**operator** { **and** | **or** }]	デフォルト：設定なし
3. マッチ条件を設定する	**if-match** *match-criteria*	デフォルト：設定なし **if-match**コマンドの詳細はコマンドマニュアルのセクション8 *ACL and QoS*”*QoS*ポリシー”を参照してください。
4. system view に戻る	**quit**	ー
5. トラフィック動作を作成し、traffic behavior view に移行する	**traffic behavior** *behavior-name*	デフォルト：設定なし
6. トラフィックリダイレクティングアクションを設定する	**redirect** { **cpu** | **interface** *interface-type interface-number* }	デフォルト：設定なし CPUへのトラフィックリダイレクティングとインタフェースへのリダイレクティングは同じtraffic 動作で同時に使用することはできません。最後に設定したリダイレクティングアクションが適用されます。
7. system view に戻る	**quit**	ー
8. QoS ポリシーを作成し、QoS policy view に移行する	**qos policy** *policy-name*	デフォルト：設定なし
9. トラフィッククラスを QoS ポリシーのトラフィック動作に関連づける	**classifier** *classifier-name* **behavior** *behavior-name*	デフォルト：設定なし
10. system view に戻る	**quit**	ー

操作	コマンド	補足
11．QoS ポリシーを適用する	• インタフェースにQoSポリシーを適用する • VLANにQoSポリシーを適用する • グローバルにQoSポリシーを適用する	必要とされるアプリケーションの宛先の1つを選択してください。 デフォルト：設定なし QoSポリシーは入力方向に適用されたときのみトラフィックリダイレクティングが適用されます。
12．（オプション設定項目）トラフィックリダイレクティングの設定情報を表示する	**display traffic behavior user-defined** [*behavior-name*]	すべてのviewで実行できます。

10.2 設定例

10.2.1 ネットワーク要件

図 10-1に示すように設定します。

- Device A は 2 つのリンクを通して Device B に接続します。互いに他の装置と同時に通信可能です。
- Device A の GigabitEthernet 1/0/2 と Device B の GigabitEthernet 1/0/2 は VLAN 200 に属しています。
- Device A の GigabitEthernet 1/0/3 と Device B の GigabitEthernet 1/0/3 は VLAN 201 に属しています。
- Device A の VLAN インタフェース 200 の IP アドレスは 200.1.1.1/24 で、VLAN インタフェース 201 の IP アドレスは 201.1.1.1/24 です。
- Device B の VLAN インタフェース 200 の IP アドレスは 200.1.1.2/24 で、VLAN インタフェース 201 の IP アドレスは 201.1.1.2/24 です。

インタフェースにトラフィックリダイレクティングアクションを設定します。

- Device A の GigabitEthernet 1/0/1 で受信した送信元 IP アドレス 2.1.1.1 のパケットは GigabitEthernet 1/0/2 に転送されます。
- Device A の GigabitEthernet 1/0/1 で受信した送信元 IP アドレス 2.1.1.2 のパケットは GigabitEthernet 1/0/3 に転送されます。
- Device A の GigabitEthernet 1/0/1 で受信した他のパケットは、ルーティングテーブルに従って転送されます。

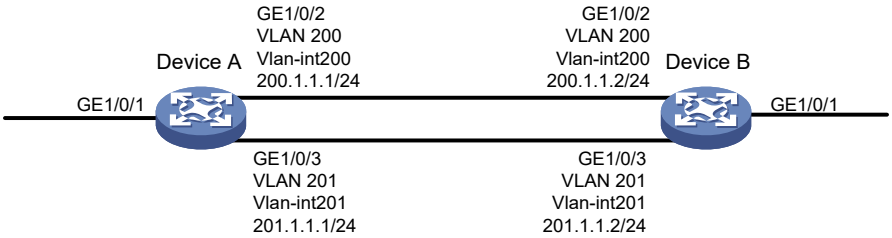


図 10-1 ネットワーク図

10.2.2 設定手順

標準 ACL 2000 を作成し、送信元 IP アドレス 2.1.1.1 のパケットにマッチするルールを設定します。

```
<DeviceA> system-view
[DeviceA] acl basic 2000
[DeviceA-acl-ipv4-basic-2000] rule permit source 2.1.1.1 0
[DeviceA-acl-ipv4-basic-2000] quit
```

標準 ACL 2001 を作成し、送信元 IP アドレス 2.1.1.2 のパケットにマッチするルールを設定します。

```
[DeviceA] acl basic 2001
[DeviceA-acl-ipv4-basic-2001] rule permit source 2.1.1.2 0
[DeviceA-acl-ipv4-basic-2001] quit
```

トラフィッククラス **classifier_1** を作成し、トラフィッククラスのマッチ条件として ACL 2000 を使用します。

```
[DeviceA] traffic classifier classifier_1
[DeviceA-classifier-classifier_1] if-match acl 2000
[DeviceA-classifier-classifier_1] quit
```

トラフィッククラス **classifier_2** を作成し、トラフィッククラスのマッチ条件として ACL 2001 を使用します。

```
[DeviceA] traffic classifier classifier_2
[DeviceA-classifier-classifier_2] if-match acl 2001
[DeviceA-classifier-classifier_2] quit
```

トラフィック動作 **behavior_1** を作成し、GigabitEthernet 1/0/2 にトラフィックリダイレクティングアクションを設定します。

```
[DeviceA] traffic behavior behavior_1
[DeviceA-behavior-behavior_1] redirect interface gigabitethernet 1/0/2
[DeviceA-behavior-behavior_1] quit
```

トラフィック動作 **behavior_2** を作成し、GigabitEthernet 1/0/3 にトラフィックリダイレクティングアクションを設定します。

```
[DeviceA] traffic behavior behavior_2
[DeviceA-behavior-behavior_2] redirect interface gigabitethernet 1/0/3
[DeviceA-behavior-behavior_2] quit
```

QoS ポリシー**policy** を作成します。

```
[DeviceA] qos policy policy
```

トラフィッククラス **classifier_1** を QoS ポリシーのトラフィック動作 **behavior_1** に関連づけます。

```
[DeviceA-qospolicy-policy] classifier classifier_1 behavior behavior_1
```

トラフィッククラス **classifier_2** を QoS ポリシーのトラフィック動作 **behavior_2** に関連づけます。

```
[DeviceA-qospolicy-policy] classifier classifier_2 behavior behavior_2
[DeviceA-qospolicy-policy] quit
```

QoS ポリシー**policy** を GigabitEthernet 1/0/1 の入力トラフィックに適用します。

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] qos apply policy policy inbound
```

目次

このセクションのページは **8-x-x** です。

11 章 クラスベースアカウンティング 11-1
11.1 設定手順 11-1
11.2 設定例 11-2
11.2.1 ネットワーク要件.....11-2
11.2.2 設定手順 11-2

11章 クラスベースアカウンティング

クラスベースアカウンティングは、クラスにもとづいてトラフィック毎の統計情報（パケット毎あるいはバイト毎）を収集します。たとえば、特定の IP アドレスからのトラフィック情報を収集できます。統計情報を分析することにより、例外動作があるかを確認でき、適切な措置をとることが可能になります。

11.1 設定手順

以下にクラスベースアカウンティングの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. トラフィッククラスを作成し、traffic class view に移行する	**traffic classifier** *classifier-name* [**operator** { **and** | **or** }]	デフォルト：設定なし
3. マッチ条件を設定する	**if-match** *match-criteria*	デフォルト：設定なし **if-match**コマンドの詳細はコマンドマニュアルのセクション8 *ACL and QoS*”*QoSポリシー*”を参照してください。
4. system view に戻る	**quit**	―
5. トラフィック動作を作成し、traffic behavior view に移行する	**traffic behavior** *behavior-name*	デフォルト：設定なし
6. アカウンティングアクションを設定する	**accounting** { **byte** | **packet** }	デフォルト：設定なし
7. system view に戻る	**quit**	―
8. QoS ポリシーを作成し、QoS policy view に移行する	**qos policy** *policy-name*	デフォルト：設定なし
9. トラフィッククラスを QoS ポリシーのトラフィック動作に関連づける	**classifier** *classifier-name* **behavior** *behavior-name*	デフォルト：設定なし
10. system view に戻る	**quit**	―
11. QoS ポリシーを適用する	• インタフェースにQoSポリシーを適用する • VLANにQoSポリシーを適用する • グローバルにQoSポリシーを適用する	必要とされるアプリケーションの宛先の1つを選択してください。 デフォルト：設定なし

操作	コマンド	補足
12.（オプション設定項目）トラフィックアカウンティングの設定情報を表示する	• **display qos policy interface** [*interface-type interface-number*] [**inbound** | **outbound**] • **display qos vlan-policy** { **name** *policy-name* | **vlan** [*vlan-id*] } [**slot** *slot-number*] [**inbound** | **outbound**]	すべてのviewで実行できます。

11.2 設定例

11.2.1 ネットワーク要件

図 11-1に示すように、GigabitEthernet 1/0/1 で受信する送信元 IP アドレスが 1.1.1.1/24 のトラフィックを、クラスベースアカウンティングで収集するように設定します。



図 11-1 ネットワーク図

11.2.2 設定手順

標準 ACL 2000 を作成し、送信元 IP アドレス 1.1.1.1 のパケットにマッチするルールを設定します。

```
<Device> system-view
[Device] acl basic 2000
[Device-acl-ipv4-basic-2000] rule permit source 1.1.1.1 0
[Device-acl-ipv4-basic-2000] quit
```

トラフィッククラス **classifier_1** を作成し、トラフィッククラスにマッチする条件として ACL 2000 を使用します。

```
[Device] traffic classifier classifier_1
[Device-classifier-classifier_1] if-match acl 2000
[Device-classifier-classifier_1] quit
```

トラフィック動作 **behavior_1** を設定し、クラスベースアカウンティングアクションを設定します。

```
[Device] traffic behavior behavior_1
```

```
[Device-behavior-behavior_1] accounting packet
[Device-behavior-behavior_1] quit
```

QoS ポリシー**policy** を作成し、トラフィッククラス **classifier_1** を QoS ポリシーのトラフィック動作 **behavior_1** に関連づけます。

```
[Device] qos policy policy
[Device-qospolicy-policy] classifier classifier_1 behavior behavior_1
[Device-qospolicy-policy] quit
```

GigabitEthernet 1/0/1 の入力トラフィックに QoS ポリシー**policy** を適用させます。

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] qos apply policy policy inbound
[Device-GigabitEthernet1/0/1] quit
```

設定を確認するために、トラフィックの統計情報を表示します。

```
[Device] display qos policy interface gigabitethernet 1/0/1

Interface: GigabitEthernet1/0/1

  Direction: Inbound

  Policy: policy
   Classifier: classifier_1
     Operator: AND
     Rule(s) :
      If-match acl 2000
     Behavior: behavior_1
      Accounting enable:
        28529 (Packets)
```

目次

このセクションのページは **8-x-x** です。

12 章 付録 12-1
12.1 付録 A 頭字語 12-1
12.2 付録 B デフォルトプライオリティマップ 12-1
12.3 付録 C パケットプレシーデンスの概要 12-2
12.3.1 IP プレシーデンスと DSCP フィールドの値 12-2
12.3.2 802.1p プライオリティ 12-3

12章 付録

12.1 付録A頭字語

頭字語	フルスペル
BE	Best Effort
CAR	Committed Access Rate
CBS	Committed Burst Size
CIR	Committed Information Rate
DiffServ	Differentiated Service
DSCP	Differentiated Services Code Point
EBS	Excess Burst Size
FIFO	First in First out
GTS	Generic Traffic Shaping
IntServ	Integrated Service
ISP	Internet Service Provider
PE	Provider Edge
PIR	Peak Information Rate
QoS	Quality of Service
RSVP	Resource Reservation Protocol
ToS	Type of Service
VPN	Virtual Private Network
WRR	Weighted Round Robin

12.2 付録B デフォルトプライオリティマップ

デフォルトの dscp-dscp プライオリティマップでは、入力した値と出力の値が同一となります。

表 12-1 デフォルトの dot1p-lp プライオリティマップ

プライオリティの入力値	dot1p-lp マッピング
dot1p	lp
0	2
1	0
2	1
3	3
4	4
5	5
6	6
7	7

表 12-2 デフォルトの dscp-dot1p プライオリティマップ

プライオリティの入力値	dscp-dot1p マッピング
dscp	dot1p
0 ～ 7	0

プライオリティの入力値	dscp-dot1p マッピング
dscp	dot1p
8 ～ 15	1
16 ～ 23	2
24 ～ 31	3
32 ～ 39	4
40 ～ 47	5
48 ～ 55	6
56 ～ 63	7

12.3 付録C パケットプレシーデンスの概要

12.3.1 IP プレシーデンスと DSCP フィールドの値

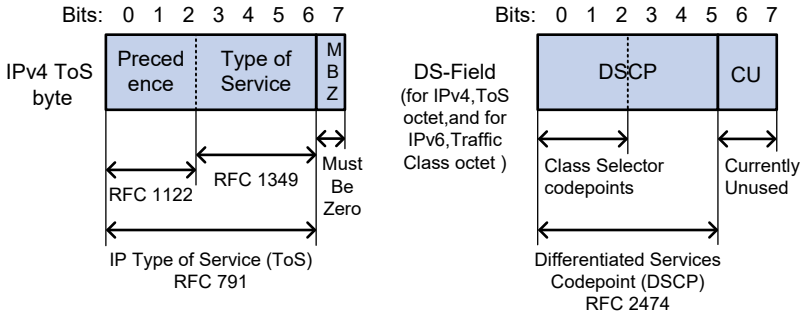


図 12-1 ToS、DS フィールド

図 12-1に示すように、IP ヘッダの ToS フィールドは 8 ビットが含まれます。最初の 3 ビット(0～2)は、0～7 までの IP プレシーデンスを示します。RFC2474 に従い、ToS フィールドは、右側の DS(Differentiated Services)フィールドとして再定義されます。ここで最初の 6 ビット(0～5)は DSCP を表し、0～63 までの値となります。残りの 2 ビット(6、7)は予約された値として使われません。

表 12-3 IP プレシーデンス

IP プレシーデンス(10 進表示)	IP プレシーデンス(2 進表示)	説明
0	000	Routine
1	001	priority
2	010	immediate
3	011	flash
4	100	flash-override
5	101	critical
6	110	internet
7	111	network

表 12-4 DSCP 値

DSCP 値(10 進表示)	DSCP 値(2 進表示)	説明
46	101110	ef
10	001010	af11
12	001100	af12
14	001110	af13
18	010010	af21
20	010100	af22
22	010110	af23
26	011010	af31
28	011100	af32
30	011110	af33
34	100010	af41
36	100100	af42
38	100110	af43
8	001000	cs1
16	010000	cs2
24	011000	cs3
32	100000	cs4
40	101000	cs5
48	110000	cs6
56	111000	cs7
0	000000	be (default)

12.3.2 802.1p プライオリティ

802.1p プライオリティは、レイヤ 2 ヘッダにありレイヤ 3 ヘッダを解析する必要がなく、QoS がレイヤ 2 で必要となるところで使用されます。

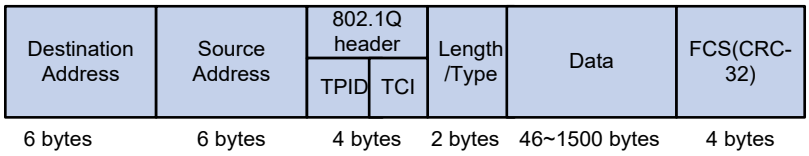


図 12-2 802.1Q タグヘッダの Ethernet フレーム

図 12-2に示すように、4 バイトの 802.1Q タグヘッダはタグプロトコル識別子(TPID、2 バイト長)とタグ管理情報(TCI、2 バイト長)から構成されます。TPID の値は 0x8100 です。図 12-3は、802.1Q ヘッダのフォーマットを示します。802.1Q タグヘッダのプライオリティフィールドは、IEEE802.1p で定義され、802.1p プライオリティと呼ばれます。表 12-5 に 802.1p プライオリティの値を示します。

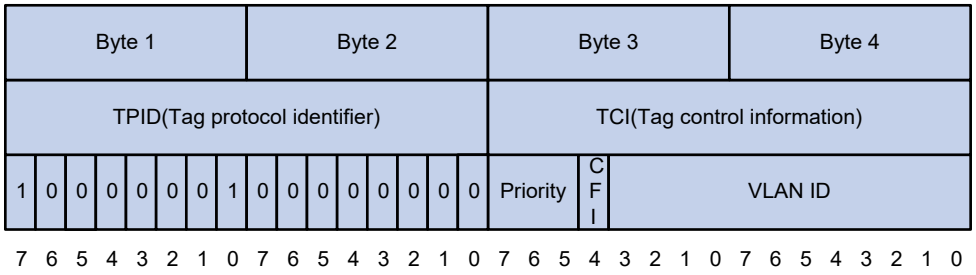


図 12-3 802.1Q タグヘッダ

表 12-5 802.1p プライオリティの説明

802.1p プライオリティ(10 進表示)	802.1p プライオリティ(2進表示)	説明
0	000	best-effort
1	001	background
2	010	spare
3	011	excellent-effort
4	100	controlled-load
5	101	video
6	110	voice
7	111	network-management

目次

このセクションのページは **8-x-x** です。

13 章 データバッファ.....13-1
13.1 設定作業リスト.....13-2
13.2 データバッファ機能の有効化.....13-2
13.3 データバッファのマニュアル設定.....13-4
13.3.1 データバッファのマニュアル 設定 について.....13-4
13.3.2 制限とガイドライン.....13-4
13.4 データバッファの表示およびメンテナンス・コマンド.....13-5
13.5 設定例.....13-5
13.5.1 ネットワーク要件.....13-5
13.5.2 設定手順.....13-5

13章 データバッファ

データバッファはパケットロスを避けるため、一時的にパケットを記録（バッファ）します。

図 13-1にデータバッファの構造を示します。装置は、衝突が発生したとき、出力バッファにパケットを送信するパケットをバッファします。CPU がビジー状態のとき、入力バッファのパケットを記録します。

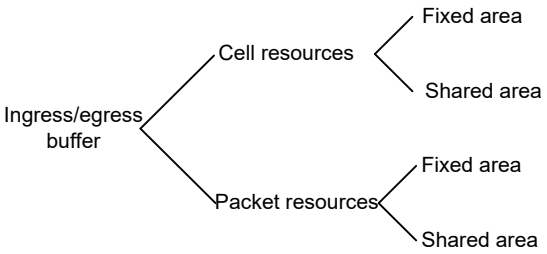


図 13-1 データバッファ構造

インタフェースは、衝突が発生したとき、出力バッファに送信するパケットを記録します。

出力バッファは以下のリソースタイプを使用します。

- **セルリソース** – パケットを記録します。バッファはパケットのサイズにもとづいて、208 バイトのセルリソースを提供します。1 つのセルリソースに 128 バイトのパケットを割り当て、2 つのセルリソースに 300 バイトのパケットを割り当てます。
- **パケットリソース** – パケットの保存場所を記録します。パケットをセルリソースに割り当てた場所を示します。バッファは、各送受信パケットに 1 つのパケットリソースを使用します。

🕮 **メモ：**

装置がブロードキャストあるいはマルチキャストパケットを受信するとき、装置は複数のパケットのコピーを転送します。この場合、セルリソースとパケットリソースは以下のように割り当てられます。

- パケット共有セルリソースのコピーを転送するすべてのインタフェースはパケットを適応させるセルリソースを共有します。
- パケットを転送する各インタフェースは1つのパケットリソースが割り当てられます。

リソースの各タイプには、専用（固定）エリアと共有エリアがあります。

- **専用エリア** – 図 13-2に示すように、すべてのインタフェースに均等に割り当てられ分割されたキューです。衝突が発生したとき以下のように動作します。

a) インタフェースはパケットをバッファするため、最初に専用エリアの関連するキューを使用します。

b) キューが一杯になったとき、インタフェースは共有エリアの対応するキューを使用し

ます。

c) 共有エリアが一杯になったとき、インタフェースは後続のパケットを廃棄します。

システムはユーザによって指定されたキューで共有エリアを割り当てます。キューが一杯でない場合でも、他のキューを使用することはできません。同様にインタフェースのキューに空きがあったとしても、キューを共有することはできません。

- **共有エリア** – 図 13-2に示すように、すべてのインタフェースに不均等に割り当てられ分割されたキューです。システムはキューが一杯でない場合、他のキューを使用することができます。

  システムはすべてのインタフェースで受信されたパケットを到着順にキューに格納します。キューが一杯のとき、後続のパケットを廃棄します。

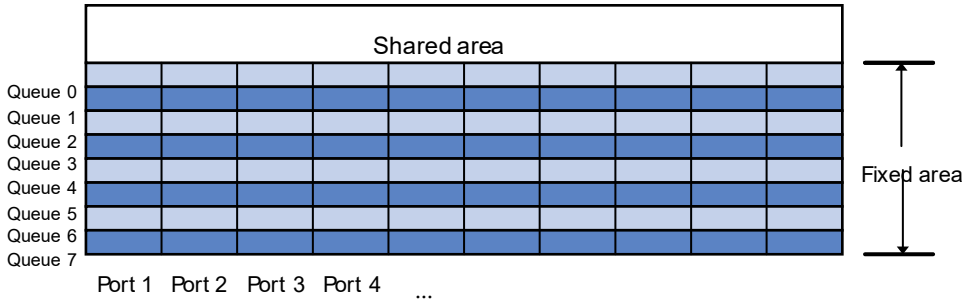


図 13-2 専用（固定）エリアと共有エリア

13.1 設定作業リスト

データバッファを自動で設定することができます。

作業リスト
データバッファ機能の有効化(推奨)
データバッファのマニュアル設定

13.2 データバッファ機能の有効化

データバッファ機能はセルリソースとパケットリソースを自動的に割り当てます。データバッファ機能は以下の状態のパケットバッファを最適化します。

- ブロードキャストあるいはマルチキャストトラフィックが密集して、トラフィックのバーストサイズが大きくなった状態にパケットバッファを最適化します。
- トラフィックが以下の状態にパケットバッファを最適化します。
  - 低速インタフェースから転送された高速トラフィックに転送されている状態にパケットバッファを最適化します。
  - 同一速度の複数ポートから受信されたトラフィックが、同一速度で一つのポートに転送されている状態にパケットバッファを最適化します。

- 装置の高速インタフェースから低速インタフェースにトラフィックが転送されます。
- 複数の同一レートのインタフェースから同一レートでインタフェースにトラフィックが転送されます。

バースト機能が無効の場合、セルリソースとパケットリソースは表 13-1に示すような割合で割り当てられます。

表 13-1 パケットバッファの割り当て（バースト機能が無効の場合）

リソースタイプ	キューの専用（固定）エリアの割合	ポートあるいはキューごとに使用できる共有エリアの割合の最大	共有エリア全体の割合
セル	12%	10%	50%
パケット	12%	10%	52%

バースト機能が有効の場合、セルリソースとパケットリソースは表 13-2に示すような割合で割り当てられます。

表 13-2 パケットバッファの割り当て（バースト機能が有効の場合）

リソースタイプ	キューの専用（固定）エリアの割合	ポートあるいはキューごとに使用できる共有エリアの割合の最大	共有エリア全体の割合
セル	12%	90%	72%
パケット	12%	90%	74%

以下にデータバッファ機能の有効化の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． データバッファ機能を有効にする	**burst-mode enable**	デフォルト：無効 データバッファ機能は既知のユニキャストパケットのみ適用します。 データバッファ機能を無効にすると、PFC機能が長時間動作し、正常に動作しない可能性があります。

13.3 データバッファのマニュアル設定

13.3.1 データバッファのマニュアル 設定について

バッファ、パケットまたはセルの各タイプのリソースには、固定サイズがあります。あるタイプのリソースに共有領域の比率を設定すると、残りは自動的に固定領域に割り当てられます。

デフォルトでは、すべてのキューが共有領域と固定領域を均等に共有します。キューの最大共有領域比率と固定領域比率を変更できます。未構成のキューは、デフォルト設定を使用します。

13.3.2 制限とガイドライン

マルチキャストビデオシナリオで次のパラメータを 100%に設定して、スタックした画像の問題を軽減できます。

- キューのセルリソースの最大共有領域の比率です。
- 細胞資源の総共有面積比。
- キューのパケットリソースの最大共有領域比率。
- パケットリソースの総共有領域比率。

上記の設定は、バースト機能と同時に行うことはできません。これらの設定を行う前に、Burst 機能を無効にしてください。

設定手順

以下にデータバッファ機能の有効化の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. バッファ割り当てルールを設定する	buffer egress [slot slot-number] { cell | packet } total-shared ratio ratio	デフォルト： セルリソース 52% パケットリソース 50%
	buffer egress [slot slot-number] { cell | packet } [queue queue-id] shared ratio ratio	デフォルト： セルリソース 10% パケットリソース 10% 各キューの実際の最大共有領域比率は、設定と送受信されるパケット数に基づいて決定されます。
	buffer egress [slot slot-number] { cell | packet } queue queue-id guaranteed ratio ratio	デフォルト： セルリソース 12% パケットリソース 12% 各キューの実際の最大共有領域比率は、設定と送受信されるパケット数に基づいて決定されます。
3. バッファ割り当てルールを適用する	buffer apply	

13.4 データバッファの表示およびメンテナンス・コマンド

任意のビューで表示コマンドを実行します。

タスク	コマンド
バッファサイズの設定を表示します。	**display buffer** [**slot** *slot-number*] [**queue** [*queue-id*]]

13.5 設定例

13.5.1 ネットワーク要件

図 13-3に示すように、Server は 1000Mbps の Ethernet インタフェースを通して装置に接続します。サーバは不規則に大量のブロードキャストあるいはマルチキャストトラフィックを Host に送信します。各 Host は 100Mbps のネットワークアダプタを通して装置に接続します。

サーバからホストにパケットを送信することを保証し、装置が大量のトラフィックを処理できるように設定します。

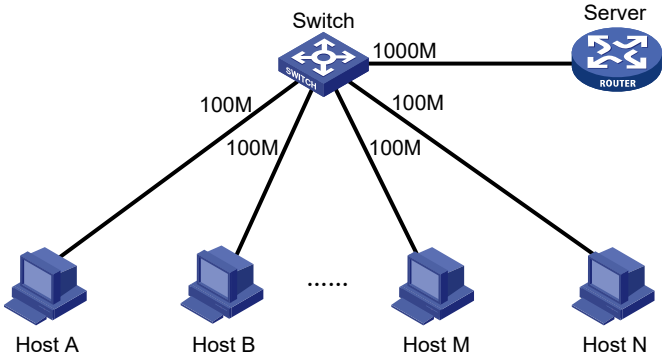


図 13-3 ネットワーク図

13.5.2 設定手順

system view に移行します。

```
<Switch> system-view
```

データバッファ機能を有効にします。

```
[Switch] burst-mode  enable
```

目次

このセクションのページは **8-x-x** です。

14 章 タイムレンジ 14-1
14.1 設定手順 14-1
14.2 タイムレンジの表示と維持 14-1
14.3 タイムレンジの設定例 14-2
14.3.1 ネットワーク要件 14-2
14.3.2 設定手順 14-2
14.3.3 設定の確認 14-2

14章 タイムレンジ

タイムレンジを適用することで、日時をもとにしたサービスを提供することができます。このタイムレンジは指定した期間のみ適用されます。たとえばタイムレンジを設定し、日時を指定した ACL を設定することができます。もしタイムレンジが存在しない場合、サービスは適用されません。

タイムレンジは以下のタイプがあります。

- **周期的タイムレンジ** － 一週間のある曜日、または複数の曜日で周期的に繰り返します。
- **絶対的タイムレンジ** － 一定期間内のみ有効になり、繰り返しません。

タイムレンジはタイムレンジ名によって一意に決められます。最大 1024 のタイムレンジを設定することができますが、各タイムレンジは、32 の周期的な記述と 12 の絶対的な記述まで設定することができます。

1) すべての周期的タイムレンジを組み合わせます。
2) すべての絶対的タイムレンジを組み合わせます。
3) タイムレンジのアクティブな期間として 2 つの記述の AND を行います。

14.1 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. タイムレンジを作成あるいは修正する	**time-range** *time-range-name* { *start-time* **to** *end-time days* [**from** *time1 date1*] [**to** *time2 date2*] | **from** *time1 date1* [**to** *time2 date2*] | **to** *time2 date2* }	デフォルト：設定なし

14.2 タイムレンジの表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
タイムレンジの設定と状態を表示する	**display time-range** { *time-range-name* | **all** }

14.3 タイムレンジの設定例

14.3.1 ネットワーク要件

図 14-1に示すように、Host A が Server に 2015 年 6 月 1 日から 2015 年 12 月 31 日の、営業時間 8:00 から 18:00 のみアクセスできるように、Device A に ACL を設定します。

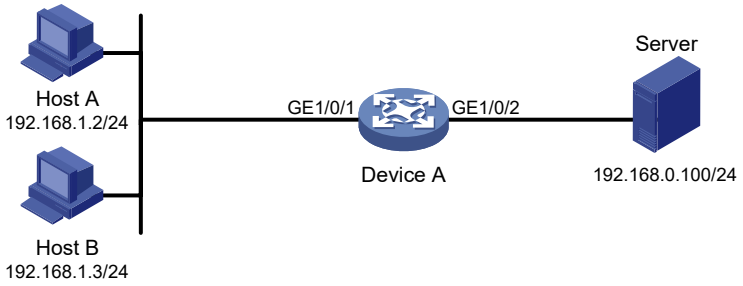


図 14-1 ネットワーク図

14.3.2 設定手順

2015 年 6 月 1 日から 2015 年 12 月 31 日の、営業時間 8:00 から 18:00 の周期的タイムレンジを作成します。

```
<DeviceA> system-view
[DeviceA] time-range work 8:0 to 18:0 working-day from 0:0 6/1/2015 to 24:00 12/31/2015
```

IPv4 標準 ACL 2001 を作成し、タイムレンジ **work** の間、192.168.1.2/32 からのパケットのみ許可するようにルールを設定します。

```
[DeviceA] acl basic 2001
[DeviceA-acl-ipv4-basic-2001] rule permit source 192.168.1.2 0 time-range work
[DeviceA-acl-ipv4-basic-2001] rule deny source any time-range work
[DeviceA-acl-ipv4-basic-2001] quit
```

GigabitEthernet 1/0/2 の出力パケットをフィルタするため、IPv4 標準 ACL 2001 を適用します。

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] packet-filter 2001 outbound
[DeviceA-GigabitEthernet1/0/2] quit
```

14.3.3 設定の確認

Device A でタイムレンジの設定と状態を表示します。

[DeviceA] display time-range all

```
Current time is 13:58:35 6/29/2015 Friday

Time-range : work ( Active )
 08:00 to 18:00 working-day
 from 00:00 6/1/2015 to 00:00 1/1/2016
```

QX-S5100G シリーズ Ethernet スイッチ

オペレーションマニュアル

9. セキュリティ

本マニュアルは以下に示す章で構成されています。

01-AAA
02-802.1X の概要
03-802.1X
04-MAC アドレス認証
05-Web 認証
06-トリプル認証
07-ポートセキュリティ
08-User profile
09-パスワード管理
10-公開鍵
11-PKI
12-SSH
13-SSL
14-TCP フラグメントアタックプロテクション
15-IP ソースガード
16-ARP アタックプロテクション
17-uRPF

目次

このセクションのページは **9-x-x** です。

1 章 AAA 1-1
1.1 概要 1-1
1.1.1 RADIUS 1-2
1.1.2 装置の AAA 実装 1-7
1.1.3 プロトコルと標準 1-9
1.1.4 RADIUS 属性 1-10
1.2 AAA 設定要件と設定作業リスト 1-13
1.3 AAA スキームの設定 1-14
1.3.1 ローカルユーザの設定 1-14
1.3.2 RADIUS スキームの設定 1-17
1.4 ISP ドメインの AAA 方式の設定 1-27
1.4.1 設定要件 1-27
1.4.2 ISP ドメインの作成 1-27
1.4.3 ISP ドメインの属性の設定 1-28
1.4.4 ISP ドメインの認証方式の設定 1-28
1.4.5 ISP ドメインの許可方式の設定 1-29
1.4.6 ISP ドメインのアカウンティング方式の設定 1-30
1.4.7 同時ログインユーザの最大数の設定 1-31
1.5 AAA の表示と維持 1-31
1.6 SSH ユーザのローカル認証、RADIUS アカウンティングの設定例 1-32
1.6.1 ネットワーク要件 1-32
1.6.2 設定手順 1-32
1.6.3 設定の確認 1-33
1.7 RADIUS のトラブルシューティング 1-33
1.7.1 RADIUS 認証の失敗 1-33
1.7.2 RADIUS パケットが到達不能 1-34
1.7.3 RADIUS アカウンティングエラー 1-35

1章 AAA

1.1 概要

AAA は認証（Authentication）、許可（Authorization）、アカウンティング（Accounting）の 3 つのセキュリティ機能の総称です。実用的なネットワークアクセス管理を行うためのフレームワークを提供します。それぞれの以下のセキュリティを提供します。

- **認証** – リモートユーザを特定し、有効なユーザか否かを判断します。
- **許可（認可）** – 認証に成功したユーザに対して提供する権限を制限します。
- **アカウンティング（課金）** – サービスタイプ、開始/終了の時間、トラフィックを含む、認証に成功したユーザのネットワークサービスの使用情報を取得します。これにより、アカウンティング機能は、時間ベースおよびトラフィックベースで、ネットワークセキュリティの監視にも使用することができます。

通常、AAA ではクライアント/サーバモデルを使用します。クライアントは NAS（Network Access Server）上で動作し、サーバで集中的にユーザ情報を管理します。AAA ネットワークにおいて、図 1-1に示すように、NAS はユーザのためのサーバですが、AAA サーバのためのクライアントでもあります。

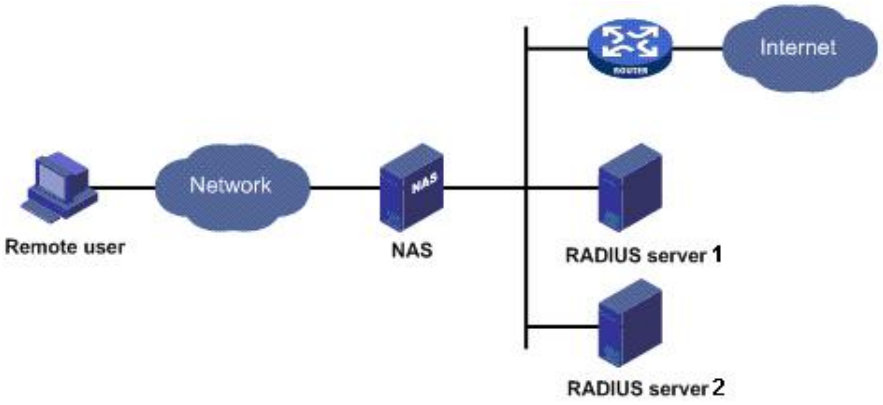


図 1-1 AAA のネットワーク構成

ユーザが NAS への接続を確立し、ほかのネットワーク、またはいくつかのネットワークリソースにアクセスするための権利を取得しようとする場合、NAS は、ユーザまたは対応する接続を認証します。NAS はユーザの AAA 情報をサーバ（RADIUS サーバ）に透過的に通すことができます。その結果 NAS はアクセス要求を許可/禁止するか決定します。

AAA を実現する方法として、最も使用されるものとして RADIUS があります。

図 1-1に示すように、RADIUS サーバ 1 と RADIUS サーバ 2 があります。この場合、必要に応じて、認証、許可、アカウンティングの役割を決めることができます。たとえば、RADIUS サーバ 2 を認証と許可に使用し、RADIUS サーバ 1 をアカウンティングサーバにすることができます。

必要に応じて、AAA を使用してセキュリティ機能を選択することができます。たとえば、会社の従業員が指定のリソースにアクセスする前に、認証を行いたい場合、認証サーバの

みを設定することで実行可能です。ネットワークの使用情報を登録したい場合、アカウンティングサーバも設定することで実行可能になります。

装置は、ダイナミックにパスワードの認証を行うことができます。

1.1.1 RADIUS

RADIUS（Remote Authentication Dial-In User Service）は、クライアント/サーバモデルにおける分散情報交換プロトコルの 1 つです。RADIUS は非許可ユーザのアクセスからネットワークを保護することから、高いセキュリティとリモートユーザアクセスの両方が必要な環境でよく使用されます。

RADIUS 許可は、RADIUS 認証と組み合わせて使用されます。ユーザ許可情報は、認証のレスポンスによって運ばれます。RADIUS はトランスポートプロトコルとして UDP を使用します。RADIUS は認証に UDP ポート 1812 を、アカウンティングに UDP ポート 1813 を使用します。

RADIUS は、元々ダイヤルインユーザアクセスのために定義されました。RADIUS は、イーサネットアクセス、ADSL アクセスのようなより多くのアクセス方式をサポートするために拡張されました。

I. クライアント／サーバモデル

RADIUS クライアントは、ネットワーク中に配置された NAS（Network Attached Storage）上で動作します。NAS は指定されたサーバにユーザ情報を転送し、そのレスポンス（たとえば、ユーザのアクセスリクエストを許可/拒否する）によって動作します。

RADIUS サーバは、ネットワークセンターのコンピュータ、またはワークステーションで動作し、ユーザ認証とネットワークアクセスサービスに関連した情報を管理します。

RADIUS サーバは以下のプロセスを実行します。

1) RADIUS クライアントから認証要求、許可要求、アカウンティング要求を受信します。
2) ユーザ認証、許可、アカウンティングを実行します。
3) ユーザアクセスコントロール情報（たとえば、ユーザのアクセスリクエストを許可/拒否する）をクライアントに送信します。

加えて RADIUS サーバは、認証プロキシのサービスを提供する別の RADIUS サーバのクライアントによって実行することができます。

通常、RADIUS サーバは、Users、Clients、Dictionary の 3 つのデータベースを管理します。

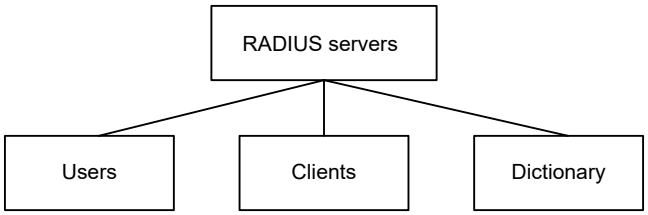


図 1-2 RADIUS サーバデータベース

- **Users** － ユーザ名、パスワード、適用プロトコル、IP アドレスのようなユーザ情報を収容します。
- **Clients** － 共有鍵や IP アドレスのような RADIUS クライアントについての情報を収容します。
- **Dictionary** － RADIUS のプロトコル属性とその値を把握するための情報を収容します。

II. 情報交換セキュリティメカニズム

RADIUS クライアントとサーバは、あらかじめ設定された共有鍵を用いて、情報の交換を行います。RADIUS パケットは Authenticator と呼ばれる 16 バイトフィールドがあります。このフィールドは、MD5 アルゴリズム、共有鍵、ほかのいくつかの情報を使用して作成されたシグネチャを送信します。パケットの受信者はシグネチャを確認し、シグネチャが正しいときのみパケットを受信します。このメカニズムは RADIUS クライアントとサーバ間の情報交換のセキュリティを保証することができます。

共有鍵は RADIUS パケットにあるユーザのパスワードを暗号化するのに使われます。

III. ユーザ認証メカニズム

RADIUS サーバは、PAP、CHAP、EAP のような複数のユーザ認証方式をサポートします。

IV. RADIUS の標準的なパケット交換プロセス

図 1-3にユーザホスト、RADIUS クライアント、RADIUS サーバ間の情報交換について示します。

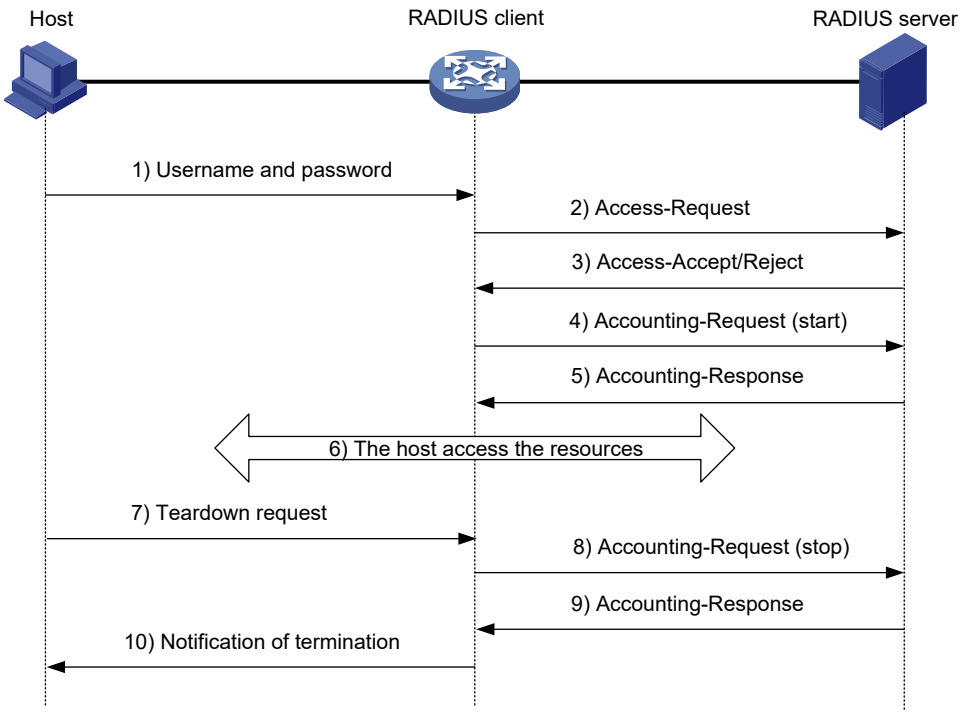


図 1-3 RADIUS の標準的なパケット交換プロセス

RADIUS は以下のように動作します。

1) ホストは、RADIUS クライアントにユーザ名とパスワードを転送し、接続リクエストを送信し始めます。
2) ユーザ名とパスワードを受信した後、RADIUS クライアントは MD5（Message-Digest5）アルゴリズムを使用して暗号化されたユーザパスワードと共有鍵を持つ認証要求（Access-Request）パケットを RADIUS サーバに送信します。
3) RADIUS サーバはユーザ名とパスワードを認証します。認証が成功した場合、ユーザの許可情報を含む Access-Accept message パケットを送り返します。認証に失敗した場合、Access-Reject message パケットを送り返します。
4) RADIUS クライアントは、返された認証結果に従ってユーザを許可、または拒否します。ユーザを許可した場合、クライアントは RADIUS サーバにアカウンティング開始要求（Accounting-Request）パケットを送信します。
5) RADIUS サーバはアカウンティング開始応答（Accounting-Response）パケットを返し、アカウンティングし始めます。
6) ユーザはネットワークリソースにアクセスすることができるようになります。
7) ホストが RADIUS クライアントに接続切断要求を行います。
8) RADIUS クライアントは RADIUS サーバにアカウンティング停止要求（Accounting-Request）パケットを送信します
9) RADIUS サーバは、ユーザのアカウンティングを停止するためにアカウンティング停止応答（Accounting-Response）パケットをクライアントに送り返します。
10) ユーザのネットワークリソースへのアクセスが停止します。

V. RADIUS パケットフォーマット

RADIUS は転送メッセージに UDP を使用します。転送メッセージは、時間管理メカニズム、再送メカニズム、バックアップサーバメカニズムを含む一連のメカニズムによって RADIUS サーバとクライアント間でのスムーズなメッセージ交換を確実にします。図 1-4 に RADIUS パケットのフォーマットを示します。

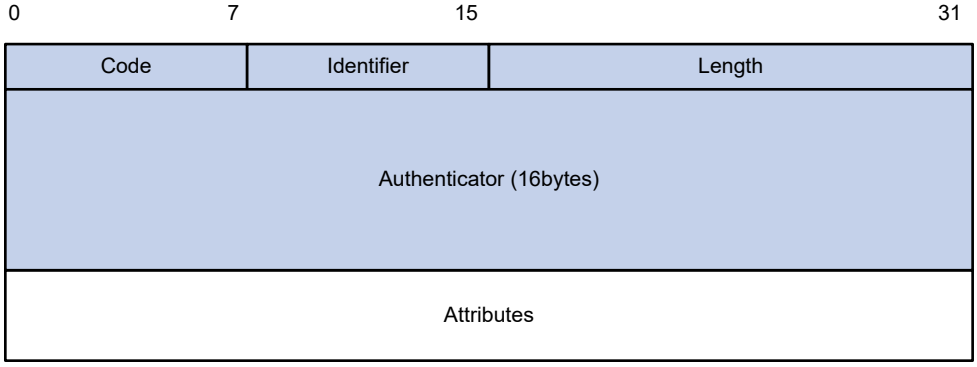


図 1-4 RADIUS パケットフォーマット

以下にフィールドの説明について記載します。

- Code フィールド（1 バイト長）は RADIUS パケットのタイプを表します。表 1-1にコードフィールドと主な値について説明します。

表 1-1 コードフィールドの主な値

Code	パケットタイプ	説明
1	Access-Request	クライアントからサーバに送信されるパケットです。このタイプのパケットは、ユーザを認証するためにサーバにユーザ情報を運ぶために使用されます。このパケットはユーザ名属性を含む必要があり、オプションとしてNAS-IPアドレス、ユーザパスワード、NAS-ポートの属性を含むことができます。
2	Access-Accept	サーバからクライアントに送信されるパケットです。Access-Requestで運ばれるすべての属性値を許可できる場合、つまり、認証が成功する場合、サーバはAccess-Accept応答パケットを送信します。
3	Access-Reject	サーバからクライアントに送信されるパケットです。Access-Requestで運ばれる情報を許可できない場合、サーバはユーザを拒否し、Access-Reject応答パケットを送信します。
4	Accounting-Request	クライアントからサーバに送信されるパケットです。このタイプのパケットはユーザのアカウンティングを開始/停止するためにサーバにユーザ情報を運ぶために使用されます。このパケットは、サーバがアカウンティングの開始/停止するための応答を示すAcct-Status-Type属性を含みます。
5	Accounting-Response	サーバからクライアントに送信されるパケットです。サーバからクライアントに送信するこのタイプのパケットは、Accounting-Requestを受信し、正確にアカウンティング情報を記録し始めたことを通知します。

- Identifier フィールド（1 バイト長）は、要求パケットと応答パケットをマッチングして、再送済みの要求パケットを検出するために使用されます。（認証あるいはアカウンティングのような）同じタイプの要求/応答パケットは同じ identifier を持ちます。
- Length フィールド（2 バイト長）は、Code、Identifier、Length、Authenticator、Attribute フィールドを含む全パケット長を示します。このフィールドの値の範囲は 20～4096 です。この範囲よりも大きい値は、不要なものとみなされ、パケットを受信されても無視します。受信パケットの長さが Length フィールドの範囲よりも小さな値の場合、そのパケットは破棄されます。
- Authenticator フィールド（16 バイト長）は、RADIUS サーバからの応答パケットを認証するために使用され、アルゴリズムを隠すパスワードにも使用されます。要求 Authenticator と応答 Authenticator の 2 種類の Authenticator があります。
- Attribute フィールド（可変長）は、要求、または応答の詳細設定を定義するために指定の認証、許可、アカウンティング情報を運びます。このフィールドは Type、Length、Value の 3 つのサブフィールドが含まれます。
  - □ **Type** – 属性のタイプを示します。
  - □ **Length** – Type、Length、Value フィールドを含む属性の長さを示します。
  - □ **Value** – 属性の値を示します。フォーマットと内容はサブフィールドに依存します。

一般的に使用される RADIUS 属性は、RFC2865、RFC2866、RFC2867、RFC2868 で定義されています。詳細は、オペレーションマニュアルのセクション 9 *セキュリティ”AAA”の”一般的に使われる標準 RADIUS 属性*”を参照してください。

表 1-2 一般的に使用される RADIUS 属性

No.	属性	No.	属性
1	User-Name	45	Acct-Authentic
2	User-Password	46	Acct-Session-Time
3	CHAP-Password	47	Acct-Input-Packets
4	NAS-IP-Address	48	Acct-Output-Packets
5	NAS-Port	49	Acct-Terminate-Cause
6	Service-Type	50	Acct-Multi-Session-Id
7	Framed-Protocol	51	Acct-Link-Count
8	Framed-IP-Address	52	Acct-Input-Gigawords
9	Framed-IP-Netmask	53	Acct-Output-Gigawords
10	Framed-Routing	54	(unassigned)
11	Filter-ID	55	Event-Timestamp
12	Framed-MTU	56-59	(unassigned)
13	Framed-Compression	60	CHAP-Challenge
14	Login-IP-Host	61	NAS-Port-Type
15	Login-Service	62	Port-Limit
16	Login-TCP-Port	63	Login-LAT-Port
17	(unassigned)	64	Tunnel-Type
18	Reply-Message	65	Tunnel-Medium-Type
19	Callback-Number	66	Tunnel-Client-Endpoint
20	Callback-ID	67	Tunnel-Server-Endpoint
21	(unassigned)	68	Acct-Tunnel-Connection
22	Framed-Route	69	Tunnel-Password
23	Framed-IPX-Network	70	ARAP-Password
24	State	71	ARAP-Features
25	Class	72	ARAP-Zone-Access
26	Vendor-Specific	73	ARAP-Security
27	Session-Timeout	74	ARAP-Security-Data
28	Idle-Timeout	75	Password-Retry
29	Termination-Action	76	Prompt
30	Called-Station-Id	77	Connect-Info
31	Calling-Station-Id	78	Configuration-Token
32	NAS-Identifier	79	EAP-Message

No.	属性	No.	属性
33	Proxy-State	80	Message-Authenticator
34	Login-LAT-Service	81	Tunnel-Private-Group-id
35	Login-LAT-Node	82	Tunnel-Assignment-id
36	Login-LAT-Group	83	Tunnel-Preference
37	Framed-AppleTalk-Link	84	ARAP-Challenge-Response
38	Framed-AppleTalk-Network	85	Acct-Interim-Interval
39	Framed-AppleTalk-Zone	86	Acct-Tunnel-Packets-Lost
40	Acct-Status-Type	87	NAS-Port-Id
41	Acct-Delay-Time	88	Framed-Pool
42	Acct-Input-Octets	89	(unassigned)
43	Acct-Output-Octets	90	Tunnel-Client-Auth-id
44	Acct-Session-Id	91	Tunnel-Server-Auth-id

VI. 拡張 RADIUS 属性

RADIUS プロトコルは優れた拡張性を持ちます。RFC 2865 で定義されている属性番号 26（Vender-Specific）は、標準 RADIUS プロトコルが提供しない機能をベンダが実装するために拡張属性を定義することができます。

ベンダはアプリケーションを拡張するために、RADIUS パケットの複数の TLV（type-length-value）のサブ属性をカプセル化することができます。図 1-5に示すように、属性番号 26 でカプセル化されるサブ属性は、以下の 4 つで構成されます。

- **Vendor-ID** – ベンダ ID を示します。最上位のバイト値は 0 で、ほかの 3 つのバイト値には RFC1700 に準拠したコードが入ります。
- **Vendor-Type** – サブ属性のタイプを示します。
- **Vendor-Length** – サブ属性の長さを示します。
- **Vendor-Data** – サブ属性の内容を示します。

RADIUS サブ属性は 25506 のベンダ ID をサポートします。拡張 RADIUS 属性の詳細については、オペレーションマニュアルのセクション 9 *セキュリティ”AAA”の”QX シリーズ用 RADIUS 属性*”を参照してください。

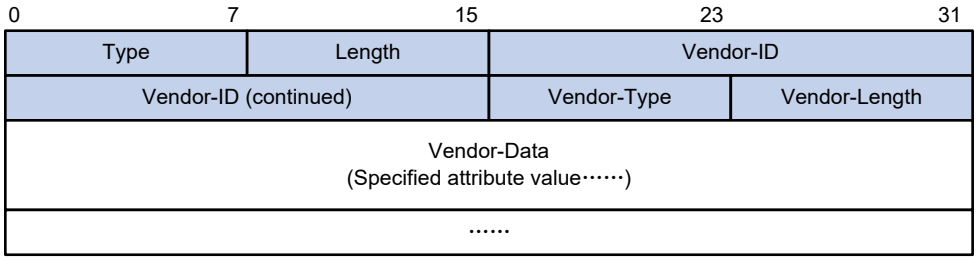


図 1-5 属性番号 26 の拡張 RADIUS 属性フォーマット

1.1.2 装置の AAA 実装

この章は AAA のユーザ管理と方法について記載します。

I. ISP ドメインにもとづくユーザ管理とユーザアクセスタイプ

AAA は ISP ドメインとアクセスタイプもとづいてユーザを管理します。

NAS で各ユーザは 1 つの ISP ドメインに属しています。通常、NAS は、ユーザがログインするために使用するユーザ名によって、ISP ドメインを決定します。

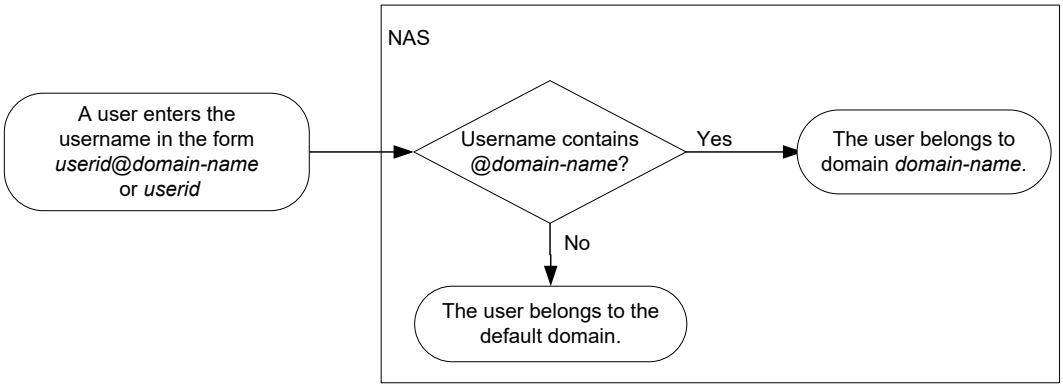


図 1-6 ユーザ名を用いた ISP ドメインの決定

AAA はアクセスタイプにもとづいて、同じ ISP ドメインのユーザを管理します。装置はログインユーザのみサポートします。ログインユーザは以下のタイプのユーザアクセスをサポートします。

- **LAN**－802.1X 認証あるいは MAC アドレス認証にパスした LAN ユーザを含みます。
- **Login**－SSH、Telnet、FTP、装置にログインしている端末のユーザを含みます。端末のユーザはコンソールポートを通してアクセスすることができます。
- **Web**－HTTP、HTTPS を用いて Web インタフェースにログインしている Web ユーザを含みます。

🕮 **メモ：**

ユーザ認証の管理ポリシーに対応するため、装置は 802.1X のような認証モジュールを提供します。認証モジュールを設定した場合、アクセスタイプのユーザの ISP ドメインは認証モジュールの設定に依存します。

II. AAA 認証方式

AAA は ISP ドメインの異なるタイプのユーザのため、異なる認証、許可、アカウンティング方式を設定することができます。NAS はユーザの ISP ドメインとアクセスタイプを決定し、ユーザのアクセスを管理するため、設定された認証方式を使用します。

AAA は ISP ドメインのデフォルト方式の設定をサポートします。デフォルト方式は、特定の AAA 方式が設定されていないユーザに使われます。

装置は、以下の認証方式をサポートします。

- **認証なし** － すべてのユーザが信頼され、認証が実施されません。通常、この方式はセキュリティ目的で使われません。
- **ローカル認証** － 認証は、ユーザ名、パスワード、属性を含むユーザ情報の設定された NAS によって実行されます。ローカル認証は、高速かつ低コストですが、収容できる情報量は、記憶容量に依存します。
- **リモート認証** － アクセス装置は、ユーザを認証するために RADIUS サーバを利用します。RADIUS に関して、装置はユーザ認証を実行するために、標準的な RADIUS プロトコルを使用することができます。リモート認証の特徴は、集中した情報管理、高い能力、高い信頼性、複数の装置のための集中した認証が挙げられます。また、リモート認証サーバが有効でないときのバックアップ方式としてローカル認証を設定することができます。

装置は、以下の許可方式をサポートします。

- **許可なし** － NAS は許可を実行しません。認証にパスするとネットワークに以下のデフォルト許可情報を適用します。
  - □ ログインユーザはネットワークにアクセスできません。
  - □ ログインユーザはレベル 0 ユーザロールを獲得します。レベル 0 ユーザロールの詳細は、オペレーションマニュアルのセクション 1 *はじめに*”*RBAC*”を参照してください。
  - □ FTP、SFTP ユーザが認証にパスしたとき、作業ディレクトリが NAS のルートディレクトリになりますが、アクセスすることはできません。
- **ローカル許可** － ユーザは、ユーザのために設定された属性に従って、NAS によって許可されます。
- **リモート許可** － NAS はユーザを許可するため、RADIUS サーバと協力します。RADIUS 許可は RADIUS 認証と結び付けられます。RADIUS 許可は、RADIUS 認証が成功した後のみ動作し、許可情報は Access-Accept で運ばれます。リモートサーバが有効でない場合は、バックアップ方式としてローカル許可、または許可なしを設定することができます。

装置は、以下のアカウンティング方式をサポートします。

- **アカウンティングなし** － NAS はユーザのアカウンティングを実行しません。
- **ローカルアカウンティング** － ローカルアカウンティング方式は NAS 上で実行されます。ユーザ数の統計情報を収集し、ローカルユーザ接続の数を制御します。ローカルアカウンティング方式は、ユーザ管理のための統計情報を提供しません。
- **リモートアカウンティング** － NAS は、ユーザアカウンティングのために、RADIUS サーバと連携します。リモートサーバが利用できない場合に備えて、バックアップ方法としてローカルアカウンティング方式を設定することができます。

加えて、装置は、セキュリティを向上させるために、以下のサービスを提供します。

- **ユーザロール切り替え認証** － ログアウトや切断を行うことなしで、一時的なユーザロールを使用してユーザを認証します。一時的なユーザロールの許可の詳細は、オペレーションマニュアルのセクション 1 *はじめに*”*RBAC*”を参照してください。

1.1.3 プロトコルと標準

以下に AAA、RADIUS に関連したプロトコルと標準を示します。

- RFC 2865, *Remote Authentication Dial In User Service (RADIUS)*
- RFC 2866, *RADIUS Accounting*
- RFC 2867, *RADIUS Accounting Modifications for Tunnel Protocol Support*
- RFC 2868, *RADIUS Attributes for Tunnel Protocol Support*
- RFC 2869, *RADIUS Extensions*

1.1.4 RADIUS 属性

I. 一般的に使われる標準 RADIUS 属性

番号	属性	説明
1	User-Name	認証されるユーザ名です。
2	User-Password	PAP認証のユーザパスワードです。PAP認証モードでAccess-Requestパケットでのみ存在します。
3	CHAP-Password	CHAP認証のユーザパスワードです。CHAP認証モードでAccess-Requestパケットでのみ存在します。
4	NAS-IP-Address	サーバがクライアントを認識するIPアドレスです。通常、クライアントはNASのアクセスインタフェースで識別され、NASのIPアドレスと呼ばれます。Access-Requestパケットでのみ存在します。
5	NAS-Port	ユーザがアクセスするNASの物理ポートです。
6	Service-Type	ユーザが要求したあるいは提供されたType of serviceです。
7	Framed-Protocol	フレーム化されるカプセル化プロトコルです。
8	Framed-IP-Address	ユーザに割り当てられるIPアドレスです。
11	Filter-ID	フィルタリスト名です。
12	Framed-MTU	ユーザとNAS間のデータリンクの最大転送ユニット（MTU）です。たとえば802.1X EAP認証です。NASはこの属性を使用してEAPパケットのMTUサイズが超過しないようにサーバに知らせます。
14	Login-IP-Host	ユーザアクセスを行うNASインタフェースのIPアドレスです。
15	Login-Service	ユーザがログインするためのサービスタイプです。
18	Reply-Message	ユーザに表示されるテキストです。認証失敗などでサーバがユーザに通知するために使われます。
26	Vendor-Specific	ベンダ仕様属性です。パケットはベンダ属性のような1つ以上の属性を含めることができます。それは1つ以上のサブ属性を含みます。
27	Session-Timeout	セッションが終了する前に提供されるサービスの最大継続時間です。
28	Idle-Timeout	セッションが終了する前に許可される最大Idle時間です。
31	Calling-Station-Id	NASがサーバに送信したユーザ識別子です。QXシリーズのデバイスによって提供されるLANアクセスサービスとして、この属性は、ユーザのHHHH-HHHH-HHHH形式のMACアドレスを保持します。
32	NAS-Identifier	NASがRADIUSサーバを識別するために使用する識別子です。

番号	属性	説明
40	Acct-Status-Type	Accounting-Requestパケットタイプです。 ● **1** – Start ● **2** – Stop ● **3** – Interim-Update ● **4** – Reset-Charge ● **7** – Accounting-On （第3世代（3G）移動体通信システムの標準化プロジェクト）で定義。） ● **8** – Accounting-Off （第3世代（3G）移動体通信システムの標準化プロジェクト）で定義。） ● **9 ～ 14**– トンネルアカウンティング用に予約 ● **15** – 故障用に予約
45	Acct-Authentic	ユーザによって使われる認証方式です。 ● **1** – RADIUS ● **2** – Local ● **3** – Remote
60	CHAP-Challenge	NASは、CHAP認証の間、MD5を計算するためにCHAPチャレンジを作成します。
61	NAS-Port-Type	ユーザによって、認証されているNASの物理ポートタイプです。 ● **15** – Ethernet ● **16** – ADSLのすべてのタイプ ● **17** – ケーブル （ケーブルTV用） ● **19** – WLAN-IEEE 802.11 ● **201** – VLAN ● **202** – ATM もしポートがATMやEthernetで、VLANがそのポートに実装された場合、この属性の値は201です。
79	EAP-Message	NASが、EAPを経由して、カプセル化しているEAPパケットを許可するために使われます。
80	Message-Authenticator	偽のAccess-Requestを防ぐため、認証し、認証パケットをチェックするのに使われます。この属性は、RADIUSがEAP認証をサポートするときに使われます。
87	NAS-Port-Id	ユーザを認証しているNASのポートです。

II. QX シリーズ用 RADIUS 属性

番号	属性	説明
1	Input-Peak-Rate	ユーザからNASへの最大レート（bps）です。
2	Input-Average-Rate	ユーザからNASへの平均レート（bps）です。
3	Input-Basic-Rate	ユーザからNASへの基本レート（bps）です。
4	Output-Peak-Rate	NASからユーザへの最大レート（bps）です。
5	Output-Average-Rate	NASからユーザへの平均レート（bps）です。
6	Output-Basic-Rate	NASからユーザへの基本レート（bps）です。
15	Remanent_Volume	異なるサーバタイプのため、異なるユニットの存在している有効な接続のトータルトラフィックです。

番号	属性	説明
20	Command	セッション管理で使われるセッション処理です。 ● 1– Trigger-Request ● 2– Terminate-Request ● 3– SetPolicy ● 4– Result ● 5– PortalClear
24	Control_Identifier	再送パケット用の識別子です。同一セッションの再送されたパケット用の属性は同じ値を使用する必要があります。異なるセッションの再送されたパケット用の属性は同じ値としてもいいです。再送パケットのクライアントの応答は、この属性を持ち、属性の値は同一にしなくてはいけません。 start、stop、interim updateタイプのAccounting-Requestパケットのための Control-Identifier属性がある場合、値は意味をなしません。
25	Result_Code	Trigger-RequestあるいはSetPolicy動作の戻り値です。値が0の場合、動作が成功し、他の値の場合、動作は失敗しています。
26	Connect_ID	ユーザ接続のインデックスです。
28	Ftp_Directory	FTPユーザの作業ディレクトリです。FTPユーザのため、RADIUSクライアントがFTPサーバとして動作するとき、この属性はRADIUSクライアントのFTPディレクトリを設定するのに使われます。
29	Exec_Privilege	実行ユーザの優先度です。
59	NAS_Startup_Timestamp	NASの開始時間です。1970年1月1日0時0分0秒（UTC時間）からの経過時間を示しています。
60	Ip_Host_Addr	認証とアカウンティング要求で使われるユーザのIPアドレス、MACアドレスです。IPアドレスA.B.C.DとMACアドレスhh:hh:hh:hh:hh:hhの間には空白が必要です。
61	User_Notify	サーバからクライアントに透過的に送信する必要がある情報です。
62	User_HeartBeat	802.1Xユーザが認証をパスした後、32バイト長で割り当てられるハッシュ値です。この属性は、デバイスのユーザリストに記録され、802.1Xユーザからハンドシェイクメッセージをチェックするために使われます。この属性はAccess-Acceptパケットと Accounting-Requestパケットでのみ存在します。
140	User_Group	SSL VPNユーザが認証をパスした後、割り当てられるユーザグループです。ユーザは複数のユーザグループに属することができます。ユーザグループは、セミコロンで区切られます。この属性はSSL VPNデバイスと共有するために使われます。
141	Security_Level	SSL VPNユーザがセキュリティ認証をパスした後、割り当てられるセキュリティレベルです。
201	Input-Interval-Octets	実時間のアカウンティング間隔に入力したバイト数です。
202	Output-Interval-Octets	実時間のアカウンティング間隔に出力したバイト数です。
203	Input-Interval-Packets	デバイスでのユニットセットにおけるアカウンティング間隔に入力したパケット数です。
204	Output-Interval-Packets	デバイスでのユニットセットにおけるアカウンティング間隔に出力したパケット数です。

番号	属性	説明
205	Input-Interval-Gigawords	4Gバイトで分割されたアカウンティング間隔に入力したバイト数の結果です。
206	Output-Interval-Gigawords	4Gバイトで分割されたアカウンティング間隔に出力したバイト数の結果です。
207	Backup-NAS-IP	RADIUSパケットを送信するためのバックアップの送信元IPアドレスです。
255	Product_ID	装置名です。

1.2 AAA設定要件と設定作業リスト

AAA を設定するため、NAS で以下の作業を完了している必要があります。

1) 必要な AAA スキームの設定
   - □ **ローカル認証** – ユーザのユーザ名、パスワードを含む、認証するために必要なローカルユーザと、属性を設定します。
   - □ **リモート認証** – 必要な RADIUS スキームを設定し、サーバに従ってユーザ属性を設定します
2) ユーザの ISP ドメインの AAA 方式を設定します。リモート AAA 方式は ISP domain view で設定された RADIUS スキームを参照します。

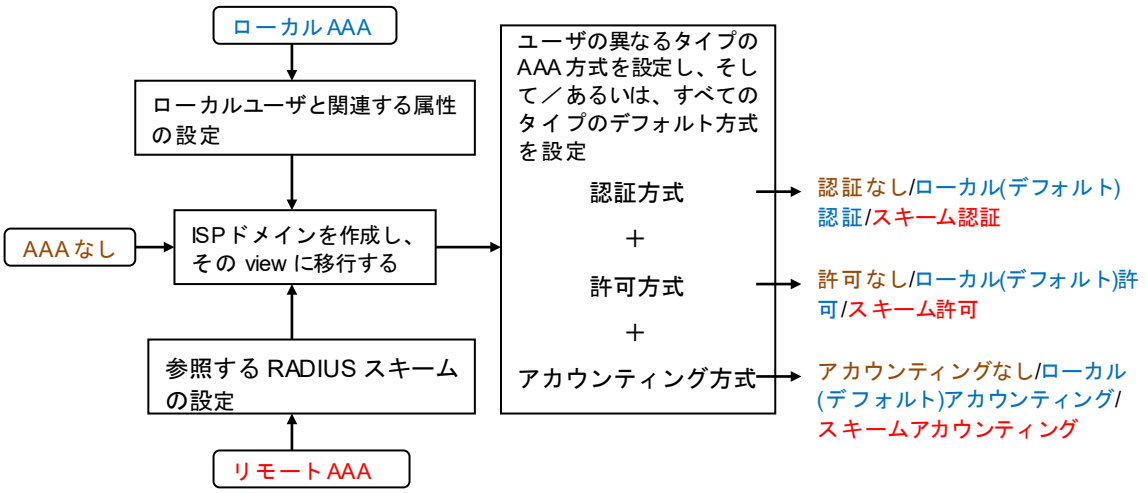


図 1-7 AAA 設定手順

以下に AAA 認証の設定作業リストを示します。

作業リスト
（必須設定項目） ローカルユーザあるいはAAAスキームの設定で、どちらか1つを実行します。 ● ローカルユーザの設定 ● RADIUSスキームの設定

作業リスト
（必須設定項目） ISP ドメインのAAA方式の設定 1. （必須設定項目） ISP ドメインの作成 2. （オプション設定項目） ISP ドメインの属性の設定 3. （必須設定項目）ISP ドメインの AAA 認証、許可、アカウンティングの設定で、少なくとも 1 つを実行します。 • ISP ドメインの認証方式の設定 • ISP ドメインの許可方式の設定 • ISP ドメインのアカウンティング方式の設定
（オプション設定項目）同時ログインユーザの最大数の設定

1.3 AAAスキームの設定

この章はローカルユーザ、RADIUS スキームの設定について記載します。

1.3.1 ローカルユーザの設定

ローカルユーザ認証、許可、アカウンティングを実装するため、装置で、ローカルユーザを作成し、ユーザの属性の設定を行う必要があります。ローカルユーザと属性は装置のローカルユーザデータベースに記録されます。ローカルユーザはユーザ名で識別されます。

ローカルユーザは以下のタイプに分類されます。

- **装置管理**－装置にログインする装置管理ユーザをサポートします。
- **ネットワークアクセスユーザ**－装置を通してネットワークリソースにアクセスするユーザをサポートします。

設定可能なローカルユーザ属性を以下に示します。

- **サービスタイプ**－ユーザが使用できるサービスタイプです。ローカル認証はローカルユーザのサービスタイプをチェックします。もしサービスタイプが有効でない場合、ユーザは認証にパスできません。

  サービスタイプは FTP、LAN アクセス、SSH、Telnet、ターミナルがあります。
- **ユーザ状態**－ローカルユーザがネットワークサービスをリクエストできるかどうかを示します。active と blocked の 2 つの状態があります。active 状態のユーザはネットワークサービスをリクエストできますが、blocked のユーザはリクエストできません。
- **同一ユーザ名を使用する同時ログインユーザの上限**－同一ユーザ名を使用して同時に装置にアクセスすることができるユーザの最大の数です。同一ユーザ名を使用するローカルユーザの数が上限に達するとき、ローカルユーザは、そのユーザ名を使用して装置にアクセスすることができません。
- **ユーザグループ**－各ローカルユーザはローカルユーザグループと、許可属性のようなグループのすべての属性を運んでいます。ローカルユーザグループの詳細は、オペレーションマニュアルのセクション 9 *セキュリティ”AAA”の”ユーザグループ属性の設定*”を参照してください。
- **許可属性**－許可属性は、ローカル認証をパスした後、ユーザの権利を示します。許可属性は ACL、アイドルカット機能、ユーザロール、VLAN、FTP/SFTP 作業ディレク

トリを含みます。許可属性の詳細は、オペレーションマニュアルのセクション 9 *セキュリティ”AAA”の”ローカルユーザ属性の設定”*を参照してください。

ローカルユーザのサービスタイプにもとづいて許可属性を設定します。

user group view ですべてのローカルユーザに適用される属性、local user view でローカルユーザのみに適用される属性となるように、許可属性を設定することができます。local user view で設定した許可属性の設定は、user group view で設定した許可属性よりも優先されます。

- □ user group view で設定した属性はユーザグループのすべてのローカルユーザに適用します。
- □ local user view で設定した属性はローカルユーザのみ適用します。

I. ローカルユーザ設定作業リスト

作業リスト
（必須設定項目） ローカルユーザ属性の設定
（オプション設定項目） ユーザグループ属性の設定
（オプション設定項目） ローカルユーザとローカルユーザグループの表示と維持

II. ローカルユーザ属性の設定

ローカルユーザ属性の設定を行うとき、以下のガイドラインに従ってください。

- 許可属性はアプリケーションの環境と目的に従って設定してください。ユーザのサービスタイプにもとづいて許可属性をサポートします。
  - □ LAN ユーザは acl、user-profile、vlan の許可属性をサポートします。
  - □ telnet、端末ユーザは idle-cut、user-role の許可属性をサポートします。
  - □ http ユーザは user-role の許可属性をサポートします。
  - □ ssh ユーザは idle-cut、user-role、work-directory の許可属性をサポートします。
  - □ ftp ユーザは user-role、work-directory の許可属性をサポートします。
  - □ ほかのユーザは許可属性をサポートしません。

以下にローカルユーザ属性の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. ローカルユーザ(装置管理ユーザ）を追加し、local user view に移行する	**local-user** *user-name* [**class** { **manage** | **network** }]	デフォルト：設定なし
3. （オプション設定項目）ローカルユーザのパスワードを設定する	**password** [{ **hash** | **simple** } *string*]	装置管理ユーザパスワードはハッシュアルゴリズムで暗号化され、cipherで保存されます。 パスワードの設定を行わないローカルユーザは正しいローカルユーザ名と属性のチェックにパスした後、認証をパスすることができます。セキュリティを確保するため、各ローカルユーザにパスワードを設定してください。

操作	コマンド	補足
4. ローカルユーザのサービスタイプを指定する	• ネットワークアクセスユーザ： **service-type lan-access** • 装置管理ユーザ： **service-type** { **ftp** | { **ssh** | **telnet** | **terminal** } * }	デフォルト：設定なし
5. （オプション設定項目）ローカルユーザを active あるいは blocked に設定する	**state** { **active** | **block** }	デフォルト：**active** ネットワークサービスを要求することができます。
6. （オプション設定項目）同時にログインするローカルユーザの上限を設定する	**access-limit** *max-user-number*	デフォルト：制限なし ローカルユーザの設定のみ適用され、アカウンティングをサポートしていないFTPユーザには適用しません。
7. （オプション設定項目）ローカルユーザの許可属性を設定する	**authorization-attribute** { **acl** *acl-number* | **idle-cut** *minute* | **user-profile** profile-name | **user-role** *role-name* | **vlan** *vlan-id* | **work-directory** *directory-name* } *	デフォルト：以下に示します。 • FTPまたはSFTPユーザはNASのルートディレクトリがありますが、アクセス許可がありません。 • network-operatorユーザロールは、network-adminまたはレベル15ユーザによって作成されるローカルユーザに割り当てられます。
8. （オプション設定項目）ローカルユーザのユーザグループを指定する	**group** *group-name*	デフォルト：ローカルユーザはデフォルトユーザグループのsystemに属しています。

III. ユーザグループ属性の設定

ユーザグループはローカルユーザの設定と管理を簡略化します。ユーザグループはローカルユーザのグループから構成され、ローカルユーザ属性の構成があります。グループ内のローカルユーザを集中化してユーザ属性の管理を行うため、ユーザグループ用のローカルユーザ属性を設定することができます。許可属性を含んだユーザ属性を設定できます。

デフォルトでは、新しく追加された各ローカルユーザは、システムデフォルトユーザグループ system に属し、グループのすべての属性に対応します。ローカルユーザが属しているユーザグループを割り当てる場合、local user view で **group** コマンドを使用します。

以下にユーザグループ属性の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	–
2. ユーザグループを作成し、その view に移行する	**user-group** *group-name*	デフォルト：デフォルトユーザグループとしてsystemがあります

操作	コマンド	補足
3. ユーザグループの許可属性を設定する	**authorization-attribute** { **acl** *acl-number* | **idle-cut** *minute* | **user-profile** *profile-name* | **vlan** *vlan-id* | **work-directory** *directory-name* }*	デフォルト：設定なし

IV. ローカルユーザとローカルユーザグループの表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
ローカルユーザの設定とオンラインユーザに関する統計情報を表示する	**display local-user** [**class** { **manage** | **network** } | **idle-cut** { **disable** | **enable** } | **service-type** { **ftp** | **lan-access** | **ssh** | **telnet** | **terminal** } | **state** { **active** | **block** } | **user-name** *user-name* **class** { **manage** | **network** } | **vlan** *vlan-id*]
ユーザグループの設定を表示する	**display user-group** { **all** | **name** *group-name* }

1.3.2 RADIUS スキームの設定

RADIUS スキームは、装置と一緒に動作する RADIUS サーバを指定し、RADIUS サーバの情報を交換するのに使われるパラメータを定義します。パラメータは、サーバの IP アドレス、UDP ポート番号、共有鍵、サーバタイプを含んでいます。

I. 設定作業リスト

作業リスト
（必須設定項目） RADIUSスキームの作成
（必須設定項目） RADIUS認証サーバの指定
（オプション設定項目） RADIUSアカウンティングサーバと関連パラメータの指定
（オプション設定項目） セキュアなRADIUS通信を行うための共有鍵の指定
（オプション設定項目） ユーザ名フォーマットとトラフィック統計情報ユニットの設定
（オプション設定項目） RADIUS要求の再送信の最大試行回数の設定
（オプション設定項目） RADIUSサーバのステータスの設定
（オプション設定項目） 出力するRADIUSパケットの送信元IPアドレスの指定
（オプション設定項目） RADIUSサーバのタイマ機能の設定
（オプション設定項目） RADIUSアカウンティング機能の設定
（オプション設定項目） RADIUSパケットのDSCP値の設定
（オプション設定項目） 再認証を行う際のRADIUSサーバの選択モードの選択
（オプション設定項目） RADIUSの表示と維持

II. RADIUS スキームの作成

ほかの RADIUS 設定を行う前に、RADIUS スキームを作成してください。RADIUS スキームを 16 まで作成することができます。RADIUS スキームは複数の ISP ドメインから参照することができます。

以下に RADIUS スキームの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． RADIUS スキームを作成し、その view に移行する	**radius scheme** *radius-scheme-name*	デフォルト : 起動するコンフィグレーションのタイプに依存します。 ● 初期設定で起動する場合、RADIUSスキームはありません。 ● デフォルトコンフィグレーションファイルで起動する場合、RADIUSスキーム名が**system**のRADIUSスキームが定義されます。 起動時の設定の詳細は、オペレーションマニュアルのセクション 1 *はじめに*”*コンフィグレーションファイル管理*”を参照してください。

III. RADIUS 認証サーバの指定

許可情報は認証の応答パケットに含めて RADIUS クライアントに送信されるため、RADIUS 認証サーバは、認証、許可を一緒に扱います。

1 つのプライマリ認証サーバと 16 のセカンダリ認証/許可サーバを指定することができます。プライマリサーバが有効でないとき、装置は、順番に設定されたセカンダリサーバと通信を行い、**active** 状態の最初のセカンダリサーバと通信を行います。

冗長性を必要としない場合、プライマリサーバのみ指定します。RADIUS 認証サーバは同時に、1 つのスキーム用にプライマリ認証サーバとして機能させ、ほかのスキーム用にセカンダリ認証サーバとして機能させることができます。

以下に RADIUS スキームの RADIUS 認証サーバの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． RADIUS scheme view に移行する	**radius scheme** *radius-scheme-name*	―
3． RADIUS 認証サーバを指定する	● プライマリRADIUS認証サーバを指定する : **primary authentication** { *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** { **cipher** | **simple** } *string*] * ● セカンダリRADIUS認証サーバを指定する : **secondary authentication** { *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** { **cipher** | **simple** } *string*] *	少なくとも1つのコマンドを設定してください。 デフォルト : 指定なし プライマリ認証サーバとセカンダリ認証サーバで、同一のIPアドレス、ポート番号を設定することはできません。

IV. RADIUS アカウンティングサーバと関連パラメータの指定

RADIUS スキームに、1 つのプライマリアカウンティングサーバと 16 のセカンダリアカウンティングサーバを指定することができます。プライマリサーバが有効でないとき、装置は、順番に設定されたセカンダリサーバと通信を行い、**active** 状態の最初のセカンダリサーバと通信を行います。

冗長性を必要としない場合、プライマリサーバのみします。RADIUS アカウンティングサーバは同時に、1 つのスキーム用にプライマリアカウンティングサーバとして機能させ、ほかのスキーム用にセカンダリアカウンティングサーバとして機能させることができます。

装置は以下の状況でアカウンティングサーバにアカウンティング停止要求（stop-accounting request）を送信します。

- ホストから接続切断要求を受信します。
- 管理者から接続切断通知を受信します。

アカウンティング要求に対して、指定した試行回数の上限に達しても応答がない場合、ユーザを切断します。

RADIUS は FTP、SFTP ユーザのアカウンティングをサポートしていません。

以下に RADIUS スキームのアカウンティングサーバと関連パラメータの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. RADIUS scheme view に移行する	**radius scheme** *radius-scheme-name*	—
3. RADIUS アカウンティングサーバを指定する	• プライマリRADIUSアカウンティングサーバを指定する： **primary accounting** { *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** { **cipher** | **simple** } *string*] * • セカンダリRADIUSアカウンティングサーバを指定する： **secondary accounting** { *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** { **cipher** | **simple** } *string*] *	少なくとも1つのコマンドを設定してください。 デフォルト：指定なし プライマリアカウンティングサーバとセカンダリアカウンティングサーバで、同一のIPアドレス、ポート番号を設定することはできません。
4. （オプション設定項目）アカウンティング要求の最大試行回数を設定する	**retry realtime-accounting** *retry-times*	デフォルト：5
5. （オプション設定項目）応答のない RADIUS ストップアカウンティング要求のバッファを有効にする	**stop-accounting-buffer enable**	デフォルト：有効

操作	コマンド	補足
6.　（オプション設定項目）RADIUS ストップアカウンティング要求の最大試行回数を設定する	**retry stop-accounting** *retries*	デフォルト：500

V. セキュアな RADIUS 通信を行うための共有鍵の指定

RADIUS クライアントと RADIUS サーバは、パケット認証とユーザパスワードの暗号化を行うため、MD5 アルゴリズムを使用して、クライアントとサーバ間で交換するパケットと共有鍵を暗号化し、パケットの検証を行います。同じ共有鍵が使用される場合のみ、パケットを適切に受信し、応答を返すことができます。

スキームで同じタイプ（アカウンティングあるいは認証）のすべてのサーバで、共有鍵が設定されます。RADIUS サーバ用に個別に設定された共有鍵よりも優先度は低くなります。

以下にセキュアな RADIUS 通信を行うための共有鍵の設定を示します。

操作	コマンド	補足
1.　system view に移行する	**system-view**	―
2.　RADIUS scheme view に移行する	**radius scheme** *radius-scheme-name*	―
3.　セキュアな RADIUS 通信を行うための共有鍵を指定する	**key** { **accounting** | **authentication** } { **cipher** | **simple** } *string*	デフォルト：指定なし 装置とRADIUSサーバで必ず同じ共有鍵を設定するようにしてください。

VI. ユーザ名フォーマットとトラフィック統計情報ユニットの設定

ユーザ名は、一般的に *userid@isp-name* のフォーマットで表されます。*isp-name* はユーザが属している ISP ドメイン名で、ユーザがどこの ISP ドメインに属しているか装置が認識するのに使われます。しかし初期の RADIUS サーバは ISP ドメイン名が含まれていないユーザ名を認識することはできません。この場合、ユーザ名を送信する前に各ユーザ名のドメイン名を削除する必要があります。

同一 RADIUS スキームを参照するために 2 つ以上の ISP ドメインを使用する場合、ドメインを識別するため、ユーザ名の中の ISP ドメイン名を削除しないでください。

装置は、アカウンティングパケットのオンラインユーザのトラフィックの統計情報を RADIUS アカウンティングサーバに周期的に通知します。正しいトラフィック統計情報を行うため、装置でのデータフローのユニットとパケットのユニットが、RADIUS サーバのユニットと同一になっていることを確認してください。

以下にユーザ名フォーマットとトラフィック統計情報ユニットの設定を示します。

操作	コマンド	補足
1.　system view に移行する	**system-view**	―
2.　RADIUS scheme view に移行する	**radius scheme** *radius-scheme-name*	―

操作	コマンド	補足
3. RADIUS サーバに送信されるユーザ名の形式を指定する	**user-name-format** { **keep-original** | **with-domain** | **without-domain** }	デフォルト：**with-domain** 起動時の設定の詳細については、オペレーションマニュアルのセクション1 *はじめに”コンフィグレーションファイル管理”* を参照してください。
4. （オプション設定項目）RADIUS サーバへ送信されるデータフロー、またはパケットの単位を指定する	**data-flow-format** { **data** { **byte** | **giga-byte** | **kilo-byte** | **mega-byte** } | **packet** { **giga-packet** | **kilo-packet** | **mega-packet** | **one-packet** }}*	データフロー：**byte** パケット：**one-packet**

VII. RADIUS 要求の再送信の最大試行回数の設定

RADIUS はデータ送信に UDP を使用しているため、通信に信頼性がありません。応答タイムアウト時間（**timer response-timeout** コマンドで設定されます。）が切れる前に RADIUS サーバから応答がなかった場合、NAS は RADIUS リクエストを再送します。再送の試行回数が上限に達しても、RADIUS サーバから応答がない場合、**active** 状態の他の RADIUS サーバと通信を試みます。**active** 状態の他の RADIUS サーバから応答がない場合、装置は認証あるいはアカウンティングが失敗したとみなします。RADIUS サーバ応答タイムアウト時間についての詳細は、オペレーションマニュアルのセクション 9 *セキュリティ”AAA”の”RADIUS サーバのタイマ機能の設定”* を参照してください。

以下に RADIUS 要求の再送信の最大試行回数の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. RADIUS scheme view に移行する	**radius scheme** *radius-scheme-name*	―
3. RADIUS 要求の再送信の最大試行回数を設定する	**retry** *retry-times*	デフォルト：3

VIII. RADIUS サーバのステータスの設定

RADIUS サーバのステータスを blocked 状態あるいは active 状態に設定することで、装置と通信を行う現在のサーバが有効でなくなったときに、接続先の制御ができます。実際には、1 つのプライマリ RADIUS サーバと、プライマリサーバのバックアップとして動作する複数のセカンダリ RADIUS サーバを指定することができます。一般的に装置は、以下のルールにもとづいてサーバを選択します。

- プライマリサーバが active 状態のとき、装置はプライマリサーバと通信します。
  - □ プライマリサーバが故障したとき装置は以下の処理を行います。
  - □ サーバのステータスを blocked 状態に変更します。
  - □ サーバの quiet タイマを開始します。
- active 状態のセカンダリサーバと通信を行います。（最初に設定されたセカンダリサーバが高い優先度を持ちます）
- セカンダリサーバが有効でなくなったとき、装置は以下の処理を行います。

- □ サーバのステータスを blocked 状態に変更します。
- □ サーバの quiet タイマを開始します。
- □ active 状態の次のセカンダリサーバのチェックを行います。このプロセスは、装置が有効なセカンダリサーバを見つける、あるいは active 状態のすべてのセカンダリサーバのチェックを完了するまで行います。

- quiet タイマの時間が経過した場合あるいは手動で active 状態に設定した場合、サーバは active 状態になります。しかし装置は認証あるいはアカウンティングプロセスの間、サーバを再度チェックしません。

  もし 1 回の検索プロセスで通信可能なサーバが見つからない場合、認証あるいはアカウンティングの試みが失敗したと認識します。
- もし使用している認証あるいはアカウンティングサーバが削除された場合、サーバと装置の通信はタイムアウトとなります。装置は最初から active 状態のサーバを検索します。最初にプライマリサーバ（もしある場合）をチェックし、次にセカンダリサーバをチェックする順番で確認します。
- プライマリとセカンダリサーバの両方が blocked 状態の場合、装置はすべてのサーバと通信しません。
- 1 つのサーバが active 状態で、ほかのすべてのサーバが blocked 状態の場合、装置は、たとえサーバが有効でない場合でも active 状態のサーバのみと通信します。
- RADIUS サーバの状態が自動的に変更する場合、装置はすべての RADIUS スキームに従いサーバの状態を変更します。

デフォルトでは、すべての RADIUS サーバの状態は active となります。必要に応じて、サーバの状態を変更できます。たとえば、サーバが故障している場合、サーバとの通信を防ぐために blocked となっているサーバの状態を変更することができます。

以下に RADIUS サーバのステータスの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. RADIUS scheme view に移行する	**radius scheme** *radius-scheme-name*	—

操作	コマンド	補足
3． RADIUS サーバのステータスを設定する	● プライマリRADIUS認証サーバのステータスを設定する： **state primary authentication** { **active** | **block** } ● プライマリRADIUSアカウンティングサーバのステータスを設定する： **state primary accounting** { **active** | **block** } ● セカンダリRADIUS認証サーバのステータスを設定する： **state secondary authentication** [{ *ipv4-address* | **ipv6** *ipv6-address* } [*port-number*] *] { **active** | **block** } ● セカンダリRADIUSアカウンティングサーバのステータスを設定する： **state secondary accounting** [{ *ipv4-address* | **ipv6** *ipv6-address* } [*port-number*] *] { **active** | **block** }	少なくとも1つのコマンドを設定します。 デフォルト：RADIUSスキームに指定されたサーバはactive状態です。 設定されたサーバのステータスは設定ファイルに保存することができません。**display radius scheme**コマンドを使用して表示することのみ可能です。 装置の再起動後、すべてのサーバはactive状態に戻ります。

IX. 出力する RADIUS パケットの送信元 IP アドレスの指定

NAS が送信した RADIUS パケットの送信元 IP アドレスは、RADIUS サーバで設定された NAS の IP アドレスとマッチする必要があります。RADIUS パケットを受信する際、RADIUS サーバはパケットの送信元 IP アドレスが管理された NAS の IP アドレスかどうか確認します。

- パケットの送信元 IP アドレスが管理された NAS の IP アドレスとマッチしている場合、サーバは処理を行います。
- パケットの送信元 IP アドレスが管理された NAS の IP アドレスとマッチしていない場合、パケットを廃棄します。

一般的に、RADIUS パケットの送信元アドレスは NAS のいずれかの出力インタフェースの IP アドレスです。ある状況においては、送信元 IP アドレスを変更する必要があります。

RADIUS scheme view、または system view で出力する RADIUS パケットの送信元 IP アドレスを指定することができます。

- RADIUS scheme view で指定された IP アドレスは、1 つの RADIUS scheme のみに適用されます。
- system view で指定された IP アドレスは、すべての RADIUS scheme に適用されます。

RADIUS パケットを送信する前に、NAS は以下の順番で送信元 IP アドレスを選択します。

1) RADIUS スキーム用に指定された送信元 IP アドレス
2) system view で指定された送信元 IP アドレス
3) ルートで指定された出力インタフェースの IP アドレス

以下にすべての RADIUS スキームの送信元 IP アドレスの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. 出力する RADIUS パケットの送信元 IP アドレスを指定する	**radius nas-ip** { *ipv4-address* | **ipv6** *ipv6-address* }	デフォルト : RADIUSパケットを送信するインタフェースのIPアドレスが指定されます。

以下に指定された RADIUS スキームの送信元 IP アドレスの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. RADIUS scheme view に移行する	**radius scheme** *radius-scheme-name*	ー
3. 出力する RADIUS パケットの送信元 IP アドレスを指定する	**nas-ip** { *ipv4-address* | **ipv6** *ipv6-address* }	デフォルト：system view で **radius nas-ip**コマンドが設定されたIPアドレスが使用されます。設定されていない場合、RADIUSパケットを送信するインタフェースのIPアドレスが指定されます。

X. RADIUS サーバのタイマ機能の設定

装置は、RADIUS サーバとの通信を管理するため、以下のタイマを使用します。

- **RADIUS サーバの応答タイムアウトタイマ**（**response-timeout**） – RADIUS リクエスト再送信間隔です。このタイマは RADIUS リクエストが送信された後、すぐに開始します。装置はタイマが満了する前に RADIUS サーバから応答を受信しない場合、リクエストを再送します。
- **サーバ停止タイマ**（**quiet**） – block 状態にある到達不能のサーバを保持する時間です。1 つのサーバが到達不能である場合、装置はサーバのステータスを blocked 状態に変更し、サーバ停止タイマを開始します。active 状態の別のサーバと通信しようとします。サーバ停止タイマが満了した後、装置はサーバの状態を active に戻します。
- **リアルタイムのアカウンティング間隔**（**realtime-accounting**） – ユーザのリアルタイムアカウンティングを実行する間隔を定義します。このタイマが設定されると、装置は指定された間隔で、オンラインユーザのアカウンティング情報を RADIUS サーバに送信します。装置がサーバからの応答を受信しない場合、ユーザの接続が強制的に切断されます。

RADIUS サーバのタイマを設定するとき、以下のガイドラインに従ってください。

- RADIUS パケットの再送信の最大試行回数の設定と RADIUS サーバ応答タイムアウトタイマの設定を行うとき、セカンダリサーバの数を考慮してください。再送プロセスに十分な時間がない場合、Telnet のようなアクセスモジュールのクライアント接続では、有効なサーバを検索しようとしている間にタイムアウトしてしまう可能性があります。
- セカンダリサーバ数が設定されたとき、たとえパケット転送試行制限とサーバ応答タイムアウト期間が小さい値で設定されている場合でも、クライアント接続タイムアウトの時間を短く設定している、アクセスモジュールのクライアント接続は、初期認証あるいはアカウンティングの間にタイムアウトしてしまう可能性があります。この場

合、装置はブロックする到達不能サーバの状態と短くした到達可能サーバを検索する時間を設定しているため、次の認証あるいはアカウンティングの試行は成功します。

- サーバ停止タイマは、適切に設定してください。短すぎると、サーバは active 状態の到達不能なサーバの通信を繰り返し試みる必要があるため、頻繁に認証あるいはアカウンティングが失敗します。タイマの時間を長くすると、タイマの期間が満了する間に blocked 状態になるため、一時的に故障から回復した到達可能なサーバをブロックする可能性があります。
- リアルタイムのアカウンティング間隔の設定は、NAS と RADIUS サーバの性能によって代わります。短い間隔にすると、より正確なアカウンティングを行うことができますが、高い性能が必要となります。ユーザの最大数が多い（1000 以上）の場合、間隔を長くしてください。

以下に RADIUS サーバのタイマ機能の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. RADIUS scheme view に移行する	**radius scheme** *radius-scheme-name*	—
3. RADIUS サーバの応答タイムアウトタイマを設定する	**timer response-timeout** *seconds*	デフォルト：3秒
4. サーバの停止タイマを設定する	**timer quiet** *minutes*	デフォルト：5分
5. リアルタイムアカウンティング間隔を設定する	**timer realtime-accounting** *interval*	デフォルト：12分

XI. RADIUS アカウンティング機能の設定

アカウンティング機能を有効にした場合、装置は再起動した後に RADIUS サーバに accounting-on パケットを自動的に送信します。accounting-on パケットを受信すると、RADIUS サーバは装置に対して再ログインできるように全オンラインユーザをログアウトします。この機能を使用しない場合、RADIUS サーバはユーザがオンライン中と見なしているため再起動後にユーザが再ログインすることができません。

装置が accounting-on パケットを再送するために待機する間隔と最大試行回数を設定できます。

以下に RADIUS スキームのアカウンティング機能設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. RADIUS scheme view に移行する	**radius scheme** *radius-scheme-name*	—
3. RADIUS サーバの応答タイムアウトタイマを設定する	**accounting-on enable** [**interval** *interval* | **send** *send-times*] *	デフォルト：無効

XII. RADIUS パケットの DSCP 値の設定

ToS フィールドの DSCP 値は、パケットの優先度レベルを指定し、パケットの優先度に影響します。値が大きいほど、優先度は高くなります。

以下に RADIUS パケットの DSCP 値の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. RADIUS パケットの DSCP 値を設定する	**radius** [**ipv6**] **dscp** *dscp-value*	—

XIII. 再認証を行う際の RADIUS サーバの選択モードの選択

この機能を使用して、再認証時の RADIUS サーバ選択メカニズムを設定します。次の RADIUS サーバ選択モードを使用できます。

- **Inherit**—装置は、ユーザの認証を実行した RADIUS サーバを使用して、そのユーザの再認証を実行します。このモードでは、再認証に使用される時間が短縮されます。ただし、RADIUS サーバに到達できない場合、再認証は失敗します。
- **Reselect**—装置は、ユーザの再認証を実行するために到達可能な RADIUS サーバを検索します。このモードは、inherit モードよりも時間がかかります。ただし、このモードでは、装置が再認証に最適な到達可能な RADIUS サーバを見つけることができます。RADIUS サーバの選択には、次の要因が影響します。
  - □ 設定順を含む RADIUS スキームのサーバ設定。
  - □ RADIUS サーバのロードシェアリング機能の有効化状態。
  - □ RADIUS スキーム内の RADIUS サーバの状態。

以下に再認証を行う際の RADIUS サーバの選択モードの選択の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. RADIUS scheme view に移行する	**radius scheme** *radius-scheme-name*	—
3. 再認証を行う際の RADIUS サーバの選択モードを設定する	**reauthentication server-select** { **inherit** | **reselect** }	デフォルト：**inherit**

XIV. RADIUS の表示と維持

すべての view で **display** コマンドを実行でき、user view で **reset** コマンドを実行できます。

操作	コマンド
RADIUSスキームの設定を表示する	**display radius scheme** [*radius-scheme-name*]
RADIUSパケットの統計情報を表示する	**display radius statistics**
応答がなくバッファされた RADIUSストップアカウンティング要求の統計情報を表示する	**display stop-accounting-buffer** { **radius-scheme** *radius-scheme-name* | **session-id** *session-id* | **time-range** *start-time end-time* | **user-name** *user-name* }

操作	コマンド
RADIUSパケットの統計情報をクリアする	**reset radius statistics**
応答がなくバッファされたRADIUSストップアカウンティング要求の統計情報をクリアする	**reset stop-accounting-buffer** { **radius-scheme** *radius-scheme-name* | **session-id** *session-id* | **time-range** *start-time end-time* | **user-name** *user-name* }

1.4 ISPドメインのAAA方式の設定

ISP domain view で設定された AAA スキームを使用して、ISP ドメインの AAA 方式を、設定することができます。各 ISP ドメインは、デフォルトの AAA 方式を持っています。この AAA 方式は、デフォルトでローカル認証、ローカル許可、ローカルアカウンティングとなっており、設定することができます。もし ISP ドメインを設定しない場合、ユーザの認証、許可、アカウンティングがデフォルトの AAA 方式を使用します。

1.4.1 設定要件

ISP ドメインでユーザのローカル認証を使用する場合、最初に装置でローカルユーザのアカウントを設定してください。詳細はオペレーションマニュアルのセクション 9 *セキュリティ”AAA”の”ローカルユーザ属性の設定”*を参照してください。

リモート認証、許可、アカウンティングを使用する場合、要求される RADIUS スキームを作成してください。RADIUS スキームについては、オペレーションマニュアルのセクション 9 *セキュリティ”AAA”の”RADIUS スキームの設定”*を参照してください。

1.4.2 ISP ドメインの作成

複数の ISP を持つネットワークシナリオでは、装置に各 ISP のユーザを接続する可能性があります。各 ISP ユーザはそれぞれのユーザ属性（たとえば、ユーザ名、パスワードの構成、サービスタイプ、権限）を持ち、ユーザを識別するために ISP ドメインを設定する必要がある可能性があります。そして ISP ドメインのために AAA 方式を含む各属性を設定する必要があります。

ドメインはあらかじめ定義されているデフォルト ISP ドメイン system を含む最大 16 の ISP ドメインを設定することができます。デフォルトのドメインとして ISP ドメインを指定することができます。ISP ドメインの設定を修正することができますが、削除することはできません。

装置では、各ユーザは ISP ドメインに属します。もしユーザがログインするとき、ISP ドメイン名がない場合、装置はデフォルト ISP ドメインに属していると認識します。

装置は以下の順にそれぞれのユーザの認証ドメインを選択します。

1) アクセスモジュールを指定された認証ドメイン
2) ユーザ名の ISP ドメイン
3) 装置のデフォルト ISP ドメイン

選択されたドメインが装置に存在しない場合、装置は存在しないドメインに割り当てられるユーザを収容する ISP ドメインを検索します。そのような ISP ドメインが設定されていない場合、ユーザ認証は失敗します。

ISP ドメインの設定をする場合、以下の制限とガイドラインに従ってください

- デフォルトの ISP ドメインを削除することはできません。**undo domain** コマンドを使用する前に **undo domain default enable** コマンドを使用して、デフォルト以外の ISP ドメインに変更してください。
- ISP ドメイン **system** の設定変更はできますが、ドメインを削除することはできません。

以下に ISP ドメインの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. ISP ドメインを作成し、ISP domain view に移行する	**domain** *isp-name*	―
3. system view に戻る	**quit**	―
4. （オプション設定項目）デフォルト ISP ドメインを指定する	**domain default enable** *isp-name*	デフォルト：system

1.4.3 ISP ドメインの属性の設定

ISP ドメインで以下の属性を設定することができます。

- **ドメイン状態**－ISP ドメインを active あるいは blocked 状態にすることによって、ユーザからのネットワークサービス要求の許可あるいは拒否することができます。

ISP ドメインの属性はドメインのすべてのユーザに適用します。

以下に ISP ドメインの属性の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. ISP domain view に移行する	**domain** *isp-name*	―
3. ISP ドメインを **active** あるいは **blocked** 状態に設定する	**state** { **active** | **block** }	デフォルト：**active** ドメインのユーザはネットワークサービスをリクエストすることができます。

1.4.4 ISP ドメインの認証方式の設定

I. 設定要件

認証方式を設定する前に、以下の作業を行ってください。

1) 設定するアクセスタイプ、またはサービスタイプを定義してください。AAA では、各アクセスタイプとサービスタイプのために認証方式を設定することができます。

2) すべてのアクセスタイプとサービスタイプでデフォルトの認証方式を設定するかどうか定義してください。デフォルト認証方式はすべてのアクセスユーザに適用しますが、指定された認証方式よりもプライオリティは低くなります。

II. 設定ガイドライン

認証方式を設定するとき、以下のガイドラインに従ってください。

- 認証方式が RADIUS スキームを使用し、許可方式が RADIUS スキームを使用しない場合、AAA は RADIUS サーバから認証結果のみを受け取ります。RADIUS サーバからの Access-Accept メッセージは許可情報を含みますが、装置は許可情報を無視します。

III. 設定手順

以下に ISP ドメインの認証方式の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. ISP domain view に移行する	**domain** *isp-name*	―
3. ユーザのすべてのタイプのためのデフォルト認証方式を指定する	**authentication default** { **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }	デフォルト：**local**
4. ログインユーザのための認証方式を指定する	**authentication login** { **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }	デフォルト: デフォルト認証方式が使用されます。

1.4.5 ISP ドメインの許可方式の設定

I. 設定要件

許可方式を設定する前に、以下の作業を行ってください。

1) 設定されるアクセスタイプあるいはサービスタイプを定義してください。AAA では各アクセスタイプとサービスタイプに許可スキームを設定することができます。
2) すべてのアクセスタイプとサービスタイプでデフォルトの許可方式を設定するかどうか定義してください。デフォルト許可方式はすべてのアクセスユーザに適用しますが、指定された許可方式よりもプライオリティは低くなります。

II. 設定ガイドライン

RADIUS 許可を設定するため、RADIUS 認証を設定し、RADIUS 認証と許可で同じ RADIUS スキームを参照してください。RADIUS 許可の設定に間違いがある場合や RADIUS 許可に失敗する場合は、RADIUS 認証も失敗します。

III. 設定手順

以下に ISP ドメインの許可方式の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―

操作	コマンド	補足
2. ISP domain view に移行する	**domain** *isp-name*	―
3. すべてのタイプのユーザのためにデフォルト許可方式を指定する	**authorization default** { **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }	デフォルト：**local**
4. コマンド許可方式を指定する	**authorization command** { **local** [**none**] | **none** }	デフォルト：デフォルト許可方式が使用されます。
5. LAN ユーザの許可方式を指定する	**authorization lan-access** { **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }	デフォルト：デフォルト許可方式が使用されます。
6. ログインユーザのために許可方式を指定する	**authorization login** { **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }	デフォルト：デフォルト許可方式が使用されます。

1.4.6 ISP ドメインのアカウンティング方式の設定

I. 設定要件

アカウンティング方式を設定する前に、以下の作業を行ってください。

1) 設定されるアクセスタイプあるいはサービスタイプを定義してください。AAA では各アクセスタイプとサービスタイプにアカウンティング方式を設定することができます。
2) すべてのアクセスタイプとサービスタイプでデフォルトのアカウンティング方式を設定するかどうか定義してください。デフォルトアカウンティング方式はすべてのアクセスユーザに適用しますが、指定されたアカウンティング方式よりもプライオリティは低くなります。

II. 設定ガイドライン

アカウンティング方式を設定するとき、以下のガイドラインに従ってください。

- FTP、SFTP サービスを使用するログインユーザはアカウンティングをサポートしていません。
- ローカルアカウンティングは、アカウンティングの統計情報を提供しません。同じローカルユーザアカウントを使用するユーザ数のカウントと管理を行います。しきい値は **access-limit** コマンドによって設定されます。

III. 設定手順

以下に ISP ドメインのアカウンティング方式の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. ISP domain view に移行する	**domain** *isp-name*	―
3. すべてのタイプのユーザに使用するデフォルトアカウンティング方式を指定する	**accounting default** { **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }	デフォルト：**local**

操作	コマンド	補足
4. LAN ユーザにアカウンティング方式を指定する	**accounting lan-access** { **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }	デフォルト : デフォルトアカウンティング方式が使用されます。
5. ログインユーザに使用するアカウンティング方式を指定する	**accounting login** { **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }	デフォルト : デフォルトアカウンティング方式が使用されます。
6. （オプション設定項目）アカウンティング開始に失敗したユーザのアクセス制御を設定する	**accounting start-fail** { **offline** | **online** }	デフォルト：**online**
7. （オプション設定項目）すべてのアカウンティング更新の試行に失敗したユーザのアクセス制御を設定する	**accounting update-fail** { [**max-times** *max-times*] **offline** | **online** }	デフォルト：**online**

1.4.7 同時ログインユーザの最大数の設定

認証方法に関わらず、FTP、SSH、Telnet プロトコルを使用して、装置にログインできる最大ユーザ数を設定することができます。

以下に同時ログインユーザの最大数の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. 同時ログインユーザの最大数を設定する	**aaa session-limit** { **ftp** | **ssh** | **telnet** } *max-sessions*	デフォルト：32

1.5 AAAの表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
ISP ドメインの設定を表示する	**display domain** [*isp-name*]

1.6 SSHユーザのローカル認証、RADIUSアカウンティングの設定例

1.6.1 ネットワーク要件

図 1-8に示すように、SSH サーバ用にローカル認証を実行するように設定します。SSH ユーザ許可、アカウンティングを行うため、RADIUS サーバを使用します。そして認証にパスした後、SSH ユーザにデフォルトユーザロール network-operator を割り当てます。

SSH ユーザにユーザ名 **hello** のアカウントを設定します。RADIUS サーバとセキュアな通信を行うため、共有鍵 **expert** を設定します。ユーザ名からドメイン名を削除してサーバに送信するように設定します。

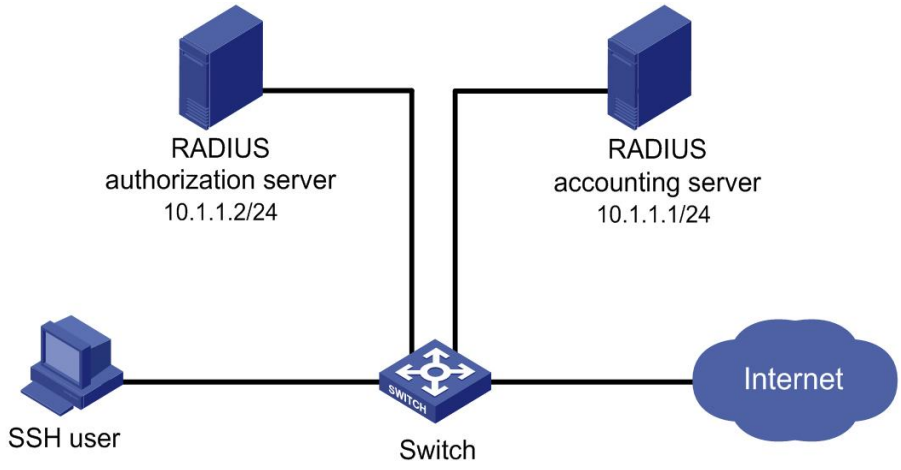


図 1-8 ネットワーク図

1.6.2 設定手順

1) RADIUS サーバを設定します。（詳細は省略します）
2) Switch を設定します。

インタフェースに IP アドレスを割り当てます。（詳細は省略します）

ローカル RSA 鍵ペアを作成します。

```
<Switch> system-view
[Switch] public-key local create rsa
```

SSH サービスを有効にします。

```
[Switch] ssh server enable
```

ユーザロール VTY0～63 のスキーム認証を有効にします。

```
[Switch] line vty 0 63
[Switch-line-vty0-63] authentication-mode scheme
```

```
[Switch-line-vty0-63] quit
```

RADIUS スキームを設定します。

```
[Switch] radius scheme rd
[Switch-radius-rd] primary accounting 10.1.1.1 1813
[Switch-radius-rd] key accounting simple expert
[Switch-radius-rd] user-name-format without-domain
[Switch-radius-rd] quit
```

装置管理ユーザを作成します。

```
[Switch] local-user hello class manage
```

ローカルユーザの SSH サービスを割り当てます。

```
[Switch-luser-manage-hello] service-type ssh
```

ローカルユーザのパスワードをプレーンテキストで **hello** に設定します。

```
[Switch-luser-manage-hello] password simple hello
[Switch-luser-manage-hello] quit
```

ISP ドメイン **bbb** を作成し、ログインユーザの AAA 方式を設定します。

```
[Switch] domain bbb
[Switch-isp-bbb] authentication login local
[Switch-isp-bbb] accounting login radius-scheme rd
[Switch-isp-bbb] quit
```

認証にパスした後、SSH ユーザがデフォルトユーザロール network-operator を取得できるようにデフォルトユーザロール許可機能を有効にします。

```
[Switch] role default-role enable
```

1.6.3 設定の確認

ユーザが、Switch への SSH 接続を開始し、ユーザ名 **hello@bbb** と正しいパスワードを入力したとき、ユーザが正常にログインし、network-operator ユーザロールでコマンドを使用することができます。

1.7 RADIUSのトラブルシューティング

1.7.1 RADIUS 認証の失敗

I. 症状

認証が常に失敗します。

II. 分析

可能性のある理由を以下に示します。

- NAS と RADIUS サーバ間で通信障害が存在します。
- ユーザ名が userid@isp-name のフォーマットではありません、あるいは NAS で ISP ドメインが正しく設定されていません。
- ユーザが RADIUS サーバで設定されていません。
- ユーザで入力したパスワードが間違っています。
- RADIUS サーバと NAS が異なる共有鍵で設定されています。

III. 解決策

以下を確認してください。

- NAS と RADIUS サーバがお互いに ping できることを確認してください。
- ユーザ名が userid@isp-name のフォーマットで、NAS で ISP ドメインが正しく設定されていることを確認してください。
- ユーザが RADIUS サーバで設定されていることを確認してください。
- 正しいパスワードを入力してください。
- RADIUS サーバと NAS の両方で同じ共有鍵が設定されていることを確認してください。

1.7.2 RADIUS パケットが到達不能

I. 症状

RADIUS パケットが RADIUS サーバに到達できません。

II. 分析

可能性のある理由を以下に示します。

- NAS と RADIUS サーバ間で通信障害が存在します。
- NAS に RADIUS サーバの IP アドレスが設定されていません。
- NAS の認証、アカウンティングの UDP ポートが正しくありません。
- RADIUS サーバの認証､アカウンティングのためのポート番号がほかのアプリケーションで使用されています。

III. 解決策

以下を確認してください。

- NAS と RADIUS サーバ間のリンクが物理レイヤ、データリンクレイヤの両方で正しく動作することを確認してください。
- RADIUS サーバの IP アドレスが NAS で正しく設定されていることを確認してください。
- NAS で設定された認証、アカウンティングの UDP ポートが RADIUS サーバで設定されているものと同じであることを確認してください。
- RADIUS サーバの認証､アカウンティングのためのポート番号が使用可能であることを確認してください。

1.7.3 RADIUS アカウンティングエラー

I. 症状

ユーザは認証と許可されましたが、アカウンティングが正常ではありません。

II. 分析

NAS のアカウンティングサーバの設定が間違っています。可能性のある理由を以下に示します。

- NAS で設定されたアカウンティングのためのポート番号が間違っています。
- NAS で設定されたアカウンティングサーバの IP アドレスが間違っています。たとえば、NAS が認証、許可、アカウンティングサービスを提供するために、1 つのサーバを使用するように設定されていますが、実際のサービスは異なるサーバによって提供されています。

III. 解決策

以下を確認してください。

- アカウンティングのためのポート番号が正しく設定されていることを確認してください。
- アカウンティングサーバの IP アドレスが NAS で正しく設定されていることを確認してください。

目次

このセクションのページは **9-x-x** です。

2 章 802.1X の概要 2-1
2.1 802.1Xの構成 2-1
2.2 制御/非制御ポートとポート許可状態 2-1
2.3 802.1X関連プロトコル 2-2
2.3.1 パケットフォーマット 2-2
2.3.2 EAP over RADIUS 2-4
2.4 802.1X認証の開始 2-5
2.4.1 802.1Xクライアントからの認証開始 2-5
2.4.2 アクセスデバイスからの認証開始 2-5
2.5 802.1Xの認証プロセス 2-5
2.5.1 EAP relay と EAP termination の比較 2-6
2.5.2 EAP relay 2-7
2.5.3 EAP termination 2-9

2章 802.1X の概要

802.1X は、無線 LAN（WLAN）のセキュリティを行うため、最初に提案されたポートベースのネットワークアクセス制御プロトコルです。

802.1X が有効な LAN ポートに接続された装置を、認証サーバ(RADIUS サーバなど)による認証をすることでネットワークを保護します。

2.1 802.1Xの構成

802.1X は、クライアント/サーバモデルで動作します。図 2-1に示すように 802.1X認証は以下の構成要素があります。

- **クライアント（サプリカント）**－クライアントは、LAN へアクセスしようとするユーザの端末です。端末はネットワークアクセスデバイスを認証する 802.1X ソフトウェアが必要です。
- **アクセスデバイス（オーセンティケータ）**－ネットワークアクセスデバイスは、クライアントを認証し、LAN へのアクセスを制御します。通常の 802.1X環境では、ネットワークアクセスデバイスは、認証サーバを使用して認証を実行します。
- **認証サーバ**－認証サーバは、ネットワークアクセスデバイスの認証サービスを提供するエンティティです。ネットワークアクセスデバイスから送信されたデータを使用して 802.1Xクライアントを認証し、ネットワークアクセスデバイスがアクセスするための認証結果を返します。認証サーバは通常、RADIUS（Remote Authentication Dial-in User Service）サーバです。小規模な LAN では、認証サーバとしてネットワークアクセスデバイスを使用することもできます。

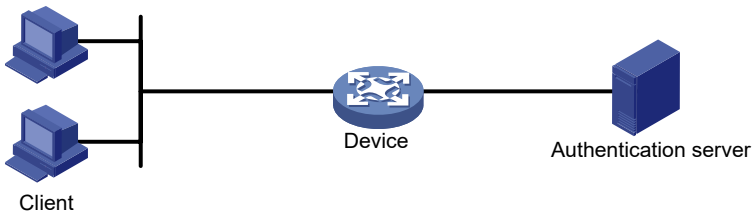


図 2-1 802.1X の構成

2.2 制御/非制御ポートとポート許可状態

802.1X は、ネットワークのアクセスポートのために、制御ポートと非制御ポートの 2 つの論理ポートを定義しています。ネットワークのアクセスポートに受信するパケットはすべて、両方の論理ポートに表示されます。

- **非制御ポート**－非制御ポートは常にオープン状態で、認証パケットを送信します。
- **制御ポート**－ポートの状態に依存してパケットをフィルタします。
  - □ **許可状態**－クライアントが認証にパスしたとき、ポートは authorized 状態になります。このポートはトラフィックを通過させることができます。

- **非許可状態**－クライアントが認証にパスしないとき、ポートは unauthorized 状態になります。以下の方法の 1 つによってトラフィックを制御します。
  - クライアントへのトラフィックとクライアントからのトラフィックを拒否するように、双方向のトラフィックを制御します。
  - クライアントからのトラフィックを拒否するように、片方向のトラフィックを制御します。本デバイスは片方向のトラフィック制御のみをサポートしています。

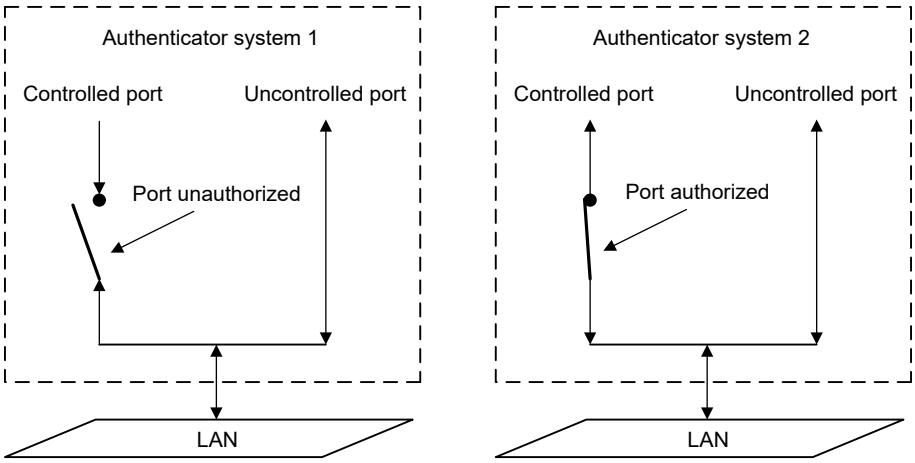


図 2-2 制御ポートの許可/非許可状態

2.3 802.1X関連プロトコル

802.1X は、クライアント、ネットワークアクセスデバイス、認証サーバの認証情報を転送するために EAP（Extensible Authentication Protocol）を使用しています。 EAP は、クライアント/サーバモデルを使用する認証フレームワークです。MD5-Challenge、EAP-TLS（EAP-Transport Layer Security）、PEAP（Protected EAP）を含む様々な認証方式をサポートしています。

802.1X は、有線または無線 LAN 経由で、クライアントとアクセスデバイス間で EAPOL（EAP over LAN）を定義します。クアクセスデバイスと認証サーバとの間で、802.1X は、次のいずれかの方法で認証情報を提供します。

- **EAP relay**：EAPOR（EAP over RADIUS）を使用して、RADIUS で EAP パケットをカプセル化します。
- **EAP termination**：EAP パケットから認証情報を抽出し、標準的な RADIUS パケット内の情報をカプセル化します。

2.3.1 パケットフォーマット

I. EAP パケットのフォーマット

図 2-3に EAP パケットのフォーマットを示します。

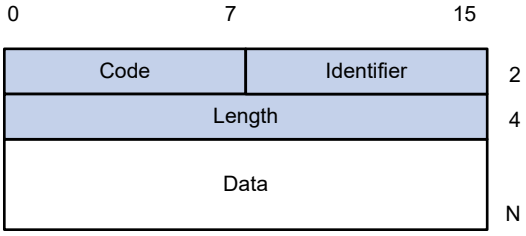


図 2-3 EAP パケットのフォーマット

- **Code**－EAP パケットのタイプです。Request(1)、Response(2)、Success(3)、Failure(4)があります。
- **Identifier**－リクエストとレスポンスを対応づけます。
- **Length**－EAP パケット長（byte）です。Code、Identifier、Length、Data フィールドの合計です。
- **Data**－EAP パケットの中身です。このフィールドは、リクエストまたはレスポンス EAP パケットにのみあります。リクエストタイプ（またはレスポンスタイプ）とタイプデータで構成されています。タイプ 1（Identify）とタイプ 4（MD5-Challenge）はタイプフィールドの 2 つの例です。

II. EAPOL パケットのフォーマット

図 2-4に EAPOL パケットのフォーマットを示します。

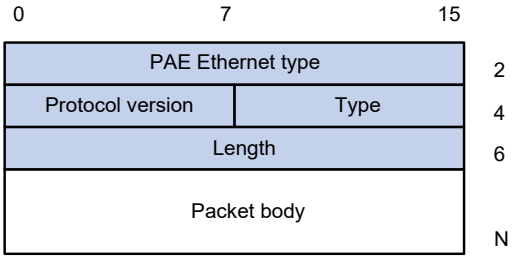


図 2-4 EAPOL パケットのフォーマット

- **PAE Ethernet type**－プロトコルタイプです。EAPOL の値は 0x888E です。
- **Protocol version**－EAPOL パケットの送信元がサポートする EAPOL プロトコルのバージョンです。
- **Type**－EAPOL パケットのタイプです。表 2-1に装置がサポートする EAPOL パケットのタイプを示します。

表 2-1 EAPOL パケットのタイプ

値	タイプ	説明
0x00	EAP-Packet	クライアントとネットワークアクセスデバイスは、認証情報を運ぶためにEAP-Packetを使用します。
0x01	EAPOL-Start	クライアントは、802.1X認証を開始させるために、ネットワークアクセスデバイスにEAPOL-Startメッセージを送ります。
0x02	EAPOL-Logoff	クライアントは、ログオフを通知するために、アクセスデバイスにEAPOL-Logoffメッセージを送ります。

- **Length**－データ長（byte）です。Packet body フィールド長を示します。パケットタイプが EAPOL-Start か EAPOL-Logoff の場合、このフィールドに 0 がセットされ、Packet body フィールドは存在しません。
- **Packet body**－パケットの中身です。EAPOL パケットタイプが EAP-Packet の時、Packet body フィールドが EAP パケットの中身です。

2.3.2 EAP over RADIUS

RADIUS は EAP 認証をサポートするため、EAP-Message と Message-Authenticator の 2 つの属性を追加します。RADIUS パケットのフォーマットについての詳細は、オペレーションマニュアルのセクション 9 *セキュリティ* "*AAA*"を参照してください。

I. EAP-Message

図 2-5に示すように RADIUS は、EAP-Message 属性に EAP パケットをカプセル化します。このパケットの Type フィールドの値は 79 です。String フィールドには最大 253 バイトまで入ります。EAP パケット長が 253 バイト以上である場合、複数の EAP-Message 属性にカプセル化されます。

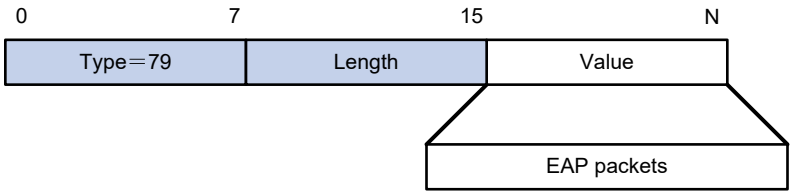


図 2-5 EAP-Message の属性フォーマット

II. Message-Authenticator

RADIUS は、整合性をチェックするため EAP-Message 属性を持つすべてのパケットに Message-Authenticator 属性を含めます。

計算されたパケットの整合性チェックサムが Message-Authenticator 属性の値と異なる場合、パケットの受信者はパケットを廃棄します。Message-Authenticator は、EAP 認証中に EAP 認証パケットが改ざんされることを防ぎます。

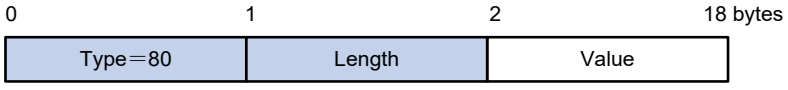


図 2-6 Message-Authenticator の属性フォーマット

2.4 802.1X認証の開始

802.1X認証は、802.1Xクライアントと装置のどちらからでも開始させることができます。

2.4.1 802.1X クライアントからの認証開始

クライアントは、アクセスデバイスに EAPOL-Start パケットを送信することで、802.1X 認証を開始します。このパケットの宛先 MAC アドレスは、IEEE 802.1Xで指定されたマルチキャストアドレス 01-80-C2-00-00-03 またはブロードキャスト MAC アドレスです。クライアントと認証サーバ間のすべての中間デバイスがマルチキャストアドレスをサポートしていない場合、ブロードキャスト EAPOL-Start パケットを送信できる 802.1Xクライアントを使用する必要があります。

2.4.2 アクセスデバイスからの認証開始

クライアントが EAPOL-Start パケットを送信できない場合、アクセスデバイスが認証を開始するよう設定します。たとえば 802.1Xクライアントは Windows XP で使用できます。

アクセスデバイスは、以下のモードをサポートしています。

- **マルチキャストトリガモード**－アクセスデバイスが、定期的に（デフォルトでは 30 秒ごと）EAP-Request/Identity パケットをマルチキャスト送信することで、802.1X 認証を開始します。
- **ユニキャストトリガモード**－MAC アドレステーブルにない送信元 MAC アドレスのフレームを受信したとき、アクセスデバイスは受信ポートから未知の MAC アドレスへ EAP-Request/Identity パケットを送信します。応答を一定時間内に受信しない場合、パケットを再送します。

2.5 802.1Xの認証プロセス

802.1X 認証には、EAP relay と EAP termination の 2 つのアプローチがあります。EAP パケットと EAP 認証方式のために RADIUS サーバのサポートに応じていずれかのモードを選択してください。

- EAP relay モード

EAP relay は、IEEE802.1X で定義されています。このモードでは、ネットワークデバイスは、図 2-7に示すように、RADIUS サーバに認証情報を送信するために EAPOL パケットを使用します。

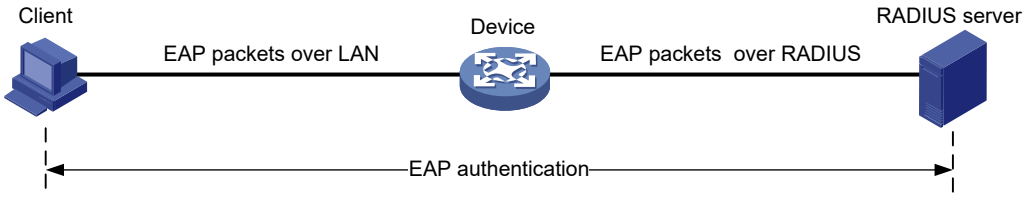


図 2-7 EAP relay

EAP relay モードでは、クライアントは RADIUS サーバと同じ認証方式を用いる必要があります。ネットワークアクセスを行うデバイス上では、EAP relay で利用するために **dot1x authentication-method eap** コマンドのみが必要です。

- EAP termination モード

図 2-8に示すように、アクセスデバイスは EAP termination モードで以下の動作を行います。

a) クライアントから受信したEAPパケットを終端します。

b) 標準RADIUSパケットにクライアント認証情報をカプセル化します。

c) RADIUSサーバに認証するため、PAPあるいはCHAPを使用します。

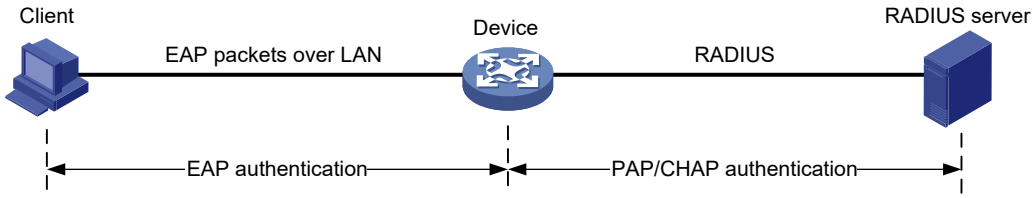


図 2-8 EAP termination

2.5.1 EAP relay と EAP termination の比較

パケット交換方式	利点	制限
EAP relay	• 様々なEAP認証方法をサポートしています。 • アクセスデバイス上の設定と処理が簡単です。	RADIUSサーバはEAP-MessageとMessage-Authenticator属性と、クライアントに使用されるEAP認証方式をサポートする必要があります。

パケット交換方式	利点	制限

EAP termination	PAPまたはCHAP認証をサポートしている任意のRADIUSサーバと連携して動作します。	• 以下のEAP認証方式のみをサポートします。
		  • MD5-Challenge EAP認証
		  • ユーザ名とパスワードのEAP認証
		• アクセスデバイス上の処理が複雑です。

2.5.2 EAP relay

図 2-9に EAP-MD5 を使用した、EAP relay モードでの基本的な 802.1X認証プロセスを示します。

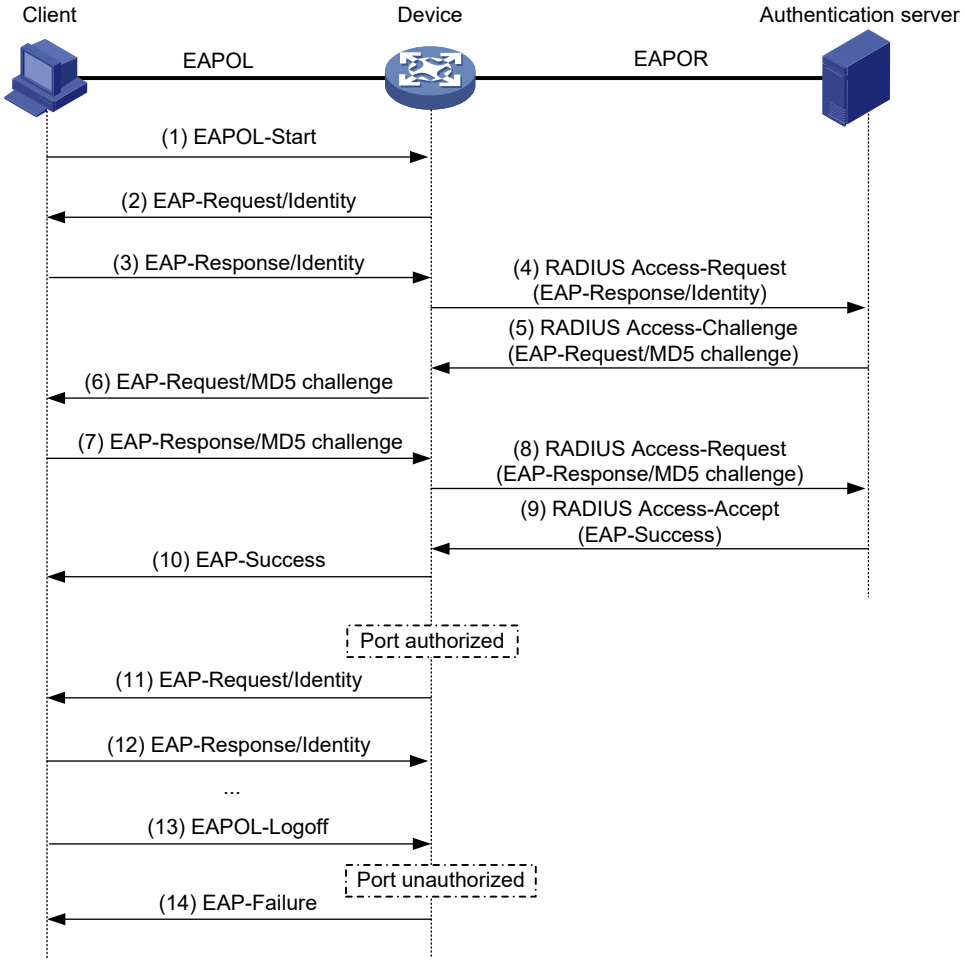


図 2-9 EAP relay モードでの 802.1X認証プロセス

以下に 802.1X認証プロセスを記載します。

1) ユーザが、802.1X クライアントを起動し、登録されたユーザ名とパスワードを入力すると、802.1Xクライアントは、アクセスデバイスに EAPOL-Start パケットを送信します。
2) アクセスデバイスは、応答としてクライアントのユーザ名を要求するために EAP-Request/Identity パケットを送信します。
3) EAP-Request/Identity パケットの応答として、クライアントは EAP-Request/Identity パケットの中にユーザ名を入れて、アクセスデバイスに送信します。
4) アクセスデバイスは、RADIUS Access-Request パケットの EAP-Request/Identity パケットを認証サーバに伝搬します。
5) 認証サーバは、ユーザのデータベースを検索するため、RADIUS Access-Request パケットの identify 情報を使用します。一致するエントリが見つかった場合、サーバはランダムに生成されるチャレンジ（EAP-Request/MD5 challenge）を使用してパスワード情報を暗号化し、RADIUS Access-Challenge パケットを通してネットワークアクセスデバイスにチャレンジ情報を送信します。
6) アクセスデバイスは、EAP-Request/MD5 Challenge パケットをクライアントに送信します。
7) クライアントは、受信したチャレンジ情報を使用してパスワードを暗号化します。そして EAP-Response/MD5 Challenge パケットの暗号化したパスワードをアクセスデバイスに送信します。
8) アクセスデバイスは、RADIUS Access-Request パケットの EAP-Response/MD5 Challenge パケットを認証サーバに伝搬します。
9) 認証サーバは、受信したパスワード情報と、5)で自身が生成したパスワード情報を比較します。2 つのパスワード情報が一致する場合、認証サーバはクライアントが有効であるとみなし、アクセスデバイスに RADIUS Access-Accept パケットを送信します。
10) RADIUS Access-Accept パケットを受信すると、アクセスデバイスは、以下の動作を行います。

a) クライアントにEAP-Successパケットを送ります。

b) 制御ポートをauthorized状態に設定します。

クライアントはネットワークにアクセスできます。

11) クライアントがオンラインになった後、クライアントがまだオンラインであるかどうかを確認するために、アクセスデバイスは定期的にハンドシェイク要求を送信します。デフォルトでは、2 回連続してハンドシェイクが失敗すると、デバイスはクライアントをログオフします。
12) ハンドシェイク要求を受け取ると、クライアントは応答を返します。クライアントが特定の回数（デフォルトで 2 回）連続してハンドシェイク応答に失敗した場合、アクセスデバイスは、クライアントをログオフします。このハンドシェイクメカニズムにより、異常にオフラインになった 802.1Xユーザによって使用されるネットワークリソースをタイムリーにリリースすることが可能になります。
13) クライアントは、アクセスデバイスにログオフを依頼する EAPOL-Logoff パケットを送信することもできます。
14) EAPOL-Logoff パケットに応答して、アクセスデバイスは、制御ポートの状態を authorized から unauthorized に変更し、クライアントへ EAP-Failure パケットを送信します。

2.5.3 EAP termination

図 2-10に CHAP 認証を使用した、EAP termination モードでの基本的な 802.1X認証プロセスを示します。

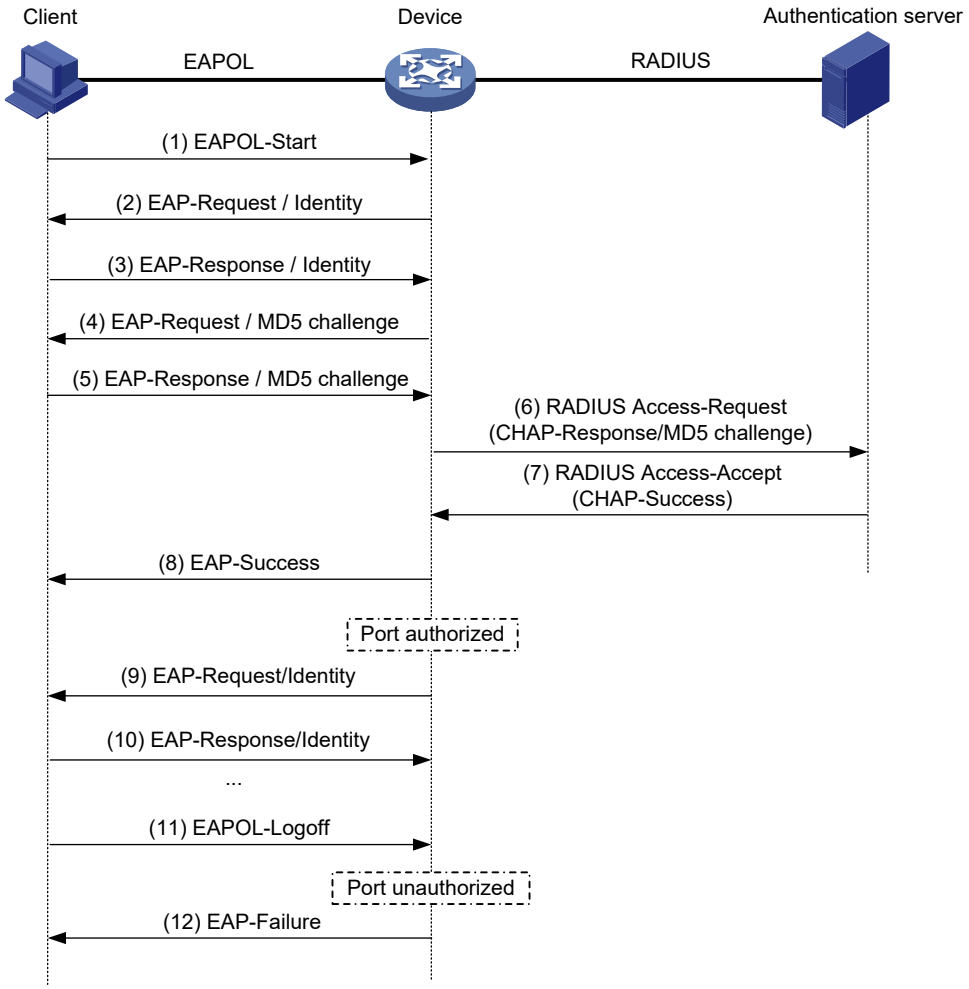


図 2-10 EAP termination での 802.1X認証プロセス

EAP termination モードでは、パスワードを暗号化するために MD5 challenge を生成するのは認証サーバでなく、アクセスデバイスです。アクセスデバイスは次に、MD5 challenge をユーザ名と暗号化されたパスワードと一緒に標準の RADIUS パケットに入れて RADIUS サーバへ送信します。

目次

このセクションのページは**9-x-x** です。

3 章 802.1X.....3-1
3.1 アクセス制御方式.....3-1
3.2 802.1X の VLAN 操作.....3-1
3.2.1 許可 VLAN.....3-1
3.2.2 ゲスト VLAN.....3-4
3.2.3 制限 VLAN.....3-5
3.3 他の機能を用いた 802.1X 認証.....3-7
3.3.1 ACL の割り当て.....3-7
3.4 802.1X 設定制限とガイドライン.....3-7
3.4.1 設定要件.....3-7
3.5 802.1X 設定作業リスト.....3-7
3.6 802.1X 認証の有効化.....3-8
3.7 EAP relay または EAP termination の有効化.....3-8
3.8 ポート許可状態の設定.....3-9
3.9 アクセス制御方式の指定.....3-10
3.10 ポートの 802.1X ユーザの最大同時接続数の設定.....3-10
3.11 認証リクエストの最大送信数の設定.....3-10
3.12 802.1X 認証タイムアウトタイマの設定.....3-11
3.13 オンラインユーザハンドシェイク機能の設定.....3-11
3.13.1 設定ガイドライン.....3-11
3.13.2 設定手順.....3-12
3.14 認証トリガ機能の設定.....3-12
3.14.1 設定ガイドライン.....3-12
3.14.2 設定手順.....3-12
3.15 ポートでの強制認証ドメインの設定.....3-13
3.16 quiet タイマの設定.....3-13
3.17 802.1X 再認証の設定.....3-14
3.17.1 概要.....3-14
3.17.2 設定ガイドライン.....3-14
3.17.3 802.1X 定期的な再認証の設定.....3-14
3.18 802.1X ゲスト VLAN の設定.....3-15
3.18.1 設定ガイドライン.....3-15
3.18.2 設定要件.....3-15
3.18.3 設定手順.....3-16
3.19 802.1X ゲスト VLAN 割り当て遅延の有効化.....3-16
3.19.1 設定ガイドライン.....3-16
3.20 802.1X 制限 VLAN の設定.....3-17
3.20.1 設定ガイドライン.....3-17
3.20.2 設定要件.....3-17
3.20.3 設定手順.....3-17
3.21 MAC アドレス移動機能の有効化.....3-18
3.22 802.1X ユーザのログオフ.....3-18
3.23 802.1 X 非認証ユーザエージングの設定.....3-19
3.24 802.1 X ユニキャストトリガーサイレント機能.....3-20

3.25 802.1X の表示と維持 3-20
3.26 802.1X 認証の設定例 3-21
3.26.1 基本的な 802.1X 認証の設定例 3-21
3.26.2 802.1X ゲスト VLAN と許可 VLAN の設定例 3-24
3.26.3 ACL の割り当てによる 802.1X の設定例 3-27

3章 802.1X

この章は、装置上で 802.1X を設定する方法について説明します。802.1X を実行時に、ポートセキュリティ機能を設定することもできます。ポートセキュリティは 802.1X と MAC アドレス認証を組み合わせて拡張します。ポート上でユーザごとに異なる認証方法を必要とするネットワークに適用します。ポートセキュリティの詳細は、オペレーションマニュアルのセクション 9 *セキュリティ*”*ポートセキュリティ*”を参照してください。

3.1 アクセス制御方式

802.1X プロトコルで定義されたポートベースのアクセス制御を実装しており、MAC ベースのアクセス制御をサポートするためにプロトコルを拡張します。

- **ポートベースアクセス制御**－ポートベースのアクセス制御では、一度 802.1X ユーザがポート上で認証を通過すると、後続のユーザは、認証なしでポートを介してネットワークにアクセスできます。認証されたユーザがログオフすると、他のすべてのユーザはログオフされます。
- **MAC ベースアクセス制御**－MAC ベースのアクセス制御では、各ユーザは個別にポート上で認証されます。ユーザがログオフしても、他のオンラインのユーザは影響を受けません。

3.2 802.1XのVLAN操作

3.2.1 許可 VLAN

802.1X ユーザが許可されたネットワークリソースへのアクセスを制御するため、許可 VLAN を指定することができます。802.1X ユーザが認証にパスしたのち、認証サーバは許可 VLAN あるいは VLAN グループをユーザに割り当てます。

I. サポートされる VLAN タイプと形式

VLAN タイプと形式は許可タイプに依存してサポートされます。

- ローカル VLAN 許可

  アクセス装置で user view あるいは user group view で VLAN ID によって 1 つの許可 VLAN のみを指定することができます。ローカルユーザの詳細は、オペレーションマニュアルのセクション 9 *セキュリティ*”*AAA*”を参照してください。

- リモート VLAN 許可

  802.1X ユーザの AAA サーバで VLAN あるいは VLAN グループを指定することができます。アクセス装置は以下の形式の VLAN をサポートします。

  - □ VLAN ID
  - □ VLAN 名

  VLAN 名はアクセス装置で VLAN の特徴を示します。

□　VLAN ID と VLAN 名の組み合わせ

文字列で、ある VLAN は VLAN ID で示し、ある VLAN は VLAN 名で示します。

□　VLAN グループ名

VLAN グループの詳細は、オペレーションマニュアルのセクション 3 *アクセス” VLAN*”を参照してください。

□　サフィックスを持つ VLAN ID

サフィックスは、t あるいは u が使用できます。VLAN がタグづけされるポートかどうかを示します。たとえば、2u は VLAN2 がタグづけされていないメンバに割り当てられていることを示します。

🕮 **メモ：**

アクセス装置は、VLAN の割り当てを行う前に、VLAN 名と VLAN グループ名を VLAN ID に置き換えます。

II. サポートされない VLAN タイプ

VLAN 許可では以下のタイプを指定することができません。アクセス装置は、802.1X ユーザに VLAN を割り当てることができません。

- ダイナミックに学習された VLAN
- 予約された VLAN

III. VLAN の選択と割り当て

サーバが VLAN のグループを割り当てるとき、アクセス装置は VLAN ID のフォーマットに従って VLAN を選択し、割り当てます。表 3-1に許可 VLAN のグループの選択と割り当てルールを記載します。

表 3-1 許可 VLAN のグループの VLAN の選択と割り当て

許可 VLAN のタイプ	VLAN の選択と割り当てルール
• VLAN ID • VLAN名 • VLANグループ名	デバイスは、ポートで他のオンラインユーザがいるかどうかに依存して、許可VLANとしてVLANを選択します。 • ポートで他のオンラインユーザがいない場合、デバイスはVLANのグループからもっとも小さいIDのVLANを選択します。 • ポートで他のオンラインユーザがいる場合、以下の処理によってVLANを選択します。 1． デバイスはオンラインユーザから一番遠い番号を持つ VLAN を選択します。 2． 2 つの VLAN がオンライン 802.1X ユーザと同じ番号を持っている場合、デバイスはもっとも小さい ID の VLAN を選択します。 表 3-2にデバイスがVLANの割り当てを行うルールを示します。

許可 VLAN のタイプ	VLAN の選択と割り当てルール
サフィックスを持つVLAN ID	1． デバイスはサフィックスを除いた一番左の VLAN ID、あるいは、タグなしとして u のサフィックスが付いた一番左の VLAN ID を選択します。 1． デバイスは PVID としてポートにタグなしの VLAN を割り当て、タグづけられた VLAN はそのまま割り当てます。もしタグなし VLAN が割り当てられていない場合、ポートの PVID は変更しません。ポートは、タグづけ VLAN とタグなし VLAN からのトラフィックを通過するように許可します。 たとえば、認証サーバはユーザ用に、1u 2t 3の文字列をアクセス装置に送信します。デバイスはタグなしVLANとして VLAN1を割り当てし、タグづけVLANとして他のVLANを割り当てます。VLAN1はPVIDになります。

🕮 **メモ：**

サフィックスを持つ VLAN ID は、ポートベースのアクセス制御を行うハイブリッドポートあるいはトランクポートのみ割り当てることができます。

表 3-2にアクセス装置が 802.1X が有効なポートで VLAN を処理する方法を記載します。（サフィックスを持つ VLAN を除きます。）

表 3-2 VLAN 操作

ポートアクセス制御方式	VLAN 操作
ポートベース	デバイスは最初の認証ユーザの許可VLANをポートに割り当てます。後続のすべての802.1Xユーザは認証なしでアクセスできます。 ポートにタグなしメンバとして許可VLANが割り当てられた場合、許可VLANはPVIDになります。ポートにタグ付きメンバとして許可VLANが割り当てられた場合、ポートのPVIDは変わりません。

MACベース	• ポートがMACベースVLAN対応のハイブリッドポートの場合、デバイスは許可VLANに各ユーザのMACアドレスをマッピングします。ポートのPVIDは変更しません。ユーザがログオフすると、ユーザのMAC-VLANマッピングは削除されます。
	• ポートがアクセス、トランク、あるいはMACベースVLANが無効のハイブリッドポートである場合
	  • ポートがタグなしメンバとして許可VLANに割り当てられた場合、デバイスは最初の認証ユーザの許可VLANをポートに割り当てます。許可VLANはPVIDになります。後続のユーザが認証に成功するために、同じVLANをすべてのポートの802.1Xユーザに許可します。異なるVLANが後続のユーザに許可されると、ユーザは認証をパスすることができません。
	  • ポートがタグ付きメンバとして許可VLANに割り当てられた場合、ポートのPVIDは変わりません。デバイスは許可VLANに各ユーザのMACアドレスをマッピングします。

🕮 **メモ：**

802.1X が有効なアクセスポートは、タグなしメンバとしてのみ許可 VLAN を割り当てられます。
ハイブリッドポートは、常にタグなしメンバとして VLAN に割り当ててください。割り当てられたのち、VLAN のタグ付きメンバとしてポートを再設定しないでください。

定期的にオンラインユーザの再認証を行うことで有効になるポートでは、MAC ベース VLAN 機能は、この機能が有効になる前にオンラインになったユーザに適用されません。

アクセス装置は、以下のユーザに MAC-VLAN マッピングを作成します。

- ユーザが再認証にパスします。
- ユーザの許可 VLAN が変更されました。

VLAN の設定と MAC ベース VLAN の詳細は、オペレーションマニュアルのセクション 3 *アクセス”VLAN”* を参照してください。

3.2.2 ゲスト VLAN

ポート上の 802.1X ゲスト VLAN は、802.1X 認証を実行していないユーザに対応します。

ゲスト VLAN のユーザは、アンチウィルスソフトウェアやシステムパッチをダウンロードするためにソフトウェアサーバなどの制限されたネットワークリソースにアクセスすることができます。ゲスト VLAN でユーザが一度 802.1X 認証にパスすると、ゲスト VLAN から削除され、許可されたネットワークリソースにアクセスすることができます。

アクセス装置は、802.1X アクセス制御方式にもとづいて、802.1X が有効なポートで VLAN を処理します。

- ポートベースアクセス制御を実行するポート

認証状態	VLAN 操作
ユーザが802.1X認証にパスしていない	デバイスはPVIDとして802.1Xゲスト VLANをポートに割り当てます。ポートのすべての802.1Xユーザはゲスト VLANのリソースのみアクセスできます。802.1Xゲスト VLANが設定されていない場合、アクセス装置は任意のVLANの操作を実行しません。
802.1Xゲスト VLANのユーザが802.1X認証に失敗した	802.1X制限VLAN（Auth-Fail VLAN、オペレーショマニュアルのセクション9 *セキュリティ”802.1X”の”制限VLAN”* を参照してください）が有効である場合、デバイスはPVIDとして制限VLANを割り当てます。 制限VLANが設定されていない場合、ポートのPVIDは802.1Xゲスト VLANのままとなります。ポートのすべてのユーザはゲスト VLANの中にいます。

認証状態	VLAN 操作
802.1XゲストVLANのユーザが802.1X認証に成功した	• デバイスはPVIDとしてユーザの認証VLANを割り当てます。802.1XゲストVLANからポートを削除します。ユーザがログオフしたのち、ポートの最初のPVIDがもとに戻ります。 • 認証サーバがVLANを許可しない場合、初期のPVIDを適用します。ユーザと後続のすべての802.1Xユーザは初期ポートに割り当てられます。ユーザがログオフしたのち、ポートVLANは変更されません。 🕮 **メモ：** 802.1Xが有効なポートの初期のPVIDは、ポートが任意の802.1X VLANに割り当てられる前にポートで使用されたPVIDです。

- MAC ベースアクセス制御を実行するポート

認証状態	VLAN 操作
ユーザが認証プロセス中に802.1X認証にパスしていない	デバイスはユーザのMACアドレスと802.1XゲストVLANのマッピングを作成します。ユーザはゲストVLANのリソースのみアクセスできます。
802.1XゲストVLANのユーザが802.1X認証に失敗した	802.1X制限VLANが有効である場合、デバイスはユーザのMACアドレスを制限VLANに再マッピングします。ユーザは制限VLANのリソースのみアクセスできます。
802.1XゲストVLANのユーザが802.1X認証に成功した	デバイスはユーザのMACアドレスを許可VLANに再マッピングします。 認証ユーザがVLANを許可しない場合、デバイスはユーザのMACアドレスをポートの初期のPVIDに再マッピングします。

802.1X ゲスト VLAN 機能のため、MAC ベースアクセス制御を実行するポートで以下の要件に対応してください。

- □ ポートがハイブリッドポートです。
- □ ポートで MAC ベースアクセス VLAN が有効です。

ネットワークデバイスはハイブリッドポートをタグなしメンバとして 802.1X ゲスト VLAN に割り当てます。

VLAN の設定と MAC ベース VLAN の詳細は、オペレーションマニュアルのセクション 3 *アクセス”VLAN”*を参照してください。

3.2.3 制限 VLAN

組織のセキュリティ戦略に適合できずに失敗したことが原因で 802.1X 認証に失敗したユーザに対応するため、制限 VLAN を設定することができます。たとえば間違ったパスワードを入力したユーザに VLAN が適応します。制限 VLAN は、アンチウィルスソフトウェアやシステムパッチをダウンロードするためにソフトウェアサーバなどの制限されたネットワークリソースのみアクセスすることができます。

制限 VLAN は、認証のタイムアウトやネットワーク接続の問題のために認証に失敗した 802.1X のユーザには対応していません。

アクセス装置がポート上の VLAN を処理する方法は、802.1X アクセス制御モードによって異なります。

- ポートベースアクセス制御を実行するポート

認証状態	VLAN 操作
ユーザが802.1X認証に失敗した	デバイスはPVIDとしてポートに制限VLANを割り当てます。ポートのすべての802.1Xユーザは制限VLANのリソースのみアクセスすることができます。
サーバ到達不能の理由を除いた他の理由によって、802.1X制限VLANのユーザが802.1X認証に失敗した	制限VLANが設定されている場合、ポートのPVIDは制限VLAN IDに変更されます。ポートのすべての802.1Xユーザはこの VLANにいます。
ユーザが802.1X認証にパスした	• デバイスはPVIDとしてポートにユーザの許可VLANを割り当て、制限VLANからポートを削除します。ユーザがログオフしたのち、ゲストVLANがPVIDとしてポートに割り当てられます。ゲストVLANが設定されていない場合、初期のPVIDに戻ります。 • 認証サーバがVLANを許可しない場合、ポートの初期のPVIDが適用されます。ユーザと後続のすべての802.1Xユーザは初期のPVIDに割り当てられますユーザがログオフしたのち、PVIDは変更されません。

- MAC ベースアクセス制御を実行するポート

認証状態	VLAN 操作
ユーザが802.1X認証に失敗した	デバイスはユーザのMACアドレスを802.1X制限VLANにマッピングします。ユーザは制限VLANのリソースのみアクセスすることができます。
サーバ到達不能の理由を除いた他の理由によって、802.1X制限VLANのユーザが802.1X認証に失敗した	ユーザは制限VLANのままです。
制限VLANのユーザが802.1X認証にパスした	デバイスはユーザのMACアドレスを認証VLANに再マッピングします。 認証サーバがVLANを許可しない場合、デバイスはユーザのMACアドレスをポートの初期のPVIDに再マッピングします。

802.1X 制限 VLAN 機能のため、MAC ベースアクセス制御を実行するポートがハイブリッドポートであることを確認し、ポート上で MAC ベース VLAN を有効にしてください。

アクセス装置はハイブリッドポートをタグなしメンバとして 802.1X 制限 VLAN に割り当てます。

VLAN の設定と MAC ベース VLAN の詳細は、オペレーションマニュアルのセクション 3 *アクセス”VLAN”* を参照してください。MAC ベース VLAN 機能のサポートは装置の種類によって異なります。

3.3 他の機能を用いた802.1X認証

3.3.1 ACL の割り当て

ネットワークリソースへのアクセスを制御するため、802.1X ユーザに ACL を指定することができます。ユーザが 802.1X 認証にパスしたのち、認証サーバはユーザのトラフィックをフィルタするためアクセスポートに ACL を割り当てます。認証サーバはローカルアクセス装置あるいは RADIUS サーバで行えます。どちらの場合でも、アクセス装置で ACL を設定する必要があります。ユーザはオンライン中に ACL を変更することができます。ACL の詳細は、オペレーションマニュアルのセクション 8 *ACL and QoS*”*ACL*”を参照してください。

3.4 802.1X設定制限とガイドライン

802.1X を設定する場合には、以下の制限とガイドラインに従ってください。

- 802.1X の設定は、レイヤ 2 イーサネットインタフェースでのみサポートされます。
- レイヤ 2 イーサネットインタフェースで 802.1X を有効にする前に、インタフェースがレイヤ 2 アグリゲーショングループに加えられていないことを確認してください。

3.4.1 設定要件

802.1X を設定する前に、以下の作業を完了してください。

- 802.1X ユーザのために ISP ドメインと AAA スキーム（ローカルまたは RADIUS 認証）を設定してください。
- RADIUS 認証を使用する場合は、RADIUS サーバにユーザアカウントを作成してください。
- ローカル認証を使用する場合は、アクセス装置にローカルユーザアカウントを作成し、サービスタイプを lan-access に設定してください。

RADIUS クライアントの設定の詳細は、オペレーションマニュアルのセクション 9 *セキュリティ*”*AAA*”を参照してください。

3.5 802.1X設定作業リスト

作業リスト
（必須設定項目）802.1X認証の有効化
（必須設定項目）EAP relayまたはEAP terminationの有効化
（オプション設定項目）ポート許可状態の設定
（オプション設定項目）アクセス制御方式の指定
（オプション設定項目）ポートの802.1Xユーザの最大同時接続数の設定
（オプション設定項目）認証リクエストの最大送信数の設定
（オプション設定項目）802.1X認証タイムアウトタイマの設定
（オプション設定項目）オンラインユーザハンドシェイク機能の設定
（オプション設定項目）認証トリガ機能の設定

作業リスト
（オプション設定項目）ポートでの強制認証ドメインの設定
（オプション設定項目）quietタイマの設定
（オプション設定項目）802.1X再認証機能の有効化
（オプション設定項目）802.1XゲストVLANの設定
（オプション設定項目）802.1XゲストVLAN割り当て遅延の有効化
（オプション設定項目）802.1X制限VLANの設定
（オプション設定項目）MACアドレス移動機能の有効化
（オプション設定項目）802.1Xユーザのログオフ
（オプション設定項目）802.1 X非認証ユーザエージングの設定

3.6 802.1X認証の有効化

802.1X 認証を有効にするとき、以下のガイドラインに従ってください。

- PVID が Voice VLAN である場合、802.1X 機能はポートに適用できません。Voice VLAN の詳細は、オペレーションマニュアルのセクション 3 *アクセス“Voice VLAN”* を参照してください。
- 802.1X 認証が有効なポートでリンクアグリゲーションまたはループバックグループサービスを設定することができません。

以下に 802.1X 認証の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． グローバルで 802.1X 認証を有効にする	**dot1x**	デフォルト：無効
3． interface view に移行する	**interface** *interface-type interface-number*	―
4． ポートで 802.1X 認証を有効にする	**dot1x**	デフォルト：無効

3.7 EAP relayまたはEAP terminationの有効化

EAP relay または EAP termination を設定するときに、以下の点を考慮してください。

- EAP パケットに関する RADIUS サーバのサポート
- 802.1X クライアントと RADIUS サーバでサポートされている認証方式

以下の状況では EAP relay と EAP termination の両方を設定することができます。

- クライアントが MD5-Challenge EAP 認証のみを使用します。
- クライアントが"ユーザ名+パスワード"の EAP 認証のみを使用します。

EAP-TL、PEAP、またはその他の EAP 認証方式を使用するには、EAP relay を使用する必要があります。

EAP relay と EAP termination の詳細は、オペレーションマニュアルのセクション 9 *セキュリティ”802.1X の概要””* を参照してください。

以下に EAP relay と EAP termination の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． EAP relay または EAP termination を設定する	**dot1x authentication-method** { **chap** | **eap** | **pap** }	デフォルトでは、ネットワークアクセス装置は、EAP terminationを実行し、RADIUSサーバとの通信にCHAPを使用します。 EAP terminationを有効にするためには、**eap**パラメータを指定してください。 CHAP対応またはPAP対応のEAP relayを有効にするためには、**chap**または**pap**パラメータを指定してください。

🕮 **メモ：**

EAP relay モードが使用されている場合、RADIUS scheme view で設定された **user-name-format** コマンドは適用されません。アクセス装置はクライアントからの認証データを何も変更せずにサーバに送信します。

3.8 ポート許可状態の設定

ポートの許可状態は、クライアントがネットワークへのアクセスを許可されているかどうかを決定します。**dot1x port-control** コマンドと以下のキーワードを使用して、ポートの認証状態を制御できます。

- **authorized-force**－ポートを authorized 状態にすると、認証なしでネットワークにアクセスするポート上のユーザを有効にします。
- **unauthorized-force**－ポートを unauthorized 状態にすると、ポート上のユーザからのアクセス要求を拒否します。
- **auto**－EAPOL パケットのみの通過を許可するために、最初にポートを unauthorized 状態にし、ユーザが認証を通過した後、ネットワークへのアクセスを許可するために、ポートを authorized 状態にします。ほとんどの場合で、このオプションを使用することができます。

以下にポート許可状態の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． interface view に移行する	**interface** *interface-type interface-number*	―
3． ポート認証状態を設定する	**dot1x port-control** { **authorized-force** | **auto** | **unauthorized-force** }	デフォルト：**auto**

3.9 アクセス制御方式の指定

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． interface view に移行する	**interface** *interface-type interface-number*	―
3． アクセス制御方式を指定する	**dot1x port-method** { **macbased** | **portbased** }	デフォルト：**macbased**

3.10 ポートの802.1Xユーザの最大同時接続数の設定

この設定を行うことにより、ユーザ過多によりシステムリソース不足になることを防ぎます。

以下にポートでの 802.1X ユーザの最大同時接続数の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． interface view に移行する	**interface** *interface-type interface-number*	―
3． ポートでの 802.1X ユーザの最大同時接続数を設定する	**dot1x max-user** *user-number*	デフォルト：4294967295

🕮 **メモ：**

QX-S5100G シリーズは 2048 まで認証動作が可能です。

3.11 認証リクエストの最大送信数の設定

アクセス装置は、指定した時間内にクライアントからの応答がない場合、認証リクエストの再送信を行います。この時間を設定する場合、**dot1x timer tx-period** *tx-period-value* コマンドまたは **dot1x timer supp-timeout** *supp-timeout-value* コマンドを使用します。

アクセス装置からリクエストの最大送信数まで再送信しても応答がない場合、リクエストの再送信を停止します。

以下に認証リクエストの最大送信数の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． クライアントへの認証リクエストの最大送信数を設定する	**dot1x retry** *max-retry-value*	デフォルト：2

3.12 802.1X認証タイムアウトタイマの設定

ネットワークデバイスは、以下の 802.1X 認証タイムアウトタイマを使用しています。

- **クライアントタイムアウトタイマ**－アクセス装置がクライアントに EAP-Request/MD5 Challenge パケットを送信するときに起動します。このタイマが時間切れになるまで応答がなかった場合、アクセス装置は、クライアントにリクエストを再送します。
- **サーバタイムアウトタイマ**－アクセス装置が認証サーバに RADIUS Access-Request パケットを送信するときに起動します。このタイマが時間切れになるまでに応答がなかった場合、アクセス装置は、サーバにリクエストを再送します。

ほとんどの場合、デフォルトの設定で十分です。ネットワークの状況に応じてタイマを設定することができます。

- パフォーマンスの低いネットワークで、クライアントタイムアウトタイマを高い値に設定します。
- 異なる性能の認証サーバがあるネットワークでサーバタイムアウトタイマを調整します。

以下に 802.1X 認証タイムアウトタイマの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	－
2． クライアントタイムアウトタイマを設定する	**dot1x timer supp-timeout** *supp-timeout-value*	デフォルト：30秒
3． サーバタイムアウトタイマを設定する	**dot1x timer server-timeout** *server-timeout-value*	デフォルト：100秒

3.13 オンラインユーザハンドシェイク機能の設定

オンラインユーザハンドシェイク機能は、オンラインの 802.1X ユーザの接続状態をチェックします。ネットワークアクセス装置は、**dot1x timer handshake-period** コマンドで指定された間隔でオンラインユーザにハンドシェイクメッセージを送信します。ハンドシェイクの最大試行回数後もオンラインユーザから応答を受信しない場合、ネットワークアクセス装置は、ユーザを offline 状態に設定します。ハンドシェイクの最大試行回数を設定する場合、**dot1x retry** コマンドを使用します。

また、本装置はデフォルトでオンラインユーザからの EAP-response に対する EAP-success を返しません。EAP-response に対する EAP-success を返すには、**dot1x handshake reply enable** コマンドを使用します。

3.13.1 設定ガイドライン

オンラインユーザハンドシェイク機能を設定するとき、以下の制限とガイドラインに従ってください。

- ネットワークに、ネットワークアクセス装置とのハンドシェイクパケットを交換できない 802.1X クライアントがある場合、オンラインユーザハンドシェイク機能を無効にしてください。これは 802.1X 接続が不適切に切断されることを防ぎます。

3.13.2 設定手順

以下にオンラインユーザハンドシェイク機能の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． （オプション設定項目）ハンドシェイクタイマを設定する	**dot1x timer handshake-period** *handshake-period-value*	デフォルト：15秒
3． interface view に移行する	**interface** *interface-type interface-number*	―
4． オンラインユーザハンドシェイク機能を有効にする	**dot1x handshake**	デフォルト：無効
5． ハンドシェイクリプライ機能を有効にする	**dot1x handshake reply enable**	デフォルト：無効

3.14 認証トリガ機能の設定

認証トリガ機能は、802.1X クライアントが認証を開始できない場合、802.1X 認証を開始するためにネットワークアクセス装置を有効にします。

この機能はマルチキャストトリガとユニキャストトリガをサポートします。オペレーションマニュアルのセクション 9 *セキュリティ*“*802.1X の概要*”を参照してください。

3.14.1 設定ガイドライン

認証トリガ機能を設定するときは、以下のガイドラインに従ってください。

- ポートに接続されたクライアントが、802.1X 認証を開始するために EAPOL-Start パケットを送信できない場合、ポート上でマルチキャストトリガを有効にします。
- 802.1X クライアントがほとんどいないポートに接続され、これらのクライアントが認証を開始できない場合は、ポート上でユニキャストトリガを有効にします。
- 重複した認証パケットを避けるために、ポート上で両方のトリガを有効にしないでください。

3.14.2 設定手順

以下にポートでの認証トリガ機能の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―

操作	コマンド	補足
2．（オプション設定項目）ユーザ名リクエストタイムアウトタイマを設定する	**dot1x timer tx-period** *tx-period-value*	デフォルト：30秒
3．interface view に移行する	**interface** *interface-type interface-number*	―
4．認証トリガ機能を有効にする	**dot1x** { **multicast-trigger** | **unicast-trigger** }	デフォルト： ・マルチキャストトリガ無効 ・ユニキャストトリガ有効

3.15 ポートでの強制認証ドメインの設定

ポート上で認証、許可、アカウンティングのための強制認証ドメイン内にすべての 802.1X ユーザを配置することができます。ユーザは、他のドメイン内のアカウントを使用して、ポートを介してネットワークにアクセスすることはできません。強制認証ドメインの実装で、802.1X アクセス制御の導入時の柔軟性を高めます。

以下にポートでの強制認証ドメインの設定を示します。

操作	コマンド	補足
1．system view に移行する	**system-view**	―
2．interface view に移行する	**interface** *interface-type interface-number*	―
3．ポートで 802.1X 強制認証ドメインを指定する	**dot1x mandatory-domain** *domain-name*	デフォルト：設定なし

3.16 quietタイマの設定

quiet タイマを有効にすると、アクセス装置は、802.1X 認証に失敗したクライアントからの認証リクエストを処理する前に一定時間待ちます。

ネットワークの状況に応じて quiet タイマを設定することができます。

- 脆弱なネットワークでは高い値を設定してください。
- 認証応答を速くするためには低い値を設定してください。

以下に quiet タイマの設定を示します。

操作	コマンド	補足
1．system view に移行する	**system-view**	―
2．quiet タイマを有効にする	**dot1x quiet-period**	デフォルト：無効
3．（オプション設定項目）quiet タイマを設定する	**dot1x timer quiet-period** *quiet-period-value*	デフォルト：60秒

3.17 802.1X再認証の設定

3.17.1 概要

802.1X 再認証は、オンラインユーザの接続状態をトラッキングし、サーバによって割り当てられた属性を更新します。属性は ACL、VLAN が含まれます。

802.1X 再認証では、再認証の間隔はユーザが設定できます。

デフォルトでは、802.1X 再認証のサーバが到達不能である場合、装置はユーザをログオフします。オンライン保持機能は、サーバが到達不能な場合、802.1X ユーザの再認証を継続します。

3.17.2 設定ガイドライン

802.1X 再認証を設定するときは、以下のガイドラインに従ってください。

サーバで割り当てられたセッションタイムアウトタイマ（セッションタイムアウト属性）と終了行動（終了行動属性）は定期的な再認証に影響することがあります。サーバで割り当てられたセッションタイムアウトと終了行動の属性を表示するには、**display dot1x connection** コマンドを使用してください。

- 終了行動が **Default**（ログオフ）の場合、session timeout タイマよりも定期的な再認証タイマが短い際に効果があります。
- 終了行動が **Radius-request** の場合、定期的な再認証は効果がありません。session timeout タイマが終了後にオンライン 802.1X ユーザを再認証します。

session timeout と termination action 属性の割り当てサポートは、サーバモデルによります。

- **dot1x timer reauth-period** コマンドを使用して、定期的な再認証タイマをシステム view とインタフェース view のどちらでも設定できます。

  デバイスは、以下の順に定期的な再認証タイマを選択します。

a) サーバ割り当てされた再認証タイマ

b) ポート指定の再認証タイマ

c) グローバル再認証タイマ

d) デフォルト再認証タイマ

- 認証前後でオンラインユーザに割り当てられた VLAN は、同一でも異なっても可能です。

3.17.3 802.1X 定期的な再認証の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	ー

操作	コマンド	補足
2.　（オプション設定項目）定期的な認証タイマを設定する	**dot1x timer reauth-period** *reauth-period-value*	デフォルト：3600秒
3.　interface view に移行する	**interface** *interface-type interface-number*	―
4.　定期的なオンラインユーザの再認証を設定する	**dot1x re-authenticate**	デフォルト：無効
5.　（オプション設定項目）ポートに定期的な認証タイマを設定する	**dot1x timer reauth-period** *reauth-period-value*	デフォルト：無効 グローバルの定期的な802.1X再認証タイマを使用します。

3.18 802.1XゲストVLANの設定

3.18.1 設定ガイドライン

802.1X ゲスト VLAN を設定するとき、以下のガイドラインに従ってください。

- ポートに 1 つのみ 802.1X ゲスト VLAN を設定することができます。異なるポートで異なる 802.1X ゲスト VLAN を設定することができます。
- ポートでポート VLAN、802.1X ゲスト VLAN に異なる ID を割り当ててください。ポートで、VLAN にタグづけられた入力トラフィックの処理を正しく処理できるように割り当ててください。
- ポートで複数のセキュリティ機能を設定するとき、表 3-3に示すガイドラインに従ってください。

表 3-3 802.1X ゲスト VLAN と他のセキュリティ機能の関係

機能	関係	補足
MACベースのアクセス制御を行うポート上の802.1X制限VLAN	802.1X制限VLANは802.1XゲストVLANより優先順位が高くなります。	オペレーションマニュアルのセクション 9 *セキュリティ" 802.1X"* を参照してください。
MACベースのアクセス制御を行うポート上のポート侵入防御	802.1XゲストVLAN機能は、MACアドレスのブロック動作よりも優先順位が高くなります。ポート侵入保護機能のポートシャットダウン動作よりも優先順位が低いです。	オペレーションマニュアルのセクション 9 *セキュリティ"ポートセキュリティ"* を参照してください。

3.18.2 設定要件

802.1X ゲスト VLAN を設定する前に、以下の作業を完了してください。

- 802.1X ゲスト VLAN として指定される VLAN を作成してください。
- 802.1X 対応ポートが MAC ベースのアクセス制御を行う場合、以下の作業を完了してください。
  - □　ハイブリッドポートとして設定してください。

- □ ポートで MAC ベース VLAN を有効にしてください。MAC ベース VLAN の詳細は、オペレーションマニュアルのセクション 3 *アクセス”VLAN”* を参照してください。
- □ ポートをタグなしメンバとして 802.1X ゲスト VLAN に割り当ててください。

3.18.3 設定手順

以下に 802.1X ゲスト VLAN の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． interface view に移行する	**interface** *interface-type interface-number*	―
3． ポートで 802.1X ゲスト VLAN を設定する	**dot1x guest-vlan** *guest-vlan-id*	デフォルト：設定なし

3.19 802.1XゲストVLAN割り当て遅延の有効化

3.19.1 設定ガイドライン

この機能は、ポートで 802.1X 認証が行われる場合に 802.1X ゲスト VLAN への 802.1X が有効なポートを割り当てるのを遅らせます。

この機能は、EAPOL 開始パケットまたはアンノウン MAC アドレスからのパケットにより 802.1X 認証が行われる場合にのみ適用されます。

この機能を使用するには、802.1X 有効ポートは MAC ベースのアクセス制御を行わなければなりません。MAC トリガの 802.1X ゲスト VLAN 割り当て遅延を使用するには、ポートに 802.1X ユニキャストトリガも設定しなければなりません。

802.1X 認証がポートで行われる場合、装置は以下の操作を行います。

- ユニキャスト EAP-Request/Identity パケットを認証のトリガとなった MAC アドレスに送信します。
- **dot1x timer tx-period** コマンドで設定されたユーザネーム要求タイムアウト期間内に応答がなかった場合、パケットを再送します。
- dot1x retry コマンドで設定された最大リクエスト試行回数に達した後、ポートに 802.1x ゲスト VLAN を割り当てます。

以下にポートへの 802.1X ゲスト VLAN 割り当て遅延の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． interface view に移行する	**interface** *interface-type interface-number*	―
3． ポートで 802.1X ゲスト VLAN 割り当て遅延を設定する	**dot1x guest-vlan-delay** { **eapol** | **new-mac** }	デフォルト：無効

3.20 802.1X制限VLANの設定

3.20.1 設定ガイドライン

802.1X 制限 VLAN を設定する前に、以下の制限とガイドラインに従ってください。

- ポートで Voice VLAN、ポート VLAN、802.1X 制限 VLAN に異なる ID を割り当ててください。ポートで、VLAN にタグづけられた入力トラフィックの処理を正しく処理できるように割り当ててください。
- ポートに 1 つのみ 802.1X 制限 VLAN を設定することができます。異なるポートで異なる 802.1X 制限 VLAN を設定することができます。
- ポートで複数のセキュリティ機能を設定するとき、表 3-4に示すガイドラインに従ってください。

表 3-4 802.1X 制限 VLAN と他のセキュリティ機能の関係

機能	関係	補足
MACベースのアクセス制御を行うポート上のMACアドレス認証ゲストVLAN	802.1X制限VLANは優先順位が高くなります。	オペレーションマニュアルのセクション 9 *セキュリティ”MAC アドレス認証”*を参照してください。
MACベースのアクセス制御を行うポート上のポート侵入防御	802.1X制限VLAN機能は、MAC動作のブロックよりも優先順位が高くなります。ポート侵入保護機能のポートシャットダウン動作よりも優先順位が低いです。	オペレーションマニュアルのセクション 9 *セキュリティ”ポートセキュリティ”*を参照してください。

3.20.2 設定要件

802.1X 制限 VLAN を設定する前に、以下の作業を完了してください。

- 802.1X 制限 VLAN として指定される VLAN を作成してください。
- 802.1X 対応ポートが MAC ベースのアクセス制御を行う場合、以下の作業を完了してください。
  - □ ハイブリッドポートとして設定してください。
  - □ ポートで MAC ベース VLAN を有効にしてください。MAC ベース VLAN の詳細は、オペレーションマニュアルのセクション 3 *アクセス”VLAN”*を参照してください。
  - □ ポートをタグなしメンバとして 802.1X 制限 VLAN に割り当ててください。

3.20.3 設定手順

以下に 802.1X 制限 VLAN の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． interface view に移行する	**interface** *interface-type interface-number*	―

操作	コマンド	補足
3． ポートで 802.1X 制限 VLAN を設定する	**dot1x auth-fail vlan** *authfail-vlan-id*	デフォルト：設定なし

3.21 MACアドレス移動機能の有効化

MAC アドレス移動機能を有効にすることで、認証が許可されたユーザが装置のポートを移動できるようになります。たとえば、認証ユーザが別のポートに移動する場合、認証セッションが最初のポートから削除され、新しいポートで再認証されます。

もし、MAC アドレス移動機能が無効で認証ユーザが別のポートに移動した場合、再認証されません。

（ローカルまたはリモートの）認証サーバのオンラインユーザ数が上限に達した場合、認証ユーザは装置上のポート間で移動はできません。

ポートのローミングを行うワイヤレスユーザがネットワークにアクセスできるように MAC アドレス移動機能を有効にすることを推奨します。

以下に MAC アドレス移動機能の有効化の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． MAC アドレス移動機能を有効にする	**port-security mac-move permit**	デフォルト：有効

3.22 802.1Xユーザのログオフ

I. 802.1X ユーザのログオフ

特定の 802.1X ユーザをログオフし、これらのユーザに関する情報を装置から消去するには、このタスクを実行します。これらのユーザは 802.1X 認証を実行して再度オンラインにする必要があります。

II. 設定手順

操作	コマンド	補足
user view で実行し、802.1X ユーザをログオフする	**reset dot1x access-user** [**interface** *interface-type interface-number* | **mac** *mac-address* | **username** *username* | **vlan** *vlan-id*]	―

3.23 802.1 X非認証ユーザエージングの設定

I. 802.1 X 非認証ユーザエージング

802.1 X 非認証ユーザエージングは、802.1 X ゲスト、Auth-Fail VLAN に追加されたユーザに適用されます。

これらの VLAN のいずれかのユーザがエージングアウトすると、装置は VLAN からユーザを削除し、アクセスポートからユーザのエントリアドレスを削除します。

1 つのポートでこれらの VLAN のいずれかのユーザが正常に認証され、別のポートでオンラインになるには、この機能を有効にします。それ以外の場合は、この機能を無効にすることをお勧めします。

ポートの 802.1 X ユーザエージングメカニズムは、そのアクセス制御モードに依存します。

- ポートがポートベースアクセス制御を使用している場合、ポートが Auth-Fail VLAN に割り当てられると、ユーザエージングタイマが開始されます。エイジングタイマが満了すると、ポートは VLAN から削除され、VLAN 内のユーザのすべてのアドレスエントリも削除されます。
- ポートが MAC ベースのアクセス制御を使用する場合、Auth-Fail、Guest VLAN に割り当てられた 802.1 X ユーザごとにユーザエージングタイマが開始されます。ユーザエージングタイマが満了すると、装置は VLAN からそのユーザを削除します。

削除されたユーザは、別の認証がトリガされるまでネットワークリソースにアクセスできません。

II. 制限とガイドライン

ベストプラクティスとしては、あるポート上の非認証ユーザを認証して別のポートでオンラインにしたい場合を除いて、802.1 X 非認証ユーザエージングを無効にします。

III. 設定手順

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． ユーザエージングタイマを 802.1 X VLAN のタイプに設定する	**dot1x timer user-aging** { **auth-fail-vlan** | **guest-vlan** } *aging-time-value*	デフォルト : すべての適用可能なタイプの802.1 X VLANのユーザエージングタイマは1000秒です。
3． interface view に移行する	**interface** *interface-type interface-number*	―
4． 802.1 X 非認証ユーザエージングを有効にする	**dot1x unauthenticated-user aging enable**	デフォルト：有効

3.24 802.1 Xユニキャストトリガーサイレント機能

🕮 **メモ：**

ポートでの認証方式のトリガー順序の設定は Version7.1.7 を含む以降のソフトウェアからサポートしています。

I. 概要

ユニキャストトリガーがイネーブルになっているポートで未知の送信元 MAC アドレスを持つパケットを受信すると、デバイスは EAP-Request/Identity 要求パケットをクライアントにユニキャストします。dot 1 x timer tx-period コマンドを使用して設定された期間内にクライアントから応答がない場合、デバイスはクライアントに要求を再送信します。デバイスは、最大回数の送信試行を行ってもクライアントから応答を受信できない場合、タイマアドレスのユニキャストトリガーサイレント MAC を開始します。要求パケットを送信する最大試行回数を設定するには、dot 1 x retry コマンドを使用します。

ユニキャストトリガー抑制タイマアドレスがある MAC アドレスから始まる場合、この MAC アドレスはユニキャストトリガー抑制アドレスと呼ばれます。タイマが期限切れになるまでは、デバイスはこの MAC アドレスを送信元 MAC アドレスとして持つパケットを受信しても、この MAC アドレスに対して EAP-Request/Identity 要求パケットをユニキャストしません。

II. 制約事項およびガイドライン

802.1 X ユニキャストトリガーサイレント機能は、慎重に使用してください。この機能は、802.1 X ユーザがオンラインになるレートに影響する場合があります。

この機能は、次の機能と組み合わせて使用しないでください。

- ゲスト VLAN
- ゲスト VSI
- EAD アシスタント

III. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. ユニキャストトリガーサイレントタイマを設定する	dot1x timer unicast-trigger quiet-period quiet-period-value	デフォルト：ディセーブル ユニキャストトリガー待機時間は0秒です。

3.25 802.1Xの表示と維持

すべての view で **display** コマンドを実行でき、user view で **reset** コマンドを実行できます。

操作	コマンド
特定、またはすべてのポートの802.1X認証情報、統計情報、設定情報を表示する	**display dot1x** [**sessions** | **statistics**] [**interface** *interface-type interface-number*]
オンライン802.1Xユーザ情報を表示する	**display dot1x connection** [**interface** *interface-type interface-number* | **slot** *slot-number* | **user-mac** *mac-addr* | **user-name** *name-string*]
802.1 Xユニキャストトリガークワイエット MACアドレスを表示する	display dot1x unicast-trigger quiet-mac **[** interface interface-type interface-number **]**
802.1X統計情報をクリアする	**reset dot1x statistics** [**interface** *interface-type interface-number*]
ポートで802.1Xゲスト VLANからユーザを取り除く	**reset dot1x guest-vlan interface** *interface-type interface-number* [**mac-address** *mac-address*]
802.1 Xユニキャストトリガークワイエット MACアドレスをクリアする	reset dot1x unicast-trigger quiet-mac **[** interface interface-type interface-number **] [** mac-address mac-address **]**

3.26 802.1X認証の設定例

3.26.1 基本的な 802.1X 認証の設定例

I. ネットワーク要件

図 3-1に示すように、アクセス装置は、GigabitEthernet 1/0/1 に接続するユーザ用に 802.1X 認証を実行します。ポート上で MAC ベースのアクセス制御を行ってください。1 ユーザのログオフは、他のオンラインの 802.1X ユーザには影響しません。

802.1X ユーザの認証、許可、アカウンティングを実行するために RADIUS サーバを使用してください。 RADIUS 認証が失敗した場合、アクセス装置上でローカル認証を実行します。

プライマリ認証およびアカウンティングサーバとして 10.1.1.1/24 のホスト、セカンダリ認証とアカウンティングサーバとして 10.1.1.2/24 のホストを設定します。すべてユーザを収容できる ISP ドメイン bbb にすべてのユーザを割り当てます。

アクセス装置と認証サーバ間のパケットに name という名称で共有鍵を、アクセス装置とアカウンティングサーバ間のパケットに money という名称で共有鍵を設定します。

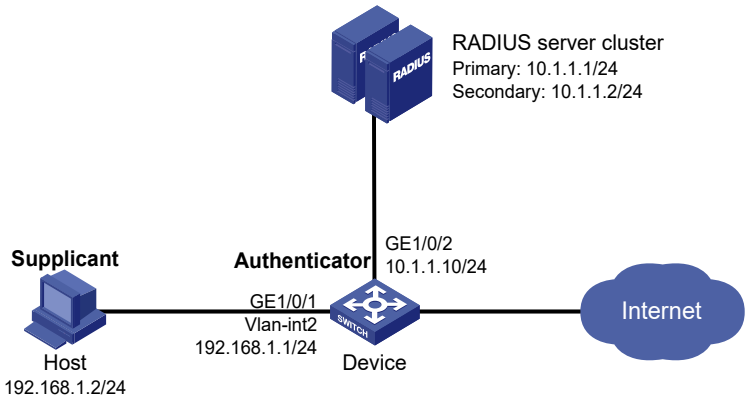


図 3-1 ネットワーク図

II. 設定手順

1) 802.1X クライアントを設定します。（詳細は省略）
2) RADIUS サーバを設定し、802.1X ユーザ用のユーザアカウントを追加します。（詳細は省略します。）

アクセス装置で使用される RADIUS コマンドについての詳細は、コマンドマニュアルのセクション 9 *セキュリティ”AAA”* を参照してください。

3) アクセス装置上の各インタフェースに IP アドレスを割り当てます。（詳細は省略します。）
4) アクセス装置上で 802.1X ユーザ用のユーザアカウントを設定します。

ユーザ名とパスワードがそれぞれ localuser と localpass のローカルユーザをプレーンテキストで追加します。（ユーザ名とパスワードは RADIUS サーバに設定されたものと同じにしてください。）

```
<Device> system-view
[Device] local-user localuser class network
[Device-luser-network-localuser] password simple localpass
```

サービスタイプに lan-access を選択します。

```
[Device-luser-network-localuser] service-type lan-access
[Device-luser-network-localuser] quit
```

5) RADIUS スキームを設定します。

RADIUS スキーム radius1 を作成し、RADIUS scheme view に移行します。

```
[Device] radius scheme radius1
```

プライマリ認証/アカウンティング RADIUS サーバの IP アドレスを指定します。

```
[Device-radius-radius1] primary authentication 10.1.1.1
[Device-radius-radius1] primary accounting 10.1.1.1
```

セカンダリ認証/アカウンティング RADIUS サーバの IP アドレスを指定します。

```
[Device-radius-radius1] secondary authentication 10.1.1.2
```

```
[Device-radius-radius1] secondary accounting 10.1.1.2
```

アクセス装置と認証サーバ間の共有鍵を指定します。

```
[Device-radius-radius1] key authentication simple name
```

アクセス装置とアカウンティングサーバ間の共有鍵を指定します。

```
[Device-radius-radius1] key accounting simple money
```

RADIUS サーバに送信されるユーザ名から ISP のドメイン名を除外します。

```
[Device-radius-radius1] user-name-format without-domain
[Device-radius-radius1] quit
```

メモ：

アクセス装置は、RADIUS サーバと同じユーザ名のフォーマットを使用する必要があります。RADIUS サーバがユーザ名に ISP のドメイン名を含む場合、アクセス装置です。

6)　ISP ドメインを設定します。

ISP ドメイン bbb を作成し、ISP domain view に移行します。

```
[Device] domain bbb
```

RADIUS スキーム radius1 を ISP ドメインに適用し、セカンダリ認証方式としてローカル認証を指定します。

```
[Device-isp-bbb] authentication lan-access radius-scheme radius1 local
[Device-isp-bbb] authorization lan-access radius-scheme radius1 local
[Device-isp-bbb] accounting lan-access radius-scheme radius1 local
[Device-isp-bbb] quit
```

7)　802.1X を設定します。

GigabitEthernet 1/0/1 で 802.1X を有効にします。

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] dot1x
```

ポート上で MAC ベースのアクセス制御を有効にします。デフォルトでポートは MAC ベースアクセス制御を使用します。

```
[Device-GigabitEthernet1/0/1] dot1x port-method macbased
```

bbb を強制認証ドメインとして設定します。

```
[Device-GigabitEthernet1/0/1] dot1x mandatory-domain bbb
[Device-GigabitEthernet1/0/1] quit
```

802.1X をグローバルで有効にします。

```
[Device] dot1x
```

III. 設定の確認

GigabitEthernet 1/0/1 の 802.1X 認証の設定を確認します。

```
[Device] display dot1x interface gigabitethernet 1/0/1
```

802.1X ユーザが RADIUS 認証を通過した後、ユーザ接続情報を表示します。

```
[Device] display dot1x connection
```

3.26.2 802.1X ゲスト VLAN と許可 VLAN の設定例

I. ネットワーク要件

図 3-2に示すように、GigabitEthernet 1/0/2 に接続される 802.1X ユーザの認証、許可、アカウンティングを実行するため、RADIUS サーバを使用します。ポートでポートベースのアクセス制御を実装します。

GigabitEthernet 1/0/2 で一定の期間内に 802.1X 認証を実行するユーザがいない場合、デバイスはゲスト VLAN である VLAN10 に GigabitEthernet 1/0/2 を追加します。ホストとアップデートサーバは両方とも VLAN10 にあります。ホストはアップデートサーバにアクセスでき、802.1X クライアントソフトウェアをダウンロードできます。

ホストが 802.1X 認証にパスしたのち、アクセス装置は GigabitEthernet 1/0/3 が所属する VLAN5 にホストを割り当てます。ホストはインタネットにアクセスできます。

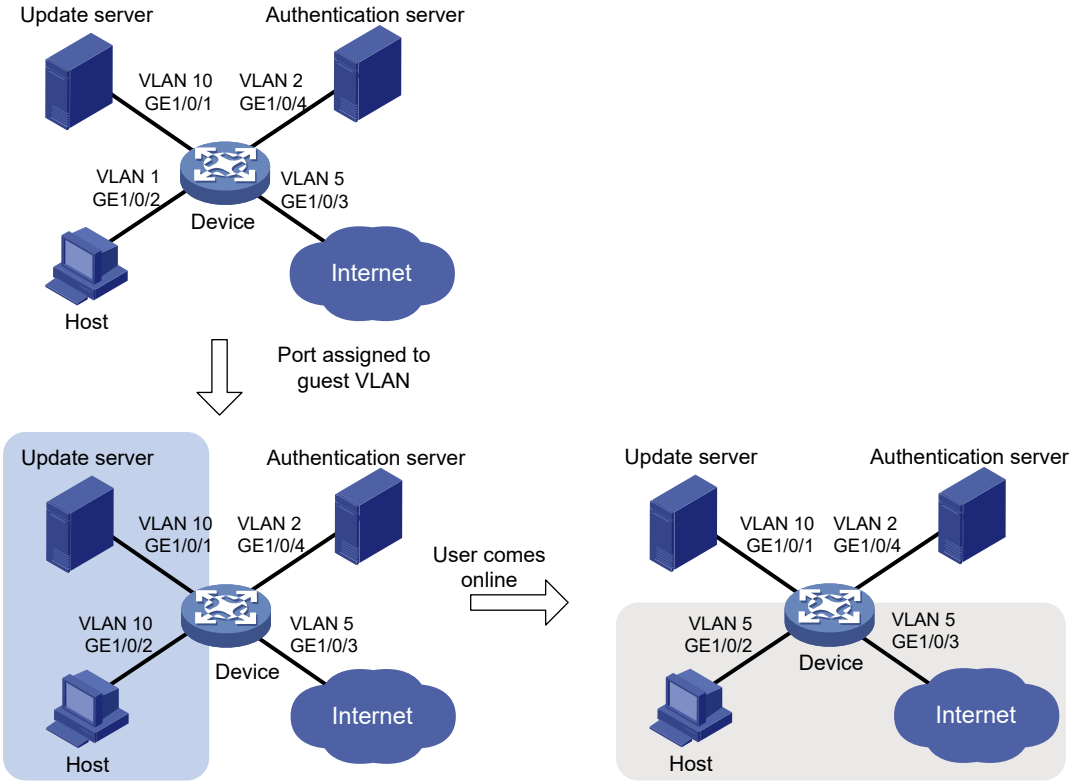


図 3-2 ネットワーク図

II. 設定手順

1) 802.1X クライアントの設定を行います。802.1X クライアントは、アクセスポートがゲスト VLAN あるいは許可 VLAN に割り当てられたのち、IP アドレスをアップデートできます。（詳細は省略します）
2) 認証、許可、アカウンティングサービスを許可する RADIUS サーバを設定します。ユーザのユーザアカウント、許可 VLAN（この例では VLAN 5）を設定します。（詳細は省略します。）
3) VLAN を作成し、アクセス装置の VLAN にポートを割り当てます。

```
<Device> system-view
[Device] vlan 1
[Device-vlan1] port gigabitethernet 1/0/2
[Device-vlan1] quit
[Device] vlan 10
[Device-vlan10] port gigabitethernet 1/0/1
[Device-vlan10] quit
[Device] vlan 2
[Device-vlan2] port gigabitethernet 1/0/4
[Device-vlan2] quit
[Device] vlan 5
```

```
[Device-vlan5] port gigabitethernet 1/0/3
[Device-vlan5] quit
```

4)　アクセス装置で RADIUS スキームを設定します。

RADIUS スキーム 2000 を作成し、RADIUS scheme view に移行します。

```
[Device] radius scheme 2000
```

プライマリ認証サーバとして 10.11.1.1 を指定し、認証ポートとして 1812 を指定します。

```
[Device-radius-2000] primary authentication 10.11.1.1 1812
```

プライマリアカウンティングサーバとして 10.11.1.1 を指定し、アカウンティングポートとして 1813 を指定します。

```
[Device-radius-2000] primary accounting 10.11.1.1 1813
```

認証サーバとデバイス間でセキュアな通信を行うため、プレーンテキストで abc の共有鍵を設定します。

```
[Device-radius-2000] key authentication simple abc
```

アカウンティングサーバとデバイス間でセキュアな通信を行うため、プレーンテキストで abc の共有鍵を設定します。

```
[Device-radius-2000] key accounting simple abc
```

RADIUS サーバに送信されたユーザ名から ISP ドメイン名を除外します。

```
[Device-radius-2000] user-name-format without-domain
[Device-radius-2000] quit
```

5)　ISP ドメインを設定します。

ISP ドメイン bbb を作成し、ISP domain view に移行します。

```
[Device] domain bbb
```

認証、許可、アカウンティング用の RADIUS スキーム 2000 を ISP ドメインに適用します。

```
[Device-isp-bbb] authentication lan-access radius-scheme 2000
[Device-isp-bbb] authorization lan-access radius-scheme 2000
[Device-isp-bbb] accounting lan-access radius-scheme 2000
[Device-isp-bbb] quit
```

6)　アクセス装置で 802.1X を設定します。

GigabitEthernet 1/0/2 で 802.1X を有効にします。

```
[Device] interface gigabitethernet 1/0/2
[Device-GigabitEthernet1/0/2] dot1x
```

ポートでポートベースのアクセス制御を行います。

```
[Device-GigabitEthernet1/0/2] dot1x port-method portbased
```

ポートの許可モードを auto に設定します。デフォルトでポートは auto モードを使用します。

```
[Device-GigabitEthernet1/0/2] dot1x port-control auto
```

GigabitEthernet 1/0/2 で 802.1X ゲスト VLAN として VLAN10 を設定します。

```
[Device-GigabitEthernet1/0/2] dot1x guest-vlan 10
[Device-GigabitEthernet1/0/2] quit
```

グローバルに 802.1X を有効にします。

```
[Device] dot1x
```

III. 設定の確認

GigabitEthernet 1/0/2 の 802.1X ゲスト VLAN の設定を確認します。

```
[Device] display dot1x interface gigabitethernet 1/0/2
```

ポートでユーザが認証にパスしないとき、GigabitEthernet 1/0/2 が VLAN10 に割り当てられていることを確認します。

```
[Device] display vlan 10
```

ユーザが認証にパスしたのち、GigabitEthernet 1/0/2 の情報を表示します。GigabitEthernet 1/0/2 が VLAN5 に割り当てられていることを確認します。

```
[Device] display interface gigabitethernet 1/0/2
```

3.26.3 ACL の割り当てによる 802.1X の設定例

I. ネットワーク要件

図 3-3に示すように、GigabitEthernet 1/0/1 に接続するホストはインタネットにアクセスするため、802.1X 認証にパスする必要があります。

GigabitEthernet 1/0/1 で 802.1X 認証を実行します。認証サーバと許可サーバとして 10.1.1.1 の RADIUS サーバを使用します。アカウンティングサーバとして 10.1.1.2 の RADIUS サーバを使用します。

平日の 8:00～18:00 までの営業時間中、FTP サーバに 802.1X ユーザのアクセスを拒否するため、GigabitEthernet 1/0/1 で ACL の割り当てを設定します。

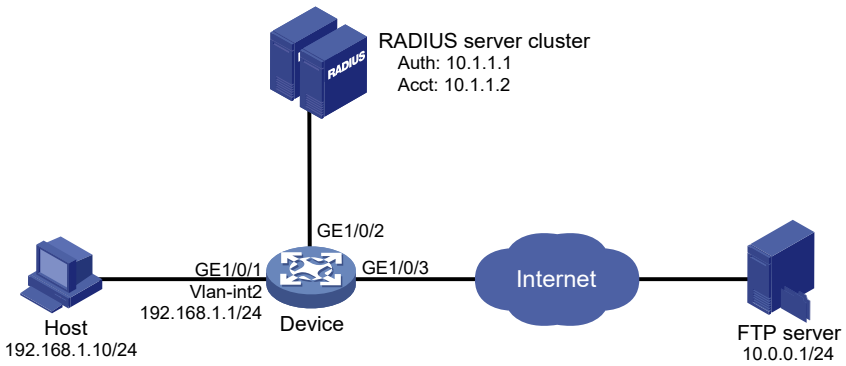


図 3-3 ネットワーク図

II. 設定手順

1) 802.1X クライアントを設定します。アクセスポートが 802.1X ゲスト VLAN あるいは許可 VLAN に割り当てられたのち、クライアントが IP アドレスをアップデートできることを確認してください。（詳細は省略します。）
2) 認証、許可、アカウンティングサービスを提供するため、RADIUS サーバを設定します。ユーザアカウントを追加し、ユーザに ACL（この例では ACL3000）を指定します。（詳細は省略します。）
3) 図 3-3に示すように、各インタフェースに IP アドレスを割り当てます。（詳細は省略します。）
4) RADIUS スキームを設定します。

RADIUS スキーム 2000 を作成し、RADIUS scheme view に移行します。

```
<Device> system-view
[Device] radius scheme 2000
```

プライマリ認証サーバとして 10.1.1.1 のサーバを指定し、認証ポートとして 1812 を指定します。

```
[Device-radius-2000] primary authentication 10.1.1.1 1812
```

プライマリアカウンティングサーバとして 10.1.1.2 のサーバを指定し、認証ポートとして 1813 を指定します。

```
[Device-radius-2000] primary accounting 10.1.1.2 1813
```

認証サーバとデバイス間でセキュアな通信を行うため、プレーンテキストで abc の共有鍵を設定します。

```
[Device-radius-2000] key authentication simple abc
```

アカウンティングサーバとデバイス間でセキュアな通信を行うため、プレーンテキストで abc の共有鍵を設定します。

```
[Device-radius-2000] key accounting simple abc
```

RADIUS サーバに送信されたユーザ名から ISP ドメイン名を除外します。

```
[Device-radius-2000] user-name-format without-domain
[Device-radius-2000] quit
```

5) ISP ドメインを設定します。

ISP ドメイン bbb を作成し、ISP domain view に移行します。

```
[Device] domain bbb
```

認証、許可、アカウンティング用の RADIUS スキーム 2000 を ISP ドメインに適用します。

```
[Device-isp-bbb] authentication lan-access radius-scheme 2000
[Device-isp-bbb] authorization lan-access radius-scheme 2000
[Device-isp-bbb] accounting lan-access radius-scheme 2000
[Device-isp-bbb] quit
```

6)　平日の 8:00～18:00 に時間範囲 ftp を設定します。

```
[Device] time-range ftp 8:00 to 18:00 working-day
```

7)　指定された時間範囲で、10.0.0.1 の FTP サーバ宛のパケットを拒否する ACL を設定します。

```
[Device] acl advanced 3000
[Device-acl-ipv4-adv-3000] rule 0 deny ip destination 10.0.0.1 0 time-range ftp
[Device-acl-ipv4-adv-3000] quit
```

8)　802.1X を設定します。

GigabitEthernet 1/0/1 で 802.1X を有効にします。

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] dot1x
[Device-GigabitEthernet1/0/1] quit
```

802.1X をグローバルで有効にします。

```
[Device] dot1x
```

III. 設定の確認

認証にパスするユーザアカウントを使用します。（詳細は省略します。）

平日の 8:00 から 18:00 の期間内に、ユーザが FTP サーバに ping できないことを確認します。

```
C:\>ping 10.0.0.1

Pinging 10.0.0.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.0.0.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

出力では、ACL 3000 がユーザに適用され、ユーザが FTP サーバにアクセスできないことを示します。

目次

このセクションのページは **9-x-x** です。

4 章 MAC アドレス認証 4-1
4.1 概要 4-1
4.1.1 ユーザアカウントポリシー 4-1
4.1.2 認証方式 4-1
4.1.3 VLAN の割り当て 4-2
4.1.4 ACL の割り当て 4-4
4.2 設定要件 4-4
4.3 設定ガイドライン 4-4
4.4 設定作業リスト 4-5
4.5 MAC アドレス認証の有効化 4-5
4.6 MAC アドレス認証ドメインの指定 4-5
4.7 ユーザアカウントフォーマットの設定 4-6
4.8 MAC アドレス認証タイマの設定 4-6
4.9 ポート上の MAC アドレス認証ユーザの同時接続最大数の設定 4-7
4.10 MAC アドレス認証の開始を遅らせる遅延時間の設定 4-7
4.11 定期的な MAC 再認証の設定 4-8
4.12 MAC アドレス認証と 802.1X 認証の並列処理の設定 4-8
4.12.1 設定ガイドライン 4-9
4.12.2 設定手順 4-9
4.13 MAC アドレス認証ゲスト VLAN の設定 4-10
4.14 MAC アドレス認証のオフライン状態検出の設定 4-11
4.15 MAC アドレス移動機能の有効化 4-11
4.16 未認証 MAC アドレス認証ユーザエージングの設定 4-11
4.17 MAC アドレス認証の表示と維持 4-12
4.18 MAC アドレス認証の設定例 4-13
4.18.1 ローカル MAC アドレス認証の設定例 4-13
4.18.2 RADIUS ベースの MAC アドレス認証の設定例 4-15
4.18.3 ACL の割り当ての設定例 4-17

4章 MAC アドレス認証

4.1 概要

MAC アドレス認証はポート上で送信元 MAC アドレスを認証することによって、ネットワークアクセスを制御します。

クライアントソフトウェアを必要とせず、ネットワークアクセス用のユーザ名とパスワードの入力も必要ありません。

MAC アドレス認証が有効になっているポート上で未知の送信元 MAC アドレスが検出された場合、装置は MAC アドレス認証プロセスを開始します。

- 認証が成功した場合、ユーザは許可されたネットワークリソースにアクセスすることができます。
- 認証が失敗した場合、装置はユーザの MAC アドレスをサイレント MAC アドレスとして登録し、パケットをドロップし、Quiet タイマを開始します。Quiet タイマは、サイレント MAC に登録された MAC アドレスからのすべての後続のパケットを破棄することで、短時間に何度も認証が行われることを回避します。

🕮 **メモ：**

認証に失敗した MAC アドレスがスタティック MAC アドレスまたは任意のセキュリティ認証をパスした MAC アドレスである場合、装置はその MAC アドレスをサイレントアドレスとして記憶しません。
QX-S5100G シリーズの MAC アドレス認証は CHAP での認証に対応していません。

4.1.1 ユーザアカウントポリシー

MAC アドレス認証は、以下のユーザアカウントポリシーをサポートしています。

- **各ユーザのための MAC ベースのユーザアカウント**－アクセス装置は、MAC アドレス認証するユーザのユーザ名とパスワードとして、パケットの送信元 MAC アドレスを使用します。このポリシーは、非セキュアな環境に適しています。
- **すべてのユーザのための共有のユーザアカウント**－アクセス装置上のすべての MAC アドレス認証ユーザのために、必ずしも MAC アドレスでないユーザ名とパスワードを指定します。このポリシーは、セキュアな環境に適しています。

4.1.2 認証方式

アクセス装置上（ローカル認証）または、RADIUS （Remote Authentication Dial-In User Service） サーバを介して、MAC アドレス認証を行うことができます。

ローカル認証：

- **MAC ベースアカウント**－アクセス装置は、一致するローカルアカウントデータベースを検索するためのユーザ名とパスワードとして、パケットの送信元 MAC アドレスを使用します。
- **共有アカウント**－アクセス装置は、一致するローカルアカウントデータベースを検索するために、共有アカウントのユーザ名とパスワードを使用します。

RADIUS 認証：

- **MAC ベースアカウント**－アクセス装置は、認証用の RADIUS サーバにユーザ名とパスワードとして送信元 MAC アドレスを送信します。
- **共有アカウント**－アクセス装置は、認証用の RADIUS サーバに共有アカウントのユーザ名とパスワードを送信します。

ローカル認証と RADIUS 認証の詳細は、オペレーションマニュアルのセクション 9 *セキュリティ”AAA”*を参照してください。

4.1.3 VLAN の割り当て

MAC アドレス認証は許可 VLAN、ゲスト VLAN をサポートします。

I. 許可 VLAN

MAC アドレス認証ユーザの許可されたネットワークリソースへのアクセスを制御するため、許可 VLAN を使用します。

- **Remote VLAN authorization**—MAC 認証ユーザの許可 VLAN 情報は、リモートサーバにより割り当てられます。装置は VLAN ID または VLAN 名でサーバ割り当て VLAN を解決できます。

  ユーザが装置にアクセスするポートは、タグ付きまたはタグなしメンバとして許可 VLAN に割り当てられます。

- **Local VLAN authorization**— MAC 認証ユーザの許可 VLAN は、装置の VLAN ID でユーザ view またはユーザグループ view で指定されます。

  ユーザが装置にアクセスするポートは、タグ付きメンバとして VLAN に割り当てられます。

  詳細は、オペレーションマニュアルのセクション 9 *セキュリティ”AAA”*を参照してください。

表 4-1 にネットワークアクセス装置が MAC アドレス認証ユーザの許可 VLAN を処理する方法を示します。

表 4-1 VLAN 操作

ポートタイプ	VLAN 操作
• アクセスポート • トランクポート • MACベースVLANが無効となったハイブリッドポート	• ポートがタグなしメンバとして許可VLANへ割り当てられた場合、装置は最初に認証されたユーザの許可VLANにポートを割り当てます。許可VLANはPVIDになります。ポートの全MAC認証ユーザは同じ許可VLANに割り当てられます。その後のユーザに異なる許可VLANが割り当てられる場合、ユーザはMAC認証に成功しません。 • ポートがタグ付きメンバとして許可VLANへ割り当てられた場合、ポートのPVIDは変わりません。装置はそれぞれのユーザのMACアドレスと許可VLANとをマッピングします。 🕮 **メモ：** アクセスポートはタグなしVLANメンバとしてのみ許可VLANに割り当てられます。
MACベースVLANが有効となったハイブリッドポート	装置は許可VLANに各ユーザのMACアドレスをマッピングします。ポートのPVIDは変更しません。ユーザがログオフすると、ユーザのMAC-to-VLANのマッピングは削除されます。

🕮 **メモ：**

タグなしメンバとしてハイブリッドポートを VLAN に割り当ててください。割り当てた後は、タグ付きメンバとしてポートを再設定しないでください。

II. ゲスト VLAN

ポートで MAC アドレス認証に失敗したユーザを適応させるため、ポートで MAC アドレス認証ゲスト VLAN を設定することができます。MAC アドレス認証ゲスト VLAN のユーザは、ソフトウェアやシステムパッチなどをダウンロードするため、ソフトウェアサーバのような制限されたネットワークリソースにアクセスすることができます。MAC アドレス認証ゲスト VLAN が設定されていない場合、MAC アドレス認証に失敗したユーザはネットワークリソースにアクセスすることができません。

ハイブリッドポートは、常に、タグなしメンバとして MAC アドレス認証ゲスト VLAN に割り当てられます。割り当て後、VLAN のタグづけメンバとしてポートを再設定しないでください。

表 4-2 にネットワークアクセス装置が MAC アドレス認証ユーザのゲスト VLAN を処理する方法を示します。

表 4-2 VLAN 操作

ポートタイプ	VLAN 操作
サーバに到達不能以外の理由でMACアドレス認証に失敗したMACアドレス認証ゲストVLANのユーザ	ユーザはMACアドレス認証ゲストVLANに属します。

ポートタイプ	VLAN 操作
MACアドレス認証にパスしたMACアドレス認証ゲストVLANのユーザ	装置はユーザのMACアドレスを認証ユーザによって割り当てられた許可VLANに再マッピングします。 ユーザ用の許可VLANが認証サーバで設定されていない場合、ユーザのMACアドレスをポートのPVIDに再マッピングします。

4.1.4 ACL の割り当て

ネットワークリソースへのアクセスを制御するため、MAC アドレス認証ユーザに ACL を指定することができます。ユーザが MAC アドレス認証にパスしたのち、認証サーバ（ローカルあるいはリモート）はユーザのアクセスポートに許可された ACL を割り当てます。ACL はユーザのトラフィックをフィルタします。ACL の割り当て機能のために、アクセス装置で許可 ACL の ACL を設定する必要があります。

ユーザのアクセス制御を変更するために、以下の方法の 1 つを使用することができます。

- アクセス装置の ACL ルールを修正します。
- 認証サーバで別の許可 ACL を指定します。

ACL の詳細は、オペレーションマニュアルのセクション 8 *ACL and QoS*”*ACL*”を参照してください。

4.2 設定要件

MAC アドレス認証を設定する前に、以下の作業を完了してください。

1) 認証ドメイン（ISP ドメイン）を設定し、AAA 方式を指定してください。詳細はオペレーションマニュアルのセクション 9 *セキュリティ*”*AAA*”を参照してください。
   - □ ローカル認証の場合、ローカルユーザアカウント（ユーザ名とパスワードを含みます。）を作成し、lan-access サービスを指定してください。
   - □ RADIUS 認証の場合、装置と RADIUS サーバ間のルートで通信ができることを確認し、RADIUS サーバにユーザアカウントを作成してください。MAC ベースアカウントを使用する場合、それぞれのアカウントのユーザ名とパスワードは MAC アドレス認証ユーザの MAC アドレスと同じにしてください。
2) ポートセキュリティが無効であることを確認してください。ポートセキュリティの詳細は、オペレーションマニュアルのセクション 9 *セキュリティ*”*ポートセキュリティ*”を参照してください。

4.3 設定ガイドライン

MAC 認証を設定する際には、以下の制限とガイドラインに従ってください。

- MAC 認証設定は、レイヤ 2 イーサネットインタフェースでのみサポートします。
- MAC 認証を有効にする前に、インタフェースがレイヤ 2 アグリゲーショングループに加わっていないことを確認してください。

4.4 設定作業リスト

作業リスト
（必須設定項目） MACアドレス認証の有効化
（オプション設定項目）MACアドレス認証ドメインの指定
（オプション設定項目）ユーザアカウントフォーマットの設定
（オプション設定項目）MACアドレス認証タイマの設定
（オプション設定項目）ポート上のMACアドレス認証ユーザの同時接続最大数の設定
（オプション設定項目）MACアドレス認証の開始を遅らせる遅延時間の設定
（オプション設定項目）定期的なMAC再認証の設定
（オプション設定項目）MACアドレス認証と802.1X認証の並列処理の設定
（オプション設定項目）MACアドレス認証ゲストVLANの設定
（オプション設定項目）MACアドレス認証のオフライン状態検出の設定
（オプション設定項目）MACアドレス移動機能の有効化
（オプション設定項目）未認証MACアドレス認証ユーザエージングの設定

4.5 MACアドレス認証の有効化

以下に MAC アドレス認証の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． グローバルで MAC アドレス認証を有効にする	**mac-authentication**	デフォルト：無効
3． Ethernet interface view に移行する	**interface** *interface-type interface-number*	―
4． ポートで MAC アドレス認証を有効にする	**mac-authentication**	デフォルト：無効

4.6 MACアドレス認証ドメインの指定

デフォルトでは、MAC アドレス認証ユーザはシステムデフォルト認証ドメイン内にあります。ユーザごとに異なるアクセスポリシーを適用するには、次の方法で MAC アドレス認証ユーザ用の認証ドメインを指定することができます。

- system view でグローバルの認証ドメインを指定します。このドメインの設定は、すべてのポートに適用されます。
- interface view で個別のポートの認証ドメインを指定します。

MAC アドレス認証は、インタフェース固有のドメイン、グローバルドメイン、デフォルトドメインの順序でポート上のユーザの認証ドメインを選択します。認証ドメインの詳細は、オペレーションマニュアルのセクション 9 *セキュリティ"AAA"*を参照してください。

以下に MAC アドレス認証ユーザの認証ドメインの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―

操作	コマンド	補足
2． MAC アドレス認証ユーザの認証ドメインを指定する	● system viewで設定する：**mac-authentication domain** *domain-name* ● Ethernet interface viewで設定する： 1． **interface** *interface-type interface-number* 2． **mac-authentication domain** *domain-name*	デフォルト：システムのデフォルト認証ドメインが使われます。

4.7 ユーザアカウントフォーマットの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． MAC アドレス認証ユーザアカウントフォーマットを設定する	● 各ユーザにMACベースユーザアカウントを使用する：**mac-authentication user-name-format mac-address** [{ **with-hyphen** | **without-hyphen** } [**lowercase** | **uppercase**]] ● すべてのユーザに共有ユーザアカウントを使用する：**mac-authentication user-name-format fixed** [**account** *name*] [**password** { **cipher** | **simple** } *string*]	デフォルト：MACアドレス認証のユーザ名とパスワードとしてユーザのMACアドレスを使用します。 MACアドレスは16進数でハイフンなし、小文字のみです。

4.8 MACアドレス認証タイマの設定

MAC アドレス認証では以下のタイマを使用します。

- **Offline detect timer**－ユーザがアイドル状態であることを検出するために、装置がユーザからのトラフィックを待つ期間を設定します。装置はタイマが終了するとユーザをログオフし、ユーザのアカウントの停止を要求します。このタイマは、MAC 認証オフライン検出機能が有効な場合にのみ効果があります。
- **Quiet timer**－MAC アドレス認証に失敗したユーザが MAC アドレス認証を実行できるようになるまで、装置が待つ時間をタイマに設定します。 Quiet タイムの間は、MAC アドレスからのパケットはすべて廃棄されます。この Quiet メカニズムは、認証が繰り返されシステムのパフォーマンスに影響を与えることを防ぎます。
- **Server timeout timer**－RADIUS サーバが使用不能であることを検出するために、アクセス装置が RADIUS サーバからの応答を待つ時間をタイマに設定します。MAC アドレス認証中にタイムアウトした場合、ユーザはネットワークにアクセスすることはできません。

以下に MAC アドレス認証タイマの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． MAC アドレス認証タイマを設定する	**mac-authentication timer** { **offline-detect** *offline-detect-value* | **quiet** *quiet-value* | **server-timeout** *server-timeout-value* }	デフォルト： offline detect timer：300秒 quiet timer：60秒 server timeout timer：100秒

4.9 ポート上のMACアドレス認証ユーザの同時接続最大数の設定

同時に接続する認証ユーザを制限することで、システムリソース不足になることを防ぎます。

以下にポート上の MAC アドレス認証ユーザの同時接続最大数の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． Ethernet interface view に移行する	**interface** *interface-type interface-number*	―
3． ポート上の MAC アドレス認証ユーザの同時接続最大数を設定する	**mac-authentication max-user** *user-number*	デフォルト：4294967295

🕮 **メモ：**

QX-S5100G シリーズは 2048 まで認証動作が可能です。

4.10 MACアドレス認証の開始を遅らせる遅延時間の設定

ポートで 802.1X 認証と MAC アドレス認証の両方の設定が有効である場合、802.1X 認証を優先させるため、MAC アドレス認証を開始する時間を遅らせます。

もし遅延時間内に、802.1X 認証が動作しないあるいは 802.1X 認証に失敗したとき、MAC アドレス認証を行います。

MAC アドレス認証の開始を遅らせる遅延時間を設定するとき、ポートセキュリティで **mac-else-userlogin-secure** あるいは **mac-else-userlogin-secure-ext** を設定しないでください。2 つのモードのどちらかでは遅延時間の設定は動作しません。ポートセキュリティの詳細は、オペレーションマニュアルのセクション 9 *セキュリティ”ポートセキュリティ”*を参照してください。

以下に MAC アドレス認証の開始を遅らせる遅延時間の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． Ethernet interface view に移行する	**interface** *interface-type interface-number*	―

操作	コマンド	補足
3． MAC アドレス認証の開始を遅らせる遅延時間を有効にし、タイマを設定する	**mac-authentication timer auth-delay** *auth-delay time*	デフォルト：無効

4.11 定期的なMAC再認証の設定

I. 制限とガイドライン

装置は、MAC 再認証用の定期的な再認証タイマを次の順序で選択します。

1) サーバ割り当て再認証タイマ
2) ポート固有の再認証タイマ
3) グローバル再認証タイマ
4) デフォルトの再認証タイマ

MAC 認証ドメインまたはユーザアカウント形式の設定を変更しても、オンライン MAC 認証ユーザの再認証には影響しません。変更した設定は、変更後にオンラインになった MAC 認証ユーザにのみ有効です。

II. 設定手順

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． 定期的な MAC 再認証タイマを設定する	• グローバル定期再認証タイマを設定する **mac-authentication timer reauth-period** *reauth-period-value* • ポート固有の定期的な再認証タイマを設定するには、次のコマンドを順番に実行する **interface** *interface-type interface-number* **mac-authentication timer reauth-period** *reauth-period-value* **quit**	（グローバル） デフォルト：3600秒 （ポート固有） デフォルト：設定なし ポートは、グローバルな定期的MAC再認証タイマを使用します。
3． interface view に移行する	**interface** *interface-type interface-number*	―
4． 定期的な MAC 再認証を有効にする	**mac-authentication re-authenticate**	デフォルト：無効

4.12 MACアドレス認証と802.1X認証の並列処理の設定

本機能は、802.1X 認証が完了したあとに MAC 認証を処理するポートで、MAC アドレス認証と 802.1X 認証を並列に処理できるようにします。

ポートがアンノウン MAC アドレスからのパケットを受信すると、ユニキャスト EAP-Request/Identity パケットを MAC アドレス宛てに送信します。その後、ポートは 802.1X 認証の結果を待つことなく MAC アドレス認証をただちに処理します。

MAC アドレス認証が成功した後、ポートは MAC 認証許可 VLAN に割り当てられます。

- 802.1X 認証が失敗した場合、MAC アドレス認証の結果が効果を生じます。
- 802.1X 認証が成功した場合、装置は 802.1X 認証の結果をもとにポートと MAC アドレスを処理します。

4.12.1 設定ガイドライン

ポートで MAC アドレス認証と 802.1X 認証の並列処理を有効にする場合、以下の制限とガイドラインに従ってください。

- ポートが以下の要件に対応していることを確認してください。
  - ポートは 802.1X 認証と MAC アドレス認証の両方が設定されており、また 802.1X 認証のための MAC ベースアクセス制御を実行している。
  - ポートは 802.1X ユニキャストトリガ機能を有効にしている。
- 802.1X ゲスト VLAN に割り当てられる前の MAC 認証を実行するポートには、新しい MAC アドレスによる 802.1X ゲスト VLAN へのポートの割り当て遅延を有効にしてください。

  新しい MAC アドレスによる 802.1X ゲスト VLAN へのポートの割り当て遅延の設定の詳細は、オペレーションマニュアルのセクション 9 *セキュリティ”802.1X”*を参照してください。
- 並列処理機能を正しく動作させるためには、ポートに MAC アドレス認証遅延を有効にしないでください。この操作は、802.1X 認証が引き起こされた後の MAC アドレス認証を遅延させます。
- 802.1X 認証と MAC アドレス認証の両方をポートに設定するには、以下のいずれかの方法を用います。
  - ポートに 802.1X 認証と MAC アドレス認証の機能を別々に有効にします。
  - ポートのセキュリティを有効にします。ポートセキュリティモードは **userlogin-secure-or-mac** または **userlogin-secure-or-mac-ext** にしなければなりません。

  ポートセキュリティモードの設定の詳細は、オペレーションマニュアルのセクション 9 *セキュリティ”ポートセキュリティ”*を参照してください。

4.12.2 設定手順

以下に MAC アドレス認証と 802.1X 認証の並列処理を有効にする設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Ethernet interface view に移行する	**interface** *interface-type interface-number*	―
3. MAC アドレス認証と 802.1X 認証の並列処理の有効に設定する	**mac-authentication parallel-with-dot1x**	デフォルト：有効

4.13 MACアドレス認証ゲストVLANの設定

MAC アドレス認証ゲスト VLAN を使用する場合、ハイブリッドポートを設定する必要があります。ハイブリッドポートで MAC アドレス認証ゲスト VLAN を設定する前に、以下の作業を完了してください。

- グローバルおよびポートで MAC アドレス認証を有効にします。
- ポートで MAC ベース VLAN を有効にします。
- MAC アドレス認証ゲスト VLAN として指定される VLAN を作成します。
- ポートでタグなしメンバとして VLAN を設定します。

表 4-3 にポートで MAC アドレス認証ゲスト VLAN を設定するときのガイドラインを示します。

表 4-3 MAC アドレス認証ゲスト VLAN と他のセキュリティ機能との関係

機能	関係	補足
MACアドレス認証のQuiet機能	MACアドレス認証ゲスト VLAN機能は優先順位が高くなります。 ユーザがMACアドレス認証に失敗したとき、ゲスト VLANにアクセスできます。 ユーザのMACアドレスはサイレントMACアドレスとして記憶されません。	オペレーションマニュアルのセクション9 *セキュリティ”MACアドレス認証”* を参照してください。
ポート侵入防止機能	ゲストVLAN機能は、ブロックMAC動作よりも優先順位が高く、ポート侵入防止機能のシャットダウン動作よりも優先順位が低くなります。	オペレーションマニュアルのセクション9 *セキュリティ”ポートセキュリティ”* を参照してください。

以下に MAC アドレス認証ゲスト VLAN の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． Ethernet interface view に移行する	**interface** *interface-type interface-number*	―
3． ポートで MAC アドレス認証ゲスト VLAN を指定する	**mac-authentication guest-vlan** *guest-vlan-id*	デフォルト：設定なし 1つのポートに1つのMACアドレス認証ゲストVLANのみ設定することができます。
4． （オプション設定項目） MAC アドレス認証ゲスト VLAN のユーザを認証する間隔を設定する	**mac-authentication guest-vlan auth-period** *period-value*	デフォルト：30秒

4.14 MACアドレス認証のオフライン状態検出の設定

offline detect timer の期間内にユーザからパケットを受信しない場合、この機能はユーザを装置からログオフします。装置は同時にユーザにアカウンティングの停止を要求します。オフライン検出機能の設定の詳細は、オペレーションマニュアルのセクション 9 *セキュリティ "MAC アドレス認証"の"MAC アドレス認証タイマの設定"*を参照してください。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． Ethernet interface view に移行する	**interface** *interface-type interface-number*	―
3． MAC アドレス認証オフライン検出機能を有効に設定する	**mac-authentication offline-detect enable**	デフォルト：有効

4.15 MACアドレス移動機能の有効化

MAC アドレス移動機能を有効にすることで、認証が許可されたユーザが装置のポートを移動できるようになります。たとえば、認証ユーザが別のポートに移動する場合、認証セッションが最初のポートから削除され、新しいポートで再認証されます。

もし、MAC アドレス移動機能が無効で認証ユーザが別のポートに移動した場合、再認証されません。

（ローカルまたはリモートの）認証サーバのオンラインユーザ数が上限に達した場合、認証ユーザは装置上のポート間で移動はできません。

ポートのローミングを行うワイヤレスユーザがネットワークにアクセスできるように MAC アドレス移動機能を有効にすることを推奨します。

以下に MAC アドレス移動機能の有効化の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． MAC アドレス移動機能を有効にする	**port-security mac-move permit**	デフォルト：有効

4.16 未認証MACアドレス認証ユーザエージングの設定

I. 未認証 MAC アドレス認証ユーザエージング

未認証 MAC アドレス認証ユーザエージングは、認証に失敗したために MAC アドレス認証ゲストに追加されたユーザに適用されます。

これらの VLAN のいずれかのユーザがエージングアウトすると、装置は VLAN からユーザを削除し、アクセスポートからユーザのエントリアドレスを削除します。

1 つのポートでこれらの VLAN のいずれかのユーザが正常に認証され、別のポートでオンラインになるには、この機能を有効にします。それ以外の場合は、この機能を無効にすることをお勧めします。

II. 制限とガイドライン

あるポートで未認証ユーザを認証して別のポートでオンラインにする必要がない限り、ベストプラクティスとして、あるポートで未認証 MAC アドレス認証ユーザエージングを無効にします。

III. 設定手順

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． MAC アドレス認証 VLAN のタイプにユーザエージングタイマを設定する	**mac-authentication timer user-aging guest-vlan** *aging-time-value*	デフォルト：ユーザエージングタイマは、すべての適用可能なタイプのMACアドレス認証VLANに対して1000秒です。
3． interface view に移行する	**interface** *interface-type interface-number*	―
4． 未認証 MAC アドレス認証ユーザエージングを有効にする	**mac-authentication unauthenticated-user aging enable**	デフォルト：有効

4.17 MACアドレス認証の表示と維持

display コマンドはすべての view で、**reset** コマンドは user view で使用できます。

操作	コマンド
MACアドレス認証情報を表示する	**display mac-authentication** [**interface** *interface-type interface-number*]
MACアドレス認証接続を表示する	**display mac-authentication connection** [**interface** *interface-type interface-number* | **slot** *slot-number* | **user-mac** *mac- address* | **user-name** *user-name*]
MACアドレス認証の統計情報を削除する	**reset mac-authentication statistics** [**interface** *interface-type interface-number*]
ポートのMACアドレス認証ゲストVLANからユーザを取り除く	**reset mac-authentication guest-vlan interface** *interface-type interface-number* [**mac-address** *mac-address*]

4.18 MACアドレス認証の設定例

4.18.1 ローカル MAC アドレス認証の設定例

I. ネットワーク要件

図 4-1 に示すように、ユーザのインターネットアクセスを制御するためにポート GigabitEthernet 1/0/1 でローカル MAC アドレス認証を設定します。

以下の要件に従うように装置を設定します。

- ユーザが 180 秒ごとにオフラインになっているかどうかを検出します。
- ユーザが認証に失敗した場合、180 秒間、ユーザを拒否します。
- すべてのユーザは ISP ドメイン bbb に属します。
- ローカルユーザは、MAC アドレス認証のユーザ名とパスワードとして、ユーザ自身の MAC アドレスを使用します。MAC アドレスは 16 進数でハイフン付き、小文字を使用します。

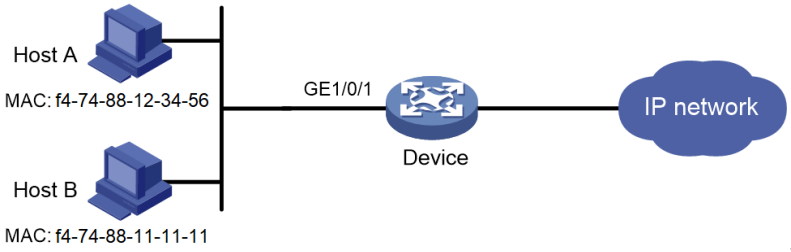


図 4-1 ネットワーク図

II. 設定手順

ローカルユーザを追加します。この例ではホストの MAC アドレス f4-74-8812-34-56 をユーザ名とパスワードに設定し、LAN アクセスサービスを有効にします。

```
<Device> system-view
[Device] local-user f4-74-88-12-34-56 class network
[Device-luser-network-f4-74-88-12-34-56] password simple f4-74-88-12-34-56
```

ユーザの LAN アクセスサービスを指定します。

```
[Device-luser-network-f4-74-88-12-34-56] service-type lan-access
[Device-luser-network-f4-74-88-12-34-56] quit
```

LAN ユーザのローカル認証を実行するため、ISP ドメイン bbb を設定します。

```
[Device] domain bbb
[Device-isp-bbb] authentication lan-access local
[Device-isp-bbb] quit
```

GigabitEthernet 1/0/1 で MAC アドレス認証を有効にします。

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] mac-authentication
[Device-GigabitEthernet1/0/1] quit
```

ISP ドメイン bbb として MAC アドレス認証ドメインを指定します。

```
[Device] mac-authentication domain bbb
```

MAC アドレス認証タイマを設定します。

```
[Device] mac-authentication timer offline-detect 180
[Device] mac-authentication timer quiet 180
```

MAC ベースのアカウントを使うよう MAC アドレス認証を設定します。MAC アドレスのユーザ名とパスワードはハイフンありで、小文字です。

```
[Device] mac-authentication user-name-format mac-address with-hyphen lowercase
```

MAC アドレス認証をグローバルで有効にします。

```
[Device] mac-authentication
```

III. 設定の確認

MAC アドレス認証の設定と統計情報を表示します。

```
[Device] display mac-authentication
Global MAC authentication parameters:
   MAC authentication     : Enabled
   User name format       : MAC address in lowercase(xx-xx-xx-xx-xx-xx)
            Username      : mac
            Password      : Not configured
   Offline detect period  : 180 s
   Quiet period           : 180 s
   Server timeout         : 100 s
   Authentication domain  : bbb
 Online MAC-auth users    : 1

 Silent MAC users:
          MAC address       VLAN ID  From port               Port index
          f474-8811-1111    8       GigabitEthernet1/0/1      1

 GigabitEthernet1/0/1  is link-up
   MAC authentication         : Enabled
   Carry User-IP              : Disabled
   Authentication domain      : Not configured
   Auth-delay timer           : Disabled
   Periodic reauth            : Disabled
   Re-auth server-unreachable : Logoff
   Guest VLAN                 : Not configured
   Guest VLAN auth-period     : 30 s
   Critical VLAN              : Not configured
   Critical voice VLAN        : Disabled
   Host mode                  : Single VLAN
   Offline detection          : Enabled
   Authentication order       : Default
   Guest VSI                  : Not configured
   Guest VSI auth-period      : 30 s
   Critical VSI               : Not configured
   Max online users           : 4294967295
   Authentication attempts    : successful 1, failed 0
```

```
    Current online users        : 1
           MAC address        Auth state
           f474-8812-3456    Authenticated
```

出力では、Host A が MAC アドレス認証にパスし、オンラインになっています。Host B は MAC アドレス認証に失敗し、サイレント MAC アドレスとして MAC アドレスが記録されます。

4.18.2 RADIUS ベースの MAC アドレス認証の設定例

I. ネットワーク要件

図 4-2 に示すように、装置はユーザの認証、許可、アカウンティングを実行するため、RADIUS サーバを使用します。

MAC アドレス認証によってインタネットにアクセスするユーザを制御するため、以下の作業を実行します。

- グローバルと GigabitEthernet 1/0/1 で MAC アドレス認証を有効にします。
- ユーザが 180 秒ごとにオフラインになっているかどうかを検出します。
- ユーザが認証に失敗した場合、装置は 180 秒間ユーザを拒否します。
- すべてのユーザは ISP ドメイン bbb に属します。
- すべてのユーザは、ユーザ名 aaa、パスワード 123456 の共有ユーザアカウントを使用します。

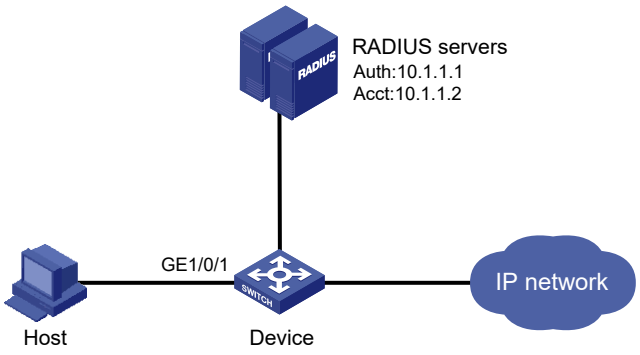


図 4-2 ネットワーク図

II. 設定手順

1) RADIUS サーバとアクセス装置で互いに通信できることを確認してください。（詳細は省略します。）
2) RADIUS サーバを設定します。

MAC アドレス認証ユーザの共有アカウントを作成します。（詳細は省略します。）

アカウントにユーザ名 aaa、パスワード 123456 を設定します。（詳細は省略します。）

3) 装置上で RADIUS ベースの MAC アドレス認証を設定します。

RADIUS スキームを設定します。

```
<Device> system-view
[Device] radius scheme 2000
[Device-radius-2000] primary authentication 10.1.1.1 1812
[Device-radius-2000] primary accounting 10.1.1.2 1813
[Device-radius-2000] key authentication simple abc
[Device-radius-2000] key accounting simple abc
[Device-radius-2000] user-name-format without-domain
[Device-radius-2000] quit
```

認証、許可、アカウンティング用の ISP ドメイン bbb の RADIUS スキームを適用します。

```
[Device] domain bbb
[Device-isp-bbb] authentication default radius-scheme 2000
[Device-isp-bbb] authorization default radius-scheme 2000
[Device-isp-bbb] accounting default radius-scheme 2000
[Device-isp-bbb] quit
```

GigabitEthernet 1/0/1 で MAC アドレス認証を有効にします。

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] mac-authentication
[Device-GigabitEthernet1/0/1] quit
```

ISP ドメイン bbb として MAC アドレス認証ドメインを指定します。

```
[Device] mac-authentication domain bbb
```

MAC アドレス認証タイマを設定します。

```
[Device] mac-authentication timer offline-detect 180
[Device] mac-authentication timer quiet 180
```

MAC アドレス認証のユーザによって共有されるアカウントのユーザ名 aaa とパスワード 123456 を指定します。

```
[Device] mac-authentication user-name-format fixed account aaa password simple 123456
```

MAC アドレス認証をグローバルで有効にします。

```
[Device] mac-authentication
```

III. 設定の確認

MAC アドレス認証の設定を表示します。

```
[Device] display mac-authentication
```

```
Global MAC authentication parameters:
   MAC authentication     : Enabled
   Username format        : Fixed account
           Username       : aaa
           Password       : ******
   Offline detect period  : 180 s
   Quiet period           : 180 s
   Server timeout         : 100 s
   Reauth period          : 3600 s
   Authentication domain  : bbb
 Max MAC-auth users       : 2048 per slot
 Online MAC-auth wired users    : 1

 Silent MAC users:
          MAC address       VLAN ID  From port               Port index

 GigabitEthernet1/0/1  is link-up
   MAC authentication         : Enabled
   Carry User-IP              : Disabled
   Authentication domain      : Not configured
   Auth-delay timer           : Disabled
   Periodic reauth            : Disabled
   Re-auth server-unreachable : Logoff
   Guest VLAN                 : Not configured
   Guest VLAN auth-period     : 30 s
   Critical VLAN              : Not configured
   Critical voice VLAN        : Disabled
   Host mode                  : Single VLAN
   Offline detection          : Enabled
   Authentication order       : Default
   Guest VSI                  : Not configured
   Guest VSI auth-period      : 30 s
   Critical VSI               : Not configured
   Max online users           : 4294967295
   Authentication attempts    : successful 1, failed 0
   Current online users       : 1
          MAC address       Auth state
          f474-8812-3456   Authenticated
```

4.18.3 ACL の割り当ての設定例

I. ネットワーク要件

図 4-3 に示すように、以下の要件に従うように装置を設定します。

- ユーザの認証、許可、アカウンティングを実行する RADIUS サーバを使用します。
- インターネットアクセスを制御するため、GigabitEthernet 1/0/1 で MAC アドレス認証を実行します。
- MAC アドレス認証ユーザの MAC ベースユーザアカウントを使用します。各 MAC アドレスは 16 進数でハイフンあり、小文字を使用します。
- FTP サーバ 10.0.0.1 にアクセスする認証ユーザを拒否するように ACL を設定します。

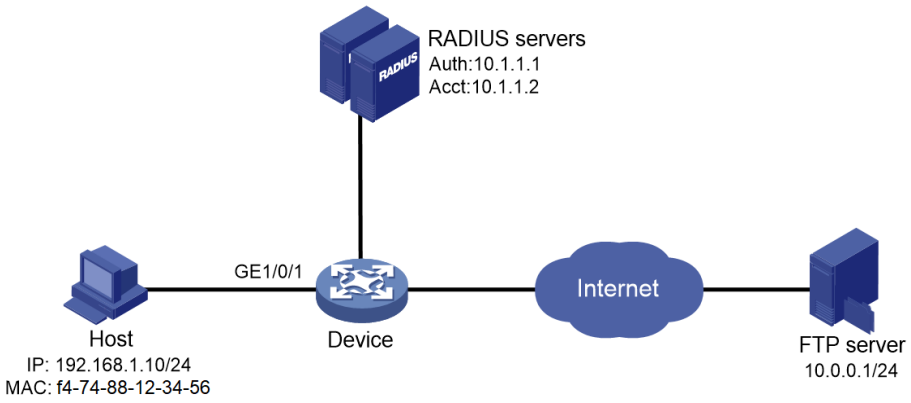


図 4-3 ネットワーク図

II. 設定手順

RADIUS サーバとアクセス装置が互いに通信できることを確認してください。

1)　10.0.0.1 へのパケットを拒否するように ACL 3000 を設定します。

```
<Switch> system-view
[Switch] acl advanced 3000
[Switch-acl-ipv4-adv-3000] rule 0 deny ip destination 10.0.0.1 0
[Switch-acl- ipv4-adv-3000] quit
```

2)　装置で RADIUS ベース MAC アドレス認証を設定します。

RADIUS スキームを設定します。

```
[Switch] radius scheme 2000
[Switch-radius-2000] primary authentication 10.1.1.1 1812
[Switch-radius-2000] primary accounting 10.1.1.2 1813
[Switch-radius-2000] key authentication simple abc
[Switch-radius-2000] key accounting simple abc
[Switch-radius-2000] user-name-format without-domain
[Switch-radius-2000] quit
```

認証、許可、アカウンティングの RADIUS スキームを ISP ドメインに適用します。

```
[Switch] domain bbb
[Switch-isp-bbb] authentication default radius-scheme 2000
[Switch-isp-bbb] authorization default radius-scheme 2000
[Switch-isp-bbb] accounting default radius-scheme 2000
[Switch-isp-bbb] quit
```

MAC アドレス認証の ISP ドメインを指定します。

```
[Switch] mac-authentication domain bbb
```

MAC ベースユーザアカウントを使用するために装置を設定します。各 MAC アドレスは 16 進数でハイフンあり、小文字を使用します。

```
[Switch] mac-authentication user-name-format mac-address with-hyphen lowercase
```

GigabitEthernet 1/0/1 で MAC アドレス認証を有効にします。

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] mac-authentication
[Switch-GigabitEthernet1/0/1] quit
```

MAC アドレス認証をグローバルで有効にします。

```
[Switch] mac-authentication
```

3)　RADIUS サーバを設定します。

各 RADIUS サーバでユーザ名とパスワードが f4-74-88-12-34-56 のユーザアカウントを追加します。（詳細は省略します。）

ユーザアカウントに ACL 3000 を許可します。（詳細は省略します。）

III. 設定の確認

MAC アドレス認証の設定を確認します。

```
[Switch] display mac-authentication
Global MAC authentication parameters:
   MAC authentication     : Enabled
   Username format        : MAC address in lowercase(xx-xx-xx-xx-xx-xx)
            Username      : mac
            Password      : Not configured
   Offline detect period  : 300 s
   Quiet period           : 60 s
   Server timeout         : 100 s
   Reauth period          : 3600 s
   Authentication domain  : bbb
 Online MAC-auth wired users    : 1

 Silent MAC users:
          MAC address       VLAN ID  From port               Port index

 GigabitEthernet1/0/1  is link-up
   MAC authentication         : Enabled
   Carry User-IP              : Disabled
   Authentication domain      : Not configured
   Auth-delay timer           : Disabled
   Periodic reauth            : Disabled
   Re-auth server-unreachable : Logoff
   Guest VLAN                 : Not configured
   Guest VLAN auth-period     : 30 s
   Critical VLAN              : Not configured
   Critical voice VLAN        : Disabled
   Host mode                  : Single VLAN
   Offline detection          : Enabled
   Authentication order       : Default
   Guest VSI                  : Not configured
   Guest VSI auth-period      : 30 s
   Critical VSI               : Not configured
   Max online users           : 4294967295
```

```
   Authentication attempts    : successful 1, failed 0
   Current online users       : 1
          MAC address       Auth state
          f474-8812-3456    Authenticated
```

Host から FTP サーバへの ping ができないことを確認します。

```
C:\>ping 10.0.0.1

Pinging 10.0.0.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.0.0.1:
   Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

出力は、FTP サーバにアクセスを拒否するため、ACL 3000 が GigabitEthernet 1/0/1 に割り当てられていることを示します。

目次

このセクションのページは **9-x-x** です。

5 章 Web 認証 5-1

5章 Web 認証

Web 認証設定に関するコンフィグについては、別紙の共通マニュアル”*QX シリーズ Ethernet スイッチ Web 認証オペレーションマニュアル（V7）*”の“*WebAuth*”を参照してください。

目次

このセクションのページは **9-x-x** です。

6 章 トリプル認証 6-1

6章 トリプル認証

トリプル認証設定に関するコンフィグについては、別紙の共通マニュアル”*QX シリーズ Ethernet スイッチ Web 認証オペレーションマニュアル（V7）*”の“*トリプル認証*”を参照してください。

目次

このセクションのページは**9-x-x** です。

7章 ポートセキュリティ 7-1
7.1 概要 7-1
7.1.1 ポートセキュリティの機能 7-1
7.1.2 ポートセキュリティのモード 7-2
7.2 設定ガイドライン 7-5
7.3 設定作業リスト 7-5
7.3.1 ポートセキュリティの有効化 7-6
7.4 ポートでのセキュアMACアドレスの最大数の設定 7-6
7.5 ポートセキュリティモードの設定 7-7
7.6 ポートセキュリティ機能の設定 7-8
7.6.1 NTKの設定 7-8
7.6.2 侵入防止の設定 7-9
7.7 セキュアMACアドレスの設定 7-9
7.7.1 設定要件 7-10
7.7.2 設定手順 7-10
7.8 サーバからの許可情報の無視 7-11
7.9 MACアドレス移動機能の有効化 7-11
7.10 ポートセキュリティに関するSNMP notification 7-12
7.11 ポートセキュリティユーザのロギングの有効化 7-12
7.12 ポートでの認証方式のトリガー順序の設定 7-13
7.13 ポートセキュリティの表示と維持 7-14
7.14 ポートセキュリティの設定例 7-14
7.14.1 autoLearnモードの設定例 7-14
7.14.2 userLoginWithOUIモードの設定例 7-16
7.14.3 macAddressElseUserLoginSecureモードの設定例 7-19
7.15 ポートセキュリティのトラブルシューティング 7-23
7.15.1 ポートセキュリティのモードが設定できない 7-23
7.15.2 セキュアMACアドレスが設定できない 7-23

7章 ポートセキュリティ

7.1 概要

ポートセキュリティは、MAC アドレスベースのネットワークアクセス制御を提供するため、802.1X 認証と MAC アドレス認証の拡張機能を組み合わせた機能です。WLAN のような、ポート上でユーザごとに異なる認証方式を必要とするネットワークに適用されます。

ポートセキュリティは、以下の機能を提供します。

- 受信トラフィックの送信元 MAC アドレスをチェックすることによるネットワークへの非認証端末のアクセスを防止します。
- 送信トラフィックの宛先 MAC アドレスをチェックすることによる非許可の装置あるいは端末へのアクセスを防止します。
- ポートが信頼できる MAC アドレスのみを学習するようにするために、ポート上で MAC アドレス学習と認証を制御することができます。

フレームの送信元 MAC アドレスがポートセキュリティモードで学習できない場合、または、802.1X または MAC アドレス認証に失敗したクライアントからのフレームの場合、それは不正なフレームです。不正なフレームを検知した場合、ポートセキュリティ機能は、自動的にあらかじめ定義した処理を実行します。これにより、メンテナンスの作業負担を減らし、システムセキュリティを大幅に強化することができます。

🕮 **メモ：**

アクセス制御に 802.1X 認証または、MAC アドレス認証のどちらか一方のみが必要な場合、ポートセキュリティではなく 802.1X 認証、または MAC アドレス認証のみ設定することを推奨します。802.1X と MAC アドレス認証についての詳細は、オペレーションマニュアルのセクション 9 *セキュリティ”802.1X”、”MAC アドレス認証”*を参照してください。

7.1.1 ポートセキュリティの機能

I. NTK

NTK （Need To Know） 機能は、出力フレームの宛先 MAC アドレスをチェックすることでトラフィックの傍受を防ぎます。この機能は以下のホストにのみフレームを送信することを保証します。

- 認証をパスしたホスト
- MAC アドレスが学習されている、あるいはアクセス装置で設定されたホスト

II. 侵入防止

侵入防止機能は、受信フレームの送信元 MAC アドレスをチェックし、不正フレームを検知すると、あらかじめ定義されたアクションを実行します。処理には、一時的/永久的に

ポートを切断する、または、3 分間（変更不可）その MAC アドレスからのフレームをブロックするといった処理があります。

7.1.2 ポートセキュリティのモード

ポートセキュリティモードには以下のタイプがあります。

- **MAC アドレス学習制御** － autoLearn と secure の 2 つのモードがあります。autoLearn は MAC アドレス学習が許可され、secure モードは無効にされます。
- **認証制御** － このタイプのセキュリティモードは、MAC アドレス認証、802.1X 認証、あるいはそれらを組み合わせて認証を実行します。

フレームを受信すると、セキュリティモードのポートは MAC アドレステーブルから送信元 MAC アドレスを検索します。一致する MAC アドレスがある場合、ポートはフレームを転送します。一致しない場合、セキュリティモードに従い、MAC アドレスの学習あるいは認証動作を行います。不正なフレームを受信すると、ポートはあらかじめ設定しておいた NTK や侵入防止機能の実行を行います。NTK 機能が動作しない限り、出力フレームは、ポートセキュリティの NTK アクションによって制限されません。

ポートがサポートするユーザの最大数は、以下の値よりも少ない値になります。

- ポートセキュリティが許可するセキュア MAC アドレスの最大数
- セキュリティモードがサポートする認証ユーザの同時接続最大数

たとえば 802.1X が許可する同時接続ユーザは、userLoginSecureExt モードのポートで MAC アドレス数のポートセキュリティの制限よりも大きいです。そのポートではポートセキュリティの制限が適用されます。

表 7-1にポートセキュリティモードとセキュリティ機能について記載します。

表 7-1 ポートセキュリティモード

目的	セキュリティモード		起動される機能
ポートセキュリティ機能の削除	noRestrictions （デフォルトモード） ポートセキュリティは無効です。また、ポートへのアクセス制限はありません。		―
MACアドレス学習の制御	autoLearn		NTK/侵入防止機能
	secure		
802.1X認証の実行	userLogin		―
	userLoginSecure		NTK/侵入防止機能
	userLoginSecureExt		
	userLoginWithOUI		
MACアドレス認証の実行	macAddressWithRadius		NTK/侵入防止機能
MACアドレス認証と802.1X認証の組み合わせの実行	Or	macAddressOrUserLoginSecure	NTK/侵入防止機能
		macAddressOrUserLoginSecureExt	
	Else	macAddressElseUserLoginSecure	
		macAddressElseUserLoginSecureExt	
	And	MacAddressAndUserLoginSecureExt	

🕮 **ポイント：**

- **userLogin** は 802.1X 認証とポートベースのアクセス制御を指定します。**Secure** の **userLogin** は 802.1X 認証と MAC ベースアクセス制御を指定します。**Ext** は複数の 802.1X 認証ユーザが認証し、同時にオンライン状態になることを許可します。**Ext** がないセキュリティモードの場合、1 つの 802.1X 認証ユーザのみオンライン状態になることを許可します。
- **macAddress** は MAC アドレス認証を指定します。
- **Else** は、**Else** の文字列の前にある認証方法が最初に実行されることを指します。たとえば、macAddressElseUserLoginSecure の **Else** の文字列の前にある認証方法は macAddress で、**Else** の文字列の後ろにある認証方法は UserLoginSecure です。最初の認証に失敗した場合、認証リクエストのプロトコルタイプに依存して、**Else** の後ろにある文字列の認証方法に変更するかどうかを判断します。
- **Or** は、**Or** の文字列の後ろにある認証方法が最初に実行されることを指します。認証が失敗した場合、**Or** の前の認証方式が適用されます。
- **And** は、**And** の文字列の前にある認証方法が最初に実行されることを指します。認証が成功した場合、次に **And** の後ろにある文字列の認証方式が適用されます。

I. MAC アドレス学習の制御

- autoLearn

  この autoLearn モードのポートは MAC アドレスを学習できます。自動的に学習された MAC アドレスはダイナミックアドレスとして MAC アドレステーブルに追加されませんが、セキュアな MAC アドレスとしてセキュア MAC アドレステーブルに追加されます。**port-security mac-address security** コマンドによってセキュア MAC アドレスを設定することもできます。

  autoLearn モードのポートは、以下の MAC アドレスからの送信元のフレームを許可します。

  - □ セキュア MAC アドレス
  - □ **mac-address dynamic** コマンドと **mac-address static** コマンドで設定された MAC アドレス

  セキュア MAC アドレスの数が上限に達すると、ポートは secure モードに移行します。

- secure

  secure モードでは、ポート上の MAC アドレス学習は無効です。**mac-address static** コマンドと **mac-address dynamic** コマンドを使用して MAC アドレスを設定することができます。MAC アドレステーブルエントリの設定についての詳細は、オペレーションマニュアルのセクション 3 *アクセス”MAC アドレステーブル”*を参照してください。

  secure モードのポートは以下の MAC アドレスからの送信元のフレームのみ許可します。

  - □ セキュア MAC アドレス
  - □ **mac-address dynamic** コマンドと **mac-address static** コマンドで設定された MAC アドレス

II. 802.1X 認証の実行

- userLogin

この userLogin モードのポートは、802.1X 認証を実行し、ポートベースのアクセス制御を実装しています。ポートは複数の 802.1X ユーザを処理できます。一度 802.1X ユーザが認証を通過すると、後続の 802.1X ユーザは認証なしでネットワークにアクセスできます。

- userLoginSecure

  この userLoginSecure モードのポートは、802.1X 認証を実行し、MAC ベースのアクセス制御を実装しています。ポートは、802.1X 認証をパスする 1 ユーザのみを処理します。

- userLoginSecureExt

  この userLoginSecureExt モードは、複数のオンライン 802.1X ユーザをサポートしていることを除いて、userLoginSecure モードと同じです。

- userLoginWithOUI

  この userLoginWithOUI モードは、userLoginSecure モードに似ています。違いは、このモードのポートが、特定の OUI（organizationally unique identifier）を含む MAC アドレスの 1 ユーザからのフレームを許可することです。

  このモードでは、ポートは OUI のチェックを最初に実行します。もし OUI のチェックに失敗した場合、ポートは 802.1X 認証を実行します。ポートは OUI のチェックあるいは 802.1X 認証にパスしたフレームを許可します。

🕮 **メモ：**

IEEE で定義によって定義される OUI は、装置ベンダ、メーカー、組織を識別する MAC アドレスの最初の 24 ビットです。MAC アドレスの最初の 3 オクテットは OUI です。

III. アドレス認証の実行

この macAddressWithRadius モードのポートは、複数のユーザに MAC アドレス認証を実行します。

IV. MAC アドレス認証と 802.1X 認証の組み合わせの実行

- macAddressOrUserLoginSecure

  このモードは、macAddressWithRadius と userLoginSecure モードの組み合わせです。1 つの 802.1X 認証ユーザと複数の MAC アドレス認証ユーザがログインすることを許可します。

  このモードでは、ポートは 802.1X 認証を最初に実行します。802.1X 認証に失敗したとき、MAC アドレス認証が実行されます。

  しかし以下の条件が存在する場合、このモードのポートは異なる認証動作になります。

  - □ ポートが MAC アドレス認証と 802.1X 認証の並列処理が有効になっている。
  - □ ポートが 802.1X ユニキャストトリガが有効になっている。
  - □ ポートがアンノウン MAC アドレスのパケットを受信する。

  このような場合、ポートは 802.1X 認証を開始するために MAC アドレスあてにユニキャスト EAP-Request/Identity パケットを送信します。その後、ポートは 802.1X 認証の結果を待つことなく、ただちに MAC アドレス認証を実行します。

- macAddressOrUserLoginSecureExt

  この macAddressOrUserLoginSecureExt モードは、ポートが複数の 802.1X と MAC アドレス認証のユーザをサポートしているのを除いて、macAddressOrUserLoginSecure モードと同じです。

- macAddressElseUserLoginSecure

  このモードは、**Else** キーワードが示すように、MAC アドレス認証が高いプライオリティを持つ macAddressWithRadius と userLoginSecure モードの組み合わせです。1 つの 802.1X 認証ユーザと複数の MAC アドレス認証ユーザがログインすることを許可します。

  このポートは非 802.1X フレームを受信した際、MAC アドレス認証を実行します。802.1X フレームを受信した際、ポートは MAC アドレス認証を実行します。もし MAC アドレス認証に失敗すると 802.1X 認証を実行します。

- macAddressElseUserLoginSecureExt

  このモードは、**Ext** キーワードが示すように、ポートが複数の 802.1X と MAC アドレス認証のユーザをサポートしているのを除いて、macAddressElseUserLoginSecure モードと同じです。

7.2 設定ガイドライン

ポートセキュリティを設定する際、以下のガイドラインに従ってください。

- 802.1X 認証または MAC アドレス認証のみを必要とするシナリオでは、ポートセキュリティではなく 802.1X 認証または MAC アドレス認証を使用してください。802.1X 認証と MAC アドレス認証の設定の詳細については、オペレーションマニュアルのセクション 9 *セキュリティ”802.1X”と”MAC アドレス認証”*を参照してください。
- ポートセキュリティを有効にする前に、ポートがアグリゲーショングループに加えられていないことを確認してください。

7.3 設定作業リスト

作業リスト	補足
（必須設定項目） ポートセキュリティの有効化	―
（オプション設定項目） ポートでのセキュアMACアドレスの最大数の設定	―
（必須設定項目） ポートセキュリティモードの設定	―
（必須設定項目） ポートセキュリティ機能の設定 • NTKの設定 • 侵入防止の設定	ネットワーク要件に従い、1つ以上のポートセキュリティ機能を設定してください。
（オプション設定項目） セキュアMACアドレスの設定	―
（オプション設定項目） サーバからの許可情報の無視	―
（オプション設定項目） MACアドレス移動機能の有効化	―

7.3.1 ポートセキュリティの有効化

ポートセキュリティを有効にする前に、グローバルで 802.1X 認証と MAC アドレス認証を無効にしてください。

ポートセキュリティが有効の場合、手動で 802.1X 認証または MAC アドレス認証を有効にしたり、アクセス制御モードやポート許可状態を変更したりすることはできません。ポートセキュリティは自動的に別のセキュリティモードでこれらの設定を変更します。

以下にポートセキュリティの有効化の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. ポートセキュリティを有効にする	**port-security enable**	デフォルト：無効

undo port-security コマンドでポートセキュリティを無効にすることができます。ポートセキュリティを無効にするために、オンラインユーザがいないことを確認してください。

ポートセキュリティの有効あるいは無効にすることで、以下のセキュリティの設定をデフォルトにします。

- 802.1X アクセス制御モードのデフォルトは MAC アドレスベースです。
- 802.1X ポート許可状態のデフォルトは auto です。

802.1X 認証と MAC アドレス認証の設定の詳細については、オペレーションマニュアルのセクション 9 *セキュリティ”802.1X”*、*”MAC アドレス認証”*を参照してください。

7.4 ポートでのセキュアMACアドレスの最大数の設定

ポートで許可するセキュア MAC アドレスの最大数を設定することで、以下のことが可能になります。

- ポートで同時に接続するユーザ数を制御します。

  security モード（autoLearn と secure を除きます。）で動作するポートで、以下の値のいずれか小さい方が上限と等しくなります。

  - ポートセキュリティが許可するセキュア MAC アドレスの制限
  - authentication モードで許可される同時接続数
- autoLearn モードのポートでセキュア MAC アドレス数を制御します。

  ポートセキュリティにおけるポートでのセキュア MAC アドレス最大数は、MAC アドレステーブルに学習できる制限と独立しています。MAC アドレステーブルの設定の詳細については、オペレーションマニュアルのセクション 3 *アクセス”MAC アドレステーブル”*を参照してください。

以下にポートでのセキュア MAC アドレスの最大数の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. interface view に移行する	**interface** *interface-type interface-number*	―

操作	コマンド	補足
3． ポートでのセキュア MAC アドレスの最大数を設定する	**port-security max-mac-count** *max-count*	デフォルト：制限なし

7.5 ポートセキュリティモードの設定

ポートでポートセキュリティモードを設定する前に、以下の作業を完了してください。

- 802.1X 認証と MAC アドレス認証を無効にしてください。
- ポートがアグリゲーショングループあるいはサービスループバックグループに属していないことを確認してください。
- autoLearn モードを設定する場合、セキュア MAC アドレスの最大許可数を設定してください。autoLearn モードに入ると設定を変更することができません。

ポートセキュリティモードを設定するとき以下のガイドラインに従ってください。

- ポートセキュリティが無効のとき、ポートセキュリティモードを指定することができますが、設定は適用されません。
- ポートのセキュリティモードを変更すると、オンラインユーザを切断します。
- ポートセキュリティが設定されている場合、ポートで 802.1X 認証あるいは MAC アドレス認証を有効にできません。
- 以下のポートセキュリティモードで RADIUS サーバにより割り当てられる URL 属性をサポートします。
  - □ mac-and-userlogin-secure-ext
  - □ mac-authentication
  - □ mac-else-userlogin-secure
  - □ mac-else-userlogin-secure-ext
  - □ userlogin-secure
  - □ userlogin-secure-ext
  - □ userlogin-secure-or-mac
  - □ userlogin-secure-or-mac-ext
  - □ userlogin-withoui

  認証の間、ユーザはサーバ割り当ての URL 属性によって指定された Web インタフェースにリダイレクトされます。Web 認証に成功した後、RADIUS サーバは Web ユーザの MAC アドレスを記録し Web ユーザをログオフするために DM（Disconnect Message）を使用します。ユーザが 802.1X または MAC アドレス認証を再び開始する際に、認証が成功し、オンラインになります。

以下にポートセキュリティモードの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． （オプション設定項目）ユーザ認証の OUI 値を設定する	**port-security oui index** *index-value* **mac-address** *oui-value*	デフォルト：設定なし この設定は**userlogin-withoui** モードで必要です。 複数のOUIを設定することができますが、**userlogin-withoui** モードのとき、ポートは指定されたOUIの1つにマッチした1つの802.1Xユーザのみ許可されます。
3． interface view に移行する	**interface** *interface-type interface-number*	―

操作	コマンド	補足
4． ポートセキュリティモードを設定する	**port-security port-mode** { **autolearn** | **mac-and-userlogin-secure-ext** | **mac-authentication** | **mac-else-userlogin-secure** | **mac-else-userlogin-secure-ext** | **secure** | **userlogin** | **userlogin-secure** | **userlogin-secure-ext** | **userlogin-secure-or-mac** | **userlogin-secure-or-mac-ext** | **userlogin-withoui** }	デフォルト：**noRestrictions** ポートセキュリティを有効にした後、モードを **noRestrictions**（デフォルト）にしたときのみ、ポートセキュリティのモードを変更することができます。ポートセキュリティのモードを変更するときは、最初に**undo port-security port-mode**コマンドで、ポートセキュリティのモードをデフォルトに戻す必要があります。

🕮 **メモ：**

mac-and-userlogin-secure-extオプションは Version7.1.7 を含む以降のソフトウェアからサポートしています。

7.6 ポートセキュリティ機能の設定

7.6.1 NTK の設定

NTK（Need To Know）機能は、認証をパスした装置に対してのみフレームを転送させるため、出力フレームの宛先 MAC アドレスをチェックします。

NTK 機能は以下のモードをサポートしています。

- **ntkonly** － 認証をパスした宛先 MAC アドレス宛のユニキャストフレームのみ転送します。
- **ntk-withbroadcasts** － 認証をパスした宛先 MAC アドレス宛の、ブロードキャストフレーム、ユニキャストフレームのみを転送します。
- **ntk-withmulticasts** － 認証をパスした宛先 MAC アドレス宛のブロードキャストフレーム、マルチキャストフレーム、ブロードキャストフレームのみを転送します。

NTK 機能を使用すると、未知の宛先 MAC アドレスのユニキャストフレームは廃棄されます。すべてのポートセキュリティモードが NTK 機能を動作するわけではありません。詳細は表 7-1を参照してください。

以下に NTK 機能の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． interface view に移行する	**interface** *interface-type interface-number*	―
3． NTK 機能を設定する	**port-security ntk-mode** { **ntk-withbroadcasts** | **ntk-withmulticasts** | **ntkonly** }	デフォルト：無効 すべてのフレームが転送されます。

7.6.2 侵入防止の設定

侵入防止機能は不正なフレームに対して以下のアクションの 1 つを実行します。

- **blockmac** – 不正なフレームの送信元 MAC アドレスをブロック MAC アドレスリストに追加し、フレームを破棄します。ブロックされた MAC アドレスからのすべての後続のフレームは廃棄されます。ブロック MAC アドレスは、3 分間ブロックされた後に、標準状態に戻ります。このブロックする時間は変更できません。
- **disableport** – 手動でポートをアップするまで、ポートを無効にします。
- **disableport-temporarily** – 指定した期間、ポートを無効にします。この期間は **port-security timer disableport** コマンドで設定できます。

以下に侵入防止の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. interface view に移行する	**interface** *interface-type interface-number*	ー
3. 侵入防止機能を設定する	**port-security intrusion-mode** { **blockmac** | **disableport** | **disableport-temporarily** }	デフォルト：無効
4. system view に戻る	**quit**	ー
5. （オプション設定項目）ポートを無効にする時間を設定する	**port-security timer disableport** *time-value*	デフォルト：20秒

🕮 **メモ：**

macAddressElseUserLoginSecure モードあるいは macAddressElseUserLoginSecureExt はモードで動作するポートにおいて、侵入防止機能は、同一フレームで MAC アドレス認証と 802.1X 認証の両方が失敗した後に動作します。

7.7 セキュアMACアドレスの設定

セキュア MAC アドレスは autoLearn モードで設定、あるいは学習されます。アドレスが保存されると、装置の再起動を行っても保持されます。セキュア MAC アドレスを VLAN の 1 つのポートにのみ割り当てることができます。

セキュア MAC アドレスエントリが最大数に到達したとき、ポートはセキュアモードに変更押します。セキュアモードでは、ポートはセキュア MAC アドレスを追加あるいは学習することができません。ポートはセキュア MAC アドレスからの送信元フレームあるいは **mac-address dynamic** コマンド、**mac-address static** コマンドで設定された MAC アドレスのみがパスすることができます。

表 7-2 スタティックセキュア MAC アドレス、Sticky セキュア MAC アドレスの比較

タイプ	アドレスソース	エージングメカニズム	再起動で保存されるか？
Static	手動で追加されます。（sticky パラメータを使用しない **port-security mac-address security**コマンドを使用します）	利用できません。 スタティックアドレスは以下の作業の1つを実行しない限り、エージアウトしません。 ● 手動でMACアドレスを削除します。 ● ポートセキュリティモードを変更します。 ● ポートセキュリティモードを無効にします。	Yes
Sticky	手動で追加されます。（**port-security mac-address security sticky**コマンドを使用します）	Sticky MACアドレスはデフォルト設定ではエージアウトしませんが、エージング時間を設定することができます。 ● エージングタイマが設定されているとき、sticky MACアドレスからのトラフィックデータに関わらずエージングを行います。	Yes 再起動でセキュアMACエージングタイマが再起動します。

7.7.1 設定要件

セキュア MAC アドレスを設定する前に、以下の作業を完了してください。

- ポートセキュリティを有効にしてください。
- autoLearn モードを有効にする前に、ポートのセキュア MAC アドレスの最大許可数を設定してください。
- ポートセキュリティのモードを autoLearn に設定してください。
- ポートで指定した VLAN のパケットが通過できるように許可する、あるいは VLAN にポートを追加するように設定を行ってください。VLAN が既に存在することを確認してください。

7.7.2 設定手順

以下にセキュア MAC アドレスの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. （オプション設定項目）セキュア MAC アドレスエージングタイマを設定する	**port-security timer autolearn aging** *time-value*	デフォルト：セキュアMACアドレスはエージアウトしません。

操作	コマンド	補足
3． セキュア MAC アドレスを設定する	● system viewで設定する： **port-security mac-address security** [**sticky**] *mac-address* **interface** *interface-type interface-number* **vlan** *vlan-id* ● interface viewで設定する： 1． **interface** *interface-type interface-number* 2． **port-security mac-address security** [**sticky**] *mac-address* **vlan** *vlan-id*	デフォルト：設定なし 同一VLANでは、スタティックセキュアMACアドレスにMACアドレスを指定することはできません。

7.8 サーバからの許可情報の無視

802.1X ユーザ、または MAC アドレス認証ユーザが認証をパスした後、サーバ（ローカルあるいはリモート）から受信した許可情報を無視するようにポートに設定することができます。

以下にサーバからの許可情報を無視する設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． interface view に移行する	**interface** *interface-type interface-number*	―
3． 認証サーバから受信した許可情報を無視するように設定する	**port-security authorization ignore**	デフォルト：ポートは認証サーバからの許可情報を使用します。

7.9 MACアドレス移動機能の有効化

MAC アドレス移動機能を有効にすることで、802.1X 認証あるいは MAC アドレス認証が許可されたユーザが装置のポートを移動できるようになります。たとえば、802.1X 認証ユーザが、802.1X が有効な装置の別のポートに移動する場合、認証セッションが最初のポートから削除され、新しいポートで再認証されます。

もし MAC アドレス移動機能が無効で 802.1X 認証ユーザが別のポートに移動した場合、再認証されません。

（ローカルまたはリモートの）認証サーバのオンラインユーザ数が上限に達した場合、802.1X または MAC アドレス認証ユーザは装置上のポート間で移動はできません。

ポートのローミングを行うワイヤレスユーザがネットワークにアクセスできるように MAC アドレス移動機能を有効にすることを推奨します。

以下に MAC アドレス移動機能の有効化の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―

操作	コマンド	補足
2． MAC アドレス移動機能を有効にする	**port-security mac-move permit**	デフォルト：有効
3． interface view に移行する	**interface interface-type interface-number**	―
4． VLAN チェックバイパス機能を有効にする	**port-security mac-move bypass-vlan-check**	デフォルト：無効 MAC ベース VLAN でダイナミック VLAN を使用するユーザがポート移動を行う環境では、本機能を有効にしてください。

7.10 ポートセキュリティに関するSNMP notification

重大なポートセキュリティイベントを NMS に通知するために使用します。ポートセキュリティイベントを正しく送信するには、装置に SNMP も設定しておかなければなりません。SNMP 設定の詳細については、オペレーションマニュアルのセクション 11 *システム管理*“*SNMP*”を参照してください。

以下にポートセキュリティに関する SNMP notification の有効化の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． ポートセキュリティの SNMP notification 機能を有効にする	**snmp-agent trap enable port-security** [**address-learned** | **dot1x-failure** | **dot1x-logoff** | **dot1x-logon** | **intrusion** | **mac-auth-failure** | **mac-auth-logoff** | **mac-auth-logon**]*	デフォルト：無効

7.11 ポートセキュリティユーザのロギングの有効化

I. 概要

この機能は装置がポートセキュリティユーザのログを生成し、Information Center にログを送信します。Information Center のログ出力ルールを設定するため、**info-center source** コマンドを使用します。Information Center の詳細は、オペレーションマニュアルのセクション 11 *システム管理*“*Information Center*”を参照してください。

II. 制限とガイドライン

頻繁に認証接続が発生する環境では、ポートセキュリティユーザのログの過剰な出力を防止するため、無効にすることを推奨します。

III. 設定手順

操作	コマンド	補足
1． system view に移行する	**system-view**	―

操作	コマンド	補足
2. ポートセキュリティユーザのログ機能を有効にする	**port-security access-user log enable** [**failed-authorization** | **mac-learning** | **violation**] *	デフォルト：有効 パラメータを指定しない場合、ポートセキュリティユーザのすべてのログ機能を有効にします。

7.12 ポートでの認証方式のトリガー順序の設定

🕮 **メモ：**

ポートでの認証方式のトリガー順序の設定は Version7.1.7 を含む以降のソフトウェアからサポートしています。

I. 概要

この機能は、トリプル認証がイネーブルになっているポートでのみ有効です。トリプル認証を使用すると、ユーザアクセス用のレイヤ 2 ポートで Web 認証、MAC アドレス認証認証、802.1 X 認証を同時にイネーブルにできます。エンドポイントパケットのタイプが異なると、最初に異なるタイプの認証がトリガーされます。詳細については、 「セキュリティ構成ガイド」 の 「トリプル認証」 を参照してください。

エンドポイントパケットが最初に MAC アドレス認証をトリガーできるようにするには、この機能を使用します。

ポートは、複数の認証方式に対して同時に認証プロセスを実行できます。1 つの認証が失敗しても、他の認証方式のプロセスには影響しません。ただし、エンドポイントがポート上で 1 つの認証を渡すと、デバイスはポート上の他の認証方式のプロセスを次のように処理します。

- エンドポイントが MAC アドレス認証を通過する場合、デバイスはポート上に MAC アドレス認証 ユーザ エントリを生成し、ポート上のエンドポイントに対して 802.1 X 認証を実行し続けます。ただし、デバイスはポート上のエンドポイントの Web 認証を続行できません。
  - MAC アドレス認証の後にエンドポイントが 802.1 X 認証に合格すると、デバイスはポート上のエンドポイントに対して 802.1 X ユーザ エントリを生成します。802.1 X ユーザ エントリは、MAC アドレス認証 ユーザ エントリを上書きします。
  - MAC アドレス認証後にエンドポイントが 802.1 X 認証に合格しない場合、MAC アドレス認証 ユーザ エントリはポートに保持されます。エンドポイントは 802.1 X 認証を再度トリガーできますが、Web 認証はトリガーできません。
- エンドポイントが MAC アドレス認証に失敗し、802.1 X または Web 認証を通過した場合、デバイスは、エンドポイントが通過した認証方式を除き、ポート上のすべての認証方式をただちに停止します。さらに、デバイスは、ポート上のエンドポイントに対して停止した認証方法の認証プロセスをトリガーできなくなります。

II. 制約事項およびガイドライン

この機能により、認証されるユーザは認証に失敗します。ユーザは、オンラインになるために認証を再トリガーする必要があります。ユーザーがオンラインにならないようにするためのベストプラクティスとして、この機能は注意して使用してください。

III. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. interface view に移行する	**interface** *interface-type interface-number*	
3. ポートの認証方式 (MAC アドレス認証、802.1 X 認証、Web 認証) のトリガー順序を設定する	**port-security triple-auth-order mac-dot 1 x-web**	デフォルト : エンドポイントから送信されるパケットのタイプによって異なる

7.13 ポートセキュリティの表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
ポートセキュリティの設定、動作情報、統計情報を表示する	**display port-security** [**interface** *interface-type interface-number*]
セキュアMACアドレス情報を表示する	**display port-security mac-address security** [**interface** *interface-type interface-number*] [**vlan** *vlan-id*] [**count**]
ブロックしたMACアドレスを表示する	**display port-security mac-address block** [**interface** *interface-type interface-number*] [**vlan** *vlan-id*] [**count**]

7.14 ポートセキュリティの設定例

7.14.1 autoLearn モードの設定例

I. ネットワーク要件

図 7-1に示すように、装置の GigabitEthernet 1/0/1 で以下の要件を設定します。

- 認証なしでアクセスできるユーザを最大 64 にします。
- ポートを学習、追加できるように設定し、セキュア MAC アドレスエージングタイマを 30 分に設定します。
- セキュア MAC アドレスの数が 64 に到達すると、ポートは MAC アドレスの学習を止めます。未知の MAC アドレスを持つフレームを受信した場合は、侵入防止機能が実行します。ポートはシャットダウンされ、30 秒間無効化されます。

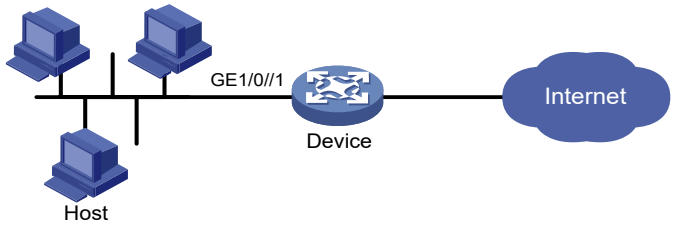


図 7-1 ネットワーク図

II. 設定手順

ポートセキュリティを有効にします。

```
<Device> system-view
[Device] port-security enable
```

セキュア MAC アドレスタイマを 30 分に設定します。

```
[Device] port-security timer autolearn aging 30
```

GigabitEthernet 1/0/1 のセキュア MAC アドレスの最大許可数を 64 に設定します。

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] port-security max-mac-count 64
```

ポートセキュリティのモードを autoLearn に設定します。

```
[Device-GigabitEthernet1/0/1] port-security port-mode autolearn
```

侵入防止機能が起動した後、30 秒後に復旧するように設定します。

```
[Device-GigabitEthernet1/0/1] port-security intrusion-mode disableport-temporarily
[Device-GigabitEthernet1/0/1] quit
[Device] port-security timer disableport 30
```

III. 設定の確認

ポートセキュリティの設定を表示します。

```
[Device] display port-security interface gigabitethernet 1/0/1
Grobal Port security parameters:
   Port security          : Enabled
   AutoLearn aging time   : 30 min
   Disableport timeout    : 30 s
   MAC move               : Denied
   Authorization fail     : Online
   NAS-ID profile         : Not configured
   Dot1x-failure trap     : Disabled
   Dot1x-logon trap       : Disabled
   Dot1x-logoff trap      : Disabled
   Intrusion trap         : Disabled
   Address-learned trap   : Disabled
   Mac-auth-failure trap  : Disabled
   Mac-auth-logon trap    : Disabled
   Mac-auth-logoff trap   : Disabled
   Open authentication    : Disabled
   OUI value list         :
    Index :  1           Value : 123401

 GigabitEthernet1/0/1 is link-up
   Port mode                     : autoLearn
   NeedToKnow mode               : Disabled
   Intrusion protection mode     : DisablePortTemporarily
   Security MAC address attribute
       Learning mode             : Sticky
       Aging type                : Periodical
   Max secure MAC addresses      : 64
   Current secure MAC addresses  : 0
   Authorization                 : Permitted
```

```
   NAS-ID profile                  : Not configured
   Free VLANs                      : Not configured
   Open authentication             : Disabled
```

設定が適用された後、ポートで MAC アドレスの学習が行われます。Current number of secure MAC addresses フィールドに学習した MAC アドレスを表示することができます。

学習した MAC アドレスの追加情報を表示します。

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] display this
#
interface GigabitEthernet1/0/1
 port-security max-mac-count 64
 port-security port-mode autolearn
 port-security mac-address security sticky 0002-0000-0015 vlan 1
 port-security mac-address security sticky 0002-0000-0014 vlan 1
 port-security mac-address security sticky 0002-0000-0013 vlan 1
 port-security mac-address security sticky 0002-0000-0012 vlan 1
 port-security mac-address security sticky 0002-0000-0011 vlan 1
#
[Device-GigabitEthernet1/0/1] quit
```

ポートで学習した MAC アドレスの数が 64 に到達した後、ポートセキュリティのモードが **secure** モードに変更したことを確認します。

```
[Device] display port-security interface gigabitethernet 1/0/1
```

未知の MAC アドレスのフレームを受信したのち、30 秒後にポートが無効になることを確認します。（詳細は省略します。）

ポートが再度有効になった後、いくつかのセキュア MAC アドレスを削除します。

```
[Device] undo port-security mac-address security sticky 0002-0000-0015 vlan 1
[Device] undo port-security mac-address security sticky 0002-0000-0014 vlan 1
```

ポートセキュリティのモードは **autoLearn** に戻り、再度 MAC アドレスを学習できるようになることを確認します。（詳細は省略します。）

7.14.2 userLoginWithOUI モードの設定例

I. ネットワーク要件

図 7-2に示すようにクライアントはDeviceのポート GigabitEthernet 1/0/1 に接続されます。Device は RADIUS サーバによってクライアントを認証します。認証に成功した場合、クライアントはインターネットへのアクセスが許可されます。

- プライマリ認証サーバとセカンダリアカウンティングサーバとして RADIUS サーバ 192.168.1.2 を、セカンダリ認証サーバとプライマリアカウンティングサーバとして RADIUS サーバ 192.168.1.3 を指定します。認証用の共有鍵を name、アカウンティング用の共有鍵を money に設定します。
- すべてのユーザは、ISP ドメイン sun のデフォルトの認証、許可、アカウンティング方式を使用します。
- RADIUS サーバのレスポンスタイムアウト時間を 5 秒、RADIUS サーバへの許容再送信数を 5 回に設定します。Device は 15 分ごとにリアルタイムアカウンティングパケットを送信し、RADIUS サーバ宛にドメイン名なしでユーザ名を送信します。

Device の GigabitEthernet 1/0/1 は 802.1X ユーザ、および認証するために指定された OUI の値の 1 つを使用するユーザのみを許可します。

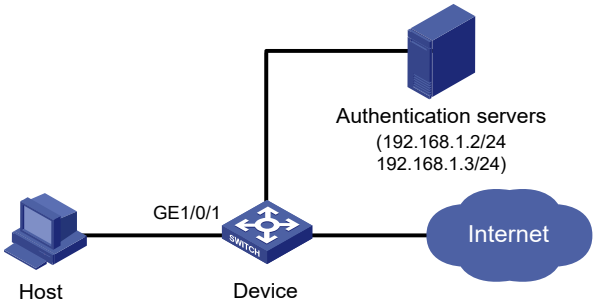


図 7-2 ネットワーク図

II. 設定手順

以下の設定手順は AAA/RADIUS の設定コマンドが含まれます。詳細はコマンドマニュアルのセクション 9 *セキュリティ*”*AAA*”を参照してください。

Host と RADIUS サーバが互いに通信可能であることを確認してください。

1)　AAA を設定します。

RADIUS スキーム radsun を設定します。

```
<Device> system-view
[Device] radius scheme radsun
[Device-radius-radsun] primary authentication 192.168.1.2
[Device-radius-radsun] primary accounting 192.168.1.3
[Device-radius-radsun] secondary authentication 192.168.1.3
[Device-radius-radsun] secondary accounting 192.168.1.2
[Device-radius-radsun] key authentication simple name
[Device-radius-radsun] key accounting simple money
[Device-radius-radsun] timer response-timeout 5
[Device-radius-radsun] retry 5
[Device-radius-radsun] timer realtime-accounting 15
[Device-radius-radsun] user-name-format without-domain
[Device-radius-radsun] quit
```

ISP ドメイン sun を設定します。

```
[Device] domain sun
[Device-isp-sun] authentication lan-access radius-scheme radsun
[Device-isp-sun] authorization lan-access radius-scheme radsun
[Device-isp-sun] accounting lan-access radius-scheme radsun
```

```
[Device-isp-sun] quit
```

2) 802.1X 認証方式を CHAP に設定します。802.1X のデフォルトの認証方式の設定は CHAP です。

```
[Device] dot1x authentication-method chap
```

ISP ドメインを sun に指定します。

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] dot1x mandatory-domain sun
[Device-GigabitEthernet1/0/1] quit
```

3) ポートセキュリティを設定します。

ポートセキュリティを有効にします。

```
[Device] port-security enable
```

5 つの OUI の値を追加します。（16 の OUI の値を追加することができます。ポートは 1 ユーザが認証をパスするため、1 つの OUI のみにマッチするように許可します。）

```
[Device] port-security oui index 1 mac-address 1234-0100-1111
[Device] port-security oui index 2 mac-address 1234-0200-1111
[Device] port-security oui index 3 mac-address 1234-0300-1111
[Device] port-security oui index 4 mac-address 1234-0400-1111
[Device] port-security oui index 5 mac-address 1234-0500-1111
```

ポートセキュリティのモードを userLoginWithOUI に設定します。

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] port-security port-mode userlogin-withoui
[Device-GigabitEthernet1/0/1] quit
```

III. 設定の確認

GigabitEthernet 1/0/1 が 1 つの 802.1X ユーザのみに認証されていることを確認します。

```
[Device] display port-security interface gigabitethernet 1/0/1
Global port security parameters:
   Port security          : Enabled
   AutoLearn aging time   : 30 min
   Disableport timeout    : 30 s
   MAC move               : Denied
   Authorization fail     : Online
   NAS-ID profile         : Not configured
   Dot1x-failure trap     : Disabled
   Dot1x-logon trap       : Disabled
   Dot1x-logoff trap      : Disabled
   Intrusion trap         : Disabled
   Address-learned trap   : Disabled
   Mac-auth-failure trap  : Disabled
   Mac-auth-logon trap    : Disabled
   Mac-auth-logoff trap   : Disabled
   Open authentication    : Disabled
   OUI value list         :
       Index :  1       Value : 123401
       Index :  2       Value : 123402
       Index :  3       Value : 123403
```

```
       Index :  4       Value : 123404
       Index :  5       Value : 123405

 GigabitEthernet1/0/1 is link-up
   Port mode                       : userLoginWithOUI
   NeedToKnow mode                 : Disabled
   Intrusion protection mode       : NoAction
Security MAC address attribute
       Learning mode               : Sticky
       Aging type                  : Periodical
   Max secure MAC addresses        : Not configured
   Current secure MAC addresses    : 1
   Authorization                   :Permitted
   NAS-ID profile                  : Not configured
   Free VLANs                      : Not configured
   Open authentication             : Disabled
```

802.1X の設定を確認するため、802.1X オンラインユーザの情報を表示します。

```
[Device] display dot1x
```

認証にパスするために指定された OUI を持つ MAC アドレスのユーザがポートで許可されているかどうか確認します。

```
[Device] display mac-address interface gigabitethernet 1/0/1
MAC Address     VLAN ID   State         Port/NickName        Aging
1234-0300-0011  1         Learned       GE1/0/1              Y
```

7.14.3 macAddressElseUserLoginSecure モードの設定例

I. ネットワーク要件

図 7-3に示すように、GigabitEthernet 1/0/1 を通してクライアントが Device に接続されます。Device は RADIUS サーバを使用してクライアントを認証します。認証が成功すると、クライアントはインターネットにアクセスするように許可されます。

Device のポート GigabitEthernet 1/0/1 を以下のように制限します。

- 1 つ以上の MAC アドレス認証ユーザがログオンすることを許可します。
- 802.1X ユーザのために、最初に MAC アドレス認証が実行されます。MAC アドレス認証に失敗した場合、802.1X 認証が実行されます。そして 1 つの 802.1X ユーザのみがログオンすることを許可します。
- MAC アドレス認証のために固定ユーザ名とパスワードを設定します。MAC アドレスはハイフン付きの 16 進数で大文字です。
- MAC アドレス認証ユーザと 802.1X 認証ユーザの総計を 64 に設定します。
- 未知の MAC アドレス宛にフレーム送信されることを防ぐために NTK（ntkonly モード）を有効にします。

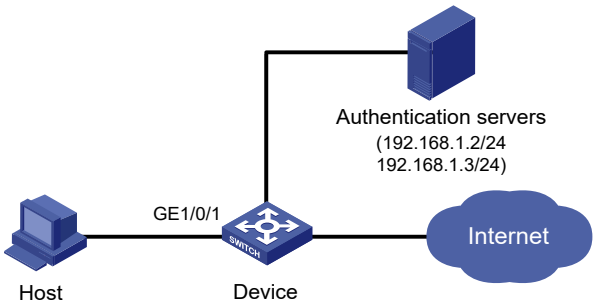


図 7-3 ネットワーク図

II. 設定手順

Host と RADIUS サーバが互いに通信可能であることを確認してください。

1) RADIUS 認証／許可、ISP ドメインの設定を行います。（オペレーションマニュアルのセクション 9 *セキュリティ”ポートセキュリティ”の”userLoginWithOUI モードの設定例*”を参照してください。）
2) ポートセキュリティを設定します。

ポートセキュリティを有効にします。

```
<Device> system-view
[Device] port-security enable
```

MAC アドレス認証に MAC ベースのアカウントを使用します。各 MAC アドレスは 16 進数でハイフンあり、大文字を使用します。

```
[Device] mac-authentication user-name-format mac-address with-hyphen uppercase
```

MAC アドレス認証ドメインを指定します。

```
[Device] mac-authentication domain sun
```

802.1X 認証方式を CHAP に設定します。802.1X のデフォルトの認証方式の設定は CHAP です。

```
[Device] dot1x authentication-method chap
```

MAC アドレスの最大許可数を 64 に設定します。

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] port-security max-mac-count 64
```

ポートセキュリティのモードを macAddressElseUserLoginSecure に設定します。

```
[Device-GigabitEthernet1/0/1] port-security port-mode mac-else-userlogin-secure
```

ISP ドメインを sun に指定します。

```
[Device-GigabitEthernet1/0/1] dot1x mandatory-domain sun
```

ポートの NTK モードを ntkonly に設定します。

```
[Device-GigabitEthernet1/0/1] port-security ntk-mode ntkonly
```

```
[Device-GigabitEthernet1/0/1] quit
```

III. 設定の確認

ポートセキュリティの設定を表示します。

```
[Device] display port-security interface gigabitethernet 1/0/1
Global Port security parameters:
   Port security          : Enabled
   AutoLearn aging time   : 30 min
   Disableport timeout    : 30 s
   MAC move               : Denied
   Authorization fail     : Online
   NAS-ID profile         : Not configured
   Dot1x-failure trap     : Disabled
   Dot1x-logon trap       : Disabled
   Dot1x-logoff trap      : Disabled
   Intrusion trap         : Disabled
   Address-learned trap   : Disabled
   Mac-auth-failure trap  : Disabled
   Mac-auth-logon trap    : Disabled
   Mac-auth-logoff trap   : Disabled
   Open authentication    : Disabled
   OUI value list

 GigabitEthernet1/0/1 is link-up
   Port mode                     : macAddressElseUserLoginSecure
   NeedToKnow mode               : NeedToKnowOnly
   Intrusion protection mode     : NoAction
   Security MAC address attribute
       Learning mode             : Sticky
       Aging type                : Periodical
   Max secure MAC addresses      : 64
   Current secure MAC addresses  : 0
   Authorization                 : Permitted
   NAS-ID profile                : Not configured
   Free VLANs                    : Not configured
   Open authentication           : Disabled
```

ユーザが認証にパスした後、MAC アドレス認証の情報を表示します。GigabitEthernet 1/0/1 で複数の MAC アドレス認証のユーザが許可されていることを確認してください。

```
[Device] display mac-authentication interface gigabitethernet 1/0/1
Global MAC authentication parameters:
   MAC authentication     : Enabled
   User name format       : MAC address in uppercase(XX-XX-XX-XX-XX-XX)
            Username      : mac
            Password      : Not configured
   Offline detect period  : 300 s
   Quiet period           : 180 s
   Server timeout         : 100 s
   Reauth period          : 3600 s
   Authentication domain  : sun
 Online MAC-auth wired users    : 3

 Silent MAC users:
          MAC address       VLAN ID  From port               Port index

GigabitEthernet1/0/1 is link-up
   MAC authentication         : Enabled
   Carry User-IP              : Disabled
   Authentication domain      : Not configured
   Auth-delay timer           : Disabled
   Periodic reauth            : Disabled
   Re-auth server-unreachable : Logoff
```

```
   Guest VLAN                 : Not configured
   Guest VLAN auth-period     : 30 s
   Critical VLAN              : Not configured
   Critical voice VLAN        : Disabled
   Host mode                  : Single VLAN
   Offline detection          : Enabled
   Authentication order       : Default
   Guest VSI                  : Not configured
   Guest VSI auth-period      : 30 s
   Critical VSI               : Not configured
   Max online users           : 4294967295
   Authentication attempts    : successful 3, failed 7
   Current online users       : 3
          MAC address       Auth state
          1234-0300-0011    Authenticated
          1234-0300-0012    Authenticated
          1234-0300-0013    Authenticated
```

802.1X 認証情報を表示します。GigabitEthernet 1/0/1 で 1 つの 802.1X ユーザのみ許可していることを確認してください。

[Device] display dot1x interface gigabitethernet 1/0/1

```
Global 802.1X parameters:
   802.1X authentication  : Enabled
   CHAP authentication    : Enabled
   Max-tx period          : 30 s
   Handshake period       : 15 s
   Quiet timer            : Disabled
       Quiet period       : 60 s
   Supp timeout           : 30 s
   Server timeout         : 100 s
   Reauth period          : 3600 s
   Max auth requests      : 2
   SmartOn supp timeout   : 30 s
   SmartOn retry counts   : 3
   EAD assistant function : Disabled
       EAD timeout        : 30 min
   Domain delimiter       : @
Online 802.1X wired users      : 1

GigabitEthernet1/0/1  is link-up
   802.1X authentication      : Enabled
   Handshake                  : Enabled
   Handshake reply            : Disabled
   Handshake security         : Disabled
   Unicast trigger            : Disabled
   Periodic reauth            : Disabled
   Port role                  : Authenticator
   Authorization mode         : Auto
   Port access control        : MAC-based
   Multicast trigger          : Enabled
   Mandatory auth domain      : sun
   Guest VLAN                 : Not configured
   Auth-Fail VLAN             : Not configured
   Critical VLAN              : Not configured
   Critical voice VLAN        : Disabled
   Add Guest VLAN delay       : Disabled
   Re-auth server-unreachable : Logoff
   Max online users           : 4294967295
   SmartOn                    : Disabled
   User IP freezing           : Disabled
   Reauth period              : 0 s
   Send Packets Without Tag   : Disabled
   Max Attempts Fail Number   : 0
   Guest VSI                  : Not configured
   Auth-Fail VSI              : Not configured
   Critical VSI               : Not configured
   Add Guest VSI delay        : Disabled
```

```
  EAPOL packets: Tx 16331, Rx 102
  Sent EAP Request/Identity packets : 16316
       EAP Request/Challenge packets: 6
       EAP Success packets: 4
       EAP Failure packets: 5
  Received EAPOL Start packets : 6
           EAPOL LogOff packets: 2
           EAP Response/Identity packets : 80
           EAP Response/Challenge packets: 6
           Error packets: 0
  Online 802.1X users: 1
         MAC address         Auth state
         0002-0000-0011      Authenticated
```

未知の宛先 MAC アドレス、マルチキャストアドレス、ブロードキャストアドレスのフレームは破棄されることを確認してください。（詳細は省略します。）

7.15 ポートセキュリティのトラブルシューティング

7.15.1 ポートセキュリティのモードが設定できない

I. 症状

ポートセキュリティのモードが設定できません。

II. 分析

ポートで noRestrictions 以外のポートセキュリティのモードが動作している場合、**port-security port-mode** コマンドによって、モードを変更することができません。

III. 解決策

問題を解決するため、以下を行います。

1)　ポートセキュリティモードを noRestrictions に設定します。

```
[Device-GigabitEthernet1/0/1] undo port-security port-mode
```

2)　新しいポートセキュリティのモードを設定します。たとえば、autoLearn です。

```
[Device-GigabitEthernet1/0/1] port-security port-mode autolearn
```

3)　問題が解決しない場合、NEC に問い合わせてください。

7.15.2 セキュア MAC アドレスが設定できない

I. 症状

セキュア MAC アドレスが設定できません。

II. 分析

ポートセキュリティのモードが autoLearn 以外で動作するポートでは、セキュア MAC アドレスを設定することはできません。

III. 解決策

問題を解決するため、以下を行います。

1)　ポートセキュリティのモードを autoLearn に設定します。

```
[Device-GigabitEthernet1/0/1] undo port-security port-mode
[Device-GigabitEthernet1/0/1] port-security max-mac-count 64
[Device-GigabitEthernet1/0/1] port-security port-mode autolearn
[Device-GigabitEthernet1/0/1] port-security mac-address security 1-1-2 vlan 1
```

2)　問題が解決しない場合、NEC に問い合わせてください。

目次

このセクションのページは **9-x-x** です。

8 章 User profile 8-1
8.1 ユーザプロファイルについて 8-1
8.2 ユーザプロファイルの前提条件 8-1
8.3 ユーザプロファイルの設定 8-1
8.4 ユーザプロファイルの表示と維持 8-1
8.5 ユーザプロファイルの設定例 8-2
8.5.1 ユーザプロファイルと QoS ポーリングの設定例 8-2

8章 User profile

8.1 ユーザプロファイルについて

ユーザプロファイルは、QoS ポリシーなどの一連のパラメータをユーザまたはユーザのクラスに対して定義します。ユーザプロファイルは、ユーザが別のインタフェースのネットワークに接続されているときに再利用できます。

ユーザプロファイルアプリケーションを使用すると、ユーザごとに柔軟にトラフィックポリシングを行うことができます。ユーザが認証を渡すたびに、サーバはユーザ用に指定されたユーザプロファイルの名前を装置に送信します。装置はユーザプロファイルのパラメータをユーザに適用します。

ユーザプロファイルは通常、ユーザごとのリソース割り当てに使用されます。たとえば、インタフェースベースのトラフィックポリシングでは、ユーザグループが使用できる帯域幅の総量が制限されます。ただし、ユーザプロファイルベースのトラフィックポリシングでは、単一のユーザで使用できる帯域幅の量が制限される場合があります。

8.2 ユーザプロファイルの前提条件

ユーザプロファイルは認証方式に対応しています。ユーザプロファイルの認証を設定する必要があります。サポートされている認証方式については、関連する認証モジュールの設定ガイドを参照してください。

8.3 ユーザプロファイルの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. ユーザプロファイルを作成し、ユーザプロファイルビューを入力する	**user-profile** *profile-name*（	―
3. 既存の QoS ポリシーをユーザプロファイルに適用する	**qos apply policy** *policy-name* { **inbound** | **outbound** }	デフォルト：QoSポリシーはユーザプロファイルに適用されません。 QoSポリシーについては、オペレーションマニュアルのセクション8 *ACL and QoS*を参照してください。

8.4 ユーザプロファイルの表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
指定したユーザプロファイルまたはすべてのユーザプロファイルの設定およびオンラインユーザ情報を表示します。	**display user-profile** [**name** *profile-name*] [**slot** *slot-number*]

8.5 ユーザプロファイルの設定例

8.5.1 ユーザプロファイルと QoS ポーリングの設定例

I. ネットワーク要件

図 8-1に示されているように、装置は認証および許可の効率のために、ドメイン **user** 内のユーザに対してローカル 802.1X認証を実行します。

次の要件を満たすように、デバイスにユーザプロファイルと QoS ポリシーを設定します。

- User A が 802.1 X認証に合格しても、User A は毎日 8:30 および 12:00 の間はインターネットにアクセスできません。
- User B は、802.1 X認証を通過した後のアップロード速度が 2Mbps です。
- User C は、802.1 X認証を通過した後のダウンロード速度が 4Mbps です。

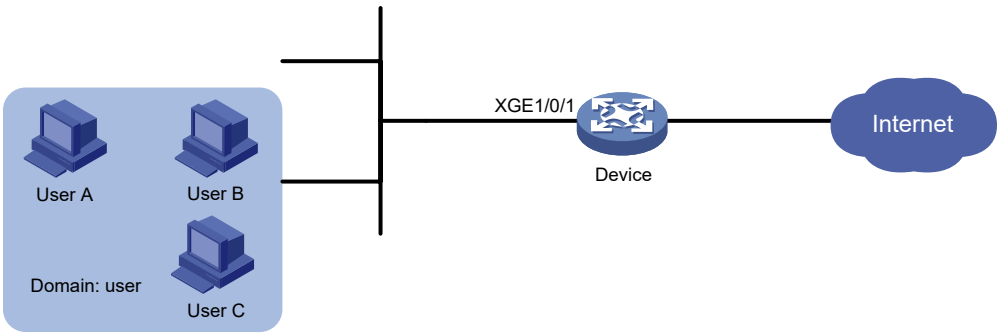


図 8-1 ネットワーク図

II. 設定手順

1)　User A の QoS ポリシーを設定します。

毎日 8:30 から 12:00 までの定期的な時間、範囲を作成します

```
<Device> system-view
[Device] time-range for_usera 8:30 to 12:00 daily
```

IPv4 基本 ACL2000 を作成し、**for_usera** の時間範囲内のすべてのパケットを照合するルールを設定します。

```
[Device] acl basic 2000
```

```
[Device-acl-basic-2000] rule permit time-range for_usera
[Device-acl-basic-2000] quit
```

for_usera という名前のトラフィッククラスを作成し、ACL 2000 を一致条件として使用します。

```
[Device] traffic classifier for_usera
[Device-classifier-for_usera] if-match acl 2000
[Device-classifier-for_usera] quit
```

for_usera という名前のトラフィック動作を作成し、deny アクションを設定します。

```
[Device] traffic behavior for_usera
[Device-behavior-for_usera] filter deny
[Device-behavior-for_usera] quit
```

for_usera という名前の QoS ポリシーを作成し、QoS ポリシー内で **for_usera** のトラフィッククラスと **for_usera** のトラフィック動作を関連付けます。

```
[Device] qos policy for_usera
[Device-qospolicy-for_usera] classifier for_usera behavior for_usera
[Device-qospolicy-for_usera] quit
```

2) User A のユーザプロファイルを作成し、QoS ポリシーをユーザプロファイルに適用します。

usera という名前のユーザプロファイルを作成します。

```
[Device] user-profile usera
```

QoS ポリシー **for_usera** をユーザプロファイル **usera** の受信方向に適用します。

```
[[Device-user-profile-usera] qos apply policy for_usera inbound
[Device-user-profile-usera] quit
```

3) User B のトラフィックレートを制限するための QoS ポリシーを設定します。

すべてのパケットに一致する **class** という名前のトラフィッククラスを作成します。

```
[Device] traffic classifier class
[Device-classifier-class] if-match any
[Device-classifier-class] quit
```

for_userb という名前のトラフィック動作を作成し、トラフィックポリシングアクションを設定します(CIR 2000 bps)。

```
[Device] traffic behavior for_userb
[Device-behavior-for_userb] car cir 2000
[Device-behavior-for_userb] quit
```

for _userb という名前の QoS ポリシーを作成し、**for _userb** 用のトラフィッククラス **class** とトラフィック動作を関連付けます。

```
[Device] qos policy for_userb
```

```
[Device-qospolicy-for_userb] classifier class behavior for_userb
[Device-qospolicy-for_userb] quit
```

4) User B のユーザプロファイルを作成し、QoS ポリシーをユーザプロファイルに適用します。

userb という名前のユーザプロファイルを作成します。

```
[Device] user-profile userb
```

for_userb の QoS ポリシーをユーザプロファイル **userb** の受信方向に適用します。

```
[Device-user-profile-userb] qos apply policy for_userb inbound
[Device-user-profile-userb] quit
```

5) User C のトラフィックレートを制限するための QoS ポリシーを設定します。

for_userc という名前のトラフィック動作を作成し、トラフィックポリシングアクションを設定します(CIR4000kbps)。

```
[Device] traffic behavior for_userc
[Device-behavior-for_userc] car cir 4000
[Device-behavior-for_userc] quit
```

for_userc という名前の QoS ポリシーを作成し、QoS ポリシーの **for_userc** にトラフィッククラス **class** とトラフィック動作を関連付けます。

```
[Device] qos policy for_userc
[Device-qospolicy-for_userc] classifier class behavior for_userc
[Device-qospolicy-for_userc] quit
```

6) User C のユーザプロファイルを作成し、QoS ポリシーをユーザプロファイルに適用します。

userc という名前のユーザプロファイルを作成します。

```
[Device] user-profile userc
```

for_userc 用の QoS ポリシーをユーザプロファイル **userc** の送信方向に適用します。

```
[Device-user-profile-userc] qos apply policy for_userc outbound
[Device-user-profile-userc] quit
```

7) ローカルユーザの設定をします。

usera という名前のローカルユーザを作成します。

```
[Device] local-user usera class network
New local user added.
```

ユーザ **usera** の場合は、パスワードを **a12345** に設定します。

```
[Device-luser-network-usera] password simple a12345
```

ユーザ **usera** に LAN アクセスサービスの使用を許可します。

```
[Device-luser-network-usera] service-type lan-access
```

ユーザプロファイル **usera** をユーザ **usera** の認証用ユーザプロファイルとして指定します。

```
[Device-luser-network-usera] authorization-attribute user-profile usera
[Device-luser-network-usera] quit
```

userb という名前のローカルユーザを作成します。

```
[Device] local-user userb class network
New local user added.
```

ユーザ **userb** のパスワードを **b12345** に設定します。

```
[Device-luser-network-userb] password simple b12345
```

ユーザ **userb** に LAN アクセスサービスの使用を許可します。

```
[Device-luser-network-userb] service-type lan-access
```

ユーザプロファイル **userb** をユーザ **userb** の認証ユーザプロファイルとして指定します。

```
[Device-luser-network-userb] authorization-attribute user-profile userb
[Device-luser-network-userb] quit
```

userc という名前のローカルユーザを作成します。

```
[Device] local-user userc class network
New local user added.
```

ユーザ **userc** のパスワードを **c12345** に設定します。

```
[Device-luser-network-userc] password simple c12345
```

ユーザ **userc** に LAN アクセスサービスの使用を許可します。

```
[Device-luser-network-userc] service-type lan-access
```

ユーザプロファイル **userc** をユーザ **userc** の認証ユーザプロファイルとして指定します。

```
[Device-luser-network-userc] authorization-attribute user-profile userc
[Device-luser-network-userc] quit
```

8)　ローカルユーザの認証、承認、およびアカウンティング方法を設定します。

```
[Device] domain user
[Device-isp-user] authentication lan-access local
[Device-isp-user] authorization lan-access local
[Device-isp-user] accounting login none
[Device-isp-user] quit
```

9)　802.1 Xの設定をします。

GigabitEthernet 1/0/1 で 802.1 Xを有効にします。

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] dot1x
```

ポートで MAC ベースのアクセス制御を有効にします。デフォルトでは、ポートは MAC ベースのアクセス制御を使用します。

```
[Device-GigabitEthernet1/0/1] dot1x port-method macbased
[Device-GigabitEthernet1/0/1] quit
```

802.1 Xをグローバルに有効にします。

```
[Device] dot1x
```

III. 設定の確認

3 人のユーザが 802.1 X認証を通過できること、および QoS ポリシーがこれらのユーザに有効であることを確認します。(詳細は省略します)

ユーザプロファイル情報を表示します。

```
<Device> display user-profile
  User-Profile: usera
    Inbound:
      Policy: for_usera

    slot 1:
      User -:
        Authentication type: 802.1X
        Network attributes:
          Interface    : GigabitEthernet1/0/1
          MAC address  : 6805-ca06-557b
          Service VLAN : 1

  User-Profile: userb
    Inbound:
      Policy: for_userb

    slot 1:
      User -:
        Authentication type: 802.1X
        Network attributes:
          Interface    : GigabitEthernet1/0/1
          MAC address  : 80c1-6ee0-2664
          Service VLAN : 1

  User-Profile: userc
    Outbound:
      Policy: for_userc

    slot 1:
      User -:
        Authentication type: 802.1X
        Network attributes:
          Interface    : GigabitEthernet1/0/1
          MAC address  : 6805-ca05-3efa
          Service VLAN : 1
```

目次

このセクションのページは **9-x-x** です。

9 章 パスワード管理..... 9-1
9.1 概要..... 9-1
9.1.1 パスワードの設定..... 9-1
9.1.2 パスワードのアップデートと有効期限の終了..... 9-3
9.1.3 ユーザログイン管理..... 9-4
9.1.4 すべての形式でのパスワードの非表示..... 9-5
9.1.5 ロギング..... 9-5
9.2 制限とガイドライン..... 9-5
9.3 パスワード管理設定作業リスト..... 9-6
9.4 パスワード管理の有効化..... 9-6
9.5 グローバルパスワード管理パラメータの設定..... 9-7
9.6 ユーザグループパスワード管理パラメータの設定..... 9-8
9.7 ローカルユーザパスワード管理パラメータの設定..... 9-9
9.8 super パスワード管理パラメータの設定..... 9-10
9.9 パスワード管理の表示と維持..... 9-10
9.10 パスワード管理の設定例..... 9-11
9.10.1 パスワード管理の設定例..... 9-11

9章 パスワード管理

9.1 概要

パスワード管理は、以下の機能ができます。

- 装置管理ユーザのログインと super パスワードのセットアップ、終了、アップデートを管理します。
- あらかじめ定義されたポリシーにもとづいたユーザログインステータスを制御します。

装置管理ユーザは、ローカルユーザの一種です。ローカルユーザについての詳細は、オペレーションマニュアルのセクション 9 *セキュリティ*”*AAA*”を参照してください。super パスワードについては、オペレーションマニュアルのセクション 1 *はじめに*”*RBAC*”を参照してください。

🕮 **メモ：**

パスワード管理機能はデフォルトで無効（**undo password-control enable**）に設定されていますが、以下に示すコマンドはパスワード管理機能が無効の場合でも動作します（以下はデフォルトの設定状態を示します）。以下に示すコマンド以外は、パスワード管理機能を有効にすると動作します。

- password-control length enable：文字列の最小値制限有効
- password-control length 10：10 文字以上の文字列（ローカルユーザ）
- password-control composition enable：文字タイプ数の最小値制限有効
- password-control composition type-number 2：最低 2 種類の文字タイプ数（ローカルユーザ）
- password-control complexity user-name check：パスワードにユーザ名と同じ文字列使用不可
- password-control super length 10：10 文字以上の文字列（super ユーザ）
- password-control super composition type-number 2：最低 2 種類の文字タイプ数（super ユーザ）

9.1.1 パスワードの設定

I. 最小パスワード長

ユーザパスワードの最小の長さを設定することができます。ユーザが最小パスワード長よりも短いパスワードを入力した場合、システムはパスワードを拒否します。

II. パスワード設定のポリシー

パスワードは以下のタイプの組み合わせで設定されます。

- A～Z の大文字の英字
- a～z の小文字の英字
- 0～9 の数字
- 特殊文字

表 9-1 特殊文字

文字名	記号	文字名	記号
アンパサンド	&	アポストロフィー	'
アスタリスク	*	アットマーク	@
逆クォート	`	バックスラッシュ	\
半角スペース	ー	キャロット	^
コロン	:	コンマ	,
ダラーマーク	$	ドット	.
イコール	=	感嘆符	!
左アングルブラケット	<	左波括弧	{
左角括弧	[	左丸括弧	(
ハイフン	-	パーセント	%
プラス	+	シャープ	#
ダブルクォーテーション	"	右アングルブラケット	>
右波括弧	}	右角括弧	]
右丸括弧	)	セミコロン	;
スラッシュ	/	チルダ	~
アンダーライン	_	垂直バー	|

システムのセキュリティ要件に応じて、パスワードに含めなくてはいけない文字タイプの最小数と、各種類の文字の最小数を設定することができます。表 9-2にパスワード設定のポリシーを示します。

表 9-2 パスワード設定のポリシー

パスワード組み合わせレベル	文字タイプの最小数	各タイプの最小文字数
Level 1	1	1
Level 2	2	1
Level 3	3	1
Level 4	4	1

すべての組み合わせレベルをパスワードとして使用できます。

ユーザがパスワードを設定あるいは変更するとき、システムはパスワードが要件の組み合わせを満たしているか確認します。満たしていない場合、パスワードの設定あるいは変更操作は失敗します。

III. パスワードの複雑性のポリシー

ユーザ名や連続した文字などのような文字が含まれる複雑でないパスワードは、不正に解読されやすくなります。より高いセキュリティを持たせるため、すべてのユーザのパスワードが相対的に複雑となっているかを確認するようにポリシーを設定することができます。ポリシーが設定され、ユーザがパスワードを設定したとき、パスワードの複雑性を確認します。パスワードがポリシーに適合しない場合、ユーザのパスワード設定は失敗します。

パスワードの複雑性の要件を以下に示します。

- パスワードはユーザ名あるいはユーザ名の逆の順番を含むことができません。たとえば、ユーザ名が **abc** であるとき、**abc982** や **2cba** のようなパスワードはポリシーに適合しません。
- 文字あるいは数字が 3 回以上連続して続くことはできません。たとえば、**a111** のパスワードはポリシーに適合しません。

9.1.2 パスワードのアップデートと有効期限の終了

I. パスワードのアップデート

この機能は、ユーザがパスワードを変更する最小間隔を設定します。ユーザがパスワードを変更するためにログインした際、最後にパスワードを変更してからの間隔が短い場合、システムはパスワードの変更を拒否します。たとえばパスワードを変更する最小間隔を 48 時間に設定した場合、ユーザが 48 時間以内に 2 回パスワードを変更することはできません。

この最小間隔は、以下の場合影響がありません。

- ユーザが最初にログインした後にパスワードを変更します。
- パスワードの有効期限が終了した後にパスワードを変更します。

II. パスワードの終了

パスワードの有効期限の終了は、ユーザのパスワードのライフサイクルを変更させるようにします。パスワードの有効期限が終了した後、ユーザはパスワードの変更が必要となります。

ユーザが期限の切れたパスワードでログインした場合、システムはエラーメッセージを表示します。新しいパスワードを入力するように表示し、新しいパスワードを確認するため、再度新しいパスワードを入力するように表示します。新しいパスワードは正式なもので、ユーザが再入力したとき、最初に入力したパスワードと同一のパスワードを正確に入力する必要があります。

Web ユーザ、Telnet ユーザ、SSH ユーザ、コンソールユーザは、自身のパスワードを変更することができます。管理者は FTP ユーザ用にパスワードを変更する必要があります。

III. パスワード有効期限の終了までの早期通知

ユーザがログインするとき、システムは、パスワードの有効期限が少しで終了となるかどうかを確認します。有効期限が終了する場合、パスワードの変更を行うように通知します。

- ユーザがポリシーに適した新しいパスワードを適用した場合、新しいパスワードと時間を記録します。
- ユーザがパスワードを変更しない、あるいは変更に失敗した場合、システムは現在のパスワードを使用したユーザのログインを許可します。

Web ユーザ、Telnet ユーザ、SSH ユーザ、コンソールユーザは、自身のパスワードを変更することができます。管理者は FTP ユーザ用にパスワードを変更する必要があります。

IV. 有効期限が終了したパスワードを使用したログイン

パスワードの有効期限が終了した後、ユーザが、指定した期間内に設定した回数のログインができるように設定することができます。たとえば、パスワードの有効期限が終了した後、最大 3 回、15 日間内にログインできるように設定した場合、ユーザは、パスワードの有効期限が終了した後、15 日以内に 3 回までログインすることができます。

V. パスワード履歴

この機能を有効にすると、システムはユーザが使用したパスワードを記録します。ユーザがパスワードを変更するとき、システムは現在のパスワードと、パスワード履歴にある記録されたパスワードを確認します。新しいパスワードは現在のパスワードとパスワード履歴に記録されたパスワードと、少なくとも 4 文字以上変更する必要があり、4 文字は互いに異なる必要があります。そうでなければ、エラーメッセージを表示し、パスワードは変更されません。

各ユーザ用でパスワード履歴に保持するパスワードの最大数を設定することができます。パスワード履歴の最大数を超えるとき、新しいパスワードが最初のパスワードに上書きされます。

装置管理ユーザの現在のログインパスワードはパスワード履歴に記録されません。これは装置管理ユーザのパスワードは暗号化テキストで保存され、プレーン（平文）テキストに回復することができないためです。

9.1.3 ユーザログイン管理

I. 初回ログイン

グローバルでパスワード管理機能が有効であるとき、ユーザはシステムにアクセスする前に初回ログイン時にパスワードを変更する必要があります。この状況では、パスワードの変更は最小変更間隔の設定に関係なく設定します。

II. ログイン試行制限

連続してログインの試行の失敗を制限することで、パスワードを類推することを効果的に防ぐことができます。

ログイン試行制限は FTP、Web および VTY ユーザに適用します。以下のタイプのユーザには適用しません。

- 存在しないユーザ（装置で設定されていないユーザ）
- コンソールポートを通して装置にログインするユーザ

ユーザがログインに失敗した場合、ユーザのアカウントとユーザの IP アドレスをパスワード管理のブラックリストに追加します。ユーザが最大連続試行回数を超えてログインに

失敗した場合、ログイン試行回数の制限によりユーザとユーザアカウントを以下の方法で制限します。

- パスワード管理ブラックリストから手動でユーザを削除するまでユーザアカウントを無効にします。
- ユーザがユーザアカウントの継続使用を許可します。ユーザがこのアカウントを使用して装置に正常にログインしたとき、ユーザの IP アドレスとユーザアカウントはパスワード管理のブラックリストから削除されます。
- 一定の時間、ユーザアカウントを無効にします。

ユーザは以下の状況のどちらかの状態の時、ログインを行うアカウントを使用することができます。

- □ ログインの試行を無効にする時間が終了したとき、アカウントを使用することができます。
- □ ログインの試行を無効にする時間が終了する前に、パスワード管理のブラックリストから手動でアカウントが削除されたとき、アカウントを使用することができます。

🕮 **メモ：**

アカウントはブラックリストに追加されたユーザのみロックされます。他のユーザはアカウントを使用することができます。ブラックリストに追加されたユーザは他のユーザアカウントを使用することができます。

III. 最大アカウントアイドルタイム

ユーザアカウントの最大アカウントアイドルタイムを設定することができます。期間内にログインしないアカウントは、無効なアカウントで無効となります。

9.1.4 すべての形式でのパスワードの非表示

セキュリティ目的のため、ユーザがパスワードを入力したとき、表示されません。

9.1.5 ロギング

システムは、すべての正常なパスワードの変更イベントと、ユーザがパスワード管理ブラックリストへ追加するイベントをロギングします。

9.2 制限とガイドライン

⚠ **重要　：**

グローバルでパスワード管理機能を正常に有効にするため、装置に装置管理ユーザがログインすることを許可し、装置に十分な記憶容量があることを確認してください。

パスワード管理機能は、いくつかの異なる view で設定することができます。異なる view は異なる機能をサポートします。異なる view の設定、異なる目的のために、以下に示すような設定範囲を持ちます。

- super パスワードの設定は、super パスワードのみ適用されます。
- local user view での設定は、ローカルユーザのパスワードのみに適用します。
- local user view でユーザのパスワード管理ポリシーが設定されていない場合、user group view での設定はユーザグループのローカルユーザのパスワードに適用します。
- local user view と user group view の両方でユーザのパスワード管理ポリシーが設定されていない場合、system view でのグローバルの設定はすべてのユーザグループのローカルユーザのパスワードに適用します。

ローカルユーザパスワードでは、より小さい設定範囲の設定が高い優先度を持ちます。

グローバルパスワード管理が有効の場合、ローカルユーザ用に設定されたパスワードは表示されず、パスワードは現在の設定に保存されません。グローバルパスワード管理が無効の場合、ローカルユーザ用に設定されたパスワードは現在の設定で回復されます。現在の設定を表示するには、**display current-configuration** コマンドを使用します。

9.3 パスワード管理設定作業リスト

以下にパスワード管理を設定するための作業リストを示します。

作業リスト
(必須設定項目) パスワード管理の有効化
(オプション設定項目) グローバルパスワード管理パラメータの設定
(オプション設定項目) ユーザグループパスワード管理パラメータの設定
(オプション設定項目) ローカルユーザパスワード管理パラメータの設定
(オプション設定項目) superパスワード管理パラメータの設定

9.4 パスワード管理の有効化

I. 概要

グローバルでパスワード管理機能を有効にすると、すべてのパスワード管理の設定が適用されます。指定したパスワード管理機能を有効にするには、独自のパスワード制御機能を有効にします。

II. 制限とガイドライン

グローバルパスワード管理をイ有効にした後は、次の制約事項および注意事項に従ってください。

- 対応する **display** コマンドを使用して装置管理者用のパスワードと superパスワードを表示することはできません。ただし、ネットワークアクセス用設定のユーザパスワードは表示できます。
- 装置管理ユーザ用に設定する最初のパスワードには、4 文字以上の異なる文字を含める必要があります。

III. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. グローバルパスワード制御機能を有効にする	**password-control enable**	デフォルト：無効
3. (オプション設定項目) 指定したパスワード機能を有効にする	**password-control** { **aging** | **composition** | **history** | **length** } **enable**	デフォルト：4つのすべてのパスワード管理機能は有効です。

9.5 グローバルパスワード管理パラメータの設定

I. 制限とガイドライン

グローバルパスワード管理パラメータを system view で設定すると、すべての装置管理ローカルユーザに適用されます。

パスワードエージング時間、最小パスワード長、およびパスワード設定ポリシーは、system view、user group view、および local user view で設定できます。アプリケーションスコープが小さい範囲でのパスワードの設定が高い優先度を持ちます。ローカルユーザの場合は、local user view で設定されたパスワード設定が最も優先され、system view のグローバル設定が最も優先度が低くなります。

password-control login-attempt コマンドは、即座に適用され、パスワード管理ブラックリストにあるユーザに適用させることができます。他のパスワード管理設定は、既にログインしているユーザ、あるいは設定したパスワードに適用されません。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. パスワードの有効期限を設定する	**password-control aging** *aging-time*	デフォルト：90日
3. パスワードアップデートの最小間隔を設定する	**password-control update-interval** *interval*	デフォルト：24時間
4. 最小パスワード長を設定する	**password-control length** *length*	デフォルト：10文字
5. パスワード設定ポリシーを設定する	**password-control composition type-number** *type-number* [**type-length** *type-length*]	デフォルト：パスワードは少なくとも2種類の文字と各タイプに1文字以上を含む必要があります。
6. パスワードの複雑性のポリシーを設定する	**password-control complexity** { **same-character** | **user-name** } **check**	デフォルト： **same-character** は無効、**user-name**は有効
7. 各ユーザのパスワード履歴の最大数を設定する	**password-control history** *max-record-number*	デフォルト：4

操作	コマンド	補足
8. ユーザが試行回数後にログインに失敗したときのアクションとログイン最大試行回数を設定する	**password-control login-attempt** *login-times* [**exceed** { **lock** | **lock-time** *time* | **unlock** }]	デフォルト： 最大試行回数：3 アクション: ユーザが試行回数後にログインに失敗したとき、1分間ログインの試行をブロックします。
9. ユーザに通知されるパスワードの有効期限までの日数を設定する	**password-control alert-before-expire** *alert-time*	デフォルト：7日
10. パスワードの有効期限が終了した後、ユーザがログインできる最大日時と最大回数を設定する	**password-control expired-user-login delay** *delay* **times** *times*	デフォルト： 最大日時：30日 最大回数：3回
11. 最大アカウントアイドルタイムを設定する	**password-control login idle-time** *idle-time*	デフォルト：90日 ユーザアカウントがこの期間アイドル状態になると、アカウントは無効になり、装置へのログインに使用できなくなります。アカウントのアイドルタイムの制限を無効にするには、アイドルタイムの値を0に設定します。
12. 初回ログイン時のパスワード変更機能を無効にする	**undo password-control change-password first-login enable**	デフォルト：有効

9.6 ユーザグループパスワード管理パラメータの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. ユーザグループを作成し、user group view に移行する	**user-group** *group-name*	デフォルト: ユーザグループは存在しません。ユーザグループを設定する方法については、オペレーションマニュアルのセクション 9 *セキュリティ*”*AAA*”を参照してください。
3. パスワードの有効期限を設定する	**password-control aging** *aging-time*	デフォルト: グローバルパスワードの有効期限と同一です。
4. 最小パスワード長を設定する	**password-control length** *length*	デフォルト: グローバル最小パスワード長と同一です。
5. パスワード設定ポリシーを設定する	**password-control composition type-number** *type-number* [**type-length** *type-length*]	デフォルト: グローバルパスワード設定ポリシーと同一です。
6. パスワードの複雑性のポリシーを設定する	**password-control complexity** { **same-character** | **user-name** } **check**	デフォルト: グローバルパスワードの複雑性のポリシーと同一です。

操作	コマンド	補足
7. ユーザが試行回数後にログインに失敗したときのアクションとログイン最大試行回数を設定する	**password-control login-attempt** *login-times* [**exceed** { **lock** | **lock-time** *time* | **unlock** }]	デフォルト : グローバルパスワードのログイン試行ポリシーと同一です。

9.7 ローカルユーザパスワード管理パラメータの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. 装置管理ユーザを作成し、local user view に移行する	**local-user** *user-name* **class manage**	ローカルユーザパスワード管理は、ネットワークアクセスユーザではなく、装置管理ユーザに適用されます。ローカルユーザを設定する方法については、オペレーションマニュアルのセクション9 *セキュリティ”AAA”* を参照してください。
3. パスワードの有効期限を設定する	**password-control aging** *aging-time*	デフォルト : ローカルユーザが属しているユーザグループの有効期限と同一です。ユーザグループの有効期限が設定されていない場合、グローバルの設定が適用されます。
4. 最小パスワード長を設定する	**password-control length** *length*	デフォルト : ローカルユーザが属しているユーザグループの最小パスワード長と同一です。ユーザグループの最小パスワード長が設定されていない場合、グローバルの設定が適用されます。
5. パスワード設定ポリシーを設定する	**password-control composition type-number** *type-number* [**type-length** *type-length*]	デフォルト : ローカルユーザが属しているユーザグループのパスワード設定ポリシーと同一です。ユーザグループのパスワード設定ポリシーが設定されていない場合、グローバルの設定が適用されます。
6. パスワードの複雑性のポリシーを設定する	**password-control complexity** { **same-character** | **user-name** } **check**	デフォルト : ローカルユーザが属しているユーザグループのパスワードの複雑性のポリシーと同一です。ユーザグループのパスワードの複雑性のポリシーが設定されていない場合、グローバルの設定が適用されます。

操作	コマンド	補足
7. ユーザが試行回数後にログインに失敗したときのアクションとログイン最大試行回数を設定する	**password-control login-attempt** *login-times* [**exceed** { **lock** | **lock-time** *time* | **unlock** }]	ローカルユーザが所属するユーザグループの設定と同一です。ユーザグループでログイン試行ポリシーが設定されていない場合、グローバルの設定が適用されます。

9.8 superパスワード管理パラメータの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. パスワードの有効期限を設定する	**password-control super aging** *aging-time*	デフォルト：90日
3. 最小パスワード長を設定する	**password-control super length** *length*	デフォルト：10文字
4. パスワード設定ポリシーを設定する	**password-control super composition type-number** *type-number* [**type-length** *type-length*]	デフォルト：superパスワードは少なくとも2種類の文字と各タイプに1文字以上を含む必要があります。

9.9 パスワード管理の表示と維持

すべての view で **display** コマンドを実行でき、user view で **reset** コマンドを実行できます。

操作	コマンド
パスワード管理の設定を表示する	**display password-control** [**super**]
パスワード管理ブラックリストのユーザ情報を表示する	**display password-control blacklist** [**user-name** *name* | **ip** *ipv4-address* | **ipv6** *ipv6-address*]
パスワード管理ブラックリストからユーザを削除する	**reset password-control blacklist** [**user-name** *name*]
パスワード履歴を削除する	**reset password-control history-record** [**user-name** *user-name* | **super** [**role** *role-name*]]

🕮 **メモ:**

reset password-control history-record コマンドは、パスワード履歴機能が無効になったとき、1つあるいはすべてのユーザのパスワード履歴を削除することができます。

9.10 パスワード管理の設定例

9.10.1 パスワード管理の設定例

I. ネットワーク要件

グローバルパスワード管理ポリシーを以下のように設定します。

- パスワードは少なくとも 16 文字が必要です。
- パスワードは少なくとも 4 種類以上の文字タイプが必要で各文字タイプに 4 文字以上が必要です。
- FTP あるいは VTY ユーザが 2 回連続してパスワードの試行に失敗すると、ログインの試行を恒久的に禁止します。
- ユーザはパスワードの有効期限後に、60 日内で 5 回ログインすることができます。
- パスワードの有効期限を 30 日に設定します。
- 最小パスワードアップデート間隔を 36 時間に設定します。
- 最大アカウントアイドルタイムを 30 日に設定します。
- パスワードはユーザ名、ユーザ名の逆の順番を含むことができません。
- パスワードに 3 回以上連続した文字を禁止します。

ユーザロール **network-operator** の super パスワード管理ポリシーを以下のように設定します。

- super パスワードは少なくとも 24 文字が必要です。
- super パスワードは少なくとも 4 種類以上の文字タイプが必要で各文字タイプに 5 文字以上が必要です。

ローカル Telnet ユーザ **test** のパスワード管理ポリシーを以下のように設定します。

- パスワードは少なくとも 24 文字が必要です。
- パスワードは少なくとも 4 種類以上の文字タイプが必要で各文字タイプに 5 文字以上が必要です。
- パスワードの有効期限を 20 日に設定します。

II. 設定手順

グローバルにパスワード管理機能を有効にします。

```
<Switch> system-view
[Switch] password-control  enable
```

ユーザが 2 回連続してパスワードの試行に失敗すると、ログインの試行を恒久的に禁止します。

```
[Switch] password-control  login-attempt  2 exceed lock
```

パスワードの有効期限を 30 日に設定します。

```
[Switch] password-control  aging  30
```

グローバルの最小パスワード長を 16 に設定します。

```
[Switch] password-control  length  16
```

最小パスワードアップデート間隔を 36 時間に設定します。

```
[Switch] password-control update-interval 36
```

パスワードの有効期限が終了した後、ユーザが 60 日内で 5 回ログインできるように設定します。

```
[Switch] password-control expired-user-login delay 60 times 5
```

最大アカウントアイドルタイムを 30 日に設定します。

```
[Switch] password-control login idle-time 30
```

ユーザ名、ユーザ名の逆の順番を含むパスワードを拒否するように設定します。

```
[Switch] password-control complexity user-name check
```

パスワードに 3 回以上連続した文字を禁止するように指定します。

```
[Switch] password-control complexity same-character check
```

グローバルのパスワードを、少なくとも 4 種類以上の文字タイプで、各文字タイプに 4 文字以上が含まれるように指定します。

```
[Switch] password-control composition type-number 4 type-length 4
```

super パスワードの最小パスワード長を 24 に設定します。

```
[Switch] password-control super length 24
```

super パスワードを、少なくとも 4 種類以上の文字タイプで、各文字タイプに 5 文字以上が含まれるように指定します。

```
[Switch] password-control super composition type-number 4 type-length 5
```

ユーザロール **network-operator** に切り替える super パスワードをプレーンテキストで **123456789ABGFTweuix@#$%!**に設定します。

```
[Switch] super password role network-operator simple 123456789ABGFTweuix@#$%!
```

装置管理ユーザ **test** を作成します。

```
[Switch] local-user test class manage
```

ユーザのサービスタイプを **Telnet** に設定します。

```
[Switch-luser-manage-test] service-type telnet
```

ローカルユーザの最小パスワード長を 24 に設定します。

```
[Switch-luser-manage-test] password-control length 24
```

ローカルユーザのパスワードを、少なくとも 4 種類以上の文字タイプで各文字タイプに 5 文字以上が含まれるように指定します。

```
[Switch-luser-manage-test] password-control composition type-number 4 type-length 5
```

ローカルユーザのパスワードの有効期限を 20 日に設定します。

```
[Switch-luser-manage-test] password-control aging 20
```

ローカルユーザのパスワードをインタラクティブモードで設定します。

```
[Switch-luser-manage-test] password
Password:
```

```
Confirm :
Updating user information. Please wait ... ...
[Switch-luser-manage-test]  quit
```

III. 設定の確認

グローバルパスワード管理の設定を表示します。

```
<Switch> display password-control
Global password control configurations:
 Password control:                       Enabled
 Password aging:                         Enabled (30 days)
 Password length:                        Enabled (16 characters)
 Password composition:                  Enabled (4 types, 4 characters per type)
 Password history:                       Enabled (max history record:4)
 Early notice on password expiration:  7 days
 Maximum login attempts:                 2
 Action for exceeding login attempts:  Lock
 Minimum interval between two updates: 36 hours
 User account idle time:                 30 days
 Logins with aged password:              5 times in 60 days
 Password complexity:                    Enabled (username checking)
                                         Enabled (repeated characters checking)
```

super パスワードのパスワード管理の設定を表示します。

```
<Switch> display password-control  super
 Super password control configurations:
 Password aging:                         Enabled (90 days)
 Password length:                        Enabled (24 characters)
 Password composition:                  Enabled (4 types, 5 characters per type)
```

ローカルユーザ **test** のパスワード管理設定を表示します。

```
<Switch> display local-user user-name  test class manage
Total 1 local users matched.

Device management user test:
  State:                     Active
  Service type:              Telnet
  User group:                system
  Bind attributes:
  Authorization attributes:
    Work directory:          flash:
    User role list:          network-operator
  Password control configurations:
    Password aging:          Enable (20 days)
    Password length:         Enable (24 characters)
    Password composition:    Enable (4 types, 5 characters per type)
```

目次

このセクションのページは **9-x-x** です。

10 章 公開鍵 10-1
10.1 概要 10-1
10.2 ローカル鍵ペアの作成 10-1
10.2.1 設定ガイドライン 10-1
10.2.2 設定手順 10-2
10.3 ローカルホスト公開鍵の分配 10-2
10.3.1 指定したフォーマットのホスト公開鍵のファイルへのエクスポート 10-3
10.3.2 ホスト公開鍵の表示 10-3
10.4 ローカル鍵ペアの削除 10-3
10.5 ピア公開鍵の設定 10-4
10.5.1 公開鍵ファイルからピアへのホスト公開鍵のインポート 10-4
10.5.2 ピアの公開鍵の入力 10-4
10.6 公開鍵の表示と維持 10-5
10.7 公開鍵の設定例 10-5
10.7.1 ピアのホスト公開鍵の入力例 10-5
10.7.2 公開鍵ファイルからの公開鍵のインポート例 10-7

10章 公開鍵

10.1 概要

この章では、以下の非対称鍵アルゴリズムの公開鍵の管理について記載します。

- RSA（Revest-Shamir-Adleman）アルゴリズム
- DSA（Digital Signature Algorithm）アルゴリズム

SSH、SSL、PKI を含む多くのセキュリティアプリケーションは、図 10-1に示すように 2 つの群の間でセキュリティの通信を行うため、非対称鍵アルゴリズムを使用します。暗号化と複号化を行うため、非対象鍵アルゴリズムは、2 つの分離した鍵（公開鍵と秘密鍵）を使用します。対称鍵は 1 つの鍵のみを使用します。

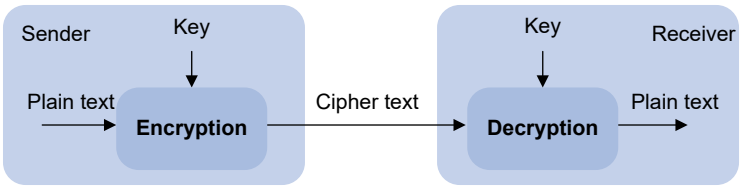


図 10-1 暗号化と複号化

鍵の所有者はプレーンテキスト（平文）で公開鍵を配布することができますが、秘密鍵を保持する必要があります。たとえ攻撃者がアルゴリズムと公開鍵を知っていたとしても秘密鍵を計算することは、数学上、実現不可能です。

セキュリティアプリケーションは以下の目的で非対象鍵アルゴリズムを使用します。

- **暗号化と複号化** – 公開鍵の受信者が情報を暗号化するために公開鍵を使用し、秘密鍵の所有者のみが情報を複号化できます。
- **デジタル署名** – 鍵の所有者は送信する”署名”情報に秘密鍵を使用します。受信者は情報が信頼できるか確認するため、送信者の公開鍵で情報を複号化します。

RSA、DSA はすべてのデジタル署名を実行できますが、RSA のみが暗号化と複号化を行うことができます。

非対称鍵アルゴリズムは、安全でないネットワークでセキュアな鍵の配布を行うことができますが、非対称鍵アルゴリズムのセキュリティの強度は、対称鍵アルゴリズムの鍵の長さに依存します。

10.2 ローカル鍵ペアの作成

10.2.1 設定ガイドライン

ローカル鍵ペアを作成するとき、以下のガイドラインに従います。

- 鍵アルゴリズムはセキュリティアルゴリズムで要求されたアルゴリズムと同一にする必要があります。
- RSA または DSA 鍵ペアを作成する際に、鍵の長さは適切に設定してください。鍵の長さが長いと高いセキュリティとなりますが、鍵を作成する時間も長くなります。
- 鍵ペアの名前を割り当てない場合、システムは鍵ペアにデフォルトの名前を割り当て、鍵ペアを default としてマーキングします。デフォルトの名前を別の鍵ペアに割り当てることができますが、鍵ペアを default としてマーキングしません。鍵ペアの名前は、同じ鍵アルゴリズムを使用する鍵ペア間で一意にする必要があります。もし名前が重複している場合、存在する鍵ペアに上書きしていいか確認メッセージが表示されます。
- 鍵ペアは自動で保存され、装置の再起動が行われても削除されません。

表 10-1 非対称鍵ペアの異なるタイプの比較

タイプ	鍵ペアの数	鍵の長さ	推奨値
RSA	● 鍵ペアの名前を指定する場合、ホスト鍵ペアを作成します。 ● 鍵ペアの名前を指定しない場合、1つのサーバ鍵ペアと1つのホスト鍵ペアを作成します。鍵ペアの名前はデフォルト名です。	範囲：512～4096ビット デフォルト：1024ビット	少なくとも768ビットにしてください。
DSA	1つのホスト鍵ペアを作成します。	範囲：512～2048ビット デフォルト：1024ビット	少なくとも768ビットにしてください。

🕮 **メモ：**

SSH 1.5 のみが RSA サーバ鍵ペアを使用します。

10.2.2 設定手順

以下にローカル鍵ペアを作成する設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. ローカル DSA あるいは RSA 鍵ペアを作成する	**public-key local create** { **dsa** | **rsa** } [**name** *key-name*]	デフォルト：作成なし

10.3 ローカルホスト公開鍵の分配

ピアの装置が以下のことを行えるようにピアの装置にローカルホスト公開鍵を分配する必要があります。

- 公開鍵を使用して、ローカル装置に送信された情報を暗号化します。
- ローカル装置によって署名されたデジタル署名を認証します。

ローカルホスト公開鍵を分配するためには以下の方法を行います。

1)　鍵を記録あるいはファイルにエクスポートします。
2)　鍵を転送します。たとえばFTP や TFTP を使用します。

ローカルホスト公開鍵を分配するには最初に鍵をエクスポートあるいは表示します。

- ホスト公開鍵をエクスポートします。
  - □　ホスト公開鍵をファイルにエクスポートします。
  - □　ホスト公開鍵をモニタ画面に表示し、表示したデータをファイルに保存します。

  ホスト公開鍵をファイルにエクスポートした後、ピアの装置にファイルを転送します。ピアの装置ではファイルからホスト公開鍵をインポートします。
- ホスト公開鍵を表示します。

ホスト公開鍵を表示した後、鍵を記録します。たとえば、フォーマットされていないファイルにコピーします。ピアの装置で鍵を正確に入力する必要があります。

10.3.1 指定したフォーマットのホスト公開鍵のファイルへのエクスポート

操作	コマンド
1.　system view に移行する	**system-view**
2.　指定したフォーマットのローカルホスト公開鍵をファイルへエクスポートする	● RSAホスト公開鍵をエクスポートする： **public-key local export rsa** [**name** *key-name*] { **openssh** | **ssh1** | **ssh2** } [*filename*] ● DSAホスト公開鍵をエクスポートする： **public-key local export dsa** [**name** *key-name*] { **openssh** | **ssh2** } [*filename*]

10.3.2 ホスト公開鍵の表示

すべての view で **display** コマンドを実行することができます。

操作	コマンド
ローカルRSA公開鍵を表示する	**display public-key local rsa public** [**name** *key-name*]
ローカルDSA公開鍵を表示する	**display public-key local dsa public** [**name** *key-name*]

🕮 **メモ：**

ピアの装置に RSAサーバの公開鍵の serverkey（デフォルト）を配布しないでください。

10.4 ローカル鍵ペアの削除

以下の状況が発生した後、ローカル非対称鍵ペアを削除し、新しいペアを生成する必要があります。

- 不正侵入が発生した場合
- 装置の記憶媒体を交換した場合

- ローカル証明書の有効期限が切れた場合

以下にローカル鍵ペアを削除する設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. ローカル鍵ペアを削除する	**public-key local destroy** { **dsa** | **rsa** } [**name** *key-name*]	ー

10.5 ピア公開鍵の設定

以下の方法を用いてピアのホスト公開鍵を設定することができます。

- 公開鍵ファイルから公開鍵をインポートします。（推奨）
- 公開鍵を手動で設定します。（鍵データを入力またはコピー）

10.5.1 公開鍵ファイルからピアへのホスト公開鍵のインポート

ホスト公開鍵をインポートする前に、ピアの装置にホスト公開鍵がエクスポートされており、ピアの装置からファイルを取得していることを確認してください。ホスト公開鍵のエクスポートについては、オペレーションマニュアルのセクション 9 *セキュリティ”公開鍵”の”ローカルホスト公開鍵の分配”*を参照してください。

鍵をインポートしたのち、システムは自動的に公開鍵を PKCS（Public Key Cryptography Standards）フォーマットの文字列へ変換します。

以下に公開鍵ファイルからピアへのホスト公開鍵のインポート手順を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. 公開鍵ファイルからピアのホスト公開鍵をインポートする	**public-key peer** *keyname* **import sshkey** *filename*	デフォルト : ピアのホスト公開鍵は存在しません。

10.5.2 ピアの公開鍵の入力

ホスト公開鍵をインポートする前に、ピアの装置にホスト公開鍵が表示されており、ホスト公開鍵が記録されていることを確認してください。

display public-key local public コマンドを使用して、公開鍵を表示してください。他の方法で表示された公開鍵のフォーマットは、正確ではない場合があります。

ホスト公開鍵が正しいフォーマットでない場合、システムはホスト公開鍵を廃棄し、エラーメッセージを表示します。ホスト公開鍵が正しいフォーマットである場合、システムはホスト公開鍵を保存します。

記録されたピアのホスト公開鍵のフォーマットをサポートしているか不明な場合、ピアのホスト公開鍵を入力する方法ではなく、ホスト公開鍵ファイルからインポートする方法を行ってください。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. ピアの公開鍵の名前を指定し、public key view に移行する	**public-key peer** *keyname*	デフォルト : ピアのホスト公開鍵は存在しません。
3. 鍵を入力あるいはコピーする	ー	空白と改行は使用できますが保存しません。
4. system view に戻る	**peer-public-key end**	public key viewから戻ると、自動的に公開鍵を保存します。

10.6 公開鍵の表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
ローカル公開鍵を表示する	**display public-key local** { **dsa** | **rsa** } **public**
ピアのホスト公開鍵を表示する	**display public-key peer** [**brief** | **name** *publickey-name*]

10.7 公開鍵の設定例

10.7.1 ピアのホスト公開鍵の入力例

I. ネットワーク要件

図 10-2に示すように、不正なアクセスを防止するため、Device B は Device A をデジタル署名によって認証します。Device B 上で認証パラメータを設定する前に、Device B 上で Device A の公開鍵を設定します。

- Device A の認証に RSA の非対称鍵アルゴリズムを使用するために Device B を設定します。
- Device B 上で、Device A の公開鍵ペアのホスト公開鍵を手動で指定します。

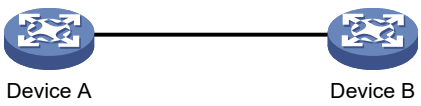


図 10-2 ネットワーク図

II. 設定手順

1)　Device A を設定します。

Device A にデフォルト名のローカル RSA 鍵ペアを作成し、鍵の長さをデフォルトの 1024 ビットに設定します。

```
<DeviceA> system-view
```

```
[DeviceA] public-key local create rsa
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
................++++++
....................................++++++
.....++++++++
.............++++++++
Create the key pair successfully.
```

すべての RSA 鍵ペアの公開鍵を表示します。

```
[DeviceA] display public-key local rsa public
=============================================
Key name: hostkey (default)
Key type: RSA
Time when key pair created: 16:48:31 2011/05/12
Key code:
   30819F300D06092A864886F70D010101050003818D003081890281810 0DA3B90F59237347B
   8D41B58F8143512880139EC9111BFD31EB84B6B7C7A1470027AC8F04A827B30C2CAF79242E
   45FDFF51A9C7E917DB818D54CB7AEF538AB261557524A7441D288EC54A5D31EFAE4F681257
   6D7796490AF87A8C78F4A7E31F0793D8BA06FB95D54EBB9F94EB1F2D561BF66EA27DFD4788
   CB47440AF6BB25ACA50203010001
=============================================
Key name: serverkey (default)
Key type: RSA
Time when key pair created: 16:48:31 2011/05/12
Key code:
   307C300D06092A864886F70D0101010500036B003068026100C9451A80F7F0A9BA1A90C7BC
   1C02522D194A2B19F19A75D9EF02219068BD7FD90FCC2AF3634EEB9FA060478DD0A1A49ACE
   E1362A4371549ECD85BA04DEE4D6BB8BE53B6AED7F1401EE88733CA3C4CED391BAE633028A
   AC41C80A15953FB22AA30203010001
```

2)　Device B を設定します。

public key view で Device A のホスト公開鍵を入力します。鍵は Device A での表示と同一になるように、正確に入力してください。

```
<DeviceB> system-view
[DeviceB] public-key peer devicea
Enter public key view. Return to system view with "peer-public-key end" command.
[DeviceB-pkey-public-key-devicea]30819F300D06092A864886F70D010101050003818D
003081890281810 0DA3B90F59237347B
[DeviceB-pkey-public-key-devicea]8D41B58F8143512880139EC9111BFD31EB84B6B7C
7A1470027AC8F04A827B30C2CAF79242E
[DeviceB-pkey-public-key-devicea]45FDFF51A9C7E917DB818D54CB7AEF538AB26155
7524A7441D288EC54A5D31EFAE4F681257
[DeviceB-pkey-public-key-devicea]6D7796490AF87A8C78F4A7E31F0793D8BA06FB95
D54EBB9F94EB1F2D561BF66EA27DFD4788
[DeviceB-pkey-public-key-devicea]CB47440AF6BB25ACA50203010001
```

system view に戻り、公開鍵を保存します。

```
[DeviceB-pkey-public-key-devicea] peer-public-key end
```

III. 設定の確認

Device A と同一の鍵であることを確認してください。

```
[DeviceB] display public-key peer name devicea

=========================================
Key name: devicea
Key type: RSA
Key modulus: 1024
Key code:
   30819F300D06092A864886F70D010101050003818D0030818902818100DA3B90F59237347B
   8D41B58F8143512880139EC9111BFD31EB84B6B7C7A1470027AC8F04A827B30C2CAF79242E
   45FDFF51A9C7E917DB818D54CB7AEF538AB261557524A7441D288EC54A5D31EFAE4F681257
   6D7796490AF87A8C78F4A7E31F0793D8BA06FB95D54EBB9F94EB1F2D561BF66EA27DFD4788
   CB47440AF6BB25ACA50203010001
```

10.7.2 公開鍵ファイルからの公開鍵のインポート例

I. ネットワーク要件

図 10-3に示すように、Device B は Device A をデジタル署名によって認証します。Device B 上で認証パラメータを設定する前に、Device B 上で Device A の公開鍵を設定します。

- Device A の認証に RSA の非対称鍵アルゴリズムを使用するために Device B を設定します。
- 公開鍵ファイルから Device B へ、Device A のホスト公開鍵をインポートします。

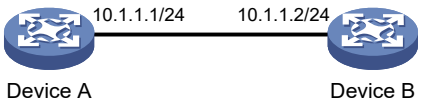


図 10-3 ネットワーク図

II. 設定手順

1)　Device A を設定します。

Device A にデフォルト名のローカル RSA 鍵ペアを作成し、鍵の長さをデフォルトの 1024 ビットに設定します。

```
<DeviceA> system-view

[DeviceA] public-key local create rsa
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.................++++++
.....................................++++++
.....++++++++
.............++++++++
Create the key pair successfully.
```

すべてのローカル RSA 鍵ペアの公開鍵を表示します。

```
[DeviceA] display public-key local rsa public
=============================================
Key name: hostkey (default)
Key type: RSA
Time when key pair created: 16:48:31 2011/05/12
Key code:
   30819F300D06092A864886F70D010101050003818D0030818902818100DA3B90F59237347B
   8D41B58F8143512880139EC9111BFD31EB84B6B7C7A1470027AC8F04A827B30C2CAF79242E
   45FDFF51A9C7E917DB818D54CB7AEF538AB261557524A7441D288EC54A5D31EFAE4F681257
   6D7796490AF87A8C78F4A7E31F0793D8BA06FB95D54EBB9F94EB1F2D561BF66EA27DFD4788
   CB47440AF6BB25ACA50203010001
=============================================
Key name: serverkey (default)
Key type: RSA
Time when key pair created: 16:48:31 2011/05/12
Key code:
   307C300D06092A864886F70D0101010500036B003068026100C9451A80F7F0A9BA1A90C7BC
   1C02522D194A2B19F19A75D9EF02219068BD7FD90FCC2AF3634EEB9FA060478DD0A1A49ACE
   E1362A4371549ECD85BA04DEE4D6BB8BE53B6AED7F1401EE88733CA3C4CED391BAE633028A
   AC41C80A15953FB22AA30203010001
```

RSA ホスト公開鍵をファイル **devicea.pub** にエクスポートします。

```
[DeviceA] public-key local export rsa ssh2 devicea.pub
[DeviceA] quit
```

FTP サーバ機能を有効にし、FTP ユーザをユーザ名 **ftp**、パスワード **123**、FTP のユーザロールを **network-admin** で作成します。

```
[DeviceA] ftp server enable
[DeviceA] local-user ftp
[DeviceA-luser-manage-ftp] password simple 123
[DeviceA-luser-manage-ftp] service-type ftp
[DeviceA-luser-manage-ftp] authorization-attribute user-role network-admin
[DeviceA-luser-manage-ftp] quit
```

2)　Device B を設定します。

Device A から、公開鍵ファイル **devicea.pub** を FTP のバイナリモードで取得します。

```
<DeviceB> ftp 10.1.1.1
Connected to 10.1.1.1 (10.1.1.1).
220 FTP service ready.
User(10.1.1.1:(none)):ftp
331 Password required for ftp.
Password:
230 User logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> binary
200 TYPE is now 8-bit binary
ftp> get devicea.pub
227 Entering Passive Mode (10,1,1,1,118,252)
150 Accepted data connection
226 File successfully transferred
301 bytes received in 0.003 seconds (98.0 kbyte/s)
ftp> quit
221-Goodbye. You uploaded 0 and downloaded 1 kbytes.
221 Logout.
```

鍵ファイル **devicea.pub** からホスト公開鍵をインポートします。

```
<DeviceB> system-view
[DeviceB] public-key peer devicea import sshkey devicea.pub
```

III. 設定の確認

ホスト公開鍵が Device A の公開鍵と同一であることを確認します。

```
[DeviceB] display public-key peer name devicea
=========================================
Key name: devicea
Key type: RSA
Key modulus: 1024
Key code:
   30819F300D06092A864886F70D010101050003818D0030818902818100DA3B90F59237347B
   8D41B58F8143512880139EC9111BFD31EB84B6B7C7A1470027AC8F04A827B30C2CAF79242E
   45FDFF51A9C7E917DB818D54CB7AEF538AB261557524A7441D288EC54A5D31EFAE4F681257
   6D7796490AF87A8C78F4A7E31F0793D8BA06FB95D54EBB9F94EB1F2D561BF66EA27DFD4788
   CB47440AF6BB25ACA50203010001
```

目次

このセクションのページは **9-x-x** です。

11 章 PKI.....11-1

11章 PKI

Web 認証設定に関するコンフィグについては、別紙の共通マニュアル”*QX シリーズ Ethernet スイッチ Web 認証オペレーションマニュアル（V7）*”の“*PKI*”を参照してください。

目次

このセクションのページは **9-x-x** です。

12 章 SSH 12-1
12.1 概要 12-1
12.1.1 SSH の動作 12-2
12.1.2 SSH 認証方式 12-2
12.2 SSH サーバの設定 12-4
12.2.1 ローカル鍵ペアの作成 12-4
12.2.2 Stelnet サーバ機能の有効化 12-5
12.2.3 SFTP サーバ機能の有効化 12-5
12.2.4 SCP サーバの有効化 12-6
12.2.5 SSH ログインのユーザラインの設定 12-6
12.2.6 クライアントのホスト公開鍵の設定 12-7
12.2.7 SSH ユーザの設定 12-8
12.2.8 SSH 管理パラメータの設定 12-9
12.2.9 SSH セッションの切断 12-10
12.3 Stelnet クライアントの設定 12-11
12.3.1 Stelnet クライアントの作業設定リスト 12-11
12.3.2 ローカル鍵ペアの作成 12-11
12.3.3 SSH パケットの送信元 IP アドレスの指定 12-11
12.3.4 Stelnet サーバとの接続の確立 12-12
12.4 SFTP クライアントの設定 12-13
12.4.1 SFTP クライアントの設定作業リスト 12-13
12.4.2 ローカル鍵ペアの作成 12-14
12.4.3 SFTP パケットの送信元 IP アドレスの指定 12-14
12.4.4 SFTP サーバとの接続の確立 12-15
12.4.5 SFTP ディレクトリの操作 12-15
12.4.6 SFTP ファイルの操作 12-16
12.4.7 ヘルプ情報の表示 12-16
12.4.8 SFTP サーバの接続の切断 12-16
12.5 SCP クライアントの設定 12-17
12.5.1 SCP クライアントの設定作業リスト 12-17
12.5.2 ローカル鍵ペアの作成 12-17
12.5.3 SCP サーバとの接続の確立 12-17
12.6 SSH の表示と維持 12-18
12.7 Stelnet 設定例 12-19
12.7.1 パスワード認証を有効にした Stelnet サーバ設定例 12-19
12.7.2 公開鍵認証を有効にした Stelnet サーバの設定例 12-21
12.7.3 パスワード認証を有効にした Stelnet クライアント設定例 12-28
12.7.4 公開鍵認証を有効にした Stelnet クライアント設定例 12-32
12.8 SFTP 設定例 12-34
12.8.1 パスワード認証を有効にした SFTP サーバの設定例 12-34
12.8.2 公開鍵認証を有効にした SFTP クライアント設定例 12-36
12.9 SCP 設定例 12-40
12.9.1 パスワード認証を有効にした SCP の設定例 12-40

12章 SSH

12.1 概要

SSH（Secure Shell）はネットワークセキュリティプロトコルです。暗号化と認証を使用して、安全にリモートアクセスや、ファイルを転送することができます。

一般的なクライアント／サーバモデルを適用して、SSH は TCP をもとにしてデータの転送を保護するチャネルを確立させます。

SSH は SSH1.x と SSH2.0 の 2 つのバージョンをサポートしています。（以降、SSH1 と SSH2 と記載します。）SSH1 と SSH2 では互換性がありません。SSH2 は SSH1 よりも性能とセキュリティを向上しています。

装置は SSH サーバあるいは SSH クライアントとして動作することができます。

- SSH サーバとして動作する場合、装置は SSH クライアントのサービスを提供し、以下のバージョンを SSH サポートします。
  - Stelnet（Secure Telnet）、SFTP（Secure File Transfer Protocol）で装置は SSH2、SSH1 の SSH バージョンをサポートします。
- SSH クライアントとして動作する場合、装置は SSH2 のみサポートします。ユーザが SSH サーバと SSH 接続を確立するために使用します。

装置は以下の SSH アプリケーションをサポートします。

- **Stelnet（Secure Telnet）** – Stelnet は安全で信頼性のあるネットワーク端末アクセスサービスを提供します。Stelnet を使用して、ユーザはリモートサーバに安全にログインすることができます。Stelnet は、IP スプーフィングやプレーンテキストのパスワードの傍受のような装置への攻撃を保護することができます。装置は Stelnet サーバあるいは Stelnet クライアントとして動作することができます。
- **SFTP（Secure File Transfer Protocol）** – SSH2 をもとにして SSH を使用した SFTP は安全なファイル転送を提供します。装置は SFTP サーバとして動作し、リモートユーザが安全なファイル管理と転送を行うため、SFTP サーバにログインできます。また装置は SFTP クライアントとして動作します。ユーザが装置からリモート装置にログインし、安全なファイル転送を行うことができます。
- **SCP（Secure Copy）** – SSH2 をもとに、SCP は安全にファイルをコピーします。安全なファイルのアップロードとダウンロードを行うためにユーザが装置にログインし、装置は SCP サーバとして動作することができます。装置はユーザが安全なファイル転送を行うため装置からリモート装置にログインすることを許可し、SCP クライアントとして動作することができます。

SSH クライアントあるいはサーバとして動作するとき、装置は以下の SSH バージョンをサポートします。

- Stelnet、SFTP、SCP サーバとして動作するとき、装置は SSH2、SSH1 の両方をサポートします。
- SSH クライアントとして動作している場合、装置は SSH2 のみをサポートします。

12.1.1 SSH の動作

この章では、SSH セッションの確立に関連するステージの例を、SSH2 を使用して示します。ステージの詳細は SSH の技術書を参照してください。

表 12-1 SSH セッションを確立するステージ

ステージ	説明
接続の確立	SSHサーバはポート番号22で接続リクエストを受け入れます。クライントが接続要求を初期化した後、サーバとクライントはTCP接続を確立します。
バージョンのネゴシエーション	2つの群（サーバとクライアント）間で使用するバージョンを決めます。
アルゴリズムのネゴシエーション	SSHは複数のアルゴリズムをサポートします。ローカルアルゴリズムにもとづいて、2つの群（サーバとクライアント）は、以下のアルゴリズムを決定します。 ● セッション鍵を作成するアルゴリズムの鍵交換アルゴリズム ● 暗号データ用の暗号アルゴリズム ● デジタル署名と認証のための公開鍵アルゴリズム ● データの完全性を保護するためのHMACアルゴリズム
鍵交換	2つの群（サーバとクライアント）は、セッション鍵とセッションIDを動的に作成するため、DH交換アルゴリズムを使用します。 ● セッション鍵はデータの転送を保護するために使用します。 ● セッションIDはSSH接続を認識するために使用します。 このステージでは、クライアントはサーバと同様に認証します。
認証	SSHサーバはクライアントからの認証要求に応答し、認証を実行します。
セッション要求	認証にパスした後、クライアントがセッション要求（あるいはStelnet、SFTP、SCPサービスのリクエスト）をサーバに送信します。
データ交換	サーバが要求に承諾した後、クライアントとサーバはセッションで互いに通信を行います。 このステージでは、テキストフォーマットでコマンドを貼り付け、CLIで実行することができます。一度に貼り付けることができるテキストは、2000バイトよりも少ない値としてください。コマンドを正常に実行するため同じviewで使用することを推奨します。 2000バイト以上のコマンドを実行する場合、設定ファイルにコマンドを保存し、SFTPを通してサーバにアップロードし、サーバを再起動してください。

12.1.2 SSH 認証方式

この章では装置を SSH サーバとして動作させるとき、サポートする認証方式について記載します。

I. パスワード認証

SSH サーバは、AAA を使用してクライアントを認証します。パスワード認証は以下のように処理します。

1) SSH クライアントは暗号化されたユーザ名とパスワードが含まれる認証要求をサーバに送信します。

2) SSH サーバは以下の処理を行います。

a) プレーンテキストのユーザ名とパスワードを取得するため要求を復号化します。

b) ローカル、あるいはリモートAAA認証によってユーザ名とパスワードが正しいか確認します。

c) 認証結果をクライアントに通知します。

セカンダリ認証のため AAA サーバがユーザのパスワードを必要とする場合、ユーザはプロンプトが運ばれる認証応答を SSH サーバに送ります。プロンプトは透過的にクライアントに送信され、ユーザに指定のパスワードを入力するように通知します。ユーザが正しいパスワードを入力したとき、AAA サーバ上でパスワードの妥当性をチェックします。パスワードが有効である場合、SSH サーバはクライアントに認証成功メッセージを返します。

AAA についての詳細は、オペレーションマニュアルのセクション 9 *セキュリティ”AAA”* を参照してください。

🕮 **メモ：**

SSH1 は AAA サーバによって開始されるセカンダリパスワード認証をサポートしていません。

II. 公開鍵認証

サーバは、クライアントのデジタル署名を使用してクライアントを認証します。公開鍵認証は以下のように処理します。

1) SSH クライアントはユーザ名、公開鍵、公開鍵アルゴリズム名が含まれる認証要求をサーバに送信します。

   クライアントのデジタル署名が認証で要求される場合、クライアントは認証要求のデジタル署名をカプセル化します。デジタル署名にはクライアントの公開鍵情報が含まれます。

2) サーバは公開鍵が有効かどうかを確認します。

- 公開鍵が無効である場合、認証が失敗します。サーバは認証が失敗したことをクライアントに通知します。
- 公開鍵が有効である場合、サーバはクライアントのデジタル署名を要求します。デジタル署名を受信したのち、サーバはデジタル署名を確認するために公開鍵を使用します。最後に認証結果をクライアントに送信します。

SSH サーバとして動作するとき、装置はデジタル署名を確認するため、公開鍵アルゴリズム RSA と DSA を使用します。

SSH クライアントとして動作するとき、装置はデジタル署名を作成するため、公開鍵アルゴリズム RSA と DSA を使用します。

公開鍵の設定についての詳細は、オペレーションマニュアルのセクション 9 *セキュリティ”公開鍵”* を参照してください。

III. パスワード-公開鍵認証

サーバは SSH2 クライアントに、パスワード認証と公開鍵認証の両方にパスするように要求します。SSH1 クライアントは、サーバの要求に関係なく、どちらか 1 つの認証のみ必要です。

IV. いずれかの認証

サーバはパスワード認証あるいは公開鍵認証のいずれかにパスするようにクライアントに要求します。

12.2 SSHサーバの設定

作業リスト	補足
（必須設定項目） ローカル鍵ペアの作成	ー
（必須設定項目） SSHサーバの有効化 ● Stelnetサーバ機能の有効化 ● SFTPサーバ機能の有効化 ● SCPサーバの有効化	ー
（必須設定項目）SSHログインのユーザラインの設定	Stelnetでのみ必須設定項目です。
（必須設定項目） クライアントのホスト公開鍵の設定	認証方法が公開鍵、パスワード-公開鍵認証あるいはいずれかの方法を使用する場合、必須設定項目です。
（必須設定項目/オプション設定項目） SSHユーザの設定	認証方法が公開鍵、パスワード-公開鍵認証あるいはいずれかの方法を使用する場合、必須設定項目です。 パスワード認証のみ使用するユーザでは、オプション設定項目です。
（オプション設定項目）SSH管理パラメータの設定	認証、接続管理の設定のようなSSH管理の設定はSSH接続のセキュリティを向上させます。
（オプション設定項目）SSHセッションの切断	ー

12.2.1 ローカル鍵ペアの作成

DSA または RSA 鍵ペアは、鍵交換ステージのセッション鍵とセッション ID を作成するために必要です。DSA または RSA 鍵ペアは、クライアントがサーバを認証するために、クライアントによって使用されます。クライアントがサーバを認証するとき、サーバから受信した公開鍵を、ローカルに保存したサーバ公開鍵と比較します。鍵が一致している場合、クライアントはサーバから受信したデジタル署名を復号化するため、クライアントがローカルに保存したサーバの公開鍵を使用します。デジタル署名の復号化に成功した場合、認証は成功します。

SSH アプリケーションを実行させるため、装置で SSH コマンドを実行するとき、SSH サーバは自動で 2 つの RSA 鍵ペアを作成します。装置の DSA 鍵ペアあるいは RSA 鍵ペアを作成するため **public-key local create** コマンドを使用します。

I. 設定ガイドライン

ローカル鍵ペアを作成するとき、以下の制限とガイドラインに従ってください。

- SSH は、デフォルト名でローカルに作成された DSA と RSA の鍵ペアのみをサポートします。
- 鍵ペアの異なるタイプを使用する SSH クライアントをサポートするため、SSH サーバで DSA と RSA 鍵ペアの両方を作成します。
- **public-key local create rsa** コマンドは RSA のサーバ鍵ペアとホスト鍵ペアのみを作成します。SSH1 ではサーバ鍵ペアの公開鍵はセッション鍵の安全な転送を行うため暗号化するのに使用されます。
- SSH2 は、SSH サーバとクライアントの各セッション鍵を作成する DH アルゴリズムを使用するため、セッション鍵の転送は必要ありません。サーバ鍵ペアは SSH2 で使われません。
- **public-key local create dsa** コマンドは DSA ホスト鍵ペアのみを作成します。SSH1 は DSA アルゴリズムをサポートしません。
- SSH サーバで **public-key local create dsa** コマンドを使用するとき、鍵の長さは 2048 ビットよりも短くしてください。

II. 設定手順

以下に SSH サーバでローカル DSA あるいは RSA 鍵ペアを生成する設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. ローカル DSA または RSA 鍵ペアを作成する	**public-key local create** { **dsa** | **rsa** }	デフォルト : 鍵ペアは存在しません。

12.2.2 Stelnet サーバ機能の有効化

装置で Stelnet サーバ機能を有効にしたのち、クライアントは Stelnet を通して装置にログインすることができます。

以下に Stelnet サーバ機能の有効化の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. Stelnet サーバ機能を有効にする	**ssh server enable**	デフォルト : 無効

12.2.3 SFTP サーバ機能の有効化

装置で SFTP サーバ機能を有効にしたのち、クライアントは SFTP を通して装置にログインすることができます。

SFTP サーバとして動作する装置は SSH1 クライアントから開始された SFTP 接続をサポートしません。

以下に SFTP サーバ機能の有効化の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. SFTP サーバ機能を有効にする	**sftp server enable**	デフォルト：無効

12.2.4 SCP サーバの有効化

I. SCP サーバの有効化

装置で SCP サーバ機能を有効にした後、クライアントは、SCP を通して装置にログインすることができます。

II. 制限とガイドライン

SCP サーバとして動作する装置は SSH1 クライアントから開始された SCP 接続をサポートしません。

III. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. SCP サーバ機能を有効にする	**scp server enable**	デフォルト：無効

12.2.5 SSH ログインのユーザラインの設定

SSH アプリケーションに依存して、SSH クライアントは Stelnet、SFTP、SCP クライアントとなります。

Stelnet 接続を確立するため、Stelnet クライアントは VTY ユーザラインを通して装置にアクセスする必要があります。SSH クライアントが SSH ログインできるようにユーザラインを設定する必要があります。この設定は次回ログインしたときにのみ適用します。

SFTP クライアントは VTY ユーザラインを使用しないで装置にアクセスします。

以下に Stelnet クライアントのユーザラインの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. VTY line view に移行する	**line vty** *first-number2* [*last-number2*]	ー
3. ログイン認証モードをスキームに設定する	**authentication-mode scheme**	デフォルト：**password** コマンドの詳細は、コマンドマニュアルのセクション1 *はじめに*”*ログイン*”を参照してください。

12.2.6 クライアントのホスト公開鍵の設定

サーバがクライアントを認証するために公開鍵を使用する場合、サーバは SSH ユーザ名とクライアントから受信したホスト公開鍵をローカルに保存されている内容と比較します。内容が一致した場合、クライアントが送信したデジタル署名を確認します。クライアントはホスト公開鍵に関連する秘密鍵にもとづいてデジタル署名を作成します。

公開鍵認証、パスワード-公開鍵認証、あるいはあらゆる認証を使用する SSH サーバのために、以下の処理を行う必要があります。

1) サーバ上でクライアントの DSA あるいは RSA ホスト公開鍵を設定します。

   SSH サーバの SSH クライアントホスト公開鍵は 20 以下に設定することを推奨します。

2) デジタル署名を作成するため関連するクライアントのホスト秘密鍵を指定します。もし装置が SSH クライアントとして動作する場合、クライアントの公開鍵アルゴリズムを指定します。アルゴリズムは、デジタル署名を作成するため、関連する秘密鍵を決定します。

クライアントのホスト公開鍵の内容を入力する、あるいは公開鍵ファイルからクライアントのホスト公開鍵をインポートすることができます。クライアントのホスト公開鍵をインポートすることを推奨します。

I. クライアントのホスト公開鍵の入力

クライアントのホスト公開鍵を入力する前に、クライアントのホスト公開鍵を取得するため、クライアントで **display public-key local public** コマンドを使用してください。他の方法で取得したホスト公開鍵は正式な形式でない可能性があるため、サーバに保存することができません。

以下にクライアントのホスト公開鍵を入力する方法を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. public key view に移行する	**public-key peer** *keyname*	ー
3. クライアントのホスト公開鍵を設定する	ホスト公開鍵の内容を入力する	ホスト公開鍵は変換されないDER復号形式である必要があります。 ホスト公開鍵の内容を入力する場合、空白と改行を使用することができます。 ホスト公開鍵を保存するとき、空白と改行は自動で削除されます。 詳細は、オペレーションマニュアルのセクション9 *セキュリティ”公開鍵”*を参照してください。
4. system view に戻る	**peer-public-key end**	ー

II. 公開鍵ファイルからのクライアントのホスト公開鍵のインポート

ホスト公開鍵をインポートする前に、クライアントの公開鍵ファイル（バイナリ形式）を FTP あるいは TFTP を使用してサーバにアップロードします。インポートを行う間、サーバは自動的に公開鍵ファイルのホスト公開鍵を、PKCS 形式に変換します。

以下に公開鍵ファイルからクライアントのホスト公開鍵をインポートする設定を示します。

操作	コマンド
1. system view に移行する	**system-view**
2. 公開鍵ファイルからクライアントの公開鍵をインポートする	**public-key peer** *keyname* **import sshkey** *filename*

12.2.7 SSH ユーザの設定

認証方式に依存して SSH ユーザとローカルユーザを設定します。

- 認証方式が公開鍵である場合、サーバに SSH ユーザとローカルユーザを作成する必要があります。SSH ユーザに正しい作業ディレクトリとユーザロールを割り当てることができるように、2 つのユーザは同一のユーザ名にする必要があります。
- 認証方式がパスワード認証である場合、以下の処理を実行する必要があります。
  - □ ローカル認証用に **local-user** コマンドを使用してローカルユーザアカウントを設定します。
  - □ リモート認証用に RADIUS サーバのようなリモート認証サーバで SSH ユーザを設定します。

  ssh user コマンドを使用して SSH ユーザあるいはローカルユーザを作成する必要はありません。しかし集中管理を行うため、パスワード認証のみの SSH ユーザを含むすべての SSH ユーザを表示する場合、SSH ユーザあるいはローカルユーザを作成するコマンドを使用することができます。そのような SSH ユーザが作成される場合、サービスタイプと認証方式が正しく指定されていることを確認してください。
- 認証方式がパスワード-公開鍵認証あるいはそれ以外の認証方式である場合、SSH ユーザを作成し、以下の処理を実行する必要があります。
  - □ ローカル認証用に **local-user** コマンドを使用してローカルユーザアカウントを設定します。
  - □ リモート認証用に RADIUS サーバのようなリモート認証サーバで SSH ユーザを設定します。

  どちらの場合においても、ローカルユーザあるいはリモート認証サーバで設定される SSH ユーザは SSH ユーザと同じユーザ名にする必要があります。

I. 設定ガイドライン

SSH ユーザを設定するとき、以下の制限とガイドラインに従ってください。

- SSH サーバは 1024 の SSH ユーザをサポートします。
- SFTP、SCP ユーザの作業ディレクトリは認証方式に依存します。
  - □ パスワード認証が使用される場合、作業ディレクトリは AAA によって許可されます。

- □ 認証方式が公開鍵あるいはパスワード-公開鍵認証である場合、作業ディレクトリは関連した local user view で **authorization-attribute** コマンドを使用して指定されます。

- SSH ユーザでは、ユーザロールは認証方式に依存します。
  - □ パスワード認証が使用される場合、ユーザロールはリモート AAA サーバあるいはローカル装置によって許可されます。
  - □ 認証方式が公開鍵あるいはパスワード-公開鍵認証である場合、ユーザロールは関連した local user view で **authorization-attribute** コマンドを使用して指定されます。
- すでにログインしている SSH ユーザの認証方式あるいは公開鍵を変更する場合、変更内容は次回ユーザがログインしたときに適用されます。
- パスワード認証を除いて、他の認証方式は、指定されたクライアントのホスト公開鍵が必要です。
  - □ クライアントが直接サーバにユーザの公開鍵の情報を送信する場合、サーバのクライアントの公開鍵を指定する必要があります。指定される公開鍵はすでに存在している必要があります。公開鍵の詳細は、オペレーションマニュアルのセクション 9 *セキュリティ*”*SSH*”の”*クライアントのホスト公開鍵の設定*”を参照してください。

ローカルユーザとリモート認証を設定する方法の詳細は、オペレーションマニュアルのセクション 9 *セキュリティ*”*AAA*”を参照してください。

II. 設定手順

以下に SSH ユーザを設定し、サービスタイプと認証方式を指定する手順を示します。

操作	コマンド
1. system view に移行する	**system-view**
2. SSH ユーザを作成し、サービスタイプと認証方式を指定する	**ssh user** *username* **service-type** { **all** | **scp** | **sftp** | **stelnet** } **authentication-type** { **password** | { **any** | **password-publickey** | **publickey** } [**assign publickey** *keyname*&<1-6>] }

12.2.8 SSH 管理パラメータの設定

以下に SSH 管理パラメータの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. SSH1 クライアントのサポートを有効にする	**ssh server compatible-ssh1x enable**	デフォルト：無効
3. RSA サーバ鍵ペアの最小アップデート間隔を設定する	**ssh server rekey-interval** *interval*	デフォルト：RSAサーバ鍵ペアのアップデートを行いません。 このコマンドはSSH1ユーザのみ適用します。
4. SSH ユーザ認証タイムアウトタイマを設定する	**ssh server authentication-timeout** *time-out-value*	デフォルト：60秒 タイムアウトタイマが終了したとき、接続用の認証が終了していない場合、接続を確立することができません。
5. SSH 認証の最大試行回数を設定する	**ssh server authentication-retries** *retries*	デフォルト：3

操作	コマンド	補足
6. SSH ユーザの接続を管理する ACL を設定する	● SSHユーザのIPv4 ACLを設定する： **ssh server acl** { *advanced-acl-number* | *basic-acl-number* | **mac** *mac-acl-number* } ● SSHユーザのIPv6 ACLを設定する： **ssh server ipv6 acl** { **ipv6** { *advanced-acl-number* | *basic-acl-number* } | **mac** *mac-acl-number* }	デフォルト：設定なし
7. SSH サーバが SSH クライアントに送信するパケットの DSCP を設定する	● IPv4パケットのDSCPを設定する： **ssh server dscp** *dscp-value* ● IPv6パケットのDSCPを設定する： **ssh server ipv6 dscp** *dscp-value*	デフォルト：48 DSCPはパケットのプライオリティを決定し、パケットを転送する優先度を決定します。DSCPの値が大きいほど優先度は高くなります。
8. SFTP 接続アイドルタイムアウトタイマを設定する	**sftp server idle-timeout** *time-out-value*	デフォルト：10分 アイドルタイマが指定したしきい値を超えたとき、システムは自動的に接続を切断します。
9. オンライン SSH ユーザの最大同時接続数を指定する	**aaa session-limit ssh** *max-sessions*	デフォルト：32 オンラインSSHユーザが上限に到達したとき、システムは新しいSSH接続要求を拒否します。オンラインSSHユーザには影響しません。

12.2.9 SSH セッションの切断

I. SSH セッションの切断

装置は同時にログインするセッションをサポートします。設定を邪魔している SSH ログインユーザを避けるため、SSH ログインユーザを切断することができます。

II. 設定手順

user view で実行できます。

操作	コマンド
SSHセッションを切断する	**free ssh** { **user-ip** { *ip-address* | **ipv6** *ipv6-address* } [**port** *port-number*] | **user-pid** *pid-number* | **username** *username* }

12.3 Stelnetクライアントの設定

12.3.1 Stelnet クライアントの作業設定リスト

設定リスト	補足
（必須設定項目） ローカル鍵ペアの作成	Stelnetサーバが**publickey**、**password-publickey**の認証方式を使用する際は必須です。
（オプション設定項目） SSHパケットの送信元IPアドレスの指定	—
（必須設定項目） Stelnetサーバとの接続の確立	—
（オプション設定項目）スーツBに基づくStelnetサーバとの接続の確立	—

12.3.2 ローカル鍵ペアの作成

Stelnet サーバが **publickey**、**password-publickey**、あるいは **any** の認証方式を使用する際は、Stelnet クライアントでローカル鍵ペアを作成してください。

I. 設定ガイドライン

Stelnet クライアントでローカル鍵ペアを設定する際には、以下のガイドラインに従ってください。

- SSH のローカル DSA、ECDSA 及び RSA 鍵ペアはデフォルト名を使用します。鍵ペアに名前を割り当てることはできません。
- DSA 鍵ペアを作成するとき、鍵の長さは 2048 ビットよりも短くしてください。

II. 設定手順

以下に Stelnet クライアントでローカル鍵ペアを生成する設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. ローカル鍵ペアを作成する	**public-key local create** { **dsa** | **rsa** }	デフォルト：鍵ペアは存在しません。

12.3.3 SSH パケットの送信元 IP アドレスの指定

以下のため、SSH パケットの送信元インタフェースとしてループバックインタフェースの IP アドレスを指定することを推奨します。

- Stelnet クライアントと Stelnet サーバが互いに通信できることを保証します。
- 認証サービスの Stelnet クライアントの管理を向上します。

以下に SSH パケットの送信元 IP アドレスの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. SSH パケットの送信元 IP アドレスを設定する	• SSHパケットの送信元IPv4アドレスを指定する: **ssh client source** { **interface** *interface-type interface-number* | **ip** *ip-address* } • SSHパケットの送信元IPv6アドレスを指定する: **ssh client ipv6 source** { **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }	デフォルト：設定なし IPv4 SSHパケットは送信元アドレスとしてルーティングエントリで指定された送信インタフェースのプライマリIPアドレスを使用します。 IPv6 SSHパケットはRFC3484互換で定義された送信元アドレスとして、自動で選択されたIPv6アドレスを選択します。

12.3.4 Stelnet サーバとの接続の確立

Stelnet サーバにアクセスするとき、装置はサーバを認証するためサーバのホスト公開鍵を使用します。装置でサーバのホスト公開鍵が設定されていない場合、装置はアクセスを継続するかどうかを確認するメッセージを表示します。

- アクセスを継続する場合、装置はサーバにアクセスし、サーバのホスト公開鍵をダウンロードします。
- アクセスを継続しない場合、接続は確立することができません。

安全でないネットワークでは装置でサーバのホスト公開鍵を設定することを推奨します。

以下に Stelnet サーバの接続を確立する設定を示します。

操作	コマンド	補足
Stelnetサーバの接続を確立する	● IPv4 Stelnetサーバの接続を確立する： **ssh2** *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] [**identity-key** { **dsa** | **rsa** } | **prefer-compress zlib** | **prefer-ctos-cipher** { **3des-cbc** | **aes128-cbc** | **des-cbc** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** } | **prefer-kex** { **dh-group-exchange-sha1** | **dh-group1-sha1** | **dh-group14-sha1** } | **prefer-stoc-cipher** { **3des-cbc** | **aes128-cbc** | **des-cbc** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** }] * [**dscp** *dscp-value* | **escape** *character* | **public-key** *keyname* | **source** { **interface** *interface-type interface-number* | **ip** *ip-address* }] * ● IPv6 Stelnetサーバの接続を確立する： **ssh2 ipv6** *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] [**-i** *interface-type interface-number*] [**identity-key** { **dsa** | **rsa** } | **prefer-compress zlib** | **prefer-ctos-cipher** { **3des-cbc** | **aes128-cbc** | **des-cbc** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** } | **prefer-kex** { **dh-group-exchange-sha1** | **dh-group1-sha1** | **dh-group14-sha1** } | **prefer-stoc-cipher** { **3des-cbc** | **aes128-cbc** | **des-cbc** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** }] * [**dscp** *dscp-value* | **escape** *character* | **public-key** *keyname* | **source** { **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }] *	どちらか一方の設定を使用します。 user viewで実行できます。

12.4 SFTPクライアントの設定

12.4.1 SFTP クライアントの設定作業リスト

作業リスト	補足
（必須設定項目） ローカル鍵ペアの作成	Stelnetサーバが**publickey**、**password-publickey**の認証方式を使用する際は必須です。
（オプション設定項目）SFTPパケットの送信元IPアドレスの指定	―
（必須設定項目） SFTPサーバとの接続の確立	―
（オプション設定項目） SFTPディレクトリの操作	―
（オプション設定項目） SFTPファイルの操作	―
（オプション設定項目） ヘルプ情報の表示	―
（オプション設定項目） SFTPサーバの接続の切断	―

12.4.2 ローカル鍵ペアの作成

SFTP サーバが **publickey**、**password-publickey**、あるいは **any** の認証方式を使用する際は、SFTP クライアントでローカル鍵ペアを作成してください。

I. 設定ガイドライン

SFTP クライアントでローカル鍵ペアを設定する際には、以下のガイドラインに従ってください。

- SSH のローカル DSA、ECDSA 及び RSA 鍵ペアはデフォルト名を使用します。鍵ペアに名前を割り当てることはできません。
- DSA 鍵ペアを作成するとき、鍵の長さは 2048 ビットよりも短くしてください。

II. 設定手順

以下に SFTP クライアントでローカル鍵ペアを生成する設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. ローカル鍵ペアを作成する	**public-key local create** { **dsa** | **rsa** }	デフォルト : 鍵ペアは存在しません。

12.4.3 SFTP パケットの送信元 IP アドレスの指定

以下のため、SFTP パケットの送信元インタフェースとしてループバックインタフェースの IP アドレスを指定することを推奨します。

- SFTP クライアントと SFTP サーバが互いに通信できることを保証します。
- 認証サービスの SFTP クライアントの管理を向上します。

以下に SFTP パケットの送信元 IP アドレスの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. SFTP パケットの送信元 IP アドレスを指定する	• SFTPパケットの送信元IPv4アドレスを指定する: **sftp client source** { **ip** *ip-address* | **interface** *interface-type interface-number* } • SFTPパケットの送信元IPv6アドレスを指定する: **sftp client ipv6 source** { **ipv6** *ipv6-address* | **interface** *interface-type interface-number* }	デフォルト : 設定なし IPv4 SFTPパケットは送信元アドレスとしてルーティングエントリで指定された送信インタフェースのプライマリIPv4アドレスを使用します。 IPv6 SFTPパケットはRFC3484互換で定義された送信元アドレスとして、自動で選択されたIPv6アドレスを選択します。

12.4.4 SFTP サーバとの接続の確立

SFTP サーバにアクセスするとき、装置はサーバを認証するためサーバのホスト公開鍵を使用します。装置でサーバのホスト公開鍵が設定されていない場合、装置はアクセスを継続するかどうかを確認するメッセージを表示します。

- アクセスを継続する場合、装置はサーバにアクセスし、サーバのホスト公開鍵をダウンロードします。
- アクセスを継続しない場合、接続は確立することができません。

安全でないネットワークでは装置でサーバのホスト公開鍵を設定することを推奨します。

接続が完了したのち、ディレクトリあるいはファイルのような操作を行うため、サーバの SFTP client view に直接移行することができます。

操作	コマンド	補足
SFTPサーバの接続を確立する	• IPv4 SFTPサーバの接続を確立する： **sftp** *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] [**identity-key** { **dsa** | **rsa** } | **prefer-compress zlib** | **prefer-ctos-cipher** { **3des-cbc** | **aes128-cbc** | **des-cbc** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** } | **prefer-kex** { **dh-group-exchange-sha1** | **dh-group1-sha1** | **dh-group14-sha1** } | **prefer-stoc-cipher** { **3des-cbc** | **aes128-cbc** | **des-cbc** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** }] * [**dscp** *dscp-value* | **public-key** *keyname* | **source** { **interface** *interface-type interface-number* | **ip** *ip-address* }] * • IPv6 SFTPサーバの接続を確立する： **sftp ipv6** *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] [**-i** *interface-type interface-number*] [**identity-key** { **dsa** | **rsa** } | **prefer-compress zlib** | **prefer-ctos-cipher** { **3des-cbc** | **aes128-cbc** | **des-cbc** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** } | **prefer-kex** { **dh-group-exchange-sha1** | **dh-group1-sha1** | **dh-group14-sha1** } | **prefer-stoc-cipher** { **3des-cbc** | **aes128-cbc** | **des-cbc** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** }] * [**dscp** *dscp-value* | **public-key** *keyname* | **source** { **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }] *	どちらか一方の設定を使用します。 user viewで実行できます。

12.4.5 SFTP ディレクトリの操作

操作	コマンド	補足
SFTPサーバの作業ディレクトリを変更する	**cd** [*remote-path*]	SFTP client viewで有効です。
上位のディレクトリに戻る	**cdup**	SFTP client viewで有効です。
SFTPサーバの現在の作業ディレクトリを表示する	**pwd**	SFTP client viewで有効です。
指定したディレクトリにあるファイルを表示する	• **dir** [**-a** | **-l**] [*remote-path*] • **ls** [**-a** | **-l**] [*remote-path*]	SFTP client viewで有効です。 **dir**コマンドは**ls**コマンドと同一です。
SFTPサーバの指定したディレクトリ名を変更する	**rename** *oldname newname*	SFTP client viewで有効です。

操作	コマンド	補足
SFTPサーバで新しいディレクトリを作成する	**mkdir** *remote-path*	SFTP client viewで有効です。
SFTPサーバから1つ以上のディレクトリを削除する	**rmdir** *remote-path*	SFTP client viewで有効です。

12.4.6 SFTP ファイルの操作

操作	コマンド	補足
SFTPサーバの指定したディレクトリ名を変更する	**rename** *old-name new-name*	SFTP client viewで有効です。
SFTPサーバからファイルをダウンロードし、ローカルに保存する	**get** *remote-file* [*local-file*]	SFTP client viewで有効です。
SFTPサーバにローカルファイルをアップロードする	**put** *local-file* [*remote-file*]	SFTP client viewで有効です。
指定したディレクトリにあるファイルを表示する	• **dir** [**-a** | **-l**] [*remote-path*] • **ls** [**-a** | **-l**] [*remote-path*]	SFTP client viewで有効です。 **dir**コマンドは**ls**コマンドと同一です。
SFTPサーバから1つ以上のディレクトリを削除する	• **delete** *remote-file* • **remove** *remote-file*	SFTP client viewで有効です。 **delete**コマンドは**remove**コマンドと同一です。

12.4.7 ヘルプ情報の表示

コマンドのフォーマットやパラメータのような SFTP クライアントコマンドのヘルプ情報を表示することができます。

以下にヘルプ情報の表示を示します。

操作	コマンド	補足
SFTPクライアントコマンドのヘルプ情報を表示する	• **help** • **?**	どちらか一方のコマンドを使用します。 SFTP client viewで有効です。 2つのコマンドは同一機能です。

12.4.8 SFTP サーバの接続の切断

操作	コマンド	補足
SFTPサーバの接続を切断し、user viewに戻る	• **bye** • **exit** • **quit**	いずれか1つのコマンドを使用します。 SFTP client viewで有効です。 3つのコマンドは同一機能です。

12.5 SCPクライアントの設定

12.5.1 SCP クライアントの設定作業リスト

作業リスト	
(必須設定項目)ローカル鍵ペアの作成	認証方法が公開鍵、パスワード-公開鍵あるいはすべての方法を使用する場合、必須設定項目です。
(必須設定項目) SCPサーバとの接続の確立	ー

12.5.2 ローカル鍵ペアの作成

I. ローカル鍵ペアの作成

SCP クライアントが公開鍵、パスワード-公開鍵あるいはすべての方法を使用する場合、SCP クライアントでローカル鍵ペアを作成する必要があります。

II. 制限とガイドライン

SSH のローカル DSA と RSA 鍵ペアはデフォルトの名前を使用します。鍵ペアに名前を割り当てることができません。

SSH サーバで DSA 鍵ペアを作成するとき、鍵の長さは 2048 ビットよりも短くしてください。

III. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. ローカル鍵ペアを作成する	**public-key local create** { **dsa** | **rsa** }	ー

12.5.3 SCP サーバとの接続の確立

I. SCP サーバとの接続の確立

装置で SCP クライアント機能を有効にし、SCP サーバと通信を確立するため、この機能を使用します。接続中に使用される公開鍵アルゴリズム、暗号化アルゴリズム、HMAC アルゴリズム、鍵交換アルゴリズムを指定します。

SCP サーバにアクセスするとき、装置はサーバを認証するためサーバのホスト公開鍵を使用する必要があります。安全でないネットワークでは装置でサーバのホスト公開鍵を設定することを推奨します。装置でサーバのホスト公開鍵が設定されていない場合、装置はアクセスを継続するかどうかを確認するメッセージを表示します。

- アクセスを継続する場合、装置はサーバにアクセスし、サーバのホスト公開鍵をダウンロードします。ダウンロードされた公開鍵は後続のアクセスでサーバの認証に使用します。
  サーバに接続するときサーバの公開鍵を指定しない場合、装置はサーバの公開鍵を公開鍵に保存します。サーバの公開鍵は設定ファイルに保存されません。
- アクセスを継続しない場合、接続は確立することができません。

II. 制限とガイドライン

SCP クライアントは IPv4、IPv6 SCP サーバの両方の接続を確立することができません。

III. IPv4 SCP サーバの接続の確立

user view で実行できます。

操作	コマンド
IPv4 SCPサーバの接続を確立する	**scp** *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] { **put** | **get** } *source-file-name* [*destination-file-name*] [**identity-key** { **dsa** | **rsa** } | **prefer-compress zlib** | **prefer-ctos-cipher** { **3des-cbc** | **aes128-cbc** | **des-cbc** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** } | **prefer-kex** { **dh-group-exchange-sha1** | **dh-group1-sha1** | **dh-group14-sha1** } | **prefer-stoc-cipher** { **3des-cbc** | **aes128-cbc** | **des-cbc** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** }] * [**public-key** *keyname* | **source** { **interface** *interface-type interface-number* | **ip** *ip-address* }] *

IV. IPv6 SCP サーバの接続の確立

user view で実行できます。

操作	コマンド
IPv6 SCPサーバの接続を確立する	**scp ipv6** *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] [**-i** *interface-type interface-number*] { **put** | **get** } *source-file-name* [*destination-file-name*] [**identity-key** { **dsa** | **rsa** } | **prefer-compress zlib** | **prefer-ctos-cipher** { **3des-cbc** | **aes128-cbc** | **des-cbc** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** } | **prefer-kex** { **dh-group-exchange-sha1** | **dh-group1-sha1** | **dh-group14-sha1** } | **prefer-stoc-cipher** { **3des-cbc** | **aes128-cbc** | **des-cbc** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** }] * [**public-key** *keyname* | **source** { **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }] *

12.6 SSHの表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
SFTPクライアントの送信元IPアドレスを表示する	**display sftp client source**
Stelnetクライアントの送信元IPアドレスを表示する	**display ssh client source**
SSHサーバのステータス情報あるいはセッション情報を表示する	**display ssh server** { **session** | **status** }
SSHサーバのSSHユーザ情報を表示する	**display ssh user-information** [*username*]

操作	コマンド
ローカル鍵ペアの公開鍵を表示する	**display public-key local** { **dsa** | **rsa** } **public** [**name** *publickey-name*]
SSH ピアの公開鍵を表示する	**display public-key peer** [**brief** | **name** *publickey-name*]

12.7 Stelnet設定例

12.7.1 パスワード認証を有効にした Stelnet サーバ設定例

I. ネットワーク要件

図 12-1に示すように設定します。

- Switch は Stelnet サーバとして動作し、Stelnet クライアントを認証するためにパスワード認証を使用します。クライアントのユーザ名とパスワードは Switch に保存されます。
- ホストは Stelnet クライアントとして動作し、Stelnet クライアントソフトウェア（SSH2）を使用します。ホストのユーザが Stelnet を通じて Switch にログインした後、ユーザは network-administrator として Switch を管理できます。

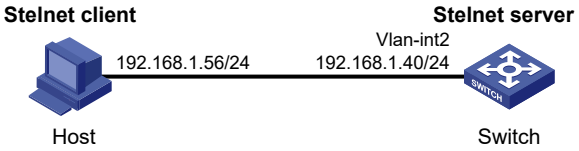


図 12-1 ネットワーク図

II. 設定手順

1)　Stelnet サーバを設定します。

RSA 鍵ペアを作成します。

```
<Switch> system-view
[Switch] public-key local create rsa
The range of public key modules is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.....................++++++
.................++++++
..++++++++
............++++++++
Create the key pair successfully.
```

DSA 鍵ペアを作成します。

```
[Switch] public-key local create dsa
The range of public key modules is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
```

```
Input the modulus length [default = 1024]:
Generating Keys...
.++++++++++++++++++++++++++++++++++++++++++++++++*
........+......+.....+.....................................+
...+.................+.........+...+.
Create the key pair successfully.
```

SSH サーバ機能を有効にします。

```
[Switch] ssh server enable
```

VLAN インタフェース 2に IP アドレスを割り当てます。SSH 接続の宛先アドレスとして Stelnet クライアントは VLAN インタフェース 2 の IP アドレスを使用します。

```
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ip address 192.168.1.40 255.255.255.0
[Switch-Vlan-interface2] quit
```

ユーザラインの認証モードを AAA に設定します。

```
[Switch] line vty 0 63
[Switch-line-vty0-63] authentication-mode scheme
[Switch-line-vty0-63] quit
```

ローカル装置管理ユーザ **client001** を作成します。

```
[Switch] local-user client001 class manage
```

#ユーザのプレーンテキストのパスワードを **aabbcc**、サービスタイプを **ssh** に設定します。

```
[Switch-luser-manage-client001] password simple aabbcc
[Switch-luser-manage-client001] service-type ssh
```

ユーザにユーザロールを **network-admin** に割り当てます。

```
[Switch-luser-manage-client001] authorization-attribute user-role network-admin
[Switch-luser-manage-client001] quit
```

SSH ユーザ **client001** を作成します。ユーザのサービスタイプを **stelnet**、認証方式を **password** に設定します。SSH ユーザが作成されていない場合、デフォルトでパスワード認証が使用されます。

```
[Switch] ssh user client001 service-type stelnet authentication-type password
```

2) Stelnet サーバとの接続を確立します。

Stelnet クライアントのソフトウェアは、PuTTY、OpenSSH など異なるタイプがあります。この例では PuTTY バージョン 0.58 を Stelnet クライアントとして使用します。

Stelnet サーバとの接続を確立します。

a) 図 12-2に示すようにPuTTY.exeを起動させ、インタフェースを入力します。

b) **Host Name**フィールド（あるいは**IP address**）で、StelnetサーバのIPアドレス192.168.1.40を入力します。

c) **Open**をクリックします。

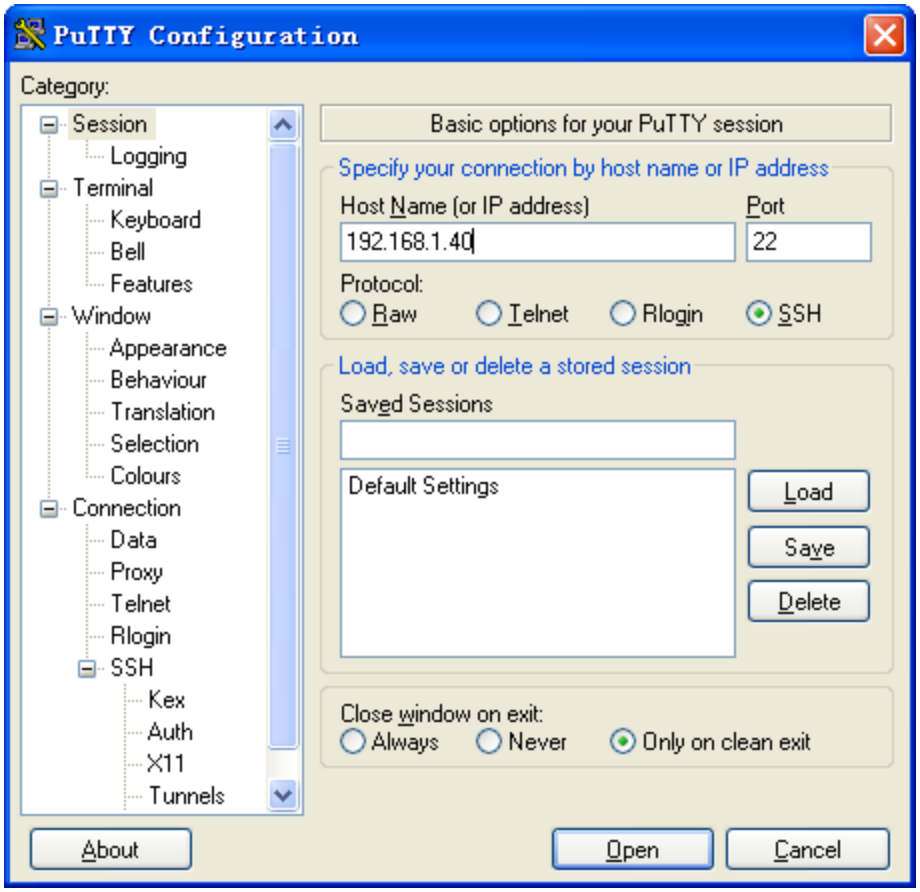


図 12-2 ホスト名（あるいは IP アドレス）の指定

d)　ユーザ名（この例では**client001**）とパスワード（この例では**aabbcc**）を入力してサーバにログインします。

12.7.2 公開鍵認証を有効にした Stelnet サーバの設定例

I. ネットワーク要件

図 12-3に示すように設定します。

- Switch は Stelnet サーバとして動作し、パスワード認証と RSA 公開鍵アルゴリズムを使用します。
- ホストは Stelnet クライアントとして動作し、Stelnet クライアントソフトウェア（SSH2）を使用します。ホストのユーザが Stelnet を通じて Switch にログインした後、ユーザは network-administrator として Switch を管理できます。

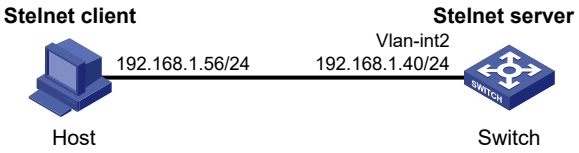


図 12-3 ネットワーク図

II. 設定手順

サーバの設定では、クライアントのホスト公開鍵が必要となります。Stelnet サーバを設定する前に、クライアントで RSA 鍵ペアを作成するため、クライアントソフトウェアを使用します。

Stelnet クライアントのソフトウェアは、PuTTY、OpenSSH など異なるタイプがあります。この例では PuTTY バージョン 0.58 を Stelnet クライアントとして使用します。

設定手順を以下に示します。

1) Stelnet クライアントで RSA 鍵ペアを作成します。

a) クライアントでPuTTY.exeを起動させ、SSH-2 RSAを選択し、Generateをクリックします。

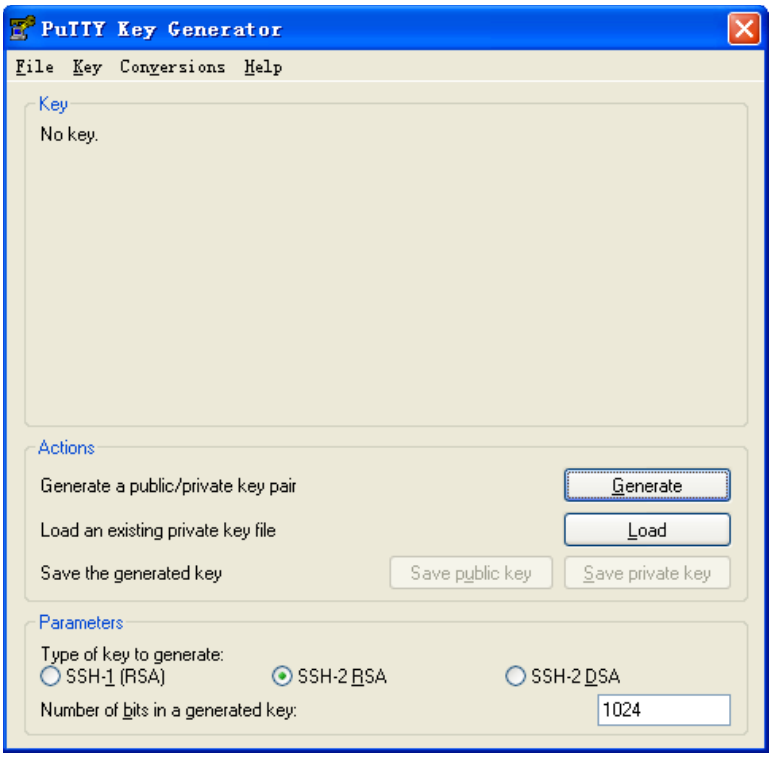


図 12-4 クライアントの鍵ペアの作成

b) 鍵ペアを作成しているとき、マウスを継続して動かしてください。図 12-5に示すように、緑の進捗バーの上にマウスを置かないでください。そうしなければ、進捗バーが動作をストップしてしまい、鍵ペアの作成をとめてしまいます。

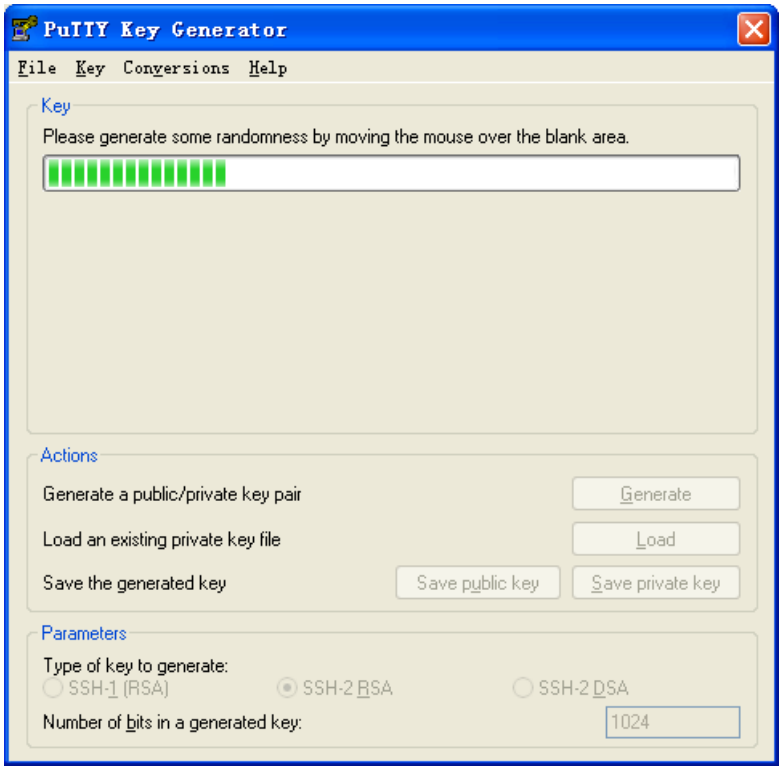


図 12-5 プロセスの作成

c) 鍵ペアが作成された後、**Save public key**をクリックし、ファイル名**key.pub**を入力し、**Save**をクリックします。ファイルの保存ウィンドウ画面が表示されます。

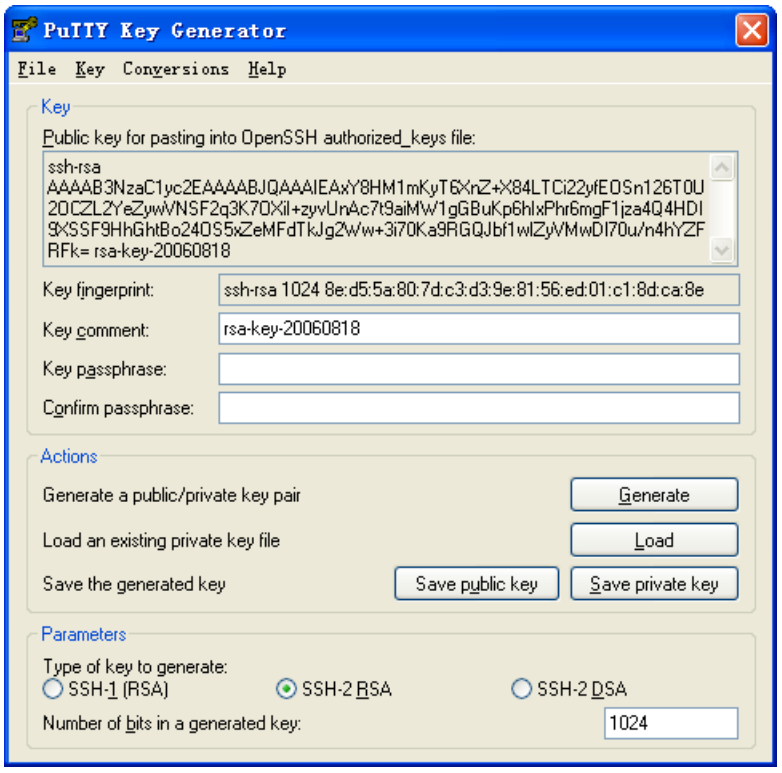


図 12-6 クライアントの鍵ペアの保存

d) ファイル名（この例では**key.pub**）を入力し、**Save**をクリックします。

e) 図 12-6に示すページで、秘密鍵を保存するため、**Save private key**をクリックします。確認ダイアログボックスが表示されます。

f) **Yes**をクリックします。ファイルの保存ウィンドウが表示されます。

g) ファイル名（この例では**private.ppk**）を入力し、**Save**をクリックします。

h) FTPあるいはTFTPを使用してサーバに公開鍵ファイルを転送します。（詳細は省略します）

2) Stelnet サーバを設定します。

RSA 鍵ペアを作成します。

```
<Switch> system-view

[Switch] public-key local create rsa
The range of public key modules is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.....................++++++
.................++++++
..++++++++
............++++++++
Create the key pair successfully.
```

DSA 鍵ペアを作成します。

```
[Switch] public-key local create dsa
The range of public key modules is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.++++++++++++++++++++++++++++++++++++++++++++++++*
.........+.......+.....+.....................................+
...+.................+..........+...+
Create the key pair successfully.
```

SSH サーバ機能を有効にします。

```
[Switch] ssh server enable
```

VLAN インタフェース 2に IP アドレスを割り当てます。SSH 接続の宛先アドレスとして Stelnet クライアントは VLAN インタフェース 2 の IP アドレスを使用します。

```
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ip address 192.168.1.40 255.255.255.0
[Switch-Vlan-interface2] quit
```

ユーザラインの認証モードを AAA に設定します。

```
[Switch] line vty 0 63
[Switch-line-vty0-63] authentication-mode scheme
[Switch-line-vty0-63] quit
```

ファイル **key.pub** からクライアントの公開鍵をインポートし、名前を **switchkey** とします。

```
[Switch] public-key peer switchkey import sshkey key.pub
```

SSH ユーザ **client002** を作成します。ユーザの認証方式を公開鍵に指定します。公開鍵 **switchkey** をユーザに割り当てます。

```
[Switch] ssh user client002 service-type stelnet authentication-type publickey assign publickey switchkey
```

ローカル装置管理ユーザ **client002** を作成します。ユーザのサービスタイプを **ssh**、ユーザロールを **network-admin** に設定します。

```
[Switch] local-user client002 class manage
[Switch-luser-manage-client002] service-type ssh
[Switch-luser-manage-client002] authorization-attribute user-role network-admin
[Switch-luser-manage-client002] quit
```

3) 秘密鍵ファイルを指定し、Stelnet サーバとの接続を確立します。

a) 図 12-7に示すようにStelnetクライアントでPuTTY.exeを起動させ、インタフェースに移行します。

b) **Host Name**フィールド（あるいは**IP address**）で、StelnetサーバのIPアドレス192.168.1.40を入力します。

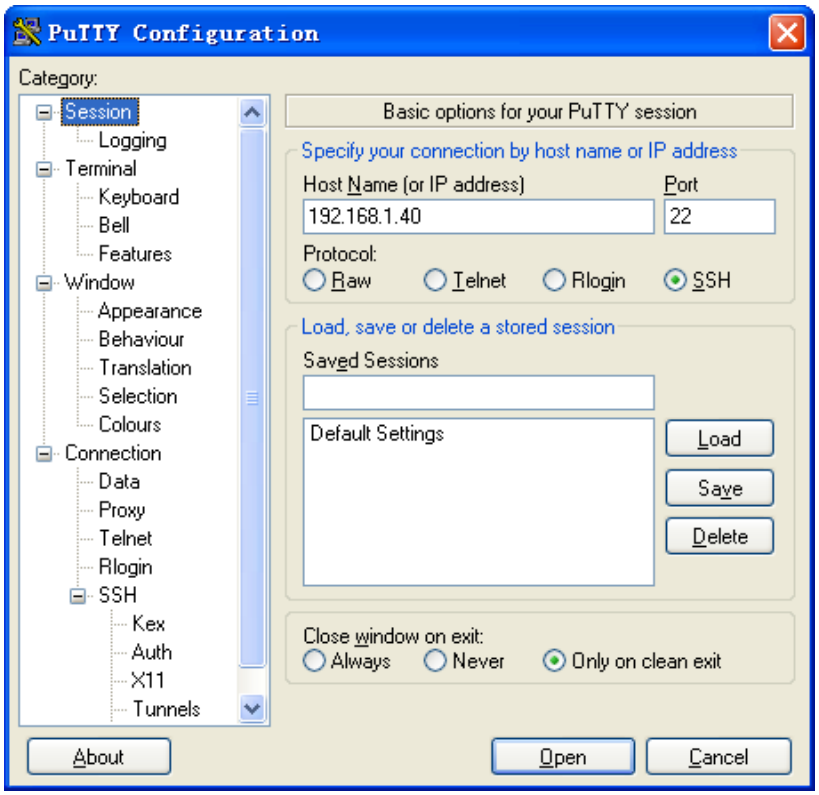


図 12-7 ホスト名（あるいは IP アドレス）の指定

c) ナビゲーションツリーから**Connection**を選択し、**SSH**を選択します。図 12-8に示すようにウィンドウ画面が表示されます。

d) **Protocol options**の**Preferred SSH protocol version**で**2**を選択します。

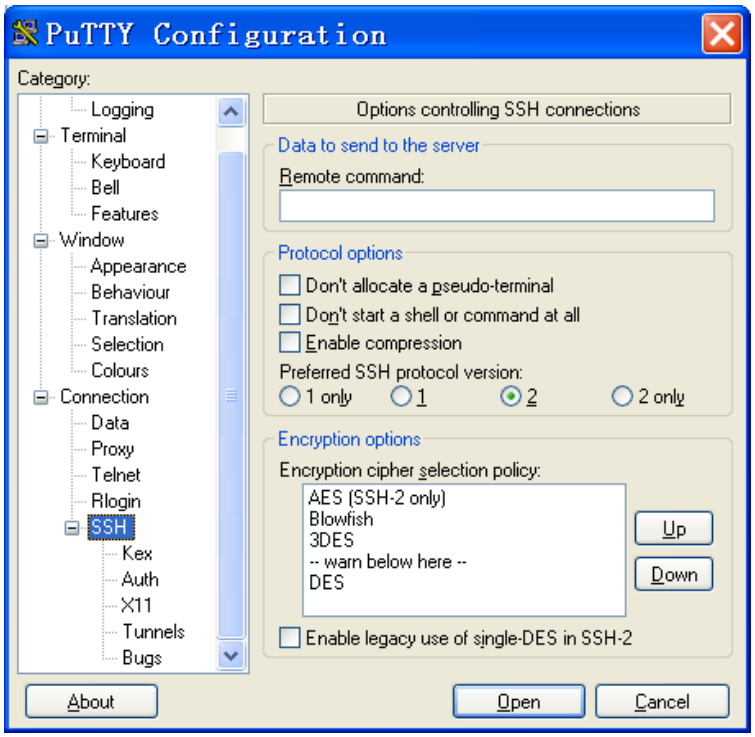


図 12-8 SSH バージョンの指定

e) ナビゲーションツリーから**Connection**を選択し、**SSH**を選択し、**Auth**を選択します。図 12-9に示すようにウィンドウ画面が表示されます。

f) ファイル選択画面から**Browse**をクリックし、秘密鍵ファイル（この例では**private.ppk**）を選択し、**OK**をクリックします。

g) **Open**をクリックします。

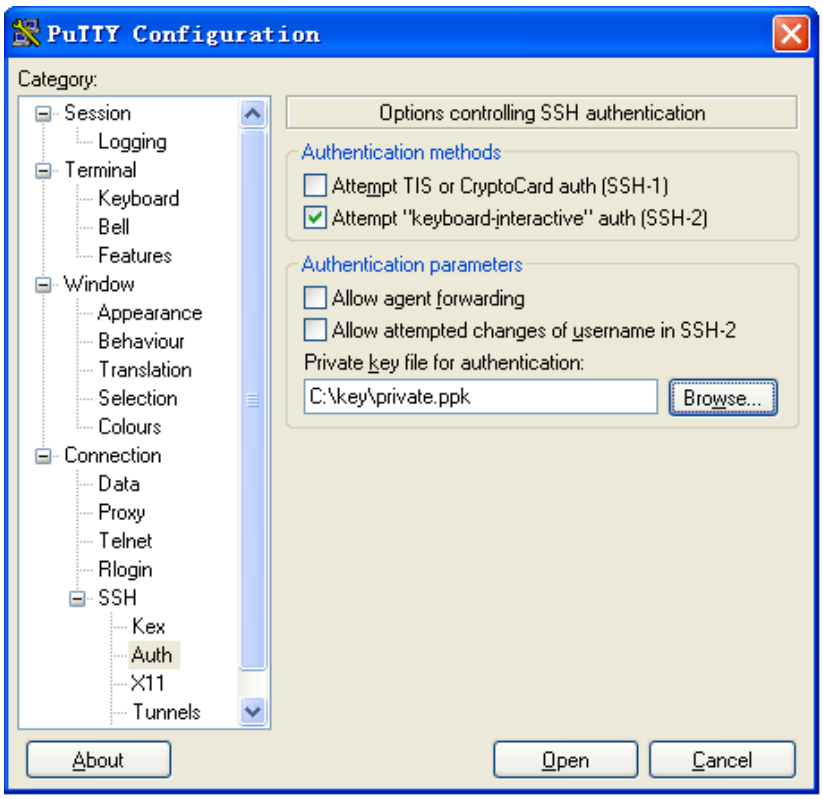


図 12-9 秘密鍵ファイルの指定

h)　ユーザ名を**client002**と入力し、Stelnetサーバにログインします。

12.7.3 パスワード認証を有効にした Stelnet クライアント設定例

I. ネットワーク要件

図 12-10に示すように設定します。

- Switch B は Stelnet サーバとして動作し、Stelnet クライアントを認証するためにパスワード認証を使用します。クライアントのユーザ名とパスワードは Switch B に保存されます。
- Switch A は Stelnet クライアントとして動作します。Switch A のユーザが Stelnet を通じて Switch B にログインした後、ユーザは network-administrator として Switch B を管理することができます。

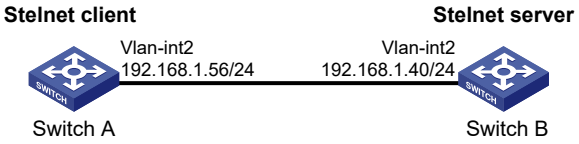


図 12-10 ネットワーク図

II. 設定手順

1)　Stelnet サーバを設定します。

RSA 鍵ペアを作成します。

```
<SwitchB> system-view
[SwitchB] public-key local create rsa
The range of public key modules is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.....++++++
.....++++++
..++++++++
.....++++++++
Create the key pair successfully.
```

DSA 鍵ペアを作成します。

```
[SwitchB] public-key local create dsa
The range of public key modules is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.++++++++++++++++++++++++++++++++++++++++++++++++*
.....+.....+.....+.....................................+
...+.................+.........+...+
Create the key pair successfully.
```

SSH サーバ機能を有効にします。

```
[SwitchB] ssh server enable
```

VLAN インタフェース 2に IP アドレスを割り当てます。SSH 接続の宛先アドレスとして Stelnet クライアントは VLAN インタフェース 2 の IP アドレスを使用します。

```
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] ip address 192.168.1.40 255.255.255.0
[SwitchB-Vlan-interface2] quit
```

ユーザラインの認証モードを AAA に設定します。

```
[SwitchB] line vty 0 63
[SwitchB-line-vty0-63] authentication-mode scheme
```

```
[SwitchB-line-vty0-63] quit
```

ローカル装置管理ユーザ **client001** を作成します。

```
[SwitchB] local-user client001 class manage
```

#ユーザのプレーンテキストのパスワードを **aabbcc**、サービスタイプを **ssh** に指定します。

```
[SwitchB-luser-manage-client001] password simple aabbcc
[SwitchB-luser-manage-client001] service-type ssh
```

ユーザのユーザロールを **network-admin** と設定します。

```
[SwitchB-luser-manage-client001] authorization-attribute user-role network-admin
[SwitchB-luser-manage-client001] quit
```

SSH ユーザ **client001** を作成します。ユーザのサービスタイプを **stelnet**、認証方式を **password** に設定します。SSH ユーザが作成されていない場合、デフォルトでパスワード認証が使用されます。

```
[SwitchB] ssh user client001 service-type stelnet authentication-type password
```

2) Stelnet サーバ 192.168.1.40 との接続を確立します。

VLAN インタフェース 2 に IP アドレスを割り当てます。

```
<SwitchA> system-view
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ip address 192.168.1.56 255.255.255.0
[SwitchA-Vlan-interface2] quit
[SwitchA] quit
```

サーバとの接続を確立する前に、クライアントでサーバのホスト公開鍵を設定するかどうかを決定することができます。

- クライアントでサーバのホスト公開鍵を設定する場合、以下の作業を行います。

サーバのホスト公開鍵を表示するため、サーバで **display public-key local dsa public** コマンドを使用します。（詳細は省略します。）

クライアントの public key view に移行し、サーバのホスト公開鍵をクライアントにコピーします。

```
[SwitchA] public-key peer key1
Enter public key view. Return to system view with "peer-public-key end" command.
[SwitchA-pkey-public-key-key1]308201B73082012C06072A8648CE3804013082011F028
18100D757262C4584C44C211F18BD96E5F0
[SwitchA-pkey-public-key-key1]61C4F0A423F7FE6B6B85B34CEF72CE14A0D3A5222F
E08CECE65BE6C265854889DC1EDBD13EC8B274
[SwitchA-pkey-public-key-key1]DA9F75BA26CCB987723602787E922BA84421F22C3C8
9CB9B06FD60FE01941DDD77FE6B12893DA76E
[SwitchA-pkey-public-key-key1]EBC1D128D97F0678D7722B5341C8506F358214B16A2
```

```
FAC4B368950387811C7DA33021500C773218C
[SwitchA-pkey-public-key-key1]737EC8EE993B4F2DED30F48EDACE915F0281810082
269009E14EC474BAF2932E69D3B1F18517AD95
[SwitchA-pkey-public-key-key1]94184CCDFCEAE96EC4D5EF93133E84B47093C52B20
CD35D02492B3959EC6499625BC4FA5082E22C5
[SwitchA-pkey-public-key-key1]B374E16DD00132CE71B020217091AC717B612391C76
C1FB2E88317C1BD8171D41ECB83E210C03CC9
[SwitchA-pkey-public-key-key1]B32E810561C21621C73D6DAAC028F4B1585DA7F4251
9718CC9B09EEF038184000 2818000AF995917
[SwitchA-pkey-public-key-key1]E1E570A3F6B1C2411948B3B4FFA256699B3BF871221
CC9C5DF257523777D033BEE77FC378145F2AD
[SwitchA-pkey-public-key-key1]D716D7DB9FCABB4ADBF6FB4FDB0CA25C761B308EF
53009F7101F7C62621216D5A572C379A32AC290
[SwitchA-pkey-public-key-key1]E55B394A217DA38B65B77F0185C8DB8095522D1EF04
4B465E8716261214A5A3B493E866991113B2D
[SwitchA-pkey-public-key-key1]485348
[SwitchA-pkey-public-key-key1] peer-public-key end
[SwitchA] quit
```

サーバへの SSH 接続を確立し、サーバのホスト公開鍵を指定します。

```
<SwitchA> ssh2 192.168.1.40 public-key key1
Username: client001
Press CTRL+C to abort.
Connecting to 192.168.1.40 port 22.
client001@192.168.1.40's password:
Enter a character ~ and a dot to abort.
<SwitchB>
```

正しいパスワードを入力した後、Switch B にログインすることができます。

- クライアントにサーバのホスト公開鍵がない場合、システムはサーバにアクセスするとき、アクセスを継続するかどうか確認する画面を表示します。サーバにアクセスするため、**Yes** を選択し、サーバのホスト公開鍵をダウンロードします。

```
<SwitchA> ssh2 192.168.1.40
Username: client001
Press CTRL+C to abort.
Connecting to 192.168.1.40 port 22.
The server is not authenticated. Continue? [Y/N]:y
Do you want to save the server public key? [Y/N]:y
client001@192.168.1.40's password:
Enter a character ~ and a dot to abort.
<SwitchB>
```

正しいパスワードを入力した後、Switch B にログインすることができます。サーバのホスト公開鍵はクライアントに保存されます。次回接続を行うとき、システムはサーバに認証するかどうか確認する画面を表示しません。

12.7.4 公開鍵認証を有効にした Stelnet クライアント設定例

I. ネットワーク要件

図 12-11に示すように設定します。

- Switch B は Stelnet サーバとして動作し、公開鍵認証と DSA 公開鍵アルゴリズムを使用します。
- Switch A は Stelnet クライアントとして動作します。Switch A のユーザが Stelnet を通じて Switch B にログインした後、ユーザは network-administrator として Switch B を管理することができます。

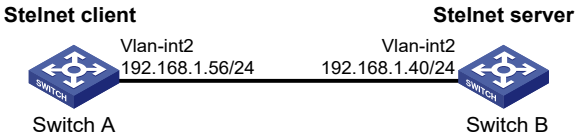


図 12-11 ネットワーク図

II. 設定手順

サーバの設定ではクライアント公開鍵が必要となります。Stelnet サーバを設定する前に、クライアントで DSA 鍵ペアを作成するためにクライアントソフトウェアを使用します。

1)　Stelnet クライアントを設定します。

VLAN インタフェース 2 に IP アドレスを割り当てます。

```
<SwitchA> system-view
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ip address 192.168.1.56 255.255.255.0
[SwitchA-Vlan-interface2] quit
```

DSA 鍵ペアを作成します。

```
[SwitchA] public-key local create dsa
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.++++++++++++++++++++++++++++++++++++++++++++++++*
........+......+.....+.....................................+
...+.................+..........+...+
Create the key pair successfully.
```

DSA ホスト公開鍵をファイル **key.pub** にエクスポートします。

```
[SwitchA] public-key local export dsa ssh2 key.pub
[SwitchA] quit
```

FTP あるいは TFTP を使用して、サーバに公開鍵ファイル **key.pub** を転送します。（詳細は省略します）

2)　Stelnet サーバを設定します。

RSA 鍵ペアを作成します。

```
<SwitchB> system-view
[SwitchB] public-key local create rsa
The range of public key modulus is (512 ~ 2048)
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.....................++++++
.................++++++
..++++++++
............++++++++
Create the key pair successfully.
```

DSA 鍵ペアを作成します。

```
[SwitchB] public-key local create dsa
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.++++++++++++++++++++++++++++++++++++++++++++++++*
........+......+.....+.....................................+
...+.................+..........+...+
Create the key pair successfully.
```

SSH サーバ機能を有効にします。

```
[SwitchB] ssh server enable
```

VLAN インタフェース 2に IP アドレスを割り当てます。SSH 接続の宛先アドレスとして Stelnet クライアントは VLAN インタフェース 2 の IP アドレスを使用します。

```
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] ip address 192.168.1.40 255.255.255.0
[SwitchB-Vlan-interface2] quit
```

ユーザラインの認証モードを AAA に設定します。

```
[SwitchB] line vty 0 63
[SwitchB-line-vty0-63] authentication-mode scheme
[SwitchB-line-vty0-63] quit
```

ファイル **key.pub** からピアの公開鍵をインポートし、名前を **switchkey** とします。

```
[SwitchB] public-key peer switchkey import sshkey key.pub
```

ローカル装置管理ユーザ **client002** を作成します。ユーザの認証方式を公開鍵に指定します。ユーザに公開鍵 **switchkey** を割り当てます。

```
[SwitchB] ssh user client002 service-type stelnet authentication-type publickey assign publickey switchkey
```

ローカル装置管理ユーザ **client002** を作成します。ユーザのサービスタイプを SSH に指定します。ユーザにユーザロール **network-admin** を割り当てます。

```
[SwitchB] local-user client002 class manage
[SwitchB-luser-manage-client002] service-type ssh
```

```
[SwitchB-luser-manage-client002] authorization-attribute user-role network-admin
[SwitchB-luser-manage-client002] quit
```

3)　Stelnet サーバ 192.168.1.40 に SSH 接続を確立します。

```
<SwitchA> ssh2 192.168.1.40 identity-key dsa
Username: client002
Press CTRL+C to abort.
Connecting to 192.168.1.40 port 22.
The server is not authenticated. Continue? [Y/N]:y
Do you want to save the server public key? [Y/N]:n
Enter a character ~ and a dot to abort.
<SwitchB>
```

サーバにアクセスするため **Yes** を選択し、サーバのホスト公開鍵をダウンロードします。次回接続を行うとき、クライアントはクライアントで保存されたサーバのホスト公開鍵を使用してサーバを認証します。

12.8 SFTP設定例

12.8.1 パスワード認証を有効にした SFTP サーバの設定例

I. ネットワーク要件

図 12-12に示すように設定します。

- SFTP サーバとして Switch が動作し、SFTP クライアントを認証するためにパスワード認証を使用します。クライアントのユーザ名とパスワードは Switch に保存されます。
- ホストは SFTP クライアントとして動作します。クライアントのユーザが SFTP を通じて Switch にログインした後、ユーザは network-administrator として Switch を設定したり管理することができます。

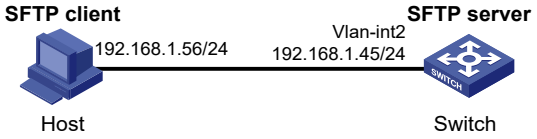


図 12-12 ネットワーク図

II. 設定手順

1)　SFTP サーバを設定します。

RSA 鍵ペアを作成します。

```
<Switch> system-view
[Switch] public-key local create rsa
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
```

```
Generating Keys...
.....................++++++
...................++++++
..++++++++
............++++++++
Create the key pair successfully.
```

DSA 鍵ペアを作成します。

```
[Switch] public-key local create dsa
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.++++++++++++++++++++++++++++++++++++++++++++++++*
........+......+.....+.................................+
...+..............+.........+...+
Create the key pair successfully.
```

SFTP サーバ機能を有効にします。

```
[Switch] sftp server enable
```

VLAN インタフェース 2 に IP アドレスを割り当てます。SFTP クライアントは SSH 接続用の宛先アドレスとして VLAN インタフェース 2 の IP アドレスを使用します。

```
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ip address 192.168.1.45 255.255.255.0
[Switch-Vlan-interface2] quit
```

ローカル装置管理ユーザ **client002** を作成します。プレーンテキストのパスワードを **aabbcc** とし、サービスタイプを **ssh** とします。ユーザにユーザロール **network-admin** を割り当て、作業ディレクトリを **flash:/**に設定します。

```
[Switch] local-user client002 class manage
[Switch-luser-manage-client002] password simple aabbcc
[Switch-luser-manage-client002] service-type ssh
[Switch-luser-manage-client002] authorization-attribute user-role network-admin work-directory flash:/
[Switch-luser-manage-client002] quit
```

ローカル装置管理ユーザ **client002** を作成します。ユーザの認証モードを **password**、サービスタイプを **sftp** に設定します。SSH ユーザが作成されていない場合、デフォルトでパスワード認証が使用されます。

```
[Switch] ssh user client002 service-type sftp authentication-type password
```

2) SFTP クライアントとサーバ間の接続を確立します。

装置は SFTP クライアントソフトウェアの異なるタイプをサポートします。この例では PuTTY バージョン 0.58 の PSFTP を動作させる SFTP クライアントを使用します。

🕮 **メモ：**

PSFTP はパスワード認証のみサポートしています。

SFTP サーバへの接続を確立するために、以下を行います。

a) 図 12-13に示すようにクライアントインタフェースを起動させるため、**psftp.exe**を動作させ、以下のコマンドを入力します。

```
open 192.168.1.45
```

b) SFTPサーバにログインするため、ユーザ名**client002**、パスワード**aabbcc**を入力します。

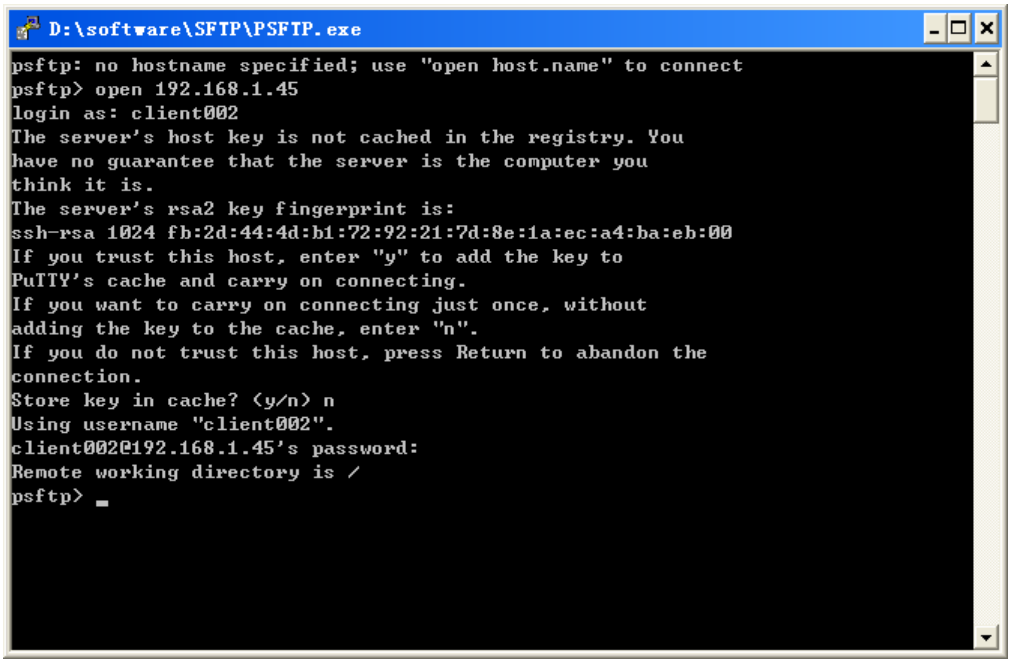


図 12-13 SFTP クライアントインタフェース

12.8.2 公開鍵認証を有効にした SFTP クライアント設定例

I. ネットワーク要件

図 12-14に示すように設定します。

- SFTP サーバとして Switch B が動作し、公開鍵認証、RSA 公開鍵アルゴリズムを使用します。
- Switch A は SFTP クライアントとして動作します。Switch A のユーザが SFTP を通じて Switch にログインした後、ユーザは network-administrator として Switch B でファイルの管理ができます。

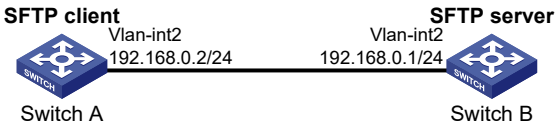


図 12-14 ネットワーク図

II. 設定手順

サーバの設定では、クライアントのホスト公開鍵が必要です。SFTP サーバを設定する前に、クライアントの RSA 鍵ペアを作成するため、クライアントソフトウェアを使用します。

1) SFTP クライアントを設定します。

VLAN インタフェース 2 に IP アドレスを設定します。

```
<SwitchA> system-view
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ip address 192.168.0.2 255.255.255.0
[SwitchA-Vlan-interface2] quit
```

RSA 鍵ペアを作成します。

```
[SwitchA] public-key local create rsa
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.....................++++++
.................++++++
..++++++++
............++++++++
Create the key pair successfully.
```

ホスト公開鍵をファイル **pubkey** にエクスポートします。

```
[SwitchA] public-key local export rsa ssh2 pubkey
[SwitchA] quit
```

公開鍵ファイル **pubkey** を FTP あるいは TFTP を使用してサーバに転送します。（詳細は省略します）

2) SFTP サーバを設定します。

RSA 鍵ペアを作成します。

```
<SwitchB> system-view
[SwitchB] public-key local create rsa
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.....................++++++
.................++++++
..++++++++
............++++++++
Create the key pair successfully.
```

DSA 鍵ペアを作成します。

```
[SwitchB] public-key local create dsa
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
```

```
.++++++++++++++++++++++++++++++++++++++++++++++++*
........+......+.....+.....................................+
...+.................+..........+...+
Create the key pair successfully.
```

SFTP サーバ機能を有効にします。

```
[SwitchB] sftp server enable
```

VLAN インタフェース 2 に IP アドレスを割り当てます。SFTP クライアントは SSH 接続用の宛先アドレスとして VLAN インタフェース 2 の IP アドレスを使用します。

```
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] ip address 192.168.0.1 255.255.255.0
[SwitchB-Vlan-interface2] quit
```

ファイルからピアの公開鍵 **pubkey** をインポートし、名前を **switchkey** とします。

```
[SwitchB] public-key peer switchkey import sshkey pubkey
```

SSH ユーザ **client001** を作成し、サービスタイプを **sftp** とし、認証方式を **publickey** とし、公開鍵を **switchkey** と設定します。

```
[SwitchB] ssh user client001 service-type sftp authentication-type publickey assign publickey switchkey
```

ローカル装置管理ユーザ **client001** を作成します。

```
[SwitchB] local-user client001 class manage
```

ユーザのサービスタイプを **ssh** に指定します。

```
[SwitchB-luser-manage-client001] service-type ssh
```

ユーザにユーザロール **network-admin** を割り当て、作業ディレクトリを **flash:/**に設定します。

```
[SwitchB-luser-manage-client001] authorization-attribute user-role network-admin work-directory flash:/
[SwitchB-luser-manage-client001] quit
```

3) SFTP クライアントとの接続を確立します。

SFTP サーバと接続を確立し、SFTP client view に移行します。

```
<SwitchA> sftp 192.168.0.1 identity-key rsa
Username: client001
Press CTRL+C to abort.
Connecting to 192.168.0.1 port 22.
The server is not authenticated. Continue? [Y/N]:y
Do you want to save the server public key? [Y/N]:n
sftp>
```

サーバで現在の作業ディレクトリのファイルを表示し、ファイル名 **z** を削除し、正常に削除されているか確認します。

```
sftp> dir -l
-rwxrwxrwx   1 noone    nogroup      1759 Aug 23 06:52 config.cfg
-rwxrwxrwx   1 noone    nogroup       225 Aug 24 08:01 pubkey2
-rwxrwxrwx   1 noone    nogroup       283 Aug 24 07:39 pubkey
drwxrwxrwx   1 noone    nogroup         0 Sep 01 06:22 new
-rwxrwxrwx   1 noone    nogroup       225 Sep 01 06:55 pub
-rwxrwxrwx   1 noone    nogroup         0 Sep 01 08:00 z
```

```
sftp> delete z
Removing /z
sftp> dir -l
-rwxrwxrwx   1 noone    nogroup      1759 Aug 23 06:52 config.cfg
-rwxrwxrwx   1 noone    nogroup       225 Aug 24 08:01 pubkey2
-rwxrwxrwx   1 noone    nogroup       283 Aug 24 07:39 pubkey
drwxrwxrwx   1 noone    nogroup         0 Sep 01 06:22 new
-rwxrwxrwx   1 noone    nogroup       225 Sep 01 06:55 pub
```

ディレクトリ名 **new1** を追加し、正常に作成されているか確認します。

```
sftp> mkdir new1
sftp> dir -l
-rwxrwxrwx   1 noone    nogroup      1759 Aug 23 06:52 config.cfg
-rwxrwxrwx   1 noone    nogroup       225 Aug 24 08:01 pubkey2
-rwxrwxrwx   1 noone    nogroup       283 Aug 24 07:39 pubkey
drwxrwxrwx   1 noone    nogroup         0 Sep 01 06:22 new
-rwxrwxrwx   1 noone    nogroup       225 Sep 01 06:55 pub
drwxrwxrwx   1 noone    nogroup         0 Sep 02 06:30 new1
```

ディレクトリ **new1** を **new2** に名前を変換し､正常に変更されていることを確認します。

```
sftp> rename new1 new2
sftp> dir -l
-rwxrwxrwx   1 noone    nogroup      1759 Aug 23 06:52 config.cfg
-rwxrwxrwx   1 noone    nogroup       225 Aug 24 08:01 pubkey2
-rwxrwxrwx   1 noone    nogroup       283 Aug 24 07:39 pubkey
drwxrwxrwx   1 noone    nogroup         0 Sep 01 06:22 new
-rwxrwxrwx   1 noone    nogroup       225 Sep 01 06:55 pub
drwxrwxrwx   1 noone    nogroup         0 Sep 02 06:33 new2
```

サーバからファイル **pubkey2** をダウンロードし、ローカルファイル **public** として保存します。

```
sftp> get pubkey2 public
Fetching / pubkey2 to public
/pubkey2                                      100% 225     1.4KB/s   00:00
```

ローカルファイル **pu** をサーバにアップロードし、**puk** として保存し、正常にアップロードされていることを確認します。

```
sftp> put pu puk
Uploading pu to / puk
sftp> dir -l
-rwxrwxrwx   1 noone    nogroup      1759 Aug 23 06:52 config.cfg
-rwxrwxrwx   1 noone    nogroup       225 Aug 24 08:01 pubkey2
-rwxrwxrwx   1 noone    nogroup       283 Aug 24 07:39 pubkey
drwxrwxrwx   1 noone    nogroup         0 Sep 01 06:22 new
drwxrwxrwx   1 noone    nogroup         0 Sep 02 06:33 new2
-rwxrwxrwx   1 noone    nogroup       283 Sep 02 06:35 pub
-rwxrwxrwx   1 noone    nogroup       283 Sep 02 06:36 puk
sftp>
```

SFTP client view から戻ります。

```
sftp> quit
<SwitchA>
```

12.9 SCP設定例

12.9.1 パスワード認証を有効にした SCP の設定例

I. ネットワーク要件

図 12-15に示すように設定します。

- SCP サーバとして Switch B が動作し、パスワード認証を使用します。クライアントのユーザ名とパスワードは Switch B に保存されます。
- SCP クライアントとして Switch A が動作します。Switch A のユーザが SCP を通して Switch B にログインした後、ネットワーク管理者として Switch 間のファイルを転送することができます。

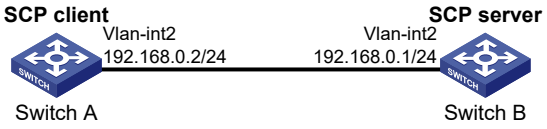


図 12-15 ネットワーク図

II. 設定手順

1)　SCP サーバを設定します。

RSA 鍵ペアを作成します。

```
<SwitchB> system-view
[SwitchB] public-key local create rsa
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.....................++++++
.................++++++
..++++++++
............++++++++
Create the key pair successfully.
```

DSA 鍵ペアを作成します。

```
[SwitchB] public-key local create dsa
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
```

```
.++++++++++++++++++++++++++++++++++++++++++++++++*
........+......+.....+.....................................+
...+................+.........+...+.
Create the key pair successfully.
```

SCP サーバ機能を有効にします。

```
[SwitchB] scp server enable
```

VLAN インタフェース 2 に IP アドレスを割り当てます。クライアントは SCP 接続用の宛先アドレスとして VLAN インタフェース 2 の IP アドレスを使用します。

```
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] ip address 192.168.0.1 255.255.255.0
[SwitchB-Vlan-interface2] quit
```

ローカル装置管理ユーザ **client001** を作成します。

```
[SwitchB] local-user client001 class manage
```

プレーンテキストのパスワードを **aabbcc** とします。

```
[SwitchB-luser-manage-client001] password simple aabbcc
```

サービスタイプを **ssh** とします。

```
[SwitchB-luser-manage-client001] service-type ssh
```

ユーザにユーザロール **network-admin** を割り当てます。

```
[SwitchB-luser-manage-client001] authorization-attribute user-role network-admin
[SwitchB-luser-manage-client001] quit
```

SSH ユーザ **client001** を作成します。ユーザの認証モードを **password**、サービスタイプを **scp** に設定します。

```
[SwitchB] ssh user client001 service-type scp authentication-type password
```

2) SCP クライアントの VLAN インタフェース 2 を IP アドレスに設定します。

```
<SwitchA> system-view
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ip address 192.168.0.2 255.255.255.0
[SwitchA-Vlan-interface2] quit
[SwitchA] quit
```

3) SCP サーバに接続し、サーバからファイル **remote.bin** をダウンロードし、ローカルファイル **local.bin** に保存します。

```
<SwitchA> scp 192.168.0.1 get remote.bin local.bin
Username: client001
Press CTRL+C to abort.
Connecting to 192.168.0.1 port 22.
The server is not authenticated. Continue? [Y/N]:y
Do you want to save the server public key? [Y/N]:n
client001@192.168.0.1's password:
remote.bin                                    100% 2875     2.8KB/s   00:00
```

目次

このセクションのページは **9-x-x** です。

13 章 SSL.....13-1

13章 SSL

SSL 設定に関するコンフィグについては、別紙の共通マニュアル”*QX シリーズ Ethernet スイッチ Web 認証オペレーションマニュアル（V7）*”の“*SSL*”を参照してください。

目次

このセクションのページは **9-x-x** です。

14 章 TCP フラグメントアタックプロテクション.....14-1
14.1 概要.....14-1
14.2 TCP フラグメントアタックプロテクション機能の設定.....14-1

14章 TCP フラグメントアタックプロテクション

14.1 概要

装置は、アタック検出機能、アタックプロテクション機能により攻撃者からの調査パケットを検出し、パケット廃棄によってプライベートネットワークの保護を行います。

装置は TCP フラグメントアタックプロテクションのみサポートします。

14.2 TCPフラグメントアタックプロテクション機能の設定

TCP フラグメントアタックプロテクション機能は、従来のパケットフィルタで検出できない TCP フラグメント攻撃を防ぐため、装置で TCP フラグメント攻撃のパケットを廃棄します。RFC 1858 で定義されているように、TCP フラグメントは以下のフラグメントを調査します。

- TCP ヘッダが 20 バイトよりも小さい、最初のフラグメント
- 8 バイトのフラグメントオフセットの 2 番目以降のフラグメント

装置の従来のパケットフィルタは、送信元 IP アドレス、宛先 IP アドレス、送信元ポート、宛先ポート、TCP パケットの最初のフラグメントのトランスポートレイヤプロトコルを検出します。最初のフラグメントが検出にパスした場合、残り全てのフラグメントパケットが透過することも許可してしまいます。

攻撃者は以下のような方法で TCP フラグメント攻撃を仕掛けることができてしまいます。

- TCP ヘッダの内、いくつかのフィールドを 2 番目のフラグメントに移動させ、2 番目のフラグメントの TCP フラグを不正にすることで、最初のフラグメントを十分に小さくします。
- フラグメントオフセットが 8 バイトになっている 2 番目以降のフラグメントを構成し、TCP フラグを最初のフラグメントとは異なる不正なものにします。フラグメントを受け取った装置はフラグメントから再構成するとき、2 番目以降の不正な TCP フラグで最初のフラグメントにある正常な TCP フラグを上書きしてしまいます。

従来のパケットフィルタでは、この最初のフラグメントでのフィルタができないために、2 番目以降のフラグメントも透過してしまいます。TCP フラグメントアタックは装置がフラグメントを再構成した後に起こります。

TCP フラグメント攻撃を防ぐため TCP フラグメントアタックプロテクションの設定を有効にします。

以下に TCP フラグメントアタックプロテクションの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. TCP フラグメントアタックプロテクションを有効にする	**attack-defense tcp fragment enable**	有効

目次

このセクションのページは **9-x-x** です。

15 章 IP ソースガード 15-1
15.1 概要 15-1
15.1.1 スタティック IP ソースガードバインディングエントリ 15-2
15.1.2 ダイナミック IP ソースバインディングエントリ 15-2
15.2 IP ソースガード設定作業リスト 15-3
15.3 IPv4 ソースガード機能の設定 15-3
15.3.1 IPv4 ソースガード機能の有効化 15-3
15.3.2 スタティック IPv4 ソースガードバインディングエントリの設定 15-4
15.4 IPv6 ソースガード機能の設定 15-5
15.4.1 IPv6 ソースガード機能の有効化 15-5
15.4.2 スタティック IPv6 ソースガードバインディングエントリの設定 15-5
15.5 IP ソースガードの表示と維持 15-6
15.6 IP ソースガードの設定例 15-6
15.6.1 スタティック IPv4 ソースガードの設定例 15-6
15.6.2 DHCP snooping を使用したダイナミック IPv4 ソースガードの設定例 15-8
15.6.3 DHCP relay を使用したダイナミック IPv4 ソースガードの設定例 15-9
15.6.4 スタティック IPv6 ソースガード設定例 15-11

15章 IP ソースガード

15.1 概要

IP ソースガード（IPSG）は、正式なパケットに一致させている IP ソースガードバインディングテーブルを使用して、なりすまし攻撃を防止します。IP ソースガードはテーブルに一致しないすべてのパケットを廃棄します。IP ソースガードはインタフェースごとのパケットフィルタです。ひとつのインタフェースに機能設定しても別のインタフェースのパケット転送には影響しません。

IP ソースガードバインディングテーブルは、グローバルとインタフェース指定バインディングを含むことができます。IP ソースガードは、最初にパケットの適合のためにインタフェース指定バインディングを使用します。適合しなかった場合、IP ソースガードはグローバルバインディングを使用します。IP ソースガードバインディングは以下のタイプに分かれます。

- IP-interface バインディングエントリ
- MAC-interface バインディングエントリ
- IP-MAC-interface バインディングエントリ
- IP-VLAN-interface バインディングエントリ
- MAC-VLAN-interface バインディングエントリ
- IP-MAC-VLAN-interface バインディングエントリ

IP ソースガードのバインディングエントリは手動で設定されたスタティックバインディングエントリと他のモジュールからの情報をもとに作成されたダイナミックバインディングエントリがあります。

図 15-1に示すように、インタフェースの IP ソースガードは IP ソースガードバインディングエントリの 1 つに一致するパケットのみ転送します。

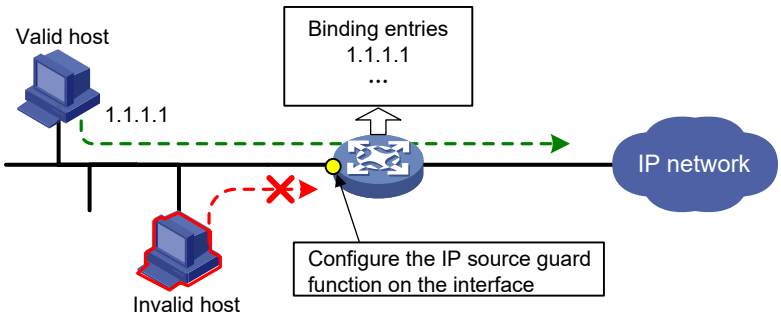


図 15-1 IP ソースガード機能のネットワーク図

🕮 メモ：

IP ソースガードはインタフェース毎にパケットをフィルタします。インタフェースで設定された IP ソースガード機能は他のインタフェースのパケットの転送には影響しません。

15.1.1 スタティック IP ソースガードバインディングエントリ

スタティックバインディングエントリは手動で設定されます。LAN 上に少数のホストしかなく、IP アドレスを手動で設定する場合に適しています。たとえば、サーバに接続するインタフェースでスタティック IP ソースガードバインディングエントリを設定することができます。このバインディングはサーバからのパケットのみ受信するインタフェースを許可します。

インタフェースの IP ソースガードバインディングは以下の機能をサポートします。

- インタフェースで受信する IPv4 パケットあるいは IPv6 をフィルタします。
- ユーザの妥当性を確認するため IPv4 パケットの ARP 検出機能と連携します。

ARP 検出についての詳細は、オペレーションマニュアルのセクション 9 *セキュリティ*" *ARP アタックプロテクション*" を参照してください。

スタティック IP ソースガードバインディングはインタフェースで有効です。IP ソースガードは最初にインタフェースで指定したバインディングを使用します。

- **指定インタフェースのスタティックバインディング**－interface view で IP アドレス、MAC アドレス、VLAN、あるいは IP アドレスと MAC アドレスと VLAN の組み合わせを割り当てます。バインディングはインタフェースにアクセスを試みるユーザの正当性を確認するため、インタフェースでのみ適用します。

🕮 **メモ**：

QX-S5100G シリーズはグローバルのスタティックバインディングをサポートしていません。

15.1.2 ダイナミック IP ソースバインディングエントリ

IP ソースガードはダイナミック IP ソースガードバインディングエントリを作成するため、他のモジュールからのユーザ情報を自動的に取得します。送信元モジュールは 802.1X、DHCP relay、DHCP snooping、DHCP server が含まれます。

DHCP ベースのダイナミック IP ソースガードは、LAN 上のホストが DHCP を通して IP アドレスを取得するシナリオに適しています。IP ソースガードは DHCP サーバ、DHCP snooping 装置あるいは DHCP リレー装置で設定されます。DHCP サーバ、DHCP snooping エントリあるいは DHCP リレーエントリをもとにしてダイナミック IP ソースガードバインディングエントリを作成します。IP ソースガードは通過できるように DHCP クライアントからのパケットのみ許可します。

I. ダイナミック IPv4 ソースガード

異なる送信元モジュールをもとにして作成されたダイナミックバインディングエントリは使用方法が異なります。

インタフェースタイプ	送信元モジュール	バインディングエントリの使用方法
レイヤ2 Ethernetポート	DHCP snooping 802.1X ARP snooping	パケットフィルタリング
VLANインタフェース	DHCPリレーエージェント	パケットフィルタリング

インタフェースタイプ	送信元モジュール	バインディングエントリの使用方法
	DHCPサーバ	モジュール（たとえばARP検出機能モジュール）と連携するため、セキュリティサービスを提供します。

802.1X についての詳細は、オペレーションマニュアルのセクション 9 *セキュリティ*”*802.1X*”を参照してください。DHCP snooping、DHCP relay、DHCP server についての詳細は、オペレーションマニュアルのセクション 4 *IP サービス*”*DHCP スヌーピング*”、”*DHCP リレーエージェント*”、”DHCP サーバ”を参照してください。

15.2 IPソースガード設定作業リスト

以下に IPv4 ソースガードを設定する作業リストを示します。

作業リスト
（必須設定項目）インタフェースのIPv4ソースガード機能の有効化
（オプション設定項目） スタティックIPv4ソースガードエントリの設定

以下に IPv6 ソースガードを設定する作業リストを示します。

作業リスト
（必須設定項目）インタフェースのIPv6ソースガード機能の有効化
（オプション設定項目） スタティックIPv6ソースガードエントリの設定

15.3 IPv4ソースガード機能の設定

15.3.1 IPv4 ソースガード機能の有効化

インタフェースで IP ソースガードを有効にするとき、スタティック IP ソースガード、ダイナミック IP ソースガードの両方が有効となります。

- スタティック IPv4 ソースガードは **ip source binding** コマンドを使用して設定されたスタティックバインディングを使用します。
- ダイナミック IPv4 ソースガードは関連する送信元モジュールからダイナミックバインディングを作成します。IPv4 ソースガードは **ip verify source** コマンドで指定された条件をもとにして受信 IPv4 パケットをフィルタするためバインディングを使用します。

ダイナミック IPv4 ソースガードを設定するために、802.1X、DHCP snooping あるいは DHCP relay 機能がネットワークで正常に動作することを確認してください。

以下にインタフェースで IPv4 ソースガード機能を有効にする設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー

操作	コマンド	補足
2． interface view に移行する	**interface** *interface-type interface-number*	サポートするインタフェースは以下です。 ● レイヤ2 Ethernetインタフェース ● VLANインタフェース
3． IPv4 ソースガード機能を有効にする	**ip verify source** { **ip-address** | **ip-address mac-address** | **mac-address** }	デフォルト：無効 このコマンドを複数行うと最後の設定が適用されます。

🕮 **メモ：**

ip verify source コマンドは運用前に設定しておくことを推奨します。DHCP snooping エントリが存在しているときに **ip verify source** コマンドを設定すると、一時的に通信が途切れる可能性があります。

15.3.2 スタティック IPv4 ソースガードバインディングエントリの設定

スタティック IPv4 ソースガードバインディングエントリはインタフェースでスタティック IPv4 ソースガードバインディングエントリを設定します。

I. インタフェースのスタティック IPv4 ソースガードバインディングエントリの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． interface view に移行する	**interface** *interface-type interface-number*	サポートするインタフェースは以下です。 ● レイヤ2 Ethernetインタフェース ● VLANインタフェース
3． スタティック IPv4 ソースガードバインディングエントリを設定する	**ip source binding** { **ip-address** *ip-address* | **ip-address** *ip-address* **mac-address** *mac-address* | **mac-address** *mac-address* } [**vlan** *vlan-id*]	デフォルト：設定なし **vlan** *vlan-id*オプションはLayer 2 Ethernet interface viewでのみサポートされます。 ARP検出機能のスタティックバインディングエントリを設定する場合、以下の設定を確認してください。 ● **ip-address** *ip-address*、**mac-address** *mac-address*、**vlan** *vlan-id*が設定されていること。 ● 指定のVLANでARP検出機能が有効になっていること。 複数のインタフェースに同じバインディングエントリを設定することができます。

15.4 IPv6ソースガード機能の設定

15.4.1 IPv6 ソースガード機能の有効化

インタフェースで IPv6 ソースガードを有効にするとき、スタティック IPv6 ソースガード、ダイナミック IPv6 ソースガードの両方が有効となります。

スタティック IPv6 ソースガードは **ipv6 source binding** コマンドを使用して設定されたスタティックバインディングを使用します。

以下にインタフェースで IPv6 ソースガード機能を有効にする設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. interface view に移行する	**interface** *interface-type interface-number*	サポートするインタフェースは以下です。 ● レイヤ2 Ethernetインタフェース ● VLANインタフェース
3. IPv6 ソースガード機能を有効にする	**ipv6 verify source** { **ip-address** | **ip-address mac-address** | **mac-address** }	デフォルト：無効 このコマンドを複数行うと最後の設定が適用されます。

15.4.2 スタティック IPv6 ソースガードバインディングエントリの設定

スタティック IPv6 ソースガードバインディングエントリはインタフェースでスタティック IPv6 ソースガードバインディングエントリを設定します。

I. インタフェースのスタティック IPv6 ソースガードバインディングエントリの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. interface view に移行する	**interface** *interface-type interface-number*	サポートするインタフェースは以下です。 ● レイヤ2 Ethernetインタフェース ● VLANインタフェース
3. スタティック IPv6 ソースガードバインディングエントリを設定する	**ipv6 source binding** { **ip-address** *ipv6-address* | **ip-address** *ipv6-address* **mac-address** *mac-address* | **mac-address** *mac-address* } [**vlan** *vlan-id*]	デフォルト：設定なし **vlan** *vlan-id*オプションはLayer 2 Ethernet interface viewでのみサポートします。 複数のインタフェースに同じバインディングエントリを設定することができます。

15.5 IPソースガードの表示と維持

すべての view で **display** コマンドを実行でき、user view で **reset** コマンドを実行できます。

以下に IPv4 ソースガードのコマンドを示します。

操作	コマンド
IPv4ソースガードバインディングエントリを表示する	**display ip source binding** [**static** | [**arp-snooping-vlan** | **dhcp-relay** | **dhcp-server** | **dhcp-snooping**]] [**ip-address** *ip-address*] [**mac-address** *mac-address*] [**vlan** *vlan-id*] [**interface** *interface-type interface-number*] [**slot** *slot-number*]

以下に IPv6 ソースガードのコマンドを示します。

操作	コマンド
IPv6ソースガードバインディングエントリを表示する	**display ipv6 source binding** [**static**] [**ip-address** *ipv6-address*] [**mac-address** *mac-address*] [**vlan** *vlan-id*] [**interface** *interface-type interface-number*] [**slot** *slot-number*]

15.6 IPソースガードの設定例

15.6.1 スタティック IPv4 ソースガードの設定例

I. ネットワーク要件

図 15-2に示すように、すべてのホストはスタティック IP アドレスを使用しています。

以下の要件に適合するように Switch A と Switch B でスタティック IPv4 ソースガードバインディングエントリを設定します。

- Switch A の GigabitEthernet 1/0/2 は Host C からの IP パケットのみ許可します。
- Switch A の GigabitEthernet 1/0/1 は Host A からの IP パケットのみ許可します。
- Switch B のすべてのインタフェースは Host A からの IP パケットのみ許可します。
- Switch B の GigabitEthernet 1/0/1 は Host B からの IP パケットのみ許可します。

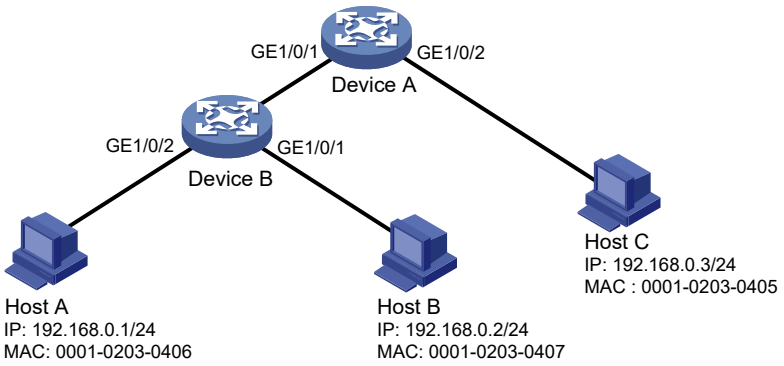


図 15-2 ネットワーク図

II. 設定手順

1)　Switch A を設定します。

インタフェースに IP アドレスを設定します。（詳細は省略します。）

GigabitEthernet 1/0/2 で IPv4 ソースガードを有効にします。

```
<SwitchA> system-view
[SwitchA] interface gigabitethernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] ip verify source ip-address mac-address
```

GigabitEthernet 1/0/2 で Host C のスタティック IPv4 ソースガードバインディングエントリを設定します。

```
[SwitchA-GigabitEthernet1/0/2] ip source binding ip-address 192.168.0.3 mac-address 0001-0203-0405
[SwitchA-GigabitEthernet1/0/2] quit
```

GigabitEthernet 1/0/1 で IPv4 ソースガードを有効にします。

```
[SwitchA] interface gigabitethernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] ip verify source ip-address mac-address
```

GigabitEthernet 1/0/1 で Host A のスタティック IPv4 ソースガードバインディングエントリを設定します。

```
[SwitchA-GigabitEthernet1/0/1] ip source binding ip-address 192.168.0.1 mac-address 0001-0203-0406
[SwitchA-GigabitEthernet1/0/1] quit
```

2)　Switch B を設定します。

インタフェースに IP アドレスを設定します。（詳細は省略します。）

GigabitEthernet 1/0/2 で IPv4 ソースガードを有効にします。

```
<SwitchB> system-view
[SwitchB] interface gigabitethernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] ip verify source ip-address mac-address
[SwitchB-GigabitEthernet1/0/2] quit
```

Host A のスタティック IPv4 ソースガードバインディングエントリを設定します。

```
[SwitchB] ip source binding ip-address 192.168.0.1 mac-address 0001-0203-0406
```

GigabitEthernet 1/0/1 で IPv4 ソースガードを有効にします。

```
[SwitchB] interface gigabitethernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] ip verify source ip-address mac-address
```

GigabitEthernet 1/0/1 で Host B のスタティック IPv4 ソースガードバインディングエントリを設定します。

```
[SwitchB-GigabitEthernet1/0/1] ip source binding mac-address 0001-0203-0407
[SwitchB-GigabitEthernet1/0/1] quit
```

III. 設定の確認

Switch A でスタティック IPv4 ソースガードバインディングエントリが正しく設定されていることを確認します。

```
<SwitchA> display ip source binding static
Total entries found: 2
IP Address      MAC Address    Interface                VLAN Type
192.168.0.1     0001-0203-0405 GE1/0/2                  N/A  Static
192.168.0.3     0001-0203-0406 GE1/0/1                  N/A  Static
```

Switch B でスタティック IPv4 ソースガードバインディングエントリが正しく設定されていることを確認します。

```
<SwitchB> display ip source binding static
Total entries found: 2
IP Address      MAC Address    Interface              VLAN Type
192.168.0.1     0001-0203-0406 N/A                    N/A  Static
N/A             0001-0203-0407 GE1/0/1                N/A  Static
```

15.6.2 DHCP snooping を使用したダイナミック IPv4 ソースガードの設定例

I. ネットワーク要件

図 15-3に示すように、Host（DHCP クライアント）は DHCP サーバから IP アドレスを取得します。

DHCP snooping エントリにホストの IPv4 アドレスと MAC アドレスを記録するため、装置で DHCP snooping を有効にします。

DHCP snooping エントリをもとにして受信したパケットをフィルタするため、GigabitEthernet 1/0/1 でダイナミック IPv4 ソースガードを有効にします。DHCP サーバから IP アドレスを取得したクライアントからのパケットのみを許可するように、フィルタします。

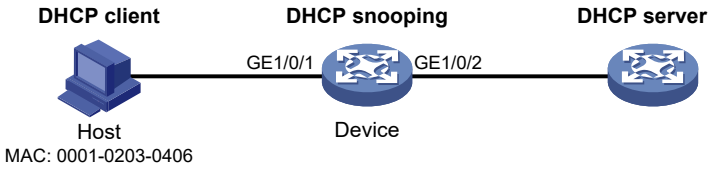


図 15-3 ネットワーク図

II. 設定手順

1)　DHCP サーバを設定します。

DHCP サーバの設定については、オペレーションマニュアルのセクション 4 *IP サービス*” *DHCP サーバ*”を参照してください。

2)　Switch を設定します。

インタフェースの IP アドレスを設定します。（詳細は省略します。）

DHCP snooping を有効にします。

```
<Switch> system-view
[Switch] dhcp snooping enable
```

トラステッドインタフェースとして GigabitEthernet 1/0/2 を設定します。

```
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] dhcp snooping trust
[Switch-GigabitEthernet1/0/2] quit
```

GigabitEthernet 1/0/1 で IPv4 ソースガードを有効にし、ダイナミック IP ソースガードの送信元 IP アドレスと送信元 MAC アドレスを確認します。

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] ip verify source ip-address mac-address
```

GigabitEthernet 1/0/1 で DHCP snooping エントリのクライアント情報を記録するように設定します。

```
[Switch-GigabitEthernet1/0/1] dhcp snooping binding record
[Switch-GigabitEthernet1/0/1] quit
```

III. 設定の確認

DHCP snooping から取得したダイナミック IPv4 ソースガードバインディングエントリを確認します。

```
[Switch] display ip source binding dhcp-snooping
Total entries found: 1
IP Address      MAC Address    Interface              VLAN Type
192.168.0.1     0001-0203-0406 GE1/0/1                1    DHCP snooping
```

出力は、IP ソースガードに DHCP snooping エントリをもとにしたダイナミック IPv4 ソースガードバインディングエントリが作成されていることを示します。

15.6.3 DHCP relay を使用したダイナミック IPv4 ソースガードの設定例

I. ネットワーク要件

図 15-4に示すように、DHCP relay は Switch で有効に設定されています。Host は DHCP relay エージェントを通して DHCP サーバから IP アドレスを取得します。

Switch で作成された DHCP relay エントリをもとにして受信したパケットをフィルタするため、VLAN インタフェース 100 でダイナミック IPv4 ソースガードを有効にします。

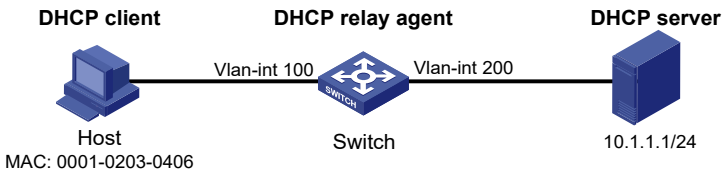


図 15-4 ネットワーク図

II. 設定手順

1)　ダイナミック IPv4 ソースガードを設定します。

インタフェースで IP アドレスを設定します。（詳細は省略します。）

VLAN インタフェース 100 で IPv4 ソースガードを有効にし、ダイナミック IP ソースガードの送信元 IP アドレスと送信元 MAC アドレスを確認します。

```
<Switch> system-view
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ip verify source ip-address mac-address
[Switch-Vlan-interface100] quit
```

2)　DHCP relay エージェントを設定します。

DHCP サービスを有効にします。

```
[Switch] dhcp enable
```

DHCP relay クライアントエントリの記録を有効にします。

```
[Switch] dhcp relay client-information record
```

DHCP relay モードで動作するように VLAN インタフェース 100 を設定します。

```
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] dhcp select relay
```

DHCP サーバの IP アドレスを指定します。

```
[Switch-Vlan-interface100] dhcp relay server-address 10.1.1.1
[Switch-Vlan-interface100] quit
```

III. 設定の確認

ダイナミック IPv4 ソースガードバインディングエントリを確認します。

```
[Switch] display ip source binding dhcp-relay
Total entries found: 1
IP Address      MAC Address    Interface              VLAN Type
192.168.0.1     0001-0203-0406 Vlan100                100  DHCP relay
```

出力は、DHCP relay エントリをもとにしたダイナミック IPv4 ソースガードバインディングエントリが作成されていることを示します。

15.6.4 スタティック IPv6 ソースガード設定例

I. ネットワーク要件

図 15-5に示すように、Host からの IPv6 パケットのみ許可するように装置の GigabitEthernet 1/0/1 のスタティック IPv6 ソースガードバインディングエントリを設定します。

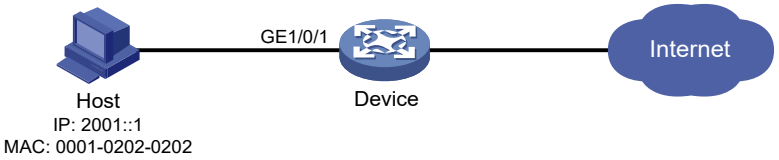


図 15-5 ネットワーク図

II. 設定手順

GigabitEthernet 1/0/1 で IPv6 ソースガードを有効にします。

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] ipv6 verify source ip-address mac-address
```

GigabitEthernet 1/0/1 で Host のスタティック IPv6 ソースガードバインディングエントリを設定します。

```
[Switch-GigabitEthernet1/0/1] ipv6 source binding ip-address 2001::1 mac-address 0001-0202-0202
[Switch-GigabitEthernet1/0/1] quit
```

装置でスタティック IPv6 ソースガードバインディングエントリを確認します。

```
[Switch] display ipv6 source binding static
Total entries found: 1
IPv6 Address          MAC Address    Interface              VLAN Type
2001::1               0001-0202-0202 GE1/0/1                N/A  Static
```

出力はスタティック IPv6 ソースガードバインディングエントリが正常に設定されていることを示します。

目次

このセクションのページは **9-x-x** です。

16 章 ARP アタックプロテクション.....16-1
16.1 ARP アタックプロテクション設定作業リスト.....16-1
16.2 宛先不明の IP アタックプロテクションの設定.....16-1
16.2.1 ARP 送信元抑制機能の設定.....16-2
16.2.2 ARP ブラックホールルーティング機能の設定.....16-2
16.2.3 宛先不明の IP アタックプロテクションの表示と維持.....16-3
16.2.4 設定例.....16-3
16.3 ARP パケットレートリミットの設定.....16-4
16.4 送信元 MAC アドレスにもとづく ARP アタック detection の設定.....16-5
16.4.1 設定手順.....16-5
16.4.2 送信元 MAC アドレスにもとづく ARP アタック detection の表示と維持.....16-6
16.4.3 設定例.....16-6
16.5 ARP パケット送信元 MAC アドレス正当性チェックの設定.....16-8
16.6 ARP 確認応答の設定.....16-8
16.7 ARP アタック detection の設定.....16-8
16.7.1 ユーザの正当性の確認の設定.....16-9
16.7.2 設定ガイドライン.....16-9
16.7.3 設定手順.....16-10
16.7.4 ARP パケット正当性の確認の設定.....16-10
16.7.5 ARP 制限転送の設定.....16-11
16.7.6 ARP アタック detection の表示と維持.....16-11
16.7.7 ユーザの正当性の確認の設定例.....16-12
16.7.8 ユーザの正当性の確認と ARP パケットの正当性の確認の設定例.....16-13
16.7.9 ARP 制限転送の設定例.....16-15
16.8 ARP スキャンの設定.....16-17
16.8.1 ARP スキャンの設定.....16-17
16.8.2 制限とガイドライン.....16-18
16.8.3 設定手順.....16-18
16.9 ARP ゲートウェイプロテクションの設定.....16-18
16.9.1 設定ガイドライン.....16-19
16.9.2 設定手順.....16-19
16.9.3 設定例.....16-19
16.10 ARP フィルタリングの設定.....16-20
16.10.1 設定ガイドライン.....16-21
16.10.2 設定手順.....16-21
16.10.3 設定例.....16-21

16章 ARP アタックプロテクション

ARP アタックとウイルスは LAN のセキュリティを脅かしています。この章では、そのような ARP アタックを発見、防御するための機能について記載します。

ARP は実装が容易ですが、セキュリティメカニズムを持っていないため、ネットワーク攻撃に対して脆弱です。攻撃者は ARP の脆弱性を悪用し、以下の方法でネットワーク装置を攻撃する可能性があります。

- 信頼されたユーザあるいは、ゲートウェイによるものとして見せかけた ARP パケットを送信し、装置は不正な ARP をエントリに追加します。
- 大量の宛先 MAC アドレス到達不能の IP パケットによって、受信装置の CPU が過負荷になるまで IP アドレスの解決処理を行います。ARP は到達不能の IP パケットに対応する MAC アドレスを検出することができません。
- 大量の ARP パケットによって、受信装置の CPU が過負荷になります。

ARP 攻撃の機能とタイプの詳細は ARP アタックプロテクションの技術資料を参照してください。

16.1 ARPアタックプロテクション設定作業リスト

作業リスト
フラッド防御： ● 宛先不明のIPアタックプロテクションの設定（ゲートウェイで設定します。） 　● ARP送信元抑制機能の設定 　● ブラックホールルーティング機能の設定 ● パケットレートリミットの設定（アクセス装置で設定します。） ● 送信元MACアドレスにもとづくARPアタックdetectionの設定（ゲートウェイで設定します。）
ユーザとゲートウェイのなりすましの防御： ● ARPパケット送信元MACアドレス正当性チェックの設定（ゲートウェイで設定します。） ● ARP 確認応答の設定（ゲートウェイで設定します。） ● ARP detectionの設定（アクセス装置で設定します。）

16.2 宛先不明のIPアタックプロテクションの設定

装置がホストから大量の宛先不明の IP パケットを受信した場合、以下の状況が発生します。

- 装置は宛先サブネットに対して大量の ARP リクエストを送信して、宛先サブネットの負荷が増大します。
- 装置は宛先 IP アドレスの解決処理を続けて、CPU の負荷が増大します。

宛先不明の IP パケット攻撃から装置を守るため、以下の機能を設定することができます。

- **ARP 送信元抑制機能**– 攻撃パケットが同じ送信元アドレスである場合、ARP 送信元抑制機能を有効にすることができます。5秒以内にホストから受信した宛先不明の IP パケットが指定したしきい値を超えた場合、装置は次の 5秒間にホストから受信したパケットによる ARP リクエスト送信を停止します。この機能は ARP 攻撃のパケットが同一送信元アドレスである場合、適用可能です。
- **ARP ブラックホールルーティング機能**– 宛先不明の IP アドレス宛のブラックホールのルートを作成します。装置はブラックホールのルートが削除されるまで宛先不明の IP アドレス宛にマッチするパケットを廃棄します。ブラックホールのルートはエージングタイマが終了する、あるいはルートが到達可能になったとき、削除されます。

  宛先不明の IP アドレスのブラックホールのルートが作成された後、装置はすぐに ARP リクエストを行う、最初の ARP ブラックホールの調査を開始します。IP アドレスの解決に失敗したとき、装置は設定に従って調査を継続します。装置がすべての調査を完了する前に ARP ブラックホールのエージングタイマが終了した場合、装置はブラックホールのルートを削除します。残りの調査は行いません。

  この機能は、攻撃パケットが同じ送信元アドレスかどうかにかかわらず、適用可能です。

16.2.1 ARP 送信元抑制機能の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. ARP 送信元抑制機能を有効にする	**arp source-suppression enable**	デフォルト：無効
3. 装置が 5秒以内にホストから受信できる宛先不明のパケットの最大数を設定する	**arp source-suppression limit** *limit-value*	デフォルト：10

16.2.2 ARP ブラックホールルーティング機能の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. ARP ブラックホールルーティング機能を有効にする	**arp resolving-route enable**	デフォルト：有効
3. （オプション設定項目）宛先不明の IP アドレスの ARP ブラックホールのルートを調査する回数を設定する	**arp resolving-route probe-count** *count*	デフォルト：3回
4. （オプション設定項目）ARP ブラックホールのルートを調査する間隔を設定する	**arp resolving-route probe-interval** *interval*	デフォルト：1秒

16.2.3 宛先不明の IP アタックプロテクションの表示と維持

すべての view で **display** コマンドを実行することができます。

操作	コマンド
ARP送信元抑制機能の設定情報を表示する	**display arp source-suppression**

16.2.4 設定例

I. ネットワーク要件

図 16-1に示すように、LAN には VLAN10 の R&D エリアと VLAN20 の Office エリアが含まれます。これら 2 つのエリアはアクセススイッチを通してゲートウェイ（Device）に接続します。

大量の ARP リクエストが Office エリアで検出された場合、宛先不明の IP パケットによる攻撃が考えられます。このような攻撃を避けるために、ARP 送信元抑制や ARP ブラックホールルーティングの設定を行います。

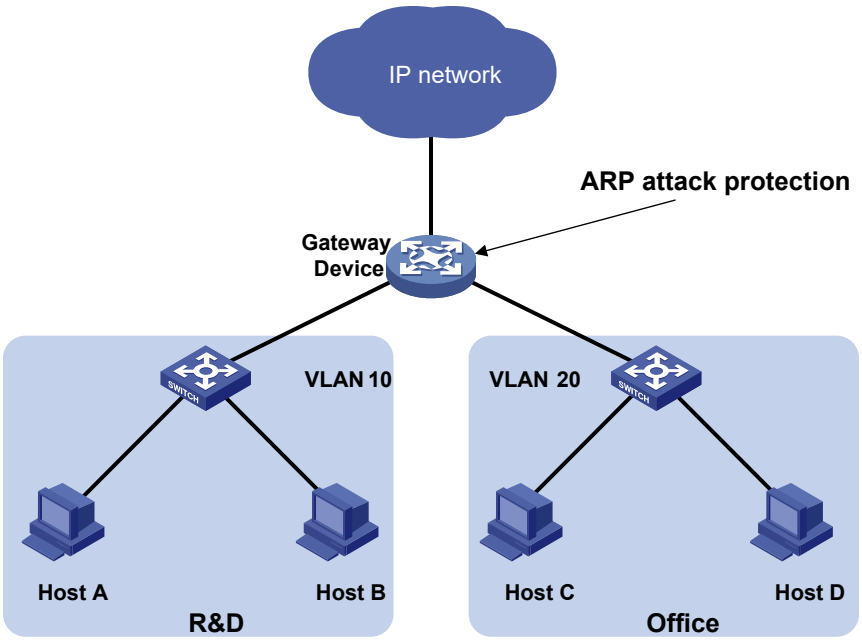


図 16-1 ネットワーク図

II. 設定手順

- 攻撃パケットが同一送信元アドレスである場合、ARP 送信元抑制機能を以下のように設定します。

ARP 送信元抑制機能を有効にします。

```
<Device> system-view
```

```
[Device] arp source-suppression enable
```

5 秒間の同一送信元からの ARP パケットのしきい値を 100 に設定します。

```
[Device] arp source-suppression limit 100
```

- 攻撃パケットが異なる送信元アドレスである場合、ゲートウェイで ARP ブラックホールルーティング機能を有効にします。

ARP ブラックホールルーティング機能を有効にします。

```
[Device] arp resolving-route enable
```

16.3 ARPパケットレートリミットの設定

I. ARP パケットレートリミットの設定

ARP パケットレートリミット機能は CPU に送信される ARP パケットのレートを制限します。ARP 検出が有効な装置は確認するため CPU に受信したすべての ARP パケットを送信します。大量の ARP パケットの処理を行う結果、他の機能への悪影響、あるいは装置がクラッシュする可能性があります。これを防ぐために、ARP パケットレートリミットを設定します。インタフェースでの ARP パケットの受信レートがレートリミットを超えると、これらのパケットは廃棄されます。

ARP パケットレートリミットにより SNMP モジュールへの notification あるいはログメッセージの送信を有効にすることができます。

- notification の送信が有効の場合、装置は notification の送信間隔以内に、もっとも高いしきい値と交差した ARP パケットのレートを、SNMP モジュールへ送信します。notification タイプ（inform あるいは trap）、宛先ホストを設定するため、**snmp-agent target-host** コマンドを使用する必要があります。notification の詳細は、コマンドマニュアルのセクション 11 *システム管理”SNMP”* を参照してください。
- ARP のログメッセージの送信が有効である場合、装置はログメッセージの送信間隔以内に、もっとも高いしきい値と交差した ARP パケットのレートを、information center へ送信します。information center の出力ルールを設定することができます。information center の詳細は、オペレーションマニュアルのセクション 11 *システム管理”Information Center”* を参照してください。

II. 制限とガイドライン

ARP アタック検知を有効にしたとき、あるいは ARP フラッド攻撃を検出したとき、ARP パケットレートリミットの設定を行うことを推奨します。

過剰な notification とログメッセージが送信された場合、ARP パケットレートリミットの設定によって、notification とログメッセージの送信間隔を増やすことができます。

アグリゲートインタフェースで ARP パケットレートリミット機能の notification、ログメッセージの送信を有効にした場合、すべてのアグリゲーションメンバポートに適用します。

III. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. （オプション設定項目）ARP パケットレートリミットの notification の送信を有効にする	**snmp-agent trap enable arp** [**rate-limit**]	デフォルト：無効
3. （オプション設定項目）ARP パケットレートリミットのロギングを有効にする	**arp rate-limit log enable**	デフォルト：無効
4. （オプション設定項目）ARP パケットレートリミットの notification、ログメッセージを送信する送信間隔を設定する	**arp rate-limit log interval** *interval*	デフォルト：60秒
5. Layer 2 Ethernet interface あるいは Layer 2 aggregate interface view に移行する	**interface** *interface-type interface-number*	―
6. ARP パケットレートリミットを有効にし、レートリミットを設定する	**arp rate-limit** [*pps*]	デフォルト：有効 レートリミット：100pps

16.4 送信元MACアドレスにもとづくARPアタックdetectionの設定

この機能は CPU に送られる ARP パケットの数を確認します。5 秒間に同じ送信元からの ARP パケットの受信した数がしきい値を超えた場合、装置は、この MAC アドレスを ARP アタックエントリテーブルに追加します。エントリのエージングタイマが終了する前に、装置は以下の方法で攻撃に対応します。

- **モニタモード** ― ログメッセージを作成します。
- **フィルタモード** ― ログメッセージを作成し、攻撃する MAC アドレスからの後続の ARP パケットをフィルタします。

送信元 MAC アドレスにもとづく ARP アタック detection 機能を有効にする前に、ARP ロギング機能を有効にしたことを確認してください。ARP ロギング機能の詳細は、オペレーションマニュアルのセクション 4 *IP サービズ*”*ARP*”を参照してください。

この機能ではゲートウェイやサーバの MAC アドレスを除外するように設定することができます。ゲートウェイやサーバの MAC アドレスを除外した場合、たとえ攻撃者からの ARP パケットだとしても、除外された ARP パケットの確認を行いません。

16.4.1 設定手順

以下に送信元 MAC アドレスにもとづく ARP アタック detection の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. 送信元 MAC アドレスにもとづく ARP アタック detection を有効にし、モードを指定する	**arp source-mac** { **filter** | **monitor** }	デフォルト：無効
3. しきい値を設定する	**arp source-mac threshold** *threshold-value*	デフォルト：30
4. ARP アタックエントリのエージングタイマを設定する	**arp source-mac aging-time** *time*	デフォルト：300秒
5. （オプション設定項目）ARP アタック detection 機能から除外する MAC アドレスを設定する	**arp source-mac exclude-mac** *mac-address*&<1-10>	デフォルト：設定なし

🕮 **メモ：**
ARP アタックエントリのエージングタイマが終了したとき、エントリの MAC アドレスからの ARP パケットは正常に処理することができます。

16.4.2 送信元 MAC アドレスにもとづく ARP アタック detection の表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
送信元MACアドレスにもとづくARPアタックdetectionで検出されたARPアタックエントリを表示する	**display arp source-mac** { **slot** *slot-number* | **interface** *interface-type interface-number* }

16.4.3 設定例

I. ネットワーク要件

図 16-2に示すように、Host はゲートウェイ（Device）を介してインターネットにアクセスします。悪意のあるユーザがゲートウェイに大量の ARP 要求を送信した場合、ゲートウェイがクラッシュする可能性があり、クライアントからの要求を処理できません。この問題を解決するために、ゲートウェイ上で送信元 MAC アドレスにもとづく ARP アタック detection を設定します。

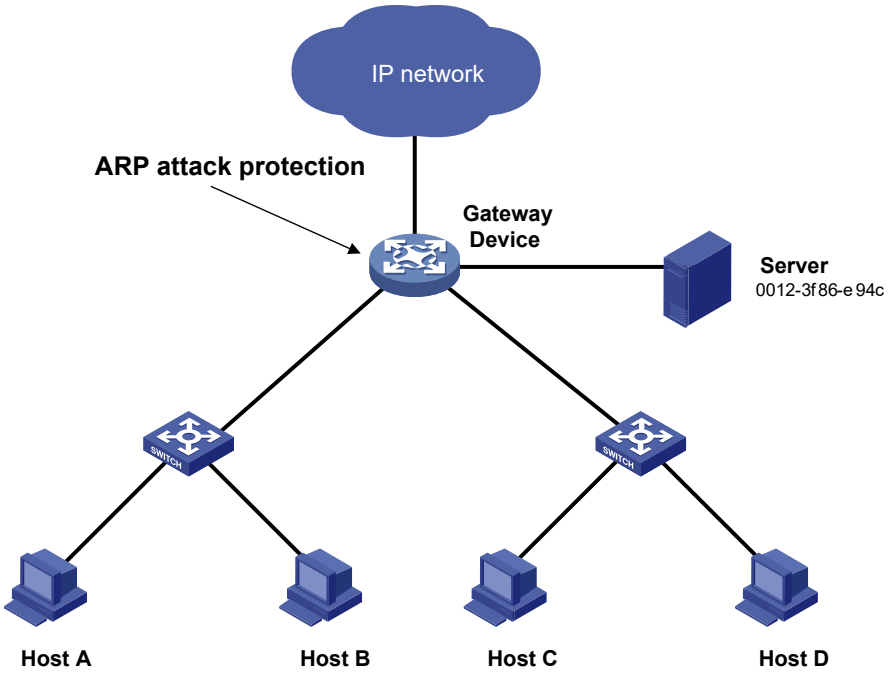


図 16-2 ネットワーク図

II. 設定要件

攻撃者は、有効な Host の MAC アドレスを送信元 MAC アドレスとして使用し、ARP パケットを大量に偽造することがあります。このような攻撃を防ぐために、次の手順でゲートウェイを設定します。

1) 送信元 MAC アドレスにもとづく ARP アタック detection を有効にし、フィルタモードを指定します。
2) しきい値を設定します。
3) ARP アタックエントリのエージングタイマを設定します。
4) この機能からサーバの MAC アドレスを除外します。

III. 設定手順

送信元 MAC アドレスにもとづく ARP アタック detection を有効にし、フィルタモードを指定します。

```
<Device> system-view
[Device] arp source-mac filter
```

しきい値を 30 に設定します。

```
[Device] arp source-mac threshold 30
```

ARP アタックエントリのエージングタイマを 60 秒に設定します。

```
[Device] arp source-mac aging-time 60
```

MAC アドレス 0012-3f86-e94c を除外します。

```
[Device] arp source-mac exclude-mac 0012-3f86-e94c
```

16.5 ARPパケット送信元MACアドレス正当性チェックの設定

この機能を有効にすることで、ゲートウェイはイーサネットヘッダの送信元 MAC アドレスが ARP メッセージのメッセージ部分にある送信元 MAC アドレスと異なる場合、ARP パケットをフィルタします。これによりゲートウェイは正しい ARP エントリを学習します。

以下に ARP パケット送信元 MAC アドレス正当性チェックの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. ARP パケット送信元 MAC アドレス正当性チェックを設定する	**arp valid-check enable**	デフォルト：無効

16.6 ARP確認応答の設定

ユーザのなりすましを防御するため、ARP 確認応答機能をゲートウェイで設定します。

ARP 確認応答機能は､ゲートウェイが不正な ARP エントリを作成することを防御します。

以下に ARP 確認応答機能の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. ARP 確認応答機能を有効にする	**arp active-ack enable**	デフォルト：無効

16.7 ARP アタックdetectionの設定

ARP アタック detection 機能は、ユーザやゲートウェイのなりすまし攻撃を防ぐため、許可されていないクライアントの ARP パケットをブロックするようにアクセス装置で有効にします。ARP detection 機能は ARP トラステッドポートから受信した ARP パケットを確認しません。

ARP アタック detection 機能は、以下の特徴があります。

- ユーザの正当性確認
- ARP パケットの正当性の確認
- ARP 制限転送
- ARP アタック detection ロギング
- ユーザの正当性の確認と ARP パケットの正当性の確認

ARP パケットの正当性とユーザの正当性の両方が有効である場合、最初に ARP パケットの正当性の確認を行い、次にユーザの正当性の確認を行います。

ARP snooping と一緒に ARP アタック detection を設定しないでください。さもないと、ARP snooping エントリが作成されません。

16.7.1 ユーザの正当性の確認の設定

以下の順に受信 ARPパケットの送信元 IP アドレスと送信元 MAC アドレスを比較します。

- ユーザの正当性確認のルール
  - □ 一致した場合、装置はルールに従って ARP パケットを処理します。
  - □ 一致するアドレスがない場合や、ユーザの正当性確認が設定されていない場合、以下の処理をします。
- スタティック IP ソースガードバインディング、DHCP snooping エントリ、802.1X セキュリティエントリ
  - □ 一致した場合、装置は ARP パケットを転送します。
  - □ 一致するアドレスがなかった場合、装置は ARP パケットを廃棄します。

スタティック IP ソースガードバインディングエントリは、**ip source binding** コマンドを使用して作成されます。詳細は、オペレーションマニュアルのセクション 9 *セキュリティ*”*IP ソースガード*”を参照してください。

DHCP snooping エントリは、DHCP snooping によって自動的に作成されます。詳細は、オペレーションマニュアルのセクション 4 *IP サービス*”*DHCP スヌーピング*”を参照してください。

802.1X セキュリティエントリは、802.1X クライアントに IP と MAC のマッピングを記録します。クライアントが 802.1X 認証に成功し ARP アタック detection が有効となった装置に IP アドレスをアップロードした後、装置は自動的に 802.1X セキュリティエントリを作成します。802.1X クライアントは、装置に IP アドレスをアップロード可能にしておかなけれなりません。詳細は、オペレーションマニュアルのセクション 9 *セキュリティ*”*802.1X*”を参照してください。

16.7.2 設定ガイドライン

ユーザの正当性確認を設定する際は、以下のガイドラインに従ってください。

- 以下の 1 つ以上のアイテムが設定されていることを確認してください。
  - □ ユーザの正当性確認ルール
  - □ スタティック IP ソースガードバインディング
  - □ DHCP snooping
  - □ 802.1X

  どのアイテムも設定されていない場合、トラステッド ARP インタフェース上のすべての受信 ARP パケットは廃棄されます。
- IP ソースガードバインディングのために ARP アタック detection が有効となっている IP アドレス、MAC アドレス、VLAN を指定してください。さもないと、ARP パケットは IP ソースガードバインディングと一致しません。

16.7.3 設定手順

以下にユーザの正当性の確認の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. VLAN view に移行する	**vlan** *vlan-id*	ー
3. ARP detection を有効にする	**arp detection enable**	デフォルト：無効
4. system view に戻る	**quit**	ー
5. Ethernet interface view あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	ー
6. （オプション設定項目）ARP 検出を除外するトラステッドインタフェースとして設定する	**arp detection trust**	デフォルト：非トラステッドインタフェース

16.7.4 ARP パケット正当性の確認の設定

非トラステッドポートで受信された ARP パケットが正当かどうか確認を行い、以下のオブジェクトについて指定します。

- **src-mac**– ARP パケットのメッセージ部分にある送信元 MAC アドレスが、イーサネットヘッダの送信元 MAC アドレスと一致するかどうか確認します。一致する場合には通過、そうでなければパケットは廃棄されます。
- **dst-mac**– ARP 応答の宛先 MAC アドレスを確認します。宛先 MAC アドレスがすべて 0、すべて 1、あるいはイーサネットヘッダの宛先 MAC アドレスと矛盾する場合、パケットは無効と判断され廃棄されます。
- **ip**– ARP 応答の送信元 IP アドレスと宛先 IP アドレスを確認します。すべて 0、すべて 1、あるいはマルチキャスト IP アドレスである場合、パケットは無効と判断して廃棄されます。

以下に ARP パケット正当性の確認の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. VLAN view に移行する	**vlan** *vlan-id*	ー
3. ARP detection を有効にする	**arp detection enable**	デフォルト：無効
4. system view に戻る	**quit**	ー
5. ARP パケット正当性の確認を有効にし、オブジェクトを指定する	**arp detection validate** { **dst-mac** | **ip** | **src-mac** } *	デフォルト：無効
6. Ethernet interface view あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	ー
7. （オプション設定項目）ARP 検出を除外するトラステッドインタフェースとして設定する	**arp detection trust**	デフォルト：非トラステッドインタフェース

16.7.5 ARP 制限転送の設定

🕮 **メモ：**
ARP 制限転送は宛先 MAC アドレスのようなマルチポート MAC アドレスの ARP パケットには適用されません。

ARP 制限転送は、非トラステッドインタフェースで受信され、ユーザの正当性の確認をパスした ARP パケットの転送を以下のように制御します。

- パケットが ARP 要求である場合、トラステッドインタフェースを通して転送されます。
- パケットが ARP 応答である場合、宛先 MAC アドレスに従って転送されます。MAC アドレステーブル内に一致するアドレスがない場合、トラステッドインタフェースを通して転送されます。

ARP 制限転送の設定をする前に、ユーザの正当性の確認の設定を行ってください。

以下に ARP 制限転送の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. VLAN view に移行する	**vlan** *vlan-id*	―
3. ARP 制限転送を有効にする	**arp restricted-forwarding enable**	デフォルト：無効

16.7.6 ARP アタック detection の表示と維持

すべての view で **display** コマンドを実行することができ、user view で **reset** コマンドを実行することができます。

操作	コマンド
ARP detectionが有効なVLANを表示する	**display arp detection**
ARP detectionの統計情報を表示する	**display arp detection statistics** [**interface** *interface-type interface-number*]
ARPアタックdetectionの送信元の統計情報を表示する	**display arp detection statistics attack-source slot** *slot-number*
ARPアタックdetectionによって廃棄されたパケットの統計情報を表示する	**display arp detection statistics packet-drop** [**interface** *interface-type interface-number* [**service-instance** *service-instance-id*]]
ARP detectionの統計情報を削除する	**reset arp detection statistics** [**interface** *interface-type interface-number*]
ARPアタックdetectionの送信元の統計情報を削除する	**reset arp detection statistics attack-source** [**slot** *slot-number*]
ARPアタックdetectionによって廃棄されたパケットの統計情報を削除する	**reset arp detection statistics packet-drop** [**interface** *interface-type interface-number* [**service-instance** *service-instance-id*]]

16.7.7 ユーザの正当性の確認の設定例

I. ネットワーク要件

図 16-3に示すように、Device B で 802.1X セキュリティエントリをもとにユーザの正当性の確認の設定を行います。

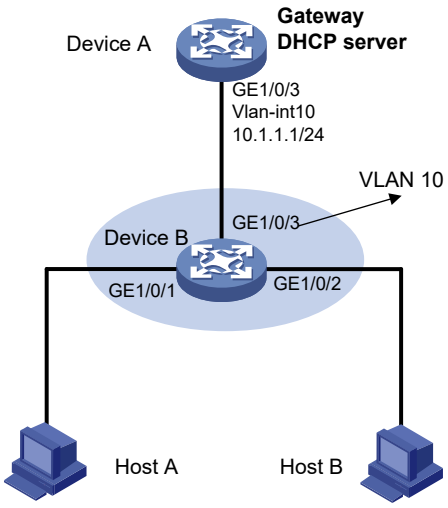


図 16-3 ネットワーク図

II. 設定手順

1) Device B のすべてのインタフェースに VLAN10 を追加し、Device A の VLAN インタフェース 10 の IP アドレスを設定します。（詳細は省略します。）
2) Device A の DHCP サーバを設定し、DHCP アドレスプール 0 を設定します。

```
<DeviceA> system-view
[DeviceA] dhcp enable
[DeviceA] dhcp server ip-pool 0
[DeviceA-dhcp-pool-0] network 10.1.1.0 mask 255.255.255.0
```

3) Host A と Host B を 802.1Xクライアントに設定し、ARP アタック detection の IP アドレスをアップロードするよう設定します。（詳細は省略します。）
4) Device B を設定します。

802.1Xを有効にします。

```
<DeviceB> system-view
[DeviceB] dot1x
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] dot1x
[DeviceB-GigabitEthernet1/0/1] quit
[DeviceB] interface gigabitethernet 1/0/2
```

```
[DeviceB-GigabitEthernet1/0/2] dot1x
[DeviceB-GigabitEthernet1/0/2] quit
```

ローカルユーザ test を追加します

```
[DeviceB] local-user test
[DeviceB-luser-test] service-type lan-access
[DeviceB-luser-test] password simple test
[DeviceB-luser-test] quit
```

802.1X エントリをもとにユーザの正当性を確認するため VLAN10 で ARP アタック detection を有効にします。

```
[DeviceB] vlan 10
[DeviceB-vlan10] arp detection enable
```

#ARP トラステッドインタフェースとしてアップストリームを設定します。デフォルトでは、インタフェースはアントラステッドインタフェースです。

```
[DeviceB-vlan10] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] arp detection trust
[DeviceB-GigabitEthernet1/0/3] quit
```

設定が完了すると、GigabitEthernet 1/0/1 と GigabitEthernet 1/0/2 のインタフェースで受信される ARP パケットは 802.1X エントリに対して確認が行われます。

16.7.8 ユーザの正当性の確認と ARP パケットの正当性の確認の設定例

I. ネットワーク要件

図 16-4に示すように、Device B でスタティック IP ソースガードバインディングと DHCP snooping エントリをもとに ARP パケットの正当性確認とユーザの正当性を実行するように設定します。

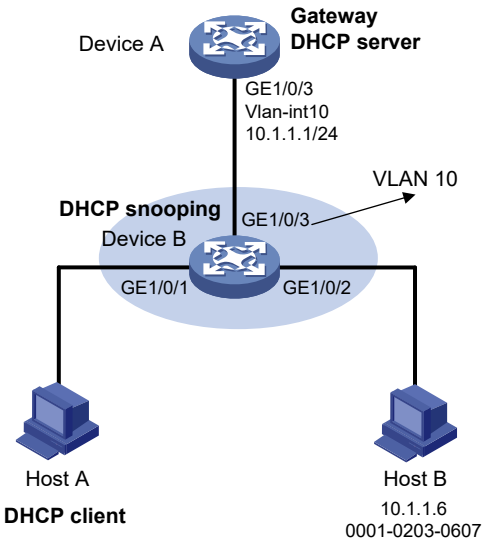


図 16-4 ネットワーク図

II. 設定手順

1) Device B のすべてのインタフェースに VLAN10 を追加し、Device A の VLAN インタフェース 10 の IP アドレスを設定します。（詳細は省略します。）
2) Device A の DHCP サーバを設定し、DHCP アドレスプール 0 を設定します。

```
<DeviceA> system-view
[DeviceA] dhcp enable
[DeviceA] dhcp server ip-pool 0
[DeviceA-dhcp-pool-0] network 10.1.1.0 mask 255.255.255.0
```

3) Host A と Host B を設定します。（詳細は省略します。）
4) Device B を設定します。

DHCP snooping を有効にします。

```
<DeviceB> system-view
[DeviceB] dhcp snooping enable
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] dhcp snooping trust
[DeviceB-GigabitEthernet1/0/3] quit
```

GigabitEthernet 1/0/1 で DHCP snooping エントリのクライアント情報を記録するように設定します。

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] dhcp snooping binding record
[DeviceB-GigabitEthernet1/0/1] quit
```

VLAN10 で ARP detection を有効にします。

```
[DeviceB] vlan 10
[DeviceB-vlan10] arp detection enable
```

トラステッドインタフェースとして上流インタフェースを設定します。（デフォルトでは非トラステッドインタフェースとなっています。）

```
[DeviceB-vlan10] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] arp detection trust
[DeviceB-GigabitEthernet1/0/3] quit
```

#ユーザの正当性の確認を行うため、GigabitEthernet 1/0/2 でスタティック IP ソースガードバインディングエントリを設定します。

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] ip source binding ip-address 10.1.1.6 mac-address 0001-0203-0607 vlan 10
[DeviceB-GigabitEthernet1/0/2] quit
```

ARP パケットの MAC アドレスと IP アドレスを確認することによって、ARP パケットの正当性の確認を有効にします。

```
[DeviceB] arp detection validate dst-mac ip src-mac
```

設定を行った後、GigabitEthernet 1/0/1 と GigabitEthernet 1/0/2 で受信された ARP パケットは、最初に MAC アドレスと IP アドレスの正当性の確認を行います。ARP パケットが有効である場合、スタティック IP ソースガードバインディングエントリに対して確認を行います。最後に DHCP snooping エントリに対して確認を行います。

16.7.9 ARP 制限転送の設定例

I. ネットワーク要件

図 16-5に示すように、ARP detection が設定されている Device B で ARP 制限転送を設定します。Device B に設定された Port Isolation はブロードキャストの ARP 要求のために適用することができます。

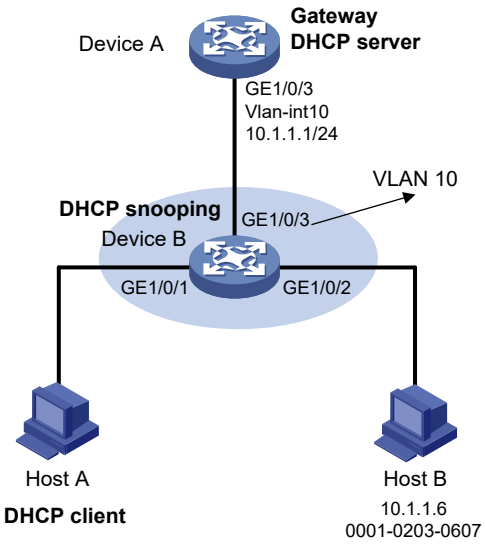


図 16-5 ネットワーク図

II. 設定手順

1) VLAN 10 を設定します。インタフェースに VLAN 10 を追加し、VLAN インタフェースの IP アドレスを設定します。（詳細は省略します。）
2) Device A で DHCP サーバを設定し、DHCP アドレスプール 0 を設定します。

```
<DeviceA> system-view
[DeviceA] dhcp enable
[DeviceA] dhcp server ip-pool 0
[DeviceA-dhcp-pool-0] network 10.1.1.0 mask 255.255.255.0
```

3) Host A と Host B を設定します。（詳細は省略します。）
4) Device B を設定します。

DHCP snooping を有効にします。DHCP トラステッドポートとして GigabitEthernet 1/0/3 を設定します。

```
<DeviceB> system-view
[DeviceB] dhcp snooping enable
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] dhcp snooping trust
[DeviceB-GigabitEthernet1/0/3] quit
```

ユーザの正当性の確認を行うため ARP detection を有効にします。

```
[DeviceB] vlan 10
[DeviceB-vlan10] arp detection enable
```

DHCP トラステッドポートとして GigabitEthernet 1/0/3 を設定します。

```
[DeviceB-vlan10] interface gigabitethernet 1/0/3
```

```
[DeviceB-GigabitEthernet1/0/3] arp detection trust
[DeviceB-GigabitEthernet1/0/3] quit
```

GigabitEthernet 1/0/2 でスタティック IP ソースガードバインディングエントリを設定します。

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] ip source binding ip-address 10.1.1.6 mac-address 0001-0203-0607 vlan 10
[DeviceB-GigabitEthernet1/0/2] quit
```

ARP パケットの MAC アドレスと IP アドレスを確認することによって、ARP パケットの正当性の確認を有効にします。

```
[DeviceB] arp detection validate dst-mac ip src-mac
```

Port Isolation を設定します。

```
[DeviceB] port-isolate group 1
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port-isolate enable group 1
[DeviceB-GigabitEthernet1/0/1] quit
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] port-isolate enable group 1
[DeviceB-GigabitEthernet1/0/2] quit
```

設定を行った後、Device B は最初に GigabitEthernet 1/0/1 と GigabitEthernet 1/0/2 で受信された ARP パケットの MAC アドレスと IP アドレスの正当性の確認を行います。ARP パケットが有効である場合、スタティック IP ソースガードバインディングエントリと DHCP snooping エントリを使用してユーザの正当性の確認を行います。しかし Host A から送信された ARP ブロードキャスト要求は Device B の確認にパスし、Host B に到達します。

ARP 制限転送を有効にします。

```
[DeviceB] vlan 10
[DeviceB-vlan10] arp restricted-forwarding enable
[DeviceB-vlan10] quit
```

設定を行った後、Device B はトラステッドインタフェース GigabitEthernet 1/0/3 を通して Host A から Device A に ARP ブロードキャスト要求を転送します。Host B はパケットを受信することができません。Port isolation は正常に動作します。

16.8 ARPスキャンの設定

16.8.1 ARP スキャンの設定

通常、ARP スキャンは、安定した小規模なネットワークで使用されます。

ARP スキャンは、アドレス範囲内の装置の ARP エントリを自動的に作成します。装置は以下の手順で ARP スキャンを実行します。

1)　アドレス範囲内の各 IP アドレスに ARP 要求を送信します。
2)　受信した ARP 応答から MAC アドレスを取得します。
3)　ダイナミック ARP エントリを作成します。

スキャン範囲に IP アドレスが多い場合は、ARP パケットの送信レートを設定できます。この設定により、ARP トラフィックのバーストが原因で CPU 使用率が高くなり、ネットワーク負荷が高くなるのを回避できます。

16.8.2 制限とガイドライン

ARP テーブルに存在する IP アドレスはスキャンされません。

ARP スキャンには時間がかかります。実行中のスキャンを停止するには、Ctrl+C を押します。ダイナミック ARP エントリは、スキャンが終了する前に受信した ARP 応答に基づいて作成されます。

スタティック ARP エントリの合計数の制限により、ダイナミック ARP からの変換に失敗する場合があります。

ダイナミック ARP から変換されたスタティック ARP エントリを削除するには、**undo arp** *ip-address* コマンドを使用します。**reset arp all** コマンドを使用してすべての ARP エントリを削除することも、**reset arp static** コマンドを使用してすべてのスタティック ARP エントリを削除することもできます。

16.8.3 設定手順

操作	コマンド	補足
1.　system view に移行する	**system-view**	—
2.　interface view に移行する	**interface** *interface-type interface-number*	—
3.　ARP スキャンを開始する	**arp scan** [*start-ip-address* **to** *end-ip-address*] [**send-rate** *pps*]	—

🕮 **メモ：**

arp scan コマンドは Version7.1.4 を含む以降のソフトウェアからサポートしています。

16.9 ARPゲートウェイプロテクションの設定

本機能は、ゲートウェイなりすまし攻撃を防止するためにゲートウェイに接続していないインタフェースで設定してください。そのインタフェースで ARP パケットを受信した際は、パケット内の送信元 IP アドレスが保護されたゲートウェイと一致しているかを確認します。一致していれば、パケットは廃棄します。一致していなければ、パケットをただしく処理します。

16.9.1 設定ガイドライン

ARP ゲートウェイプロテクションを設定する際は、以下のガイドラインに従ってください。

- 一つのインタフェースで最大 8 個のゲートウェイに ARP ゲートウェイプロテクションを有効にできます。
- インタフェースでは **arp filter source** コマンドと **arp filter binding** コマンドの両方を設定することはしないでください。
- ARP ゲートウェイプロテクションを ARP アタック detection と ARP snooping と一緒に使用する場合、最初に ARP ゲートウェイプロテクションが適用されます。

16.9.2 設定手順

以下に ARP ゲートウェイプロテクションの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Ethernet interface view あるいはレイヤ 2aggregate interface view に移行する	**interface** *interface-type interface-number*	―
3. 指定のゲートウェイに ARP ゲートウェイプロテクションを設定する	**arp filter source** *ip-address*	デフォルト：無効

16.9.3 設定例

I. ネットワーク要件

図 16-6に示すように、ホスト B は装置 B にゲートウェイなりすまし攻撃を始めます。結果として、装置 B は装置 A に送信しようとしている通信はホスト B に送信されます。

装置 B に攻撃をブロックするように設定します。

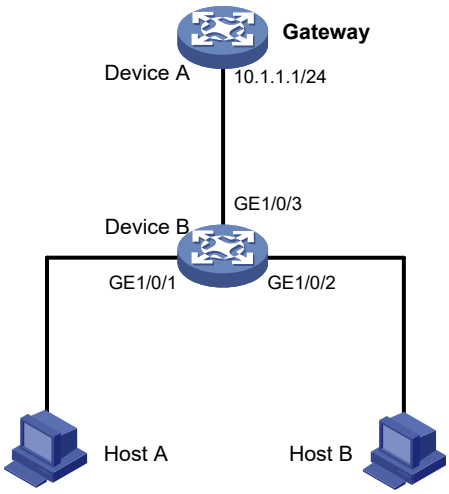


図 16-6 ネットワーク図

II. 設定手順

装置 B に ARP ゲートウェイプロテクションを設定します。

```
<DeviceB> system-view
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] arp filter source 10.1.1.1
[DeviceB-GigabitEthernet1/0/1] quit
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] arp filter source 10.1.1.1
```

III. 設定確認

送信元 IP アドレスがゲートウェイの IP アドレスになっている受信 ARP パケットを GigabitEthernet 1/0/1 と GigabitEthernet 1/0/2 ポートが廃棄していることを確認してください。

16.10 ARPフィルタリングの設定

ARP フィルタリング機能は、ゲートウェイなりすましとユーザなりすましの攻撃を防ぐことができます。

この機能を有効にしたインタフェースは、パーミットされたエントリに対して受信 ARP パケットの IP アドレスと MAC アドレスを確認します。一致した場合、パケットは正しく処理されます。一致しなかった場合、パケットは廃棄されます。

16.10.1 設定ガイドライン

ARP フィルタリングを設定する際は、以下のガイドラインに従ってください。

- 一つのインタフェースで最大 8 個のパーミットエントリを設定できます。
- インタフェースでは **arp filter source** コマンドと **arp filter binding** コマンドの両方を設定することはしないでください。
- ARP フィルタリングを ARP アタック detection と ARP snooping と一緒に使用する場合、最初に ARP フィルタリングが適用されます。

16.10.2 設定手順

以下に ARP ゲートウェイプロテクションの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Ethernet interface view あるいはレイヤ 2aggregate interface view に移行する	**interface** *interface-type interface-number*	―
3. 指定のゲートウェイに ARP ゲートウェイプロテクションを設定する	**arp filter binding** *ip-address mac-address*	デフォルト：無効

16.10.3 設定例

I. ネットワーク要件

図 16-7に示すように、ホスト A の IP アドレスと MAC アドレスはそれぞれ 10.1.1.2 と 000f-e349-1233 です。ホスト B の IP アドレスと MAC アドレスはそれぞれ 10.1.1.3 と 000f-e349-1234 です。

ホスト A とホスト B からのみ ARP パケットをパーミットするために、装置 B の GigabitEthernet1/0/1 と GigabitEthernet1/0/2 に ARP フィルタリングを設定します。

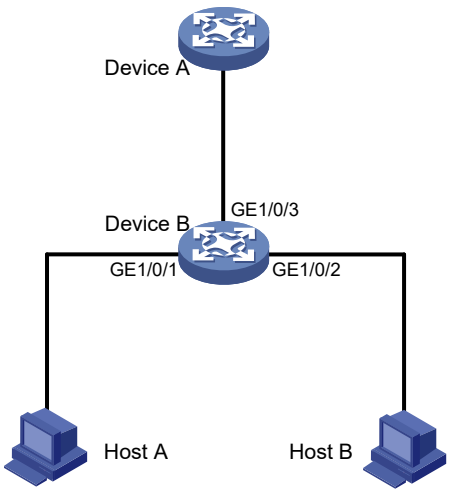


図 16-7 ネットワーク図

II. 設定手順

装置 B に ARP フィルタリングを設定します。

```
<DeviceB> system-view
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] arp filter binding 10.1.1.2 000f-e349-1233
[DeviceB-GigabitEthernet1/0/1] quit
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] arp filter binding 10.1.1.3 000f-e349-1234
```

III. 設定確認

GigabitEthernet 1/0/1 がホスト A からの ARP パケットを許可し、他の ARP パケットを廃棄していることを確認してください。

GigabitEthernet 1/0/2 がホスト B からの ARP パケットを許可し、他の ARP パケットを廃棄していることを確認してください。

目次

このセクションのページは**9-x-x** です。

17章 uRPF 17-1
17.1 概要 17-1
17.1.1 uRPFアプリケーションシナリオ 17-1
17.1.2 uRPFの確認モード 17-1
17.1.3 ネットワークアプリケーション 17-2
17.2 グローバルでのuRPFの有効化 17-2
17.3 uRPFの表示と維持 17-2

17章 uRPF

17.1 概要

uRPF（Unicast Reverse Path Forwarding)は、送信元アドレスのなりすましによる攻撃に対する防御を行います。

17.1.1 uRPF アプリケーションシナリオ

攻撃者は、認可されたユーザあるいは管理者の名前を用いて、IP ベースの認証を使用したシステムにアクセスするため、ねつ造された送信元アドレスのパケットを送信します。たとえ攻撃者あるいは他のホストが、いかなるパケットに応答できないとしても、攻撃者は、一段と攻撃目標に破壊をもたらします。

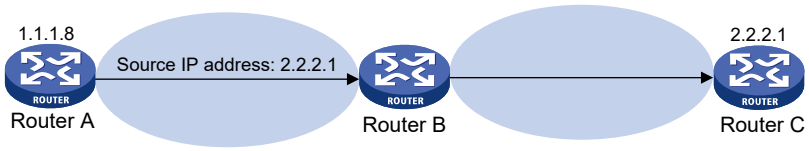


図 17-1 送信元アドレスなりすましによる攻撃

図 17-1に示すように、Router A の攻撃者がサーバ（Router B)に高いレートで偽の送信元 IP アドレス 2.2.2.1 のリクエストを送信します。そして Router B は IP アドレス 2.2.2.1（Router C）に応答パケットを送信します。その結果、Router B と Router C は攻撃されます。管理者が誤って Router C と切断した場合、ネットワークサービスが中断されます。

また攻撃者は接続をブロックするかネットワークに侵入するため、異なる偽の送信元アドレスのパケットを送信する、あるいは同時に複数のサーバに攻撃することができます。

uRPF は、これらの送信元アドレスなりすまし攻撃（スプーフィング攻撃）を防御することができます。パケットを受信したインタフェースが、パケットの送信元アドレスに一致する FIB エントリの出力インタフェースであるかどうかを確認します。もし、パケットを受信したインタフェースが FIB エントリにある出力インタフェースと異なる場合、uRPF はなりすまし攻撃であると認識し、パケットを廃棄します。

17.1.2 uRPF の確認モード

strict uRPF にパスするため、パケットの送信元アドレスと受信インタフェースは FIB エントリの宛先アドレスと出力インタフェースに一致する必要があります。非対称ルーティングなどの特定の状況下では、strict uRPF は正当なパケットを廃棄する可能性があります。strict uRPF は多くの場合 PE と CE 間で設定されます。

17.1.3 ネットワークアプリケーション

図 17-2に示すように strict uRPF チェックは ISP とカスタマネットワーク間で設定され、loose uRPF チェックは ISP 間で設定されます。

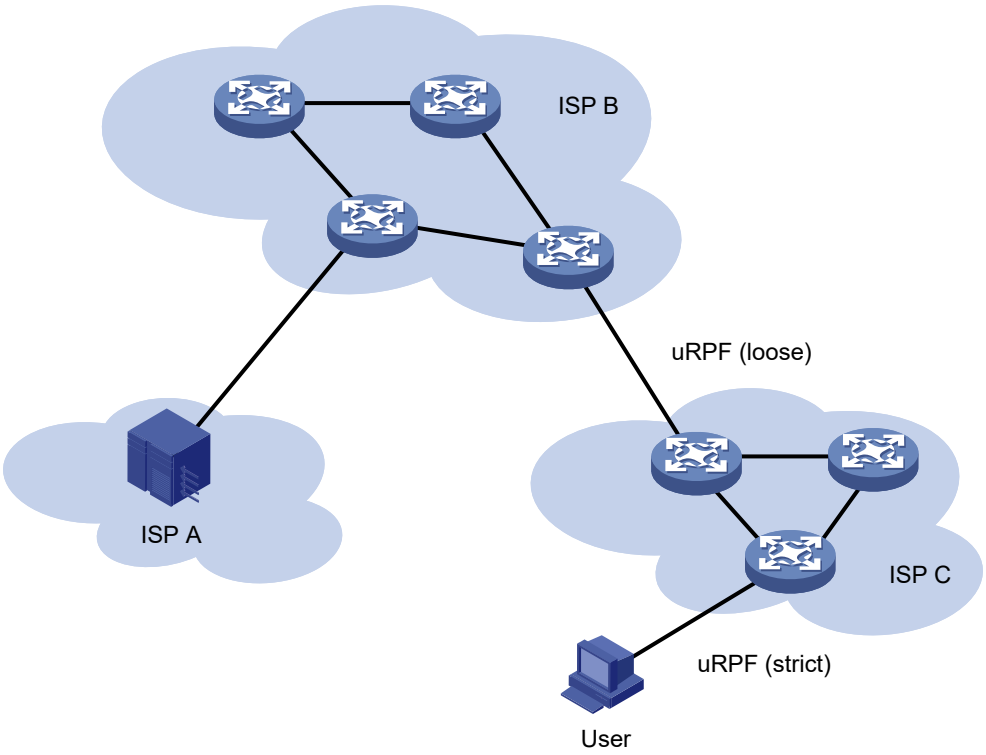


図 17-2 ネットワーク図

17.2 グローバルでのuRPFの有効化

I. 制限とガイドライン

グローバルでの uRPF は装置のすべてのインタフェースに適用します。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. グローバルで uRPF を有効にする	**ip urpf** { **strict** }	デフォルト：無効

17.3 uRPFの表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
uRPFの設定を表示する	**display ip urpf** [**slot** *slot-number*]

QX-S5100G シリーズ Ethernet スイッチ

オペレーションマニュアル

10. 高可用性

本マニュアルは以下に示す章で構成されています。

01-Ethernet OAM

02-CFD

03-DLDP

04-RRPP

05-Smart Link

06-Monitor Link

07-VRRP

08-BFD

09-Track

目次

このセクションのページは **10-x-x** です。

1 章 Ethernet OAM 1-1
1.1 概要 1-1
1.1.1 Ethernet OAM の主な機能 1-1
1.1.2 Ethernet OAMPDU 1-1
1.1.3 Ethernet OAM の動作 1-2
1.1.4 プロトコルと標準 1-4
1.2 Ethernet OAM 設定作業リスト 1-4
1.3 Ethernet OAM の基本機能の設定 1-5
1.4 Ethernet OAM 接続検出タイマの設定 1-5
1.5 リンクモニタリングの設定 1-6
1.5.1 エラーフレームイベント検出の設定 1-6
1.5.2 エラーフレーム期間イベント検出の設定 1-7
1.5.3 エラーフレーム秒イベント検出の設定 1-7
1.6 リモートエンドから Ethernet OAM イベント受信後のポートのアクション設定 1-8
1.7 Ethernet OAM リモートループバックの設定 1-9
1.7.1 設定ガイドライン 1-9
1.7.2 指定したポートの Ethernet OAM リモートループバックの有効化 1-9
1.7.3 ポートの Ethernet OAM リモートループバックの有効化 1-10
1.7.4 リモートポートからの Ethernet OAM リモートループバックリクエストの拒否 1-10
1.8 Ethernet OAM の表示と維持 1-10
1.9 Ethernet OAM 設定例 1-11
1.9.1 ネットワーク要件 1-11
1.9.2 設定手順 1-11
1.9.3 設定の確認 1-12

1章 Ethernet OAM

1.1 概要

Ethernet OAM（Ethernet Operation, Administration and Maintenance）はレイヤ 2 リンク状態をモニタし、「ラストマイル」に関するリンク関連の問題に対処するツールです。Ethernet OAM を使用することで、2 台の直接接続された装置間のポイントツーポイント接続の状態をモニタできます。

1.1.1 Ethernet OAM の主な機能

以下に Ethernet OAM の主な機能を示します。

- **リンクパフォーマンスのモニタ** － パケットロス、遅延、ジッタを含むリンクの性能指標をモニタし、様々なタイプのトラフィック統計情報を収集します。
- **障害検出とアラーム** － リンク異常が発生したとき、OAM プロトコルデータ単位（OAMPDU）とレポートをネットワーク管理者に送ることによって、リンクの接続性をチェックします。
- **リモートループバック** － ループバック OAMPDUによってリンク品質の確認とリンクエラーの検出を行います。

1.1.2 Ethernet OAMPDU

Ethernet OAM はデータリンクレイヤで動作します。Ethernet OAM は、管理者が効率的にネットワークを管理できるように、装置間で定期的に OAMPDU を交換することによってリンクの状態を通知します。

表 1-1に Ethernet OAMPDU のタイプによる違いを示します。

表 1-1 OAMPDU の異なるタイプによる機能

OAMPDU タイプ	機能
Information OAMPDU	リモートEthernet OAMエンティティとOAM接続を維持するため、Ethernet OAMエンティティの転送状態の情報に使用します。この情報はローカルデバイス、リモートデバイス、カスタマイズ情報を含みます。
Event Notification OAMPDU	リンクモニタリングによりリンク間で問題を検出したとき、リモートOAMエンティティに通知するために使用します。
Loopback Control OAMPDU	リモートループバック制御に使用します。ループバック制御OAMPDUにループバックの有効/無効情報を挿入することにより、リモートOAMエンティティのループバックを有効/無効にすることができます。

🕮 メモ：
この章では Ethernet OAM が有効なポートは Ethernet OAM エンティティあるいは OAM エンティティと呼ばれます。

1.1.3 Ethernet OAM の動作

この章では Ethernet OAM の動作手順について記載します。

I. Ethernet OAM 接続の確立

Ethernet OAM 機能を使用するため、最初にリモートとの接続の確立が必要となります。Ethernet OAM 接続の確立とは、Ethernet OAM エンティティがリモート OAM エンティティを発見し、セッションを確立するディスカバリフェーズです。

このフェーズでは、OAM の内部接続エンティティは、リモートの OAM 設定情報とローカルノードの OAM ケーパビリティを Information OAMPDU を交換することにより通知し、Ethernet OAM 接続が確立できるか判断します。Ethernet OAM 接続は、ループバック接続、リンク検出、リンクイベントの設定が一致しているエンティティ間で確立できます。Ethernet OAM 接続が確立後は Ethernet OAM が有効になります。

OAM エンティティはアクティブモードあるいはパッシブモードで動作します。アクティブモードの OAM エンティティは OAM 接続を開始します。パッシブモードの OAM エンティティは相手からの OAM 接続要求を待ち応答します。2 つの OAM エンティティ間の OAM 接続を行うため、少なくとも 1 つのモードはアクティブモードに設定する必要があります。

表 1-2に異なるモードで装置が実行する動作を示します。

表 1-2 アクティブ Ethernet OAM モードとパッシブ Ethernet OAM モード

アイテム	アクティブ Ethernet OAM モード	パッシブ Ethernet OAM モード
Initiating OAM Discovery	可能	不可能
Responding to OAM Discovery	可能	可能
Transmitting Information OAMPDUs	可能	可能
Transmitting Event Notification OAMPDUs	可能	可能
Transmitting Information OAMPDUs without any TLV	可能	可能
Transmitting Loopback Control OAMPDUs	可能	不可能
Responding to Loopback Control OAMPDUs	双方がアクティブOAMモードのとき可能	可能

Ethernet OAM 接続が確立した後、Ethernet OAM エンティティは Information OAMPDU を定期的に交換し Ethernet OAM 接続を保持します。Ethernet OAM エンティティが Information OAMPDU を Ethernet OAM タイムアウト時間内に受信しない場合、Ethernet OAM 接続は切断されます。

II. リンクモニタリング

Ethernet のエラー検出は、困難を伴います。特にネットワークが物理的に切断されていないが、ネットワークパフォーマンスが徐々に低下している状況では、検出が困難になります。

リンクモニタリングは様々な環境でリンクエラーを検出するために使用します。Ethernet OAM のリンクモニタリングは Event Notification OAMPDU の交換により確立します。

表 1-3に示す Ethernet OAM リンクエラーイベントを検出すると、ローカル OAM エンティティは Event Notification OAMPDU をリモート OAM エンティティに送信します。ログ情報を取得することによりネットワーク管理者は速やかにネットワークステータスの変更を追跡できます。

表 1-3 Ethernet OAM リンクエラーイベント

Ethernet OAM リンクイベント	説明
Errored symbol event	検出ウィンドウ（受信したシンボル数）内に、所定のしきい値を超過したエラーシンボルを検出したときにエラーシンボルイベントが発生します。
Errored frame event	検出ウィンドウ（検出期間）内に、所定のしきい値を超過したエラーフレームを検出したときにエラーフレームイベントが発生します。
Errored frame period event	検出ウィンドウ（受信したフレーム数）内に、エラーフレームが所定のしきい値を超過したときにエラーフレーム期間イベントが発生します。
Errored frame seconds event	検出ウィンドウ（検出期間）内に、ポートでエラーフレーム秒（エラーフレームが1秒以内に発生したエラーフレーム）の数が設定しきい値を超過したときにエラーフレーム秒イベントが発生します。

III. リモート障害検出

Information OAMPDU は、OAM 接続が確立された Ethernet OAM エンティティ間で定期的に交換されます。装置の障害または使用不能により通信が中断したネットワークでは、Ethernet OAM エンティティがピアにエラー情報を送信するために Information OAMPDU のフラグフィールドを使用できます。（表 1-4にクリティカルリンクイベントを示します）現在のリンク状態を追跡するため、ログ情報を使用し、問題を早急にトラブルシュートすることができます。

表 1-4 クリティカルリンクイベント

タイプ	説明	OAMPDU 送信間隔
Link Fault	相手リンク信号のロスト	1秒に1回
Dying Gasp	電源障害のような予測不能な障害の発生	ノンストップ
Critical Event	不確定なクリティカルイベントの発生	ノンストップ

装置は、表 1-4に示すクリティカルリンクイベントが運ばれる Information OAMPDU を受信することができます。

装置は Link Fault イベントが運ばれる Information OAMPDU の送信を行うことができます。

装置の再起動や関連したポートが手動で shutdown された際の Dying Gasp イベントが運ばれる Information OAMPDU の送信をサポートしています。物理的な IRF ポートは、この information OAMDPU を送信することができません。

装置は Critical Event が運ばれる information OAMPDU の送信はサポートしていません。

IV. リモートループバック

リモートループバックは Ethernet OAM コネクションが確立されている場合のみ利用可能です。リモートループバックを有効にすると、アクティブモードの Ethernet OAM エンティティは non-OAMPDU を相手に送信します。フレームを受信したのち、相手は送信先アドレスへは転送せずにオリジナルパスで返信します。

リモートループバックはリンク状態やリンク障害箇所を確認するために使用します。定期的なリモートループバックの実行は、ネットワーク障害を速やかに検出するのに役立ちます。さらにネットワークセグメントでのリモートループバックの実行は、ネットワーク障害箇所の検出の手助けとなります。

1.1.4 プロトコルと標準

IEEE 802.3ah, *Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications*

1.2 Ethernet OAM設定作業リスト

作業リスト
（必須設定項目） Ethernet OAMの基本機能の設定
（オプション設定項目） Ethernet OAM接続検出タイマの設定
（オプション設定項目） リンクモニタリングの設定 • エラーフレームイベント検出の設定 • エラーフレーム期間イベント検出の設定 • エラーフレーム秒イベント検出の設定
(オプション設定項目) リモートエンドからEthernet OAMイベント受信後のポートのアクション設定
（オプション設定項目） Ethernet OAMリモートループバックの設定 • 指定したポートのEthernet OAMリモートループバックの有効化 • ポートのEthernet OAMリモートループバックの有効化 • リモートポートからのEthernet OAMリモートループバックリクエストの拒否

1.3 Ethernet OAMの基本機能の設定

2 つの Ethernet OAM エンティティ間で Ethernet OAM 接続を確立するために、装置を少なくとも 1つをアクティブモードに設定します。アクティブモードでのみ Ethernet OAM エンティティはコネクションを開始することができます。

Ethernet OAM が有効になったポートの Ethernet OAM モードを変更するには、最初に Ethernet OAM を無効にする必要があります

以下に Ethernet OAM の基本機能の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. Ethernet interface view に移行する	**interface** *interface-type interface-number*	ー
3. Ethernet OAM モードを設定する	**oam mode** { **active** | **passive** }	デフォルト：active
4. Ethernet OAM を有効にする	**oam enable**	デフォルト：無効

1.4 Ethernet OAM接続検出タイマの設定

Ethernet OAM の接続が確立された後、Ethernet OAM エンティティは、Ethernet OAM 接続が有効であるか検出するため、指定された間隔で Ethernet OAM ハンドシェークパケットとして Information OAMPDU の交換を行います。Ethernet OAM が有効になっているポートで Ethernet OAM コネクションタイムアウトの前に Information OAMPDU を受信しない場合は、Ethernet OAM 接続が切断されたと判断します。

ハンドシェークパケットの転送間隔と接続タイムアウトタイマを調整することで、Ethernet OAM の検出時間を変更することができます。

このコマンドは system view あるいは interface view で設定することができます。system view での設定はすべてのポートで適用され、interface view での設定は指定されたポートで適用されます。interface view での設定が優先されます。

Ethernet OAM 接続のタイムアウトタイマが終了した後、ローカル OAM エンティティは、OAM 接続を切断し、ピアの OAM エンティティの接続を終了させます。Ethernet OAM 接続を安定的に維持するために、Ethernet OAM コネクションタイムアウト値は Ethernet OAMハンドシェークパケットの送信間隔の少なくとも 5倍以上にすることを推奨します。

以下にグローバルでの Ethernet OAM 接続検出タイマの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. Ethernet OAM ハンドシェークパケットの送信間隔を設定する	**oam global timer hello** *interval*	デフォルト：1000ms
3. Ethernet OAM コネクションタイムアウトタイマを設定する	**oam global timer keepalive** *interval*	デフォルト：5000ms

以下にポートでの Ethernet OAM 接続検出タイマの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Ethernet interface view に移行する	**interface** *interface-type interface-number*	―
3. Ethernet OAM ハンドシェークパケットの送信間隔を設定する	**oam timer hello** *interval*	デフォルト : グローバルに設定された値を使用します。
4. Ethernet OAM コネクションタイムアウトタイマを設定する	**oam timer keepalive** *interval*	デフォルト : グローバルに設定された値を使用します。

1.5 リンクモニタリングの設定

Ethernet OAM が確立された後、この章で設定されたリンクモニタリング期間としきい値がすべての Ethernet インタフェースで自動的に設定されます。

1.5.1 エラーフレームイベント検出の設定

検出ウィンドウ（検出期間）内に、フレームエラー数がしきい値を超えたとき、エラーフレームイベントが発生します。

このコマンドは system view あるいは interface view で設定することができます。system view での設定はすべてのポートで適用され、interface view での設定は指定されたポートで適用されます。interface view での設定が優先されます。

以下にグローバルでのエラーフレームイベント検出の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. エラーフレームイベント検出期間を設定する	**oam global errored-frame window** *window-value*	デフォルト : 1000 ms
3. エラーフレームイベント検出のしきい値を設定する	**oam global errored-frame threshold** *threshold-value*	デフォルト : 1

以下にポートでのエラーフレームイベント検出の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Ethernet interface view に移行する	**interface** *interface-type interface-number*	―
3. エラーフレームイベント検出期間を設定する	**oam errored-frame window** *window-value*	デフォルト : グローバルに設定された値を使用します。
4. エラーフレームイベント検出のしきい値を設定する	**oam errored-frame threshold** *threshold-value*	デフォルト : グローバルに設定された値を使用します。

1.5.2 エラーフレーム期間イベント検出の設定

検出ウィンドウ(受信したフレーム数)内に、エラーフレームが所定のしきい値を超過したときにエラーフレーム期間イベントが発生します。

このコマンドは system view あるいは interface view で設定することができます。system view での設定はすべてのポートで適用され、interface view での設定は指定されたポートで適用されます。interface view での設定が優先されます。

以下にグローバルでのエラーフレーム期間イベント検出の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. エラーフレーム期間イベント検出のフレーム数を設定する	**oam global errored-frame-period window** *window-value*	デフォルト：10000000
3. エラーフレーム期間イベント検出のしきい値を設定する	**oam global errored-frame-period threshold** *threshold-value*	デフォルト：1

以下にポートでのエラーフレーム期間イベント検出の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Ethernet interface view に移行する	**interface** *interface-type interface-number*	―
3. エラーフレーム期間イベント検出のフレーム数を設定する	**oam errored-frame-period window** *window-value*	デフォルト: グローバルに設定された値を使用します。
4. エラーフレーム期間イベント検出のしきい値を設定する	**oam errored-frame-period threshold** *threshold-value*	デフォルト: グローバルに設定された値を使用します。

1.5.3 エラーフレーム秒イベント検出の設定

注意：
エラーフレーム秒イベントを動作させるために、エラーフレーム秒検出しきい値は、エラーフレーム秒イベントの検出期間より小さくする必要があります。そうでなければエラーフレーム秒イベントが動作しません。

検出ウィンドウ（検出期間）内に、ポートでエラーフレーム秒（エラーフレームが 1 秒以内に発生したエラーフレーム）の数が設定しきい値を超過したときにエラーフレーム秒イベントが発生します。

このコマンドは system view あるいは interface view で設定することができます。system view での設定はすべてのポートで適用され、interface view での設定は指定されたポートで適用されます。interface view での設定が優先されます。

以下にグローバルでのエラーフレーム秒イベント検出の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. エラーフレーム秒イベント検出を設定する	**oam global errored-frame-seconds window** *window-value*	デフォルト：60000ms
3. エラーフレーム秒イベント検出のしきい値を設定する	**oam global errored-frame-seconds threshold** *threshold-value*	デフォルト：1

以下にポートでのエラーフレーム秒イベント検出の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Ethernet interface view に移行する	**interface** *interface-type interface-number*	―
3. エラーフレーム秒イベント検出を設定する	**oam errored-frame-seconds window** *window-value*	デフォルト : グローバルに設定された値を使用します。
4. エラーフレーム秒イベント検出のしきい値を設定する	**oam errored-frame-seconds threshold** *threshold-value*	デフォルト : グローバルに設定された値を使用します。

1.6 リモートエンドからEthernet OAMイベント受信後のポートのアクション設定

この機能によって、ポートはイベントのログを有効にし、OAM 接続を自動で終了させ、リンク状態をダウンさせます。

リモートエンドから Ethernet OAM イベントを受信したのち、ポートが行うアクションを設定します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Ethernet interface view に移行する	**interface** *interface-type interface-number*	―
3. リモートエンドから Ethernet OAM イベントを受信した後のポートのアクションを設定する	**oam remote-failure** { **connection-expired** | **critical-event** | **dying-gasp** | **link-fault** } **action error-link-down**	デフォルト：設定なし（ポートはリモートエンドからEthernet OAMイベントを受信した際のEthernet OAMイベントのログのみを行います）

1.7 Ethernet OAMリモートループバックの設定

⚠ **注意：**
OAM リモートループバック機能は、他のサービスに大きな影響を与える可能性があるので、注意して使用してください。

ポートで OAM リモートループバックを有効にすると、ポートはリモートポートに Loopback Control OAMPDU を送信し、リモートポートがループバック状態になります。ポートはリモートポートにテストフレームを送信します。このテストフレームのポートでの受信数をチェックすることで、パケットロス率によるリンク性能の評価ができます。

user view、system view、Ethernet interface view で Ethernet OAM リモートループバックを有効にすることができます。設定の適用範囲は同じです。

1.7.1 設定ガイドライン

- Ethernet OAM リモートループバックは、Ethernet OAM 接続が確立され、Ethernet OAM エンティティがアクティブ Ethernet OAM モードであるとき実行可能です。
- リモートループバックは、リモートループバックを行う両端の通信モードが全 2 重である必要があります。
- Ethernet OAM リモートループバックは、リモートポートと送信ポートの両方でサポートしている必要があります。
- Ethernet OAM リモートループバックはデータ通信に割り込みます。Ethernet OAM リモートループバックを無効化した後、関係するすべてのポートがシャットダウンしたのちアップします。 Ethernet OAM リモートループバックは、Ethernet OAM の無効化、Ethernet OAM リモートループバックの無効化、Ethernet OAM 接続のタイムアウトのイベントで無効にすることができます。
- リモートループバックテストを行っているポートで内部ループバックテストを有効にするとリモートループバックテストを終了できます。ループバックテストについての詳細は、オペレーションマニュアルのセクション 3 *アクセス "Ethernet インタフェース"*を参照してください。

1.7.2 指定したポートの Ethernet OAM リモートループバックの有効化

操作	コマンド	補足
1.　（オプション設定項目）system view に移行する	**system-view**	―
2.　指定したポートで Ethernet OAM リモートループバックを有効にする	**oam remote-loopback start interface** *interface-type interface-number*	デフォルト：無効 このコマンドはuser viewあるいはsystem viewで実行できます。

1.7.3 ポートの Ethernet OAM リモートループバックの有効化

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Ethernet interface view に移行する	**interface** *interface-type interface-number*	―
3. ポートの Ethernet OAM リモートループバックを有効にする	**oam remote-loopback start**	デフォルト：無効

1.7.4 リモートポートからの Ethernet OAM リモートループバックリクエストの拒否

Ethernet OAM リモートループバック機能は、他のサービスに影響を与えます。この問題を解決するために、リモートポートから送信された Loopback Control OAMPDU によって制御されるポートを無効にすることができます。ローカルポートはリモートポートからの Ethernet OAM リモートループバック要求を拒否することができます。

以下にリモートポートからの Ethernet OAM リモートループバック要求を拒否する設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Ethernet interface view に移行する	**interface** *interface-type interface-number*	―
3. リモートポートからの Ethernet OAM リモートループバック要求を拒否する	**oam remote-loopback reject-request**	デフォルト：拒否しません。この設定はポートで実行されたループバックテストには影響しません。ポートで次にループバックが行われるときに適用されます。

1.8 Ethernet OAMの表示と維持

すべての view で **display** コマンドを表示することができ、user view で **reset** コマンドを実行することができます。

操作	コマンド
Ethernet OAMの接続を表示する	**display oam** { **local** | **remote** } [**interface** *interface-type interface-number*]
Ethernet OAMの設定を表示する	**display oam configuration** [**interface** *interface-type interface-number*]
Ethernet OAM確立後のクリティカルイベントの統計情報を表示する	**display oam critical-event** [**interface** *interface-type interface-number*]
Ethernet OAM確立後のEthernet OAMリンクエラーイベントの統計情報を表示する	**display oam link-event** { **local** | **remote** } [**interface** *interface-type interface-number*]

操作	コマンド
Ethernet OAMパケットとEthernet OAMリンクエラーイベントの統計情報を削除する	**reset oam** [**interface** *interface-type interface-number*]

🕮 メモ：

- **display oam configuration** コマンドの Errored symbol period フィールド、Errored frame period フィールドは現在のソフトウェアバージョンでサポートしていません。
- **display oam link-event** コマンドの OAM local/remote errored symbol event フィールド、OAM local/remote errored frame period event フィールドは現在のソフトウェアバージョンでサポートしていません。

1.9 Ethernet OAM設定例

1.9.1 ネットワーク要件

図 1-1に示すように、以下の動作を実行します。

- 2 台の装置間でリンクエラーを自動検出するため、Device A と Device B で Ethernet OAM を有効にします。
- Device A が受信するエラーフレームの統計情報を収集することによって、Device A と Device B 間のリンク性能を測定できます。

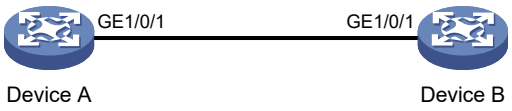


図 1-1 ネットワーク図

1.9.2 設定手順

1)　Device A を設定します。

アクティブ Ethernet OAM モードで動作するように、GigabitEthernet 1/0/1 を設定し、Ethernet OAM を有効にします。

```
<DeviceA> system-view
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] oam mode active
[DeviceA-GigabitEthernet1/0/1] oam enable
```

エラーフレーム検出期間を 20000ms に設定し、エラーフレームイベント検出しきい値を 10 に設定します。

```
[DeviceA] oam errored-frame  period 200
[DeviceA] oam errored-frame  threshold 10
[DeviceA-GigabitEthernet1/0/1]  quit
```

2)　Device B を設定します。

#パッシブ Ethernet OAM モード（デフォルト）で動作するように、GigabitEthernet 1/0/1 を設定し、Ethernet OAM を有効にします。

```
<DeviceB> system-view
[DeviceB] interface gigabitethernet  1/0/1
[DeviceB-GigabitEthernet1/0/1]  oam mode passive
[DeviceB-GigabitEthernet1/0/1]  oam enable
[DeviceB-GigabitEthernet1/0/1]  quit
```

1.9.3 設定の確認

display oam critical-event コマンドを使用し、Ethernet OAM クリティカルリンクイベントの統計情報を表示します。

Device A のすべてのポートの Ethernet OAM クリティカルリンクイベントの統計情報を表示します。

```
[DeviceA] display oam critical-event
-----------[GigabitEthernet1/0/1] -----------
 Local link status   : UP
 Event statistics
   Link fault        : Not occurred
   Dying gasp        : Not occurred
   Critical event    : Not occurred
```

出力は、Device A と Device B 間のリンクでクリティカルリンクイベントが発生していないことを示します。

display oam link-event コマンドを使用し、Ethernet OAM リンクイベントの統計情報を表示します。

Device A のリモートエンドの Ethernet OAM リンクエラーイベントの統計情報を表示します。

```
[DeviceA] display oam link-event local
------------ [GigabitEthernet1/0/1] -----------
 Link status: UP
 OAM local errored frame event
   Event time stamp        : 5789 x 100 milliseconds
   Errored frame window    : 200 x 100 milliseconds
   Errored frame threshold : 10 error frames
   Errored frame           : 13 error frames
   Error running total     : 350 error frames
   Event running total     : 17 events
```

出力は、Device A で Ethernet OAM が有効になった後、350 回エラーが発生し、エラーフレームが 17 あったことを示します。リンクが不安定となっています。

目次

このセクションのページは **10-x-x** です。

2 章 CFD 2-1
2.1 概要 2-1
2.1.1 CFD の基本概念 2-1
2.1.2 CFD レベル 2-2
2.1.3 MIP のパケット処理 2-4
2.1.4 CFD の機能 2-4
2.1.5 プロトコルと標準 2-5
2.2 設定の制限とガイドライン 2-5
2.3 CFD 設定作業リスト 2-5
2.4 CFD の設定条件 2-6
2.5 CFD の基本設定 2-6
2.5.1 CFD の有効化 2-6
2.5.2 サービスインスタンスの設定 2-6
2.5.3 MEP の設定 2-7
2.5.4 MIP 自動生成ルールの設定 2-8
2.6 CFD 機能の設定 2-9
2.6.1 MEP 上の CC の設定 2-9
2.6.2 MEP 上の LB の設定 2-10
2.6.3 MEP 上の LT の設定 2-10
2.7 CFD の表示と維持 2-11
2.8 CFD 設定例 2-11

2章 CFD

2.1 概要

CFD(Connectivity Fault Detection)は、IEEE802.1ag-CFM(Connectivity Fault Management)と ITU-T Y.1731 に準拠し、1VLAN あたりの end-to-end のリンクレイヤ OAM メカニズムです。CFD はリンク接続性検出、故障検証、障害箇所検出のために使用されます。

2.1.1 CFD の基本概念

I. Maintenance domain

MD(maintenance domain)は CFD が動作するネットワークを定義します。MD は、MD 名によって識別されます。

II. Maintenance association

MA(maintenance association）は、MD の一組の MP(maintenance points）です。MA は、"MD 名+ MA 名"によって識別されます。必要に応じて MD に MA を設定できます。

MA は VLAN を利用します。VLAN を利用する MA は VLAN 属性を送信すると認識します。VLAN を利用しない MA は VLAN 属性がないと認識します。MP は、同じ MA 内の他の MP から送信されるパケットを受信することができます。MA のレベルは MA が属している MD のレベルと同一です。

III. Maintenance point

MP はポートで設定され、MA に属します。MP は、MEP(maintenance association end points) と MIP(maintenance association intermediate points) の 2 つのタイプに分類されます。

MEP は、MD の境界を定義します。各 MEP は MEP ID によって識別されます。

MEP が属している MA は、MEP が送信したパケットの VLAN を定義します。MEP のレベルは MEP が属している MD のレベルと同一です。MEP によって送信されたパケットのレベルは MEP のレベルと同一です。

MEP のレベルは、MEP が処理できるパケットのレベルを規定します。MEP は高いレベルのパケットから転送し、そのレベルあるいは低いレベルのパケットを転送します。処理手順は同一 VLAN でのパケットに固有です。異なる VLAN のパケットは独立した処理手順となります。

MEP は内側向きの MEP と外側向きの MEP に分類されます。

- 外側向きの MEP はホストがあるポートにパケットを送信します。
- 内側向き MEP はホストがあるポートにパケットを送信しません。装置上の他のポートにパケットを送信します。

IV. MEP リスト

MEP リストは、同じ MA 内に設定されたローカルな MEP と、モニタのためのリモート MEP のリストです。同じ MA 内のデバイスに設定されるすべての MEP が一覧表示されます。MEP はすべて固有な ID を持っています。MEP はリモートデバイスから、MA の MEP リストに含まれない MEP の ID を転送する CCM(Continuity Check Message)を受信すると、そのメッセージを廃棄します。

ローカル装置は、リモート障害表示(RDI)フラグビットを転送する CCM メッセージを送らなければなりません。そうでなければ、隣接装置は確実な障害を検知することができません。MA 内の少なくとも一つのローカル MEP が、MEP リストから他のすべてのリモート MEP を学習していないとき、MEP は CCM の RDI(Remote Detect Indication)フラグを転送できません。

2.1.2 CFD レベル

I. MD レベル

正確に障害個所を見つけるために、CFD は MD に 8 つのレベル（0 から 7 まで）を導入します。数値が大きいほうが高レベルで、カバー可能な領域も大きくなります。ドメインをタッチしたり、入れ子にできたりしますが(外のドメインに入れ子にされたものより高いレベルがある場合)、交差、または重なることはできません。

MD レベルは障害個所の特定を容易にして、障害箇所をより明確にします。図 2-1に、MD_A をライトブルー、MD_B を濃いブルーで示します。MD_A で接続障害が発生した場合、どの装置にも問題がある可能性があります。MD_B との境界で障害が発生した場合は、Device B、Device C、Device D の間のどこかが問題点となります。MD_B の装置で障害が発生していなければ、Device C には問題点がないことが分かります。

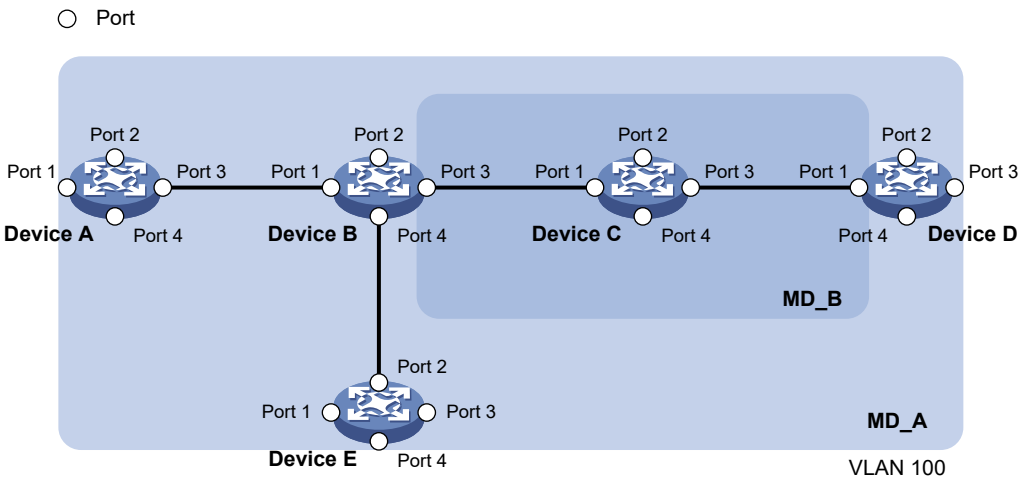


図 2-1 2 つの入れ子の MD

CFD はメッセージを交換し、ドメイン単位でオペレーションを実行します。ネットワークで正しく MD を計画し、CFD を構築することにより、問題点を早く見つけ出すことができます。

II. MA と MIP レベル

MA のレベルは MA が属する MD のレベルと同じです。

MEP のレベルは MA が属する MEP のレベルと同じです。

MIP のレベルは生成ルールと MIP が属している MD によって定義されます。MIP は以下に示す MIP 生成ルールにしたがって各ポートで自動的に生成されます。

- **デフォルトルール** － インタフェースで低いレベルの MIP が存在しない場合、MIP は現在のレベルで作成されます。MIP はインタフェースで MEP が設定されていなくても作成することができます。
- **明示ルール** － インタフェースで低いレベルの MIP と低いレベルの MEP がない場合、MEP は現在のレベルで作成されます。MIP はインタフェースで低いレベルの MEP が作成されたときのみ MIP を作成することができます。

ポートが MIP を持たないとき、システムは各 MD(低いレベルから高いレベル)の MA を確認し、現在のレベルで MIP を作成するか作成しないか、図 2-2に記載されている手順に従います。

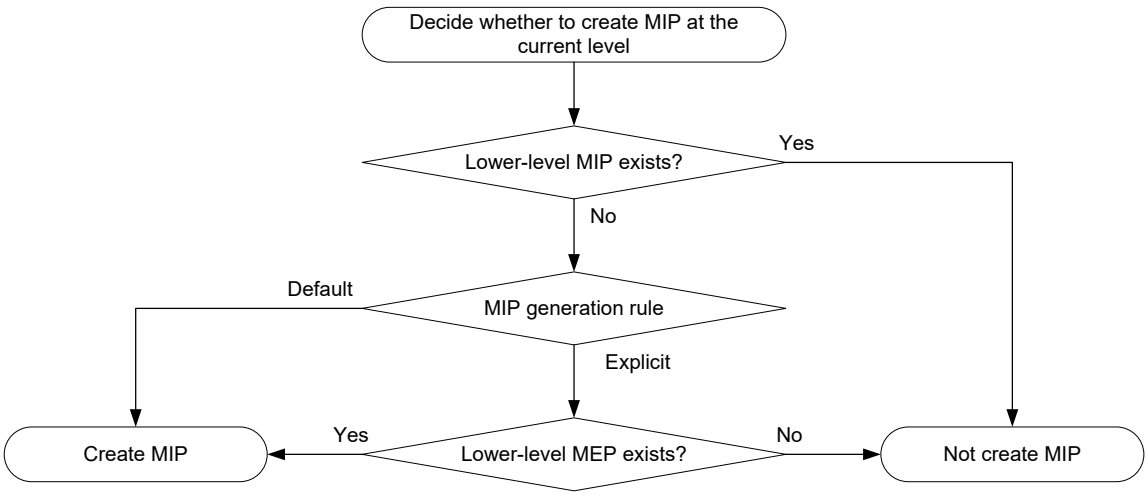


図 2-2 MIP の作成手順

III. CFD 等級例

図 2-3に CFD モジュールの等級づけの例を示します。MD の 4 つのレベル(0、2、3、5)があります。大きい値は高いレベルで、より大きい範囲がサポートされます。MP は Device A から Device F のポートで設定されます。

Device B のポート 1 は以下の MP で設定されます。

- レベル 5 の MIP
- レベル 3 の内側向き MEP
- レベル 2 の内側向き MEP
- レベル 0 の外側向き MEP

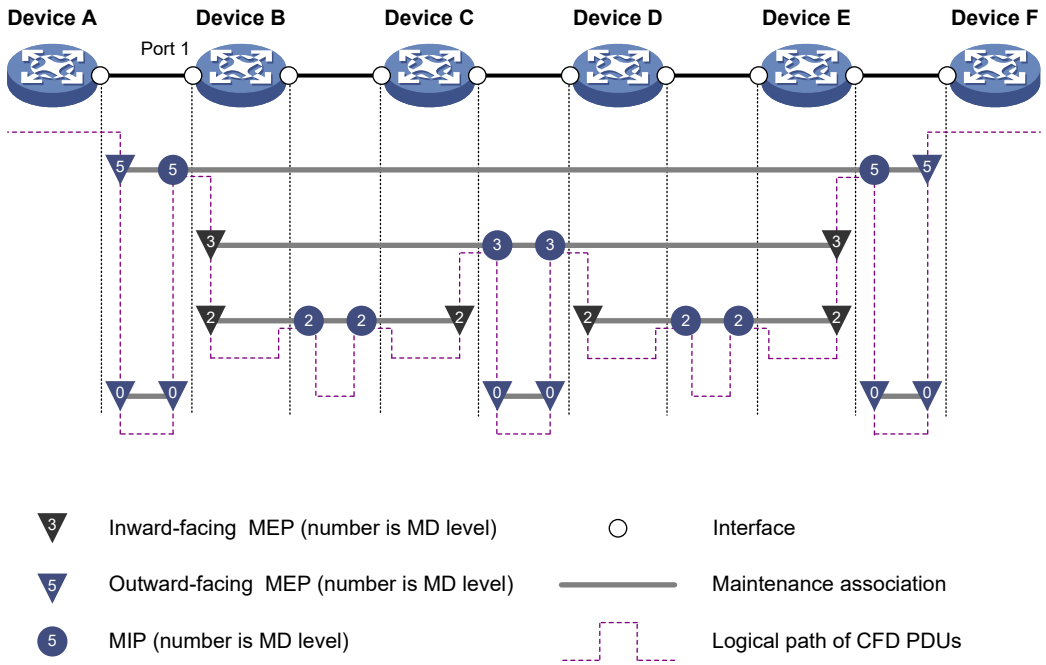


図 2-3 CFD の等級付け例

2.1.3 MIP のパケット処理

VLAN 属性がある MA には、MA の MP は MA が提供する VLAN のみパケットを送ります。

MP から送信されたパケットのレベルは、MP が所属している MD のレベルと同じになります。VLAN 属性がない MA には、MA の MP は外側向け MEP のみサポートします。外側向け MEP によって送信されたパケットのレベルは、MEP が所属している MD のレベルと同じになります。

MEP は高いレベルのパケットは処理せず転送し、同じレベルまたは低いレベルのパケットは処理のみ行います。

MIP は異なるレベルのパケットを処理せず転送し、同じレベルのパケットは処理のみ行います。

2.1.4 CFD の機能

CFD 機能は MP を通して実行されます。以下を含みます。

- Continuity check (CC)
- Loopback (LB)
- Linktrace (LT)

I. Continuity check

接続障害は、装置障害または設定エラーに起因します。Continuity check は、MEP の接続性をチェックします。この機能は MEP によって CCM(continuity check massage)を定期的に送信することで実行されます。1 つの MEP から送信された CCM は、同じ MA 内のすべての MEP で受信されることを意図しています。MEP を 3.5 回 送信する間に CCM を受

信しない場合、リンクが確立していないと判断し、ログが生成されます。複数の MEP が同時に CCM を送信すると、多点から多点へのリンクチェックが行われます。CCM はマルチキャストフレームです。

II. Loopback

IP レイヤの ping と同様に、loopback はローカルデバイスと宛先デバイスの接続性を検証します。この機能を実行するために、ローカル MEP は、宛先 MEP に LBM(loopback massage)を送信します。ローカル MEP が宛先 MEP からの LBR(loopback reply massage）を受信するかどうかで、2 つの間のリンク状態をチェックします。

LBM と LBR は、ユニキャストフレームです。

III. Linktrace

Linktrace は、traceroute と同様です。ソース MEP と宛先 MEP の間のパスを識別します。ソース MEP は、宛先 MEP に LTM(linktrace messages)を送信します。メッセージ受信後、宛先 MEP および MIP は、LTM フレームのソース MEP に LTR(linktrace reply massage)を送り返します。reply メッセージにもとづいて、ソース MEP は、宛先 MEP までの経路を識別できます。LTR はユニキャストフレームですが、LTM はマルチキャストフレームとなります。

2.1.5 プロトコルと標準

- IEEE 802.1ag, *Virtual Bridged Local Area Networks Amendment 5: Connectivity Fault Management*

2.2 設定の制限とガイドライン

CFD を設定するとき、以下の設定の制限とガイドラインに従ってください。

- 他の CFD 機能を設定するためにリモート MEP の MEP ID を使う場合は事前に CC を設定してください。リモート MEP の MAC アドレスを使う場合には、この制限には該当しません。
- 一般的に、スパニングツリーによってブロックポートとなった場合、以下のケースを除いて、CFD メッセージの送受信ができません。
  - □ ポートが外側向き MEP として設定されています。
  - □ ポートが、CCM メッセージを除く CFD メッセージを送受信できるよう設定された内側向きの MEP として設定されています。

スパニングツリーの詳細は、オペレーションマニュアルのセクション 3 *アクセス "STP"* を参照してください。

2.3 CFD設定作業リスト

以下に CFD の設定作業リストを示します。

作業リスト
CFDの基本設定 ● (必須設定項目) CFDの有効化 ● (必須設定項目) サービスインスタンスの設定 ● (必須設定項目) MEPの設定 ● (必須設定項目) MIP自動生成ルールの設定
CFD機能の設定: ● (必須設定項目) MEP上のCCの設定 ● (オプション設定項目) MEP上のLBの設定 ● (オプション設定項目) MEP上のLTの設定

2.4 CFDの設定条件

CFD が正しく動作するように、以下の作業を実行して、ネットワークを設計する必要があります。

- 全体のネットワークで MD のレベル付けを行い、各 MD の境界を定義します。
- MD ごとに名前を割り当てます。同一 MD 内にある装置は同じ MD の名前を使用していることを確認してください。
- 監視したい VLAN にしたがって、各 MD の MA を定義します。
- MA ごとに名前を割り当てます。同じ MD 内の同じ MA の装置が、同じ MA の名前を使用することを確認してください。
- 各 MD で各 MA の MEP リストを決定してください。同じ MA の装置が同じ MEP リストを持っていることを確認してください。
- MD と MA はエッジ、MEP はデバイスポートに設定する必要があります。MIP は、エッジではない装置またはポートに設計することができます。

2.5 CFDの基本設定

2.5.1 CFD の有効化

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. CFD を有効にする	**cfd enable**	デフォルト：無効

2.5.2 サービスインスタンスの設定

I. サービスインスタンスについて

MEP と MIP を設定する前に、最初にサービスインスタンスを設定する必要があります。サービスインスタンスはサービスアクセスポイント(SAP)で、MD 中の MA に属しています。

MD と MA は、サービスインスタンスの MP によって処理されたメッセージのレベルと VLAN 属性を定義します。VLAN 属性がない MA の MP は、VLAN に属していません。

以下に MD 名のサービスインスタンスを設定する手順を示します。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. MD を作成する	**cfd md** *md-name* [**index** *index-value*] **level** *level-value*	デフォルト：設定なし
3. サービスインスタンスを作成する	**cfd service-instance** *instance-id* **ma-id** { **icc-based** *icc-name* | **integer** *ma-num* | **string** *ma-name* | **vlan-based** [*vlan-id*] } [**ma-index** *index-value*] **md** *md-name* [**vlan** *vlan-id*]	デフォルト：設定なし

2.5.3 MEP の設定

I. MEP について

CFD は MEP のオペレーションを通して実行されます。MEP はサービスインスタンス上で構成され、MD レベルとサービスインスタンスの VLAN 属性は MEP の属性になります。

MEP を作成する前に、MEP リストを設定してください。MEP リストは MA で設定されたローカル MEP と監視用のリモート MEP の組み合わせです。MEP ID がサービスインスタンスの MEP リストに含まれない場合、MEP を作成することはできません。

インタフェースが同一レベルで、VLAN 属性なしで 1 つの MA の外側向けの MEP を設定することができます。

II. 制限事項とガイドライン

MEP を設定するとき、以下のガイドラインに従ってください。

- 同じレベルの 1 つの VLAN 指定がない MA を MEP インタフェースに指定できます。MEP は外側向けとして設定します。
- VLAN 指定がない MA における MEP がリモート MEP から 3.5CM インターバル以内に CCM メッセージを受信しない場合、ローカル MEP はそのインタフェースをリンクダウンさせます。これにより RRPP や Smart Link での高速切り替えを可能にします。
- aggregate interface view での設定はアグリゲートインタフェースとすべてのメンバポートで適用されます。
- アグリゲーショングループに所属するメンバポート（interface view）に設定したときは MEP 設定が適用されません。一部のメンバポートだけに適用することはできません。

III. 設定条件

MEP を設定する前に、サービスインスタンスを設定してください。

IV. 設定手順

以下に MEP の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. MEP リストを設定する	**cfd meplist** *mep-list* **service-instance** *instance-id*	デフォルト：設定なし
3. Layer 2 interface view あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	ー
4. MEP を作成する	**cfd mep** *mep-id* **service-instance** *instance-id* { **inbound** | **outbound** }	デフォルト：設定なし

2.5.4 MIP 自動生成ルールの設定

I. MIP 自動生成ルールについて

サービスインスタンスの機能的な実体として、MIP は、LTM フレーム、LBM フレームなどの様々な CFD フレームに応答します。システムは MIP 自動作成ルールにもとづいて MIP を自動的に作成します。

cfd mip-rule コマンドが設定された後、以下の要因によって MIP を作成あるいは削除することができます。

- CFD の有効化あるいは無効化
- ポートの MEP の作成あるいは削除
- ポートの VLAN 属性の変更
- **cfd mip-rule** コマンドで指定されるルールの変更

II. 制限事項とガイドライン

MIP 自動生成ルールを設定するとき、以下のガイドラインに従ってください。

- VLAN 属性がない MA は主にダイレクトリンクの状態を検出するのに使用されます。VLAN 属性がない MA は MIP を生成することはできません。
- VLAN 属性がある MA で、インタフェースで同一以上のレベルの MEP が存在する場合、MA 用の MIP はインタフェースで作成されません。

III. 設定手順

以下に MA 生成ルールの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. MIP 自動生成ルールを設定する	**cfd mip-rule** { **default** | **explicit** } **service-instance** *instance-id*	デフォルト : 生成ルールは設定されておらず、自動的に MIPを作成しません。

2.6 CFD機能の設定

2.6.1 MEP 上の CC の設定

I. CC について

他の CFD を設定する前に CC を設定してください。CC を設定したのち、MA の MEP は接続性のチェックを行うために定期的に CCM フレームを送信できます。

CCM フレームのタイムアウト時間が終了したとき、MEP はリンクが切断されたと認識します。CCM の interval フィールドを設定するとき、表 2-1に示す値を使用します。

表 2-1 CCM の interval フィールドの変換

CCM の interval フィールドの値	CCM の送信間隔	最大 CCM ライフタイム時間
1	10/3 ミリ秒	35/3 ミリ秒
2	10 ミリ秒	35 ミリ秒
3	100 ミリ秒	350 ミリ秒
4	1 秒	3.5 秒
5	10 秒	35 秒
6	60 秒	210 秒
7	600 秒	2100 秒

🕮 **メモ：**

CCM interval フィールドは 1 から 2 の値をサポートしていません。

II. 制限事項とガイドライン

MEP で CC を設定するとき、以下のガイドラインに従ってください。

- 同一 MA 内のすべての MEP は、同一 CCM の interval フィールドの値を設定してください。
- CCM interval フィールドを変更した後、MEP は CCM を送信する前に他の CCM interval を待ちます。
- aggregate interface view での設定はアグリゲートインタフェースとすべてのメンバポートで適用されます。
- アグリゲーショングループに所属するメンバポート（interface view）に設定したときは MEP 設定が適用されません。一部のメンバポートだけに適用することはできません。

III. 設定手順

以下に MEP 上の CC の設定を示します。

操作	コマンド	補足
1.　system view に移行する	**system-view**	ー

操作	コマンド	補足
2. (オプション設定項目) MEP から送信される CCM メッセージの送信間隔を設定する	**cfd cc interval** *interval-value* **service-instance** *instance-id*	デフォルト：4
3. Layer 2 interface view あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	―
4. MEP 上で CCM の送信を有効にする	**cfd cc service-instance** *instance-id* **mep** *mep-id* **enable**	デフォルト：無効

2.6.2 MEP 上の LB の設定

LB は、ローカル MEP、リモート MEP、あるいは MIP の間のリンクの状態を確認することができます。

以下に MEP 上の LB の設定を示します。

操作	コマンド	補足
LBを有効にする	**cfd loopback service-instance** *instance-id* **mep** *mep-id* { **target-mac** *mac-address* | **target-mep** *target-mep-id* } [**number** *number*]	デフォルト：無効 すべてのviewで設定可能です。

2.6.3 MEP 上の LT の設定

I. LT について

LT はソース MEP とターゲット MEP の間で経路をたどることができ、自動的に LT メッセージを送信することで、リンク障害を検出します。2 つの機能は、以下のようにして実装されます。

- **経路確認**－最初の機能を実装するため、ソース MEP は、ターゲット MEP に LTM にメッセージを送信します。LTM メッセージに応答した LTR メッセージにより、2 つの MEP 間の経路確認ができます。
- **LT メッセージの自動送信**－LT メッセージの自動送信が有効になると、ソース MEP が 3.5 回送信する間にターゲット MEP からの CCM フレームを受信しなれば、2 つの間のリンクは不完全であると考えられ、LTM フレーム（宛先がターゲットの MEP で、LTM フレームの TTL フィールドに最大値 255 がセットされています）が送信されます。MIP が応答した LTR にもとづいて、障害場所の特定ができます。

II. 設定条件

VLAN 属性を送信する MA の MEP で LT を設定する前に、MA が所属する VLAN を作成してください。

III. 設定手順

以下に MEP 上の LT の設定を示します。

操作	コマンド	補足
1. ソース MEP とターゲット MEP 間のパスを検出する	**cfd linktrace service-instance** *instance-id* **mep** *mep-id* { **target-mac** *mac-address* | **target-mep** *target-mep-id* } [**ttl** *ttl-value*] [**hw-only**]	すべてのviewで設定可能です。
2. system view に移行する	**system-view**	ー
3. LTメッセージの自動送信を有効にする	**cfd linktrace auto-detection** [**size** *size-value*]	デフォルト：無効

2.7 CFDの表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
MEPで受信したLTR情報を表示する	**display cfd linktrace-reply** [**service-instance** *instance-id* [**mep** *mep-id*]]
LTMに自動応答したLTRメッセージの受信情報を表示する	**display cfd linktrace-reply auto-detection** [**size** *size-value*]
MD設定情報を表示する	**display cfd md**
MEPの属性と稼動状況を表示する	**display cfd mep** *mep-id* **service-instance** *instance-id*
サービスインスタンスのMEPリストを表示する	**display cfd meplist** [**service-instance** *instance-id*]
MP情報を表示する	**display cfd mp** [**interface** *interface-type interface-number*]
リモートMEP情報を表示する	**display cfd remote-mep service-instance** *instance-id* **mep** *mep-id*
サービスインスタンス設定情報を表示する	**display cfd service-instance** [*instance-id*]
CFDの状態を表示する	**display cfd status**

2.8 CFD設定例

I. ネットワーク要件

図 2-4に示すように以下の設定を行います。

- ネットワークには 5 つの装置があり、MD_A(Level 5)、MD_B(Level 3)の 2 つの MD に分かれています。すべてのポートは VLAN100 に属し、2つの MD の MA はすべて VLAN100 で動作しています。Device A～Device E の MAC アドレスを、それぞれ 0010-FC00-6511 、 0010-FC00-6512 、 0010-FC00-6513 、 0010-FC00-6514 、 0010-FC00-6515 とします。
- MD_A は Device A の GigabitEthernet 1/0/1、Device D の GigabitEthernet 1/0/3、Device E の GigabitEthernet 1/0/4 の 3 つのエッジポートがあります。すべて内向き MEP(Inward-facing MEP)です。MD_B は Device B の GigabitEthernet 1/0/3、Device D の GigabitEthernet 1/0/1 の 2 つのエッジポートがあります。そのポートは外向き MEP(Outward-facing MEP)です。
- MD_A では、Device B のポートは、低レベルの MEP が設定されたときに MIP を持つように設計されています。GigabitEthernet 1/0/3 は MD_B の MEP と設定され、

MD_A の MIP がこのポートに設定されます。MD_A の MIP 生成ルールを明示的にする必要があります。

- Device C のすべてのポートで MD_B の MIP が設定されています。デフォルトの MIP 生成ルールを設定します。
- ソース MEP とターゲット MEP の間の経路、またはリンク障害を検出するために、LT を使用してください。
- すべてのネットワークのステータス情報を取得した後、LT を使って回線障害を見つけます。

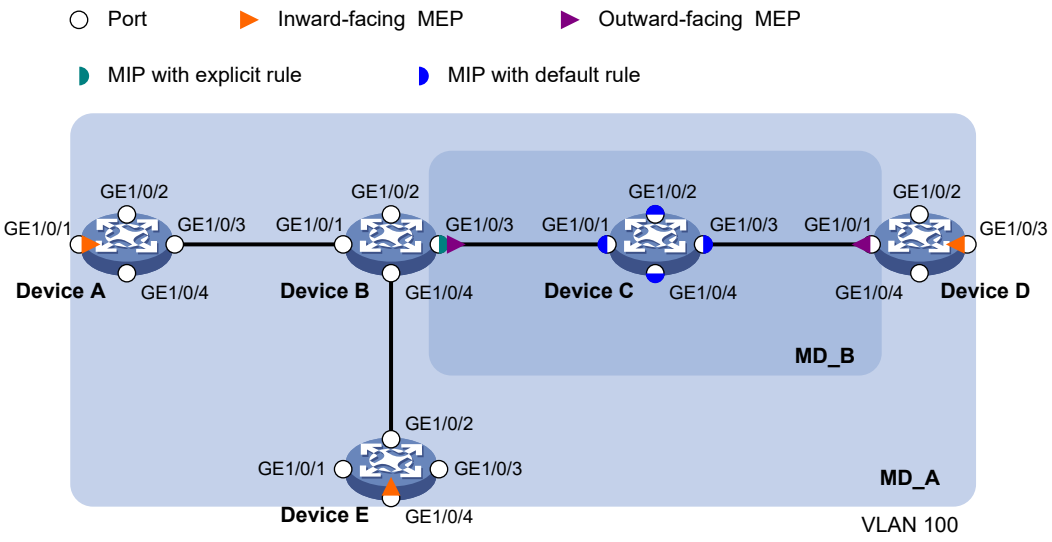


図 2-4 ネットワーク図

II. 設定手順

1)　VLAN を作成し、ポートを割り当てます。

図 2-4に示す各 Device で、VLAN 100 を作成し、GigabitEthernet 1/0/1～GigabitEthernet 1/0/4 に VLAN100 を割り当てます。

2)　CFD を有効にします。

Device A で CFD を有効にします。

```
<DeviceA> system-view
[DeviceA] cfd enable
```

Device A の設定と同様に、Device B～Device E で CFD を有効にします。（詳細は省略します）

3)　サービスインスタンスを設定します。

Device A で MD_A(level 5)を作成し、サービスインスタンス 1 を作成します。サービスインスタンス 1 では MA は VLAN によって識別され、VLAN100 を提供します。

```
[DeviceA] cfd md MD_A level 5
[DeviceA] cfd service-instance 1 ma-id vlan-based md MD_A vlan 100
```

Device A の設定と同様に Device E を設定します。（詳細は省略します）

Device B で MD_A(level 5)を作成し、サービスインスタンス 1 を作成します。サービスインスタンス 1 では MA は VLAN によって識別され、VLAN100 を提供します。

```
[DeviceB] cfd md MD_A level 5
[DeviceB] cfd service-instance 1 ma-id vlan-based md MD_A vlan 100
```

MD_B(level 3)を作成し、サービスインスタンス 2 を作成します。サービスインスタンス 2 では MA は VLAN によって識別され、VLAN100 を提供します。

```
[DeviceB] cfd md MD_B level 3
[DeviceB] cfd service-instance 2 ma-id vlan-based md MD_B vlan 100
```

Device B の設定と同様に Device D を設定します。（詳細は省略します）

Device C で MD_B(level 3)を作成し、サービスインスタンス 2 を作成します。サービスインスタンス 2 では MA は VLAN によって識別され、VLAN100 を提供します。

```
[DeviceC] cfd md MD_B level 3
[DeviceC] cfd service-instance 2 ma-id vlan-based md MD_B vlan 100
```

4) MEP を設定します。

Device A で、サービスインスタンス 1 の MEP リストを設定し、GigabitEthernet 1/0/1 のサービスインスタンス 1 の内向き MEP 1001 を作成します。

```
[DeviceA] cfd meplist 1001 4002 5001 service-instance 1
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] cfd mep 1001 service-instance 1 inbound
[DeviceA-GigabitEthernet1/0/1] quit
```

Device B でサービスインスタンス 1、2 の MEP リストを設定します。

```
[DeviceB] cfd meplist 1001 4002 5001 service-instance 1
[DeviceB] cfd meplist 2001 4001 service-instance 2
```

Device B で GigabitEthernet 1/0/3 のサービスインスタンス 2 の外向き MEP 2001 を作成します。

```
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] cfd mep 2001 service-instance 2 outbound
[DeviceB-GigabitEthernet1/0/3] quit
```

Device D でサービスインスタンス 1、2 の MEP リストを設定します。

```
[DeviceD] cfd meplist 1001 4002 5001 service-instance 1
[DeviceD] cfd meplist 2001 4001 service-instance 2
```

Device D で GigabitEthernet 1/0/1 のサービスインスタンス 2 の外向き MEP 4001 を作成します。

```
[DeviceD] interface gigabitethernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] cfd mep 4001 service-instance 2 outbound
[DeviceD-GigabitEthernet1/0/1] quit
```

Device D で GigabitEthernet 1/0/3 のサービスインスタンス 1 の内向き MEP 4002 を作成します。

```
[DeviceD] interface gigabitethernet 1/0/3
[DeviceD-GigabitEthernet1/0/3] cfd mep 4002 service-instance 1 inbound
[DeviceD-GigabitEthernet1/0/3] quit
```

Device E でサービスインスタンス 1 の MEP リストを設定します。

```
[DeviceE] cfd meplist 1001 4002 5001 service-instance 1
```

Device E で GigabitEthernet 1/0/4 のサービスインスタンス 1 の内向き MEP 5001 を作成します。

```
[DeviceE] interface gigabitethernet 1/0/4
[DeviceE-GigabitEthernet1/0/4] cfd mep 5001 service-instance 1 inbound
[DeviceE-GigabitEthernet1/0/4] quit
```

5) MIP を設定します。

Device B のサービスインスタンス 1 で MIP の作成ルールを明示的に設定します。

```
[DeviceB] cfd mip-rule explicit service-instance 1
```

Device C のサービスインスタンス 2 で MIP のデフォルトの作成ルールを明示的に設定します。

```
[DeviceC] cfd mip-rule default service-instance 2
```

6) CC を設定します。

Device A の GigabitEthernet 1/0/1 で、サービスインスタンス 1 の MEP 1001 用の CCM フレームの送信を有効にします。

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] cfd cc service-instance 1 mep 1001 enable
[DeviceA-GigabitEthernet1/0/1] quit
```

Device B の GigabitEthernet 1/0/3 で、サービスインスタンス 2 の MEP 2001 用の CCM フレームの送信を有効にします。

```
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] cfd cc service-instance 2 mep 2001 enable
[DeviceB-GigabitEthernet1/0/3] quit
```

Device D の GigabitEthernet 1/0/1 で、サービスインスタンス 2 の MEP 4001 用の CCM フレームの送信を有効にします。

```
[DeviceD] interface gigabitethernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] cfd cc service-instance 2 mep 4001 enable
[DeviceD-GigabitEthernet1/0/1] quit
```

Device D の GigabitEthernet 1/0/3 で、サービスインスタンス 1 の MEP 4002 用の CCM フレームの送信を有効にします。

```
[DeviceD] interface gigabitethernet 1/0/3
[DeviceD-GigabitEthernet1/0/3] cfd cc service-instance 1 mep 4002 enable
[DeviceD-GigabitEthernet1/0/3] quit
```

Device E の GigabitEthernet 1/0/4 で、サービスインスタンス 1 の MEP 5001 用の CCM フレームの送信を有効にします。

```
[DeviceE] interface gigabitethernet 1/0/4
[DeviceE-GigabitEthernet1/0/4] cfd cc service-instance 1 mep 5001 enable
[DeviceE-GigabitEthernet1/0/4] quit
```

III. 設定の確認

1) CC 機能がリンク障害を検出した場合、LB 機能を確認します。

Device A で LB 機能を有効にし、サービスインスタンス 1 の MEP 1001 と MEP 5001 間のリンクステータスをチェックします。

```
[DeviceA] cfd loopback service-instance 1 mep 1001 target-mep 5001
Loopback to 0010-fc05-6515 with the sequence number start from 1001-43404:
Reply from 0010-fc05-6515: sequence number=1001-43404 time=5ms
Reply from 0010-fc05-6515: sequence number=1001-43405 time=5ms
Reply from 0010-fc05-6515: sequence number=1001-43406 time=5ms
Reply from 0010-fc05-6515: sequence number=1001-43407 time=5ms
Reply from 0010-fc05-6515: sequence number=1001-43408 time=5ms
Sent: 5        Received: 5        Lost: 0
```

2) すべてのネットワークのステータス状態を CC 機能で取得した後、LT 機能を確認します。

Device A のサービスインスタンス 1 で、MEP 1001 と MEP 5001 間の経路を確認します。

```
[DeviceA] cfd linktrace service-instance 1 mep 1001 target-mep 5001
Linktrace to MEP 5001 with the sequence number 1001-43462:
MAC Address               TTL     Last Mac         Relay Action
0010-fc05-6515            63      0010-fc02-6512   Hit
```

目次

このセクションのページは **10-x-x** です。

3章 DLDP 3-1
3.1 概要 3-1
3.1.1 基本概念 3-2
3.1.2 DLDPの動作 3-3
3.2 設定の制限とガイドライン 3-6
3.3 DLDP設定作業リスト 3-6
3.4 DLDPの有効化 3-7
3.5 Advertisementパケットの送信間隔の設定 3-7
3.6 DelayDownタイマの設定 3-7
3.7 ポートシャットダウンモードの設定 3-8
3.8 DLDP認証の設定 3-9
3.9 DLDPの表示と維持 3-9
3.10 DLDP設定例 3-9
3.10.1 片方向リンクの自動シャットダウンの設定例 3-9
3.10.2 片方向リンクの手動シャットダウンの設定例 3-13
3.10.3 片方向リンクのハイブリッドシャットダウンの設定例 3-17

3章 DLDP

3.1 概要

片方向リンクが発生すると、片方のリンクは反対側からパケットを受信できますが、もう一方のリンクはパケットを受信できません。

片方向リンクは、以下のタイプがあります。

- ファイバがクロス接続されている場合に発生します。
- ファイバがもう一方に接続されていない場合、あるいはファイバのペアケーブルの一本が断線した場合に発生します。

図 3-1に正常な接続と 2 つの片方向リンクの例を示します。

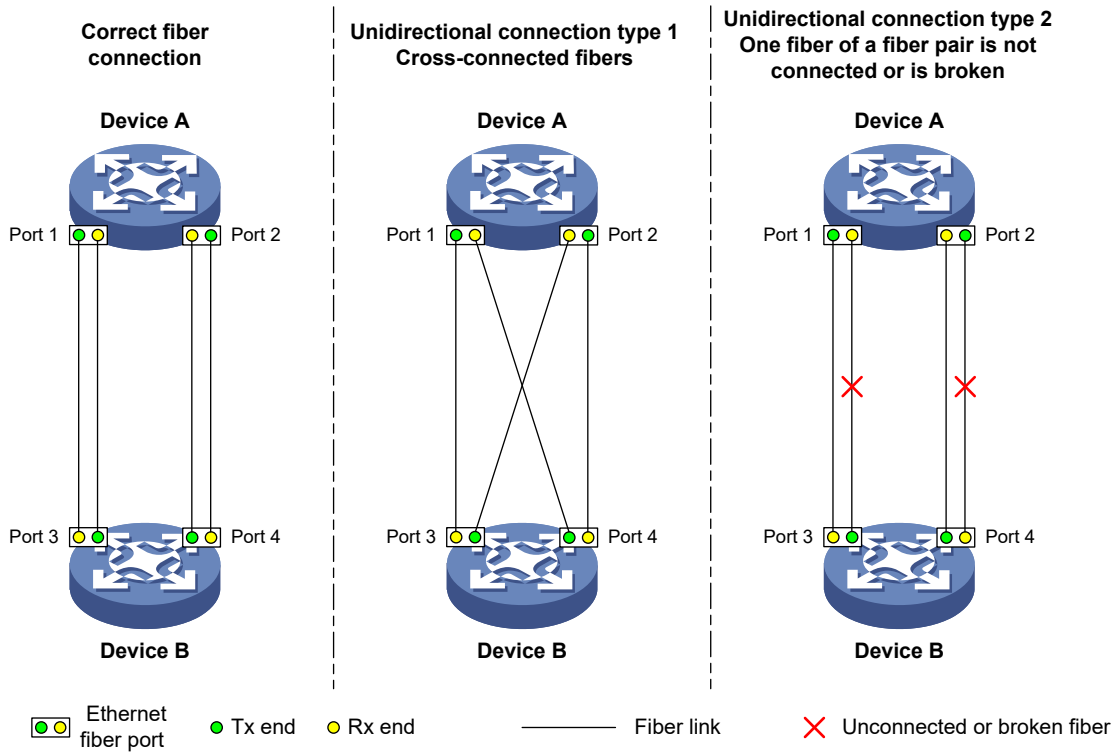


図 3-1 ファイバの正常な接続と異常な接続

オートネゴシエーションなどの物理レイヤの検出メカニズムが物理的な信号や故障を検出しても、物理レイヤで接続されているが片方向リンクによって接続故障を検出することはできません。

データリンクレイヤプロトコルの DLDP（Device Link Detection Protocol）は、リンクレイヤで正しく接続されているか、2 つのエンド間でパケットが正しく交換できるかどうかを検出します。DLDP が片方向リンクを検出した場合、ネットワークの問題を避けるため、故障ポートを自動的にシャットダウンする、あるいはユーザが故障ポートを手動でシャッ

トダウンすることができます。DLDP は物理レイヤプロトコルと連携して、リンク状態をモニタし、物理と論理の片方向リンクになることを回避します。

3.1.1 基本概念

I. DLDP ネイバ状態

もしポート A とポート B が同一リンクにあり、ポート A がポート B からリンクレイヤパケットを受信できる場合、ポート B はポート A の DLDP ネイバとなります。パケットの交換を行うことができる 2 つのポートはネイバです。

表 3-1 DLDP ネイバ状態

DLDP タイマ	説明
Confirmed	DLDPネイバのリンクが双方向です。
Unconfirmed	新しく発見されたネイバのリンク状態が、確定されていません。

II. DLDP ポート状態

DLDP が有効なポートは、DLDP ポートと呼ばれます。DLDP ポートは複数のネイバを持つことができます。DLDP のポート状態は、DLDP ネイバ状態に依存します。

表 3-2 DLDP ポート状態

状態	説明
Initial	DLDPがポートで有効ですが、グローバルで無効となっています。
Inactive	DLDPがポートとグローバルで有効ですが、リンクが物理的にダウンしています。
Bidirectional	DLDPがポートとグローバルで有効で、1つ以上のConfirmed 状態のネイバが存在します。
Unidirectional	DLDPがポートとグローバルで有効ですが、Confirmed 状態のネイバがありません。この状態では、ポートはこれ以上DLDPパケット以外のパケットを送受信しません。

III. DLDP タイマ

表 3-3 DLDP タイマ

DLDP タイマ	説明
Advertisementタイマ	Advertisementパケットの送信間隔です。（デフォルトは5秒で、設定可能です）
Probeタイマ	Probeパケットの送信間隔です。このタイマは1秒に設定されます。
Echoタイマ	新しいネイバ用にProbe状態になったときにEchoタイマが起動します。タイマは10秒に設定されます。

DLDP タイマ	説明
Entryタイマ	新しいネイバが追加されたとき、ネイバがConfirmedの場合、ネイバエントリが作成され、対応するEntryタイマが起動します。 Advertisementパケットを受信したとき、装置は対応するネイバエントリとEntryタイマをアップデートします。 Entryタイマの設定はAdvertisementタイマの3倍です。
Enhancedタイマ	Entryタイマが終了したとき、Echoタイマと一緒にEnhancedタイマが起動します。Enhancedタイマは1秒に設定されます。
DelayDownタイマ	ポートが物理的にダウンしたとき、装置はDelayDownタイマを開始します。それは対応するネイバエントリを削除するまでの時間です。デフォルトは1秒で、設定可能です。 DelayDownタイマが終了したとき、ポートがダウンである場合、装置は対応するDLDPネイバ情報を削除します。ポートがアップである場合は、装置は対応するDLDPネイバ情報を削除しません。
RecoverProbeタイマ	タイマは2秒に設定されます。Unidirectional状態のポートは、片方向リンクが双方向リンクに回復したかどうかを検出するために、RecoverProbeパケットを規則的に送信します。

IV. DLDP 認証モード

ネットワークの攻撃と不正な検出を防ぐために、DLDP 認証を使用することができます。

表 3-4 DLDP 認証モード

認証モード	DLDP パケット送信側の処理	DLDP パケット受信側の処理
Non-authentication	DLDPパケットの認証フィールドを0に設定します。	受信したDLDPパケットの認証情報を確認し、認証情報がローカル設定と矛盾しているパケットを廃棄します。
Plaintext authentication	認証フィールドを平文で設定されたパスワードに設定します。	
MD5 authentication	MD5アルゴリズムを使用してユーザが設定したパスワードを暗号化し、認証フィールドをダイジェストで割り当てます。	

3.1.2 DLDP の動作

I. 1 つのネイバの検出

2 つの装置がファイバあるいはネットワークケーブルで接続されているとき、ネイバの片方向リンクを検出するため、DLDP を有効にします。片方向リンクの検出処理を以下の 2 つのケースで示します。

- DLDP を有効にする前に片方向リンクが発生

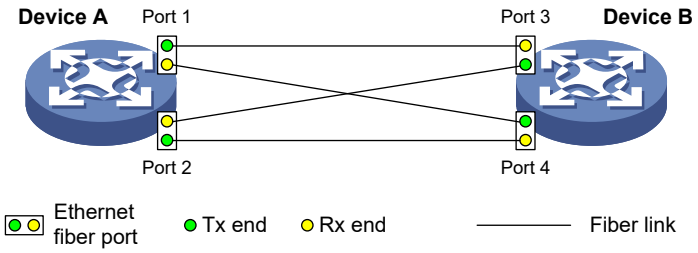


図 3-2 クロス接続ファイバ

図 3-2に示すように、DLDP を有効にする前に、Device A と Device B 間のファイバがクロス接続されています。DLDP を有効にした後、4 つのポートがすべてアップし、Unidirectional 状態になります。RecoverProbe パケットを送信します。例として、ポート 1 の片方向リンク検出処理を示します。

a) ポート1がポート4からRecoverProbeパケットを受信し、RecoverEchoパケットを返します。

b) ポート4はポート1からRecoverEchoパケットを受信することができないため、ポート4はポート1のネイバになることができません。

c) ポート3はポート1からRecoverEchoパケットを受信できますが、ポート3は宛先でないため、ポート3はポート1のネイバになることができません。

他の 3 つのポートで同一の処理が行われます。4 つのポートは Unidirectional 状態となります。

- DLDP を有効にした後に片方向リンクが発生

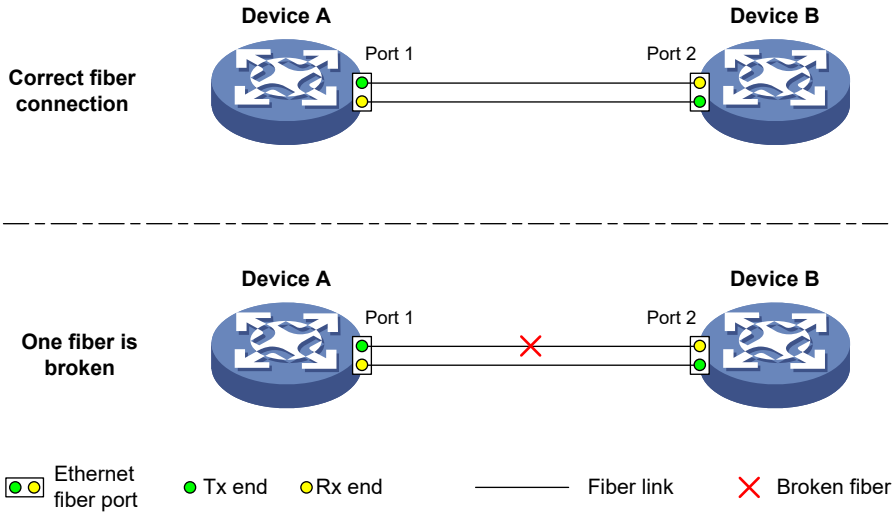


図 3-3 ファイバの故障

図 3-3に示すように、Device A と Device B はファイバで接続されています。DLDP を有効にした後、ポート 1 とポート 2 は以下のように双方向隣接関係を構築します。

a) 物理的にアップ状態のポート1はUnidirectional状態になり、RecoverProbeパケットを送信します。

b) RecoverProbeパケットを受信した後、ポート2はRecoverEchoパケットを返します。

c) ポート1がRecoverEchoパケットを受信した後、パケットの隣接情報がローカルの情報にマッチするか確認します。ポート1はポート2と隣接関係を確立し、Bidirectional状態に移行します。ポート1はEntryタイマを開始し、Advertisementパケットを定期的に送信します。

d) ポート2がAdvertisementパケットを受信した後、ポート1と未確認の隣接状態を確立します。ポート2はEchoタイマ、Probeタイマを開始し、定期的にProbeパケットを送信します。

e) Probeパケットを受信した後、ポート1はEchoパケットを返します。

f) ポート2がEchoパケットを受信した後、パケットの隣接情報がローカル情報にマッチするか確認します。ポート1のneighbor状態がConfirmed状態になります。ポート2はBidirectional状態になります。ポート2はEntryタイマを開始し、定期的にAdvertisementパケットを送信します。

このようにしてポート 1 とポート 2 の双方向隣接関係が確立されます。

隣接関係の構築が行われた後、ポート 2 の Rx のエンド側が信号を受信するのに失敗すると、ポート 2 は物理的にダウンし、Inactive 状態になります。ポート 2 の Tx のエンド側はポート 1 に信号を送信することができるため、ポート 1 はアップ状態となり続けます。ポート 2 の Entry タイマが終了した後、ポート 1 は Enhanced タイマと Echo タイマを開始し、ポート 2 に Probe パケットを送信します。ポート 1 の Tx ラインが故障しているため、Echo タイマが終了した後、ポート 1 はポート 2 から Echo パケットを受信することができません。ポート 1 は Unidirectional 状態になり、ポート 2 に Disable パケットを送信します。同時に、ポート 1 はポート 2 の隣接関係を削除し、RecoverProbe タイマを開始します。この処理の間、ポート 2 は Inactive 状態を維持します。

II. 複数ネイバの検出

複数の装置がハブを介して接続されているとき、ハブに接続されたすべてのインタフェースの DLDP をネイバ間の片方向リンクを検出するために有効にします。確認されたネイバが存在しないとき、インタフェースは Unidirectional 状態になります。

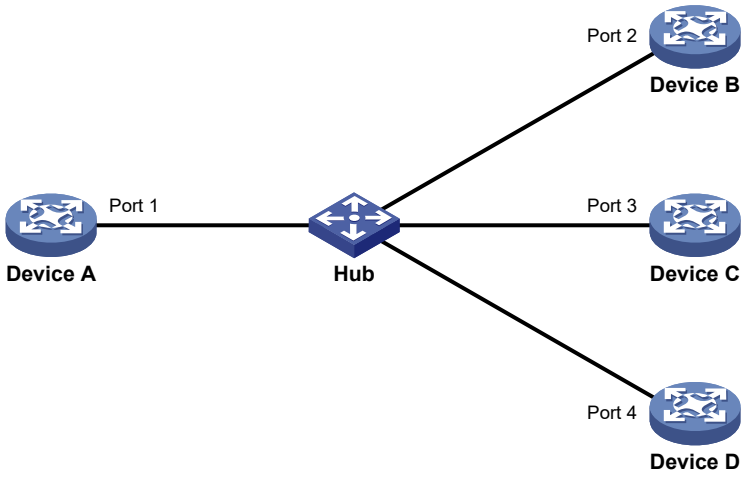


図 3-4 ネットワーク図

図 3-4に示すように、Device A から Device D はハブを介して接続され、DLDP が有効になっています。ポート 1、ポート 2、ポート 3 がポート 4 のリンクが故障したと検出したとき、ポート 4 との隣接関係を削除しますが、Bidirectional 状態を維持します。

3.2 設定の制限とガイドライン

DLDP を設定するとき、以下の設定の制限とガイドラインに従ってください。

- DLDP を正しく動作させるため、両端で DLDP を有効にし、Advertisement パケットを送信する間隔、DLDP 認証モード、パスワードの設定が同一であることを確認してください。
- DLDP を正しく動作させるため、2 つのリンクの終端ポートが全 2 重モードで、同一速度が設定されていることを確認してください。
- 両端のポートでオートネゴシエーションが動作する場合はリンクダウンが直ちに発生します。

3.3 DLDP設定作業リスト

作業リスト
（必須設定項目） DLDPの有効化
（オプション設定項目） Advertisementパケットの送信間隔の設定
（オプション設定項目） DelayDownタイマの設定
（オプション設定項目） ポートシャットダウンモードの設定
（オプション設定項目） DLDP認証の設定

3.4 DLDPの有効化

装置で DLDP を正しく設定するため、グローバルとポートで DLDP を有効にする必要があります。

以下に DLDP を有効にする設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． グローバルに DLDP を有効にする	**dldp global enable**	デフォルト：無効
3． Ethernet interface view に移行する	**interface** *interface-type interface-number*	―
4． DLDP を有効にする	**dldp enable**	デフォルト：無効

🕮 **メモ：**

両端のポートでオートネゴシエーションが動作する場合、リンクダウンが直ちに発生します。

3.5 Advertisementパケットの送信間隔の設定

ネットワーク性能が悪化する前に、片方向リンクを検出することができるようするため、ネットワーク環境で適切に Advertisement パケットの送信間隔を設定します。（デフォルトの間隔を使用することを推奨します。）

以下に Advertisement パケットの送信間隔の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． Advertisement パケットの送信間隔を設定する	**dldp interval** *time*	デフォルト：5秒

3.6 DelayDownタイマの設定

いくつかのポートで Tx ラインの故障が発生すると、ポートはアップダウンを繰り返し、Rx ラインの光信号ジッタを引き起こします。この問題を避けるため、Tx の故障によってポートがダウンするとき、装置は、対応するネイバエントリが削除されるのを防ぐため、DelayDown タイマを開始します。タイマが終了したときポートがダウンしたままである場合、装置は DLDP ネイバ情報を削除します。ポートがアップである場合、何もアクションを行いません。

以下に DelayDown の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―

操作	コマンド	補足
2． DelayDown タイマを設定する	**dldp delaydown-timer** *time*	デフォルト：1秒 すべてのDLDPが設定されているポートに適用されます。

3.7 ポートシャットダウンモードの設定

片方向リンクを検出したとき、DLDP は次のいずれかのモードでポートをシャットダウンすることができます。

- **自動モード**－DLDP が単方向リンクを検出すると、単方向ポートをシャットダウンします。リンクが双方向になると、シャットダウンされたポートが起動されます。
- **手動モード**－DLDP が単方向リンクを検出すると、ポートをシャットダウンしません。手動でシャットダウンする必要があります。リンクステータスを確認するには、**undo shutdown** コマンドを使用してポートを起動します。リンクが双方向になると、ポートは双方向になります。このモードを使用して、次の場合に単一方向リンクレポートのために通常のリンクがシャットダウンされないようにします。
  - ネットワークのパフォーマンスが低い状態です。
  - 装置がビジー状態です。
  - CPU 使用率が高い状態です。
- **ハイブリッドモード**:DLDP は片方向リンクを検出すると、片方向ポートをシャットダウンし、リンク検出を停止します。リンクステータスを確認するには、**undo shutdown** コマンドを使用してポートを起動します。リンクが双方向になると、ポートは双方向になります。

I. 制限とガイドライン

system view 内のすべてのインタフェース、または interface view の一つのインタフェースのポートシャットダウンモードを設定できます。interface view の設定は、system view の設定よりも優先されます。

DLDP ポートでリモート OAM ループバックを有効にするには、ポートシャットダウンモードを手動に設定します。それ以外の場合、DLDP は自動的にパケットを受信したときにポートをシャットダウンします。これにより、リモート OAM ループバック障害が発生します。Ethernet OAM の詳細については、オペレーションマニュアルのセクション 10 *高可用性 “Ethernet OAM”* を参照してください。

II. グローバルでのポートシャットダウンモードの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	－
2． グローバルポートシャットダウンモードを設定する	**dldp unidirectional-shutdown** { **auto** | **hybrid** | **manual** }	デフォルト：**auto**

III. インタフェースでのポートシャットダウンモードの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	－
2． Ethernet interface view に移行する	**interface** *interface-type interface-number*	－

操作	コマンド	補足
3． インタフェースのポートシャットダウンモードを設定する	**dldp port unidirectional-shutdown** { **auto** | **hybrid** | **manual** }	デフォルト：グローバル設定が使用されます。

3.8 DLDP認証の設定

平文テキスト認証あるいは MD5 認証の DLDP 認証モードを適切に設定することにより、アタックや悪意のあるアクセスからネットワークを保護できます。もしネットワークが安全である場合、認証を行わないように選択することができます。

以下に DLDP 認証の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． DLDP 認証モードを設定する	**dldp authentication-mode** { **md5** | **none** | **simple** }	デフォルト：**none**
3． DLDP 認証のパスワードを設定する	**dldp authentication-password** { **cipher** | **simple** } *string*	デフォルト：設定なし 認証モードを設定した後、パスワードを設定しない場合、設定した認証モードにかかわらず、認証モードは**none**になります。

3.9 DLDPの表示と維持

すべての view で **display** コマンドを実行でき、user view で **reset** コマンドを実行できます。

操作	コマンド
グローバルとポートのDLDPの設定を表示する	**display dldp** [**interface** *interface-type interface-number*]
ポートを通過したDLDPパケットの統計情報を表示する	**display dldp statistics** [**interface** *interface-type interface-number*]
ポートを通過したDLDPパケットの統計情報をクリアする	**reset dldp statistics** [**interface** *interface-type interface-number*]

3.10 DLDP設定例

3.10.1 片方向リンクの自動シャットダウンの設定例

I. ネットワーク要件

図 3-5に示すように、Device A と Device B が 2 対のファイバで接続されています。

片方向リンクの検出時に障害のあるポートを自動的にシャットダウンし、障害がクリアされた後に自動的にポートをアップするように DLDP を設定します。

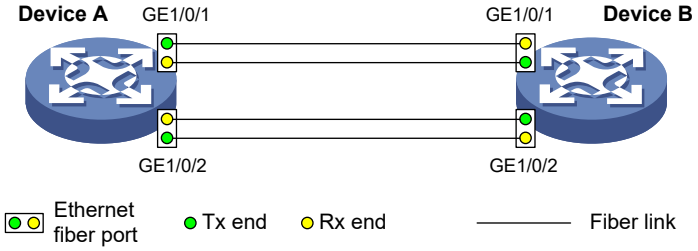


図 3-5 ネットワーク図

II. 設定手順

1)　Device A を設定します。

グローバルに DLDP を有効にします。

```
<DeviceA> system-view
[DeviceA] dldp global enable
```

GigabitEthernet 1/0/1 を全 2 重モード、1000 Mbps に設定し、ポートで DLDP を有効にします。

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] duplex full
[DeviceA-GigabitEthernet1/0/1] speed 1000
[DeviceA-GigabitEthernet1/0/1] dldp enable
[DeviceA-GigabitEthernet1/0/1] quit
```

GigabitEthernet 1/0/2 を全 2 重モード、1000 Mbps に設定し、ポートで DLDP を有効にします。

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] duplex full
[DeviceA-GigabitEthernet1/0/2] speed 1000
[DeviceA-GigabitEthernet1/0/2] dldp enable
[DeviceA-GigabitEthernet1/0/2] quit
```

ポートシャットダウンモードを auto に設定します。

```
[DeviceA] dldp unidirectional-shutdown auto
```

2)　Device B を設定します。

グローバルに DLDP を有効にします。

```
<DeviceB> system-view
[DeviceB] dldp global enable
```

GigabitEthernet 1/0/1 を全 2 重モード、1000 Mbps に設定し、ポートで DLDP を有効にします。

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] duplex full
[DeviceB-GigabitEthernet1/0/1] speed 1000
[DeviceB-GigabitEthernet1/0/1] dldp enable
[DeviceB-GigabitEthernet1/0/1] quit
```

GigabitEthernet 1/0/2 を全 2 重モード、1000 Mbps に設定し、ポートで DLDP を有効にします。

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] duplex full
[DeviceB-GigabitEthernet1/0/2] speed 1000
[DeviceB-GigabitEthernet1/0/2] dldp enable
[DeviceB-GigabitEthernet1/0/2] quit
```

ポートシャットダウンモードを auto に設定します。

```
[DeviceB] dldp unidirectional-shutdown auto
```

III. 設定の確認

設定が完了した後、グローバルとポートで DLDP の設定を表示するため、**display dldp** コマンドを使用します。

Device A のグローバルと DLDP が有効になっているすべてのポートの DLDP の設定を表示します。

```
[DeviceA] display dldp
 DLDP global status: Enabled
 DLDP advertisement interval: 5s
 DLDP authentication-mode: None
 DLDP unidirectional-shutdown mode: Auto
 DLDP delaydown-timer value: 1s
 Number of enabled ports: 2

Interface GigabitEthernet1/0/1
 DLDP port state: Bidirectional
 Number of the port's neighbors: 1
  Neighbor MAC address: 0023-8956-3600
  Neighbor port index: 1
  Neighbor state: Confirmed
  Neighbor aged time: 11s

Interface GigabitEthernet1/0/2
 DLDP port state: Bidirectional
 Number of the port's neighbors: 1
  Neighbor MAC address: 0023-8956-3600
  Neighbor port index: 2
  Neighbor state: Confirmed
  Neighbor aged time: 12s
```

出力は、GigabitEthernet 1/0/1 と GigabitEthernet 1/0/2 の両方が、双方向リンクであることを示す Bidirectional 状態であることを示します。

Device A の現在の端末でログのモニタリングを有効にし、現在の端末に出力するログレベルをもっとも低いレベルの 6 に設定します。

```
[DeviceA] quit
<DeviceA> terminal monitor
<DeviceA> terminal logging level 6
```

以下のログ情報が Device A で表示されます。

```
<DeviceA>%Jul 11 17:40:31:089 2012 DeviceA IFNET/3/PHY_UPDOWN:
GigabitEthernet1/0/1 link status is DOWN.
%Jul 11 17:40:31:091 2012 DeviceA IFNET/5/LINK_UPDOWN: Line protocol on the
interface GigabitEthernet1/0/1 is DOWN.
%Jul 11 17:40:31:677 2012 DeviceA IFNET/3/PHY_UPDOWN: GigabitEthernet1/0/2 link
status is DOWN.
%Jul 11 17:40:31:678 2012 DeviceA IFNET/5/LINK_UPDOWN: Line protocol on the
interface GigabitEthernet1/0/2 is DOWN.
%Jul 11 17:40:38:544 2012 DeviceA IFNET/3/PHY_UPDOWN: GigabitEthernet1/0/1 link
status is UP.
%Jul 11 17:40:38:836 2012 DeviceA IFNET/3/PHY_UPDOWN: GigabitEthernet1/0/2 link
status is UP.
```

出力は、GigabitEthernet 1/0/1 と GigabitEthernet 1/0/2 の両方のポートの状態が、ダウンとなり、その後アップとなりますが、リンク状態がダウンのままとなっていることを示します。

グローバルと DLDP が有効になっているすべてのポートの DLDP の設定を表示します。

```
<DeviceA> display dldp
 DLDP global status: Enabled
 DLDP advertisement interval: 5s
 DLDP authentication-mode: None
 DLDP unidirectional-shutdown mode: Auto
 DLDP delaydown-timer value: 1s
 Number of enabled ports: 2

Interface GigabitEthernet1/0/1
 DLDP port state: Unidirectional
 Number of the port's neighbors: 0 (Maximum number ever detected: 1)

Interface GigabitEthernet1/0/2
 DLDP port state: Unidirectional
 Number of the port's neighbors: 0 (Maximum number ever detected: 1)
```

出力は、GigabitEthernet 1/0/1 と GigabitEthernet 1/0/2 の DLDP ポート状態が Unidirectional 状態であることを示します。それは DLDP が片方向リンクを検出し、2 つのポートを自動的にシャットダウンしたことを示します。

片方向リンクは、クロス接続ファイバによって引き起こされています。ファイバの接続を正しく接続します。その結果、DLDP によってポートのシャットダウンは自動的に回復します。Device A は以下のログ情報を表示します。

```
<DeviceA>%Jul 11 17:42:57:709 2012 DeviceA IFNET/3/PHY_UPDOWN:
GigabitEthernet1/0/1 link status is DOWN.
%Jul 11 17:42:58:603 2012 DeviceA IFNET/3/PHY_UPDOWN: GigabitEthernet1/0/2 link
status is DOWN.
%Jul 11 17:43:02:342 2012 DeviceA IFNET/3/PHY_UPDOWN: GigabitEthernet1/0/1 link
status is UP.
%Jul 11 17:43:02:343 2012 DeviceA DLDP/6/DLDP_NEIGHBOR_CONFIRMED: A neighbor was
confirmed on interface GigabitEthernet1/0/1. The neighbor's system MAC is
0023-8956-3600, and the port index is 1.
%Jul 11 17:43:02:344 2012 DeviceA DLDP/6/DLDP_LINK_BIDIRECTIONAL: DLDP detected
a bidirectional link on interface GigabitEthernet1/0/1.
%Jul 11 17:43:02:353 2012 DeviceA IFNET/5/LINK_UPDOWN: Line protocol on the
interface GigabitEthernet1/0/1 is UP.
```

```
%Jul 11 17:43:02:357 2012 DeviceA IFNET/3/PHY_UPDOWN: GigabitEthernet1/0/2 link
status is UP.
%Jul 11 17:43:02:362 2012 DeviceA DLDP/6/DLDP_NEIGHBOR_CONFIRMED: A neighbor was
confirmed on interface GigabitEthernet1/0/2. The neighbor's system MAC is
0023-8956-3600, and the port index is 2.
%Jul 11 17:43:02:362 2012 DeviceA DLDP/6/DLDP_LINK_BIDIRECTIONAL: DLDP detected
a bidirectional link on interface GigabitEthernet1/0/2.
%Jul 11 17:43:02:368 2012 DeviceA IFNET/5/LINK_UPDOWN: Line protocol on the
interface GigabitEthernet1/0/2 is UP.
```

出力は、GigabitEthernet 1/0/1 と GigabitEthernet 1/0/2 の両方のポート状態とリンク状態がアップになり、DLDP ネイバが確認されたことを示します。

3.10.2 片方向リンクの手動シャットダウンの設定例

I. ネットワーク要件

図 3-6に示すように、Device A と Device B が 2 対のファイバで接続されています。

片方向リンクを検出するように DLDP の設定を行います。片方向リンクの検出時、障害のあるポートを手動でシャットダウンさせるように設定します。

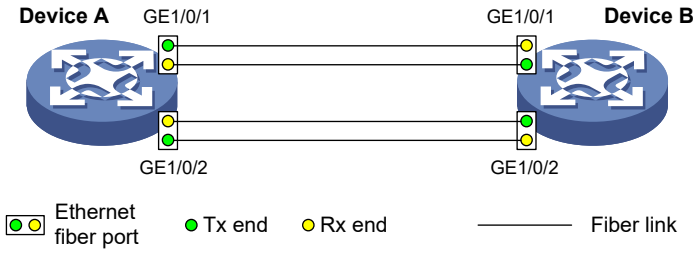


図 3-6 ネットワーク図

II. 設定手順

1)　Device A を設定します。

グローバルに DLDP を有効にします。

```
<DeviceA> system-view
[DeviceA] dldp enable
```

GigabitEthernet 1/0/1 を全 2 重モード、1000 Mbps に設定し、ポートで DLDP を有効にします。

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] duplex full
[DeviceA-GigabitEthernet1/0/1] speed 1000
[DeviceA-GigabitEthernet1/0/1] dldp enable
[DeviceA-GigabitEthernet1/0/1] quit
```

GigabitEthernet 1/0/2 を全 2 重モード、1000 Mbps に設定し、ポートで DLDP を有効にします。

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] duplex full
[DeviceA-GigabitEthernet1/0/2] speed 1000
[DeviceA-GigabitEthernet1/0/2] dldp enable
[DeviceA-GigabitEthernet1/0/2] quit
```

ポートシャットダウンモードを manual に設定します。

```
[DeviceA] dldp unidirectional-shutdown manual
```

2) Device B を設定します。

グローバルに DLDP を有効にします。

```
<DeviceB> system-view
[DeviceB] dldp global enable
```

GigabitEthernet 1/0/1 を全 2 重モード、1000 Mbps に設定し、ポートで DLDP を有効にします。

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] duplex full
[DeviceB-GigabitEthernet1/0/1] speed 1000
[DeviceB-GigabitEthernet1/0/1] dldp enable
[DeviceB-GigabitEthernet1/0/1] quit
```

GigabitEthernet 1/0/2 を全 2 重モード、1000 Mbps に設定し、ポートで DLDP を有効にします。

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] duplex full
[DeviceB-GigabitEthernet1/0/2] speed 1000
[DeviceB-GigabitEthernet1/0/2] dldp enable
[DeviceB-GigabitEthernet1/0/2] quit
```

ポートシャットダウンモードを manual に設定します。

```
[DeviceB] dldp unidirectional-shutdown manual
```

III. 設定の確認

設定が完了した後、グローバルとポートで DLDP の設定を表示するため、**display dldp** コマンドを使用します。

Device A のグローバルと DLDP が有効になっているすべてのポートの DLDP の設定を表示します。

```
[DeviceA] display dldp
 DLDP global status: Enabled
 DLDP advertisement interval: 5s
 DLDP authentication-mode: None
 DLDP unidirectional-shutdown mode: Manual
```

```
 DLDP delaydown-timer value: 1s
 Number of enabled ports: 2

Interface GigabitEthernet1/0/1
 DLDP port state: Bidirectional
 Number of the port's neighbors: 1
  Neighbor MAC address: 0023-8956-3600
  Neighbor port index: 1
  Neighbor state: Confirmed
  Neighbor aged time: 11s

Interface GigabitEthernet1/0/2
 DLDP port state: Bidirectional
 Number of the port's neighbors: 1
  Neighbor MAC address: 0023-8956-3600
  Neighbor port index: 2
  Neighbor state: Confirmed
  Neighbor aged time: 12s
```

出力は、GigabitEthernet 1/0/1 と GigabitEthernet 1/0/2 の両方が、双方向リンクであることを示す Bidirectional 状態であることを示します。

Device A の現在の端末でログのモニタリングを有効にし、現在の端末に出力するログレベルをもっとも低いレベルの 6 に設定します。

```
[DeviceA] quit
<DeviceA> terminal monitor
<DeviceA> terminal logging level 6
```

以下のログ情報が Device A で表示されます。

```
<DeviceA>%Jul 12 08:29:17:786 2012 DeviceA IFNET/3/PHY_UPDOWN:
GigabitEthernet1/0/1 link status is DOWN.
%Jul 12 08:29:17:787 2012 DeviceA IFNET/5/LINK_UPDOWN: Line protocol on the
interface GigabitEthernet1/0/1 is DOWN.
%Jul 12 08:29:17:800 2012 DeviceA IFNET/3/PHY_UPDOWN: GigabitEthernet1/0/2 link
status is DOWN.
%Jul 12 08:29:17:800 2012 DeviceA IFNET/5/LINK_UPDOWN: Line protocol on the
interface GigabitEthernet1/0/2 is DOWN.
%Jul 12 08:29:25:004 2012 DeviceA IFNET/3/PHY_UPDOWN: GigabitEthernet1/0/1 link
status is UP.
%Jul 12 08:29:25:005 2012 DeviceA IFNET/5/LINK_UPDOWN: Line protocol on the
interface GigabitEthernet1/0/1 is UP.
%Jul 12 08:29:25:893 2012 DeviceA IFNET/3/PHY_UPDOWN: GigabitEthernet1/0/2 link
status is UP.
%Jul 12 08:29:25:894 2012 DeviceA IFNET/5/LINK_UPDOWN: Line protocol on the
interface GigabitEthernet1/0/2 is UP.
```

出力は、GigabitEthernet 1/0/1 と GigabitEthernet 1/0/2 の両方のポートの状態とリンクの状態がダウンとなり、その後アップとなります。

グローバルと DLDP が有効になっているすべてのポートの DLDP の設定を表示します。

```
<DeviceA> display dldp
 DLDP global status: Enabled
 DLDP advertisement interval: 5s
 DLDP authentication-mode: None
 DLDP unidirectional-shutdown mode: Manual
 DLDP delaydown-timer value: 1s
 Number of enabled ports: 2

Interface GigabitEthernet1/0/1
 DLDP port state: Unidirectional
 Number of the port's neighbors: 0 (Maximum number ever detected: 1)

Interface GigabitEthernet1/0/2
```

```
 DLDP port state: Unidirectional
 Number of the port's neighbors: 0 (Maximum number ever detected: 1)
```

出力は、GigabitEthernet 1/0/1 と GigabitEthernet 1/0/2 の DLDP ポート状態が unidirectional 状態であることを示します。それは DLDP が片方向リンクを検出しますが、2 つのポートをシャットダウンしていないことを示します。

片方向リンクは、クロス接続ファイバによって引き起こされています。2 つのポートを手動でシャットダウンします。

GigabitEthernet 1/0/1 をシャットダウンします。

```
<DeviceA> system-view
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] shutdown
```

以下のログ情報が Device A で表示されます。

```
[DeviceA-GigabitEthernet1/0/1]%Jul 12 08:34:23:717 2012 DeviceA
IFNET/3/PHY_UPDOWN: GigabitEthernet1/0/1 link status is DOWN.
%Jul 12 08:34:23:718 2012 DeviceA IFNET/5/LINK_UPDOWN: Line protocol on the
interface GigabitEthernet1/0/1 is DOWN.
%Jul 12 08:34:23:778 2012 DeviceA IFNET/3/PHY_UPDOWN: GigabitEthernet1/0/2 link
status is DOWN.
%Jul 12 08:34:23:779 2012 DeviceA IFNET/5/LINK_UPDOWN: Line protocol on the
interface GigabitEthernet1/0/2 is DOWN.
```

出力は、GigabitEthernet 1/0/1 と GigabitEthernet 1/0/2 の両方のポートの状態とリンクの状態が、ダウンとなります。

GigabitEthernet 1/0/2 をシャットダウンします。

```
[DeviceA-GigabitEthernet1/0/1] quit
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] shutdown
```

ファイバの接続を正しく接続し、2 つのポートをアップにします。

GigabitEthernet 1/0/2 をアップにします。

```
[DeviceA-GigabitEthernet1/0/2] undo shutdown
```

以下のログ情報が Device A で表示されます。

```
[DeviceA-GigabitEthernet1/0/2]%Jul 12 08:46:17:677 2012 DeviceA
IFNET/3/PHY_UPDOWN: GigabitEthernet1/0/2 link status is UP.
%Jul 12 08:46:17:678 2012 DeviceA IFNET/5/LINK_UPDOWN: Line protocol on the
interface GigabitEthernet1/0/2 is UP.
%Jul 12 08:46:17:959 2012 DeviceA DLDP/6/DLDP_NEIGHBOR_CONFIRMED: A neighbor was
confirmed on interface GigabitEthernet1/0/2. The neighbor's system MAC is
0023-8956-3600, and the port index is 2.
%Jul 12 08:46:17:959 2012 DeviceA DLDP/6/DLDP_LINK_BIDIRECTIONAL: DLDP detected
a bidirectional link on interface GigabitEthernet1/0/2.
```

出力は、GigabitEthernet 1/0/2 のポートの状態とリンクの状態がアップとなり、DLDP ネイバが確認されたことを示します。

GigabitEthernet 1/0/1 をアップにします。

```
[DeviceA-GigabitEthernet1/0/2] quit
[DeviceA] interface gigabitethernet 1/0/1
```

```
[DeviceA-GigabitEthernet1/0/1] undo shutdown
```

以下のログ情報が Device A で表示されます。

```
[DeviceA-GigabitEthernet1/0/1]%Jul 12 08:48:25:952 2012 DeviceA
IFNET/3/PHY_UPDOWN: GigabitEthernet1/0/1 link status is UP.
%Jul 12 08:48:25:952 2012 DeviceA DLDP/6/DLDP_NEIGHBOR_CONFIRMED: A neighbor was
confirmed on interface GigabitEthernet1/0/1. The neighbor's system MAC is
0023-8956-3600, and the port index is 1.
%Jul 12 08:48:25:953 2012 DeviceA IFNET/5/LINK_UPDOWN: Line protocol on the
interface GigabitEthernet1/0/1 is UP.
%Jul 12 08:48:25:953 2012 DeviceA DLDP/6/DLDP_LINK_BIDIRECTIONAL: DLDP detected
a bidirectional link on interface GigabitEthernet1/0/1.
```

出力は、GigabitEthernet 1/0/1 のポートの状態とリンクの状態がアップとなり、DLDP ネイバが確認されたことを示します。

3.10.3 片方向リンクのハイブリッドシャットダウンの設定例

I. ネットワーク要件

図 3-7に示すように、Device A と Device B が 2 対のファイバで接続されています。

単方向リンクを検出すると障害のあるポートを自動的にシャットダウンし、障害をクリアした後にポートを自動的に立ち上げるように DLDP を設定します。

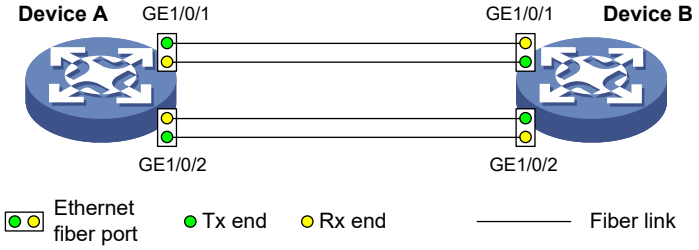


図 3-7 ネットワーク図

II. 設定手順

1)　Device A を設定します。

DLDP をグローバルに有効にします。

```
<DeviceA> system-view
[DeviceA] dldp enable
```

GigabitEthernet1 / 0/1 を全 2 重モード、1000 Mbps に設定し、ポートで DLDP を有効にします。

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] duplex full
[DeviceA-GigabitEthernet1/0/1] speed 1000
[DeviceA-GigabitEthernet1/0/1] dldp enable
```

```
[DeviceA-GigabitEthernet1/0/1] quit
```

GigabitEthernet1 / 0/2 を全 2 重モード、1000 Mbps に設定し、ポートで DLDP を有効にします。

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] duplex full
[DeviceA-GigabitEthernet1/0/2] speed 1000
[DeviceA-GigabitEthernet1/0/2] dldp enable
[DeviceA-GigabitEthernet1/0/2] quit
```

グローバルポートシャットダウンモードを hybrid に設定します。

```
[DeviceA] dldp unidirectional-shutdown hybrid
```

2) Device B を設定します。

DLDP をグローバルに有効にします。

```
<DeviceB> system-view
[DeviceB] dldp global enable
```

GigabitEthernet1 / 0/1 を全 2 重モード、1000 Mbps に設定し、ポートで DLDP を有効にします。

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] duplex full
[DeviceB-GigabitEthernet1/0/1] speed 1000
[DeviceB-GigabitEthernet1/0/1] dldp enable
[DeviceB-GigabitEthernet1/0/1] quit
```

GigabitEthernet1 / 0/2 を全 2 重モード、1000 Mbps に設定し、ポートで DLDP を有効にします。

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] duplex full
[DeviceB-GigabitEthernet1/0/2] speed 1000
[DeviceB-GigabitEthernet1/0/2] dldp enable
[DeviceB-GigabitEthernet1/0/2] quit
```

グローバルポートシャットダウンモードを hybrid に設定します。

```
[DeviceB] dldp unidirectional-shutdown hybrid
```

III. 設定の確認

グローバルおよび Device A のすべての DLDP 対応ポートで DLDP 設定を表示します。

```
[DeviceA] display dldp
 DLDP global status: Enabled
 DLDP advertisement interval: 5s
 DLDP authentication-mode: None
```

```
 DLDP unidirectional-shutdown mode: Hybrid
 DLDP delaydown-timer value: 1s
 Number of enabled ports: 2

Interface GigabitEthernet1/0/1
 DLDP port state: Bidirectional
 DLDP port unidirectional-shutdown mode: None
 Number of the port's neighbors: 1
  Neighbor MAC address: 0023-8956-3600
  Neighbor port index: 1
  Neighbor state: Confirmed
  Neighbor aged time: 11s

Interface GigabitEthernet1/0/2
 DLDP port state: Bidirectional
 DLDP port unidirectional-shutdown mode: None
 Number of the port's neighbors: 1
  Neighbor MAC address: 0023-8956-3600
  Neighbor port index: 2
  Neighbor state: Confirmed
  Neighbor aged time: 12s
```

出力は、GigabitEthernet 1/0/1 と GigabitEthernet 1/0/2 の両方が、双方向リンクであることを示す Bidirectional 状態であることを示します。

Device A の現在の端末でログのモニタリングを有効にし、現在の端末に出力するログレベルをもっとも低いレベルの 6 に設定します。

```
[DeviceA] quit

<DeviceA> terminal monitor

<DeviceA> terminal logging level 6
```

以下のログ情報が Device A で表示されます。

```
<DeviceA>%Jan  4 07:16:06:556 2011 DeviceA DLDP/5/DLDP_NEIGHBOR_AGED: A neighbor
on interface
GigabitEthernet1/0/1 was deleted because the neighbor was aged. The neighbor's
system MAC is 0023-8956-3600, and the port index is 162.
%Jan   4  07:16:06:560  2011  DeviceA  DLDP/5/DLDP_NEIGHBOR_AGED:  A  neighbor  on
interface
GigabitEthernet1/0/2 was deleted because the neighbor was aged. The neighbor's
system MAC is 0023-8956-3600, and the port index is 165.
%Jan   4  07:16:06:724  2011  DeviceA  IFNET/3/PHY_UPDOWN:  Physical  state  on  the
interface GigabitEthernet1/0/1 changed to down.
%Jan   4  07:16:06:730  2011  DeviceA  IFNET/3/PHY_UPDOWN:  Physical  state  on  the
interface GigabitEthernet1/0/2 changed to down.
%Jan  4 07:16:06:736 2011 DeviceA IFNET/5/LINK_UPDOWN: Line protocol state on the
interface GigabitEthernet1/0/1 changed to down.
%Jan  4 07:16:06:738 2011 DeviceA IFNET/5/LINK_UPDOWN: Line protocol state on the
interface GigabitEthernet1/0/2 changed to down.
%Jan  4 07:16:07:152 2011 DeviceA DLDP/3/DLDP_LINK_UNIDIRECTIONAL: DLDP detected
a unidirectional link on interface GigabitEthernet1/0/1. DLDP automatically shut
down the interface. Please manually bring up the interface.
%Jan  4 07:16:07:156 2011 DeviceA DLDP/3/DLDP_LINK_UNIDIRECTIONAL: DLDP detected
a unidirectional link on interface GigabitEthernet1/0/2. DLDP automatically shut
down the interface. Please manually bring up the interface.
```

出力は、GigabitEthernet1 / 0/1 と GigabitEthernet1 / 0/2 の両方のポートの状態とリンクの状態がダウンしていることを示しています。

グローバルと DLDP が有効になっているすべてのポートの DLDP の設定を表示します。

```
<DeviceA> display dldp
 DLDP global status: Enabled
 DLDP advertisement interval: 5s
 DLDP authentication-mode: None
 DLDP unidirectional-shutdown mode: Hybrid
```

```
 DLDP delaydown-timer value: 1s
 Number of enabled ports: 2

Interface GigabitEthernet1/0/1
 DLDP port state: Inactive
 DLDP port unidirectional-shutdown mode: None
 Number of the port's neighbors: 0 (Maximum number ever detected: 1)
Interface GigabitEthernet1/0/2
 DLDP port state: Inactive
 DLDP port unidirectional-shutdown mode: None
 Number of the port's neighbors: 0 (Maximum number ever detected: 1)
```

出力には DLDP が片方向リンクを検出し、GigabitEthernet 1/0/1 と GigabitEthernet 1/0/2 をシャットダウンすることが示されています。

片方向リンクは、クロス接続されたファイバによって発生します。ファイバ接続を修正した後、2 つのポートを起動します。

GigabitEthernet 1/0/1 を起動します。

```
<DeviceA> system-view

[DeviceA] interface gigabitethernet 1/0/1

[DeviceA-GigabitEthernet1/0/1] undo shutdown
```

以下のログ情報が Device A で表示されます。

```
[DeviceA-GigabitEthernet1/0/1]%Jan 4 07:33:26:574 2011 DeviceA
IFNET/3/PHY_UPDOWN: Physical state on the interface GigabitEthernet1/0/1 changed
to up.
%Jan 4 07:33:57:562 2011 DeviceA DLDP/6/DLDP_NEIGHBOR_CONFIRMED: A neighbor was
confirmed on interface GigabitEthernet1/0/1. The neighbor's system MAC is
0023-8956-3600, and the port index is 162.
%Jan 4 07:33:57:563 2011 DeviceA DLDP/6/DLDP_LINK_BIDIRECTIONAL: DLDP detected
a bidirectional link on interface GigabitEthernet1/0/1.
%Jan 4 07:33:57:590 2011 DeviceA IFNET/5/LINK_UPDOWN: Line protocol state on the
interface GigabitEthernet1/0/1 changed to up.
%Jan 4 07:33:57:609 2011 DeviceA STP/6/STP_DETECTED_TC: Instance 0's port
GigabitEthernet1/0/1 detected a topology change.
```

出力には、GigabitEthernet 1/0/1 のポートの状態とリンクの状態がアップになり、DLDP ネイバが決定されたことが示されています。

GigabitEthernet 1/0/2 を起動します。

```
[DeviceA-GigabitEthernet1/0/1] quit

[DeviceA] interface gigabitethernet 1/0/2

[DeviceA-GigabitEthernet1/0/2] undo shutdown
```

以下のログ情報が Device A で表示されます。

```
[DeviceA-GigabitEthernet1/0/2]%Jan 4 07:35:26:574 2011 DeviceA
IFNET/3/PHY_UPDOWN: Physical state on the interface GigabitEthernet1/0/2 changed
to up.
%Jan 4 07:35:57:562 2011 DeviceA DLDP/6/DLDP_NEIGHBOR_CONFIRMED: A neighbor was
confirmed on interface GigabitEthernet1/0/2. The neighbor's system MAC is
0023-8956-3600, and the port index is 162.
%Jan 4 07:35:57:563 2011 DeviceA DLDP/6/DLDP_LINK_BIDIRECTIONAL: DLDP detected
a bidirectional link on interface GigabitEthernet1/0/2.
%Jan 4 07:35:57:590 2011 DeviceA IFNET/5/LINK_UPDOWN: Line protocol state on the
interface GigabitEthernet1/0/2 changed to up.
%Jan 4 07:35:57:609 2011 DeviceA STP/6/STP_DETECTED_TC: Instance 0's port
GigabitEthernet1/0/2 detected a topology change.
```

出力には、GigabitEthernet 1/0/2 のポートの状態とリンクの状態がアップになり、DLDP ネイバが決定されたことが示されています。

目次

このセクションのページは **10-x-x** です。

4章 RRPP 4-1
4.1 概要 4-1
4.1.1 RRPPの基本コンセプト 4-1
4.1.2 RRPPDU 4-4
4.1.3 RRPPタイマ 4-5
4.1.4 RRPPの動作 4-5
4.1.5 RRPPの典型的なネットワーク 4-7
4.2 RRPPの設定作業リスト 4-11
4.3 RRPPドメインの作成 4-12
4.4 コントロールVLANの設定 4-12
4.5 プロテクトVLANの設定 4-13
4.6 RRPPリングの設定 4-14
4.6.1 RRPPポートの設定 4-14
4.6.2 RRPPノードの設定 4-15
4.7 RRPPドメインの有効化 4-17
4.8 RRPPタイマの設定 4-17
4.9 RRPPリンググループの設定 4-18
4.10 RRPPに関するSNMP notificationの有効化 4-19
4.11 RRPPの表示と維持 4-19
4.12 RRPPの設定例 4-19
4.12.1 シングルリング設定例 4-19
4.12.2 交差リング（Intersectingリング、マルチリング）の設定例 4-23
4.12.3 デュアルホームリングの設定例 4-31
4.12.4 交差リング（Intersectingリング、マルチリング）ロードバランシングの設定例 4-45
4.13 RRPPのトラブルシューティング 4-59

4章 RRPP

4.1 概要

RRPP（Rapid Ring Protection Protocol）はイーサネットリング専用のリンクレイヤプロトコルです。RRPP は、イーサネットリングを構成したときのデータループによるブロードキャストストームの発生を効果的に防止することができます。そして、リング上のノード間のリンクが切断されたとき、ノード間の通信パスをすばやく復旧させることができます。RRPP の収束時間はイーサネットリング上のノード数に影響されません。RRPP は大規模ネットワークに適用することができます。

4.1.1 RRPP の基本コンセプト

図 4-1に 2 つのイーサネットリングと複数ノードを持つ一般的な RRPP ネットワークを示します。RRPP はノード間で RRPPDU（Rapid Ring Protection Protocol Data Units）を交換することで、リングの状態を検出し、トポロジの変更情報を送信します。

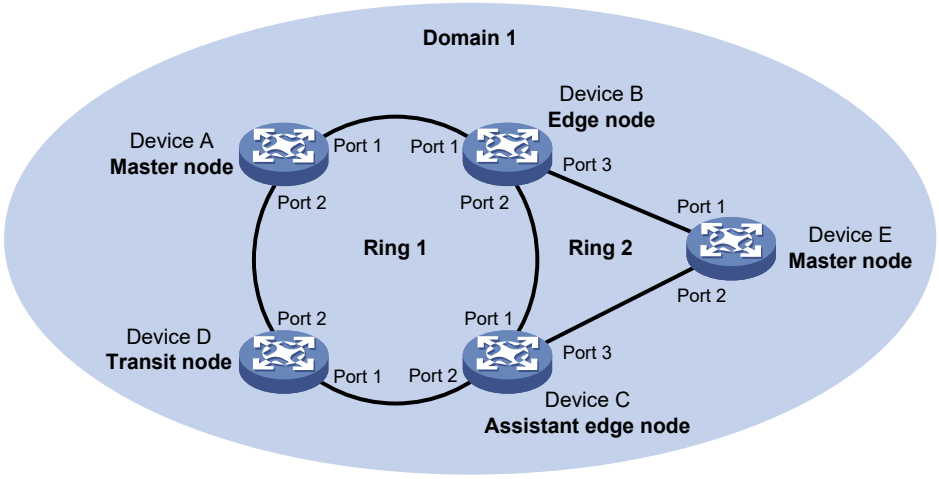


図 4-1 RRPP のネットワーク図

I. RRPP ドメイン

RRPP ドメインは、ドメイン ID によって一意に識別されます。同じドメイン ID を持った相互接続された装置とコントロール VLAN は RRPP ドメインを構成します。RRPP ドメインは以下の要素で構成されます。

- プライマリリングとサブリング
- コントロール VLAN
- マスタノード、トランジットノード、アシスタントエッジノード
- プライマリポート、セカンダリポート、共通ポート、エッジノード

図 4-1に示すように、ドメイン 1 は Ring 1、Ring 2 の RRPP リングから構成される RRPP ドメインです。2 つのリング上のすべてのノードは RRPP ドメインに所属しています。

II. RRPP リング

リング型のイーサネットトポロジを RRPP リングと呼びます。RRPP リングにはプライマリリングとサブリングが含まれます。リングレベルを指定することにより、リングをプライマリリングもしくはサブリングのどちらかに設定することができます。レベル 0 がプライマリリング、レベル 1 がサブリングです。複数の RRPP リングにより構成された RRPP ドメインは、1 つのプライマリリングとそれ以外のサブリングにより構成されます。

リングは以下のどちらかの状態になります。

- **Health 状態**－イーサネットリング上のすべての物理リンクが接続されています。
- **Disconnect 状態**－イーサネットリング上のいくつかの物理リンクが接続されていません。

図 4-1において、Domain1 は 2 つの RRPP リング（Ring 1 と Ring 2）を含みます。Ring 1 のレベルは 0 に設定され、Ring 2 のレベルは 1 に設定されています。Ring 1 はプライマリリングで、Ring 2 はサブリングとなります。

III. コントロール VLAN とプロテクト VLAN

1)　コントロール VLAN

RRPP ドメインにおいて、コントロール VLAN は RRPPDU（Rapid Ring Protection Protocol Data Units）を転送するための専用の VLAN です。装置で RRPP リングにアクセスしているポートはリングのコントロール VLAN に所属します。そのポートのみがコントロール VLAN に加わることができます。

RRPP ドメインは以下のコントロール VLAN が設定されます。

- プライマリコントロール VLAN です。これはプライマリリングのためのプライマリコントロール VLAN です。
- セカンダリコントロール VLAN です。これはサブリングのためのセカンダリコントロール VLAN です。

プライマリコントロール VLAN として VLAN を指定した後、システムは自動的にセカンダリコントロール VLAN を設定します。VLAN ID はプライマリコントロール VLAN の VLAN-ID に 1 を追加したものとなります。同一の RRPP ドメイン上のすべてのサブリングは同じセカンダリコントロール VLAN を共有します。コントロール VLAN インタフェースで IP アドレスの設定は行うことができません。

2)　プロテクト VLAN

プロテクト VLAN はデータパケットを転送するための VLAN です。RRPP ポートと非 RRPP ポートはプロテクト VLAN に割り当てることができます。

IV. ノード

RRPP リング上の各装置はノードと呼ばれます。ノードの役割を設定することができます。RRPP は以下のノードがあります。

- **マスタノード**－各リングには必ずマスタノードが 1 つあります。マスタノードはポーリングメカニズムを初期化し、トポロジが変更された後の動作を決定します。
- **トランジットノード**－プライマリリングで、マスタノードを除くすべてのノードをトランジットノードとなります。サブリングで、マスタノードを除くすべてのノードと、プライマリリングとサブリングが交差するノードはトランジットノードとなります。トランジットノードは、直接接続された RRPP リングの状態をモニタし、リンク状態の変更がある場合、変更をマスタノードに通知します。リンク状態の変更にもとづいて、マスタノードは実行される動作を決定します。
- **エッジノード**－プライマリリングとサブリングの両方に同時に所属する特別なノードです。エッジノードは、プライマリリングではマスタノードあるいはトランジットノードとして動作し、サブリングではエッジノードとなります。
- **アシスタントエッジノード**－プライマリリングとサブリングの両方に同時に所属する特別なノードです。エッジノードは、プライマリリングではマスタノードあるいはトランジットノードとして動作し、サブリングではエッジノードとなります。アシスタントエッジノードは、プライマリリングの正常性を検出しループガードを行うため、エッジノードと連携します。

図 4-1に示すように、Ring 1 はプライマリリング、Ring 2 はサブリングです。Device A は Ring 1 のマスタノード、Device B、Device C、Device D は Ring 1 のトランジットノードです。Device E は Ring 2 のマスタノード、Device B は Ring 2 のエッジノード、Device C は Ring 2 のアシスタントエッジノードです。

V. ポート

1)　プライマリポートとセカンダリポート

マスタノードあるいはトランジットノードはそれぞれ RRPP リングに接続する 2 つのポートを持ちます。1 つはプライマリポート、もう 1 つはセカンダリポートとして動作します。ポートの役割はユーザが設定できます。

マスタノードにおいて、プライマリポートとセカンダリポートの動作の違いを以下に示します。

- プライマリポートは Hello パケットを送信し、セカンダリポートは Hello パケットを受信します。
- RRPP リングが正常（Health 状態）である場合、マスタノードのセカンダリポートは論理的にプロテクト VLAN のパケットをブロックし、コントロール VLAN のパケットのみ通過を許可します。
- RRPP リングに障害（Disconnect 状態）が発生した場合、マスタノードのセカンダリポートはプロテクト VLAN のパケットの受信を許可し、そのパケットを転送します。

トランジットノードのプライマリポートとセカンダリポートに動作の違いはありません。両方とも RRPP リング上でリングプロトコルパケットとデータパケットを転送するように設計されています。

図 4-1に示すように、Device A は Ring 1 のマスタノードです。Port 1 と Port 2 はそれぞれ Ring 1 のマスタノードのプライマリポートとセカンダリポートです。Device B と Device C と Device D は Ring 1 のトランジットノードです。これらの Port 1 と Port 2 はそれぞれ Ring 1 上でプライマリポートとセカンダリポートです。

2)　共有ポートとエッジポート

共有ポートは、エッジノードとアシスタントエッジノードからプライマリリングに接続されているポートを示します。エッジポートはエッジノードとアシスタントエッジノードからサブリングにのみ接続されているポートです。

図 4-1に示すように、Device B と Device C は Ring 1 と Ring 2 上にあります。Device B の Port 1 と Port 2、Device C の Port 1 と Port 2 はプライマリリングに接続されているので、これらのポートは共有ポートとなります。Device B の Port 3 と Device C の Port 3 はサブリングにのみ接続されているので、これらのポートはエッジポートとなります。

VI. RRPP リンググループ

Edge-Hello パケットのトラフィックを減らすため、エッジノードまたはアシスタントエッジノード上でサブリングのグループを設定することができます。これらのサブリングのエッジノードとして装置を設定し、サブリングのアシスタントエッジノードとして別の装置を設定する必要があります。また同じサブリングパケットを主要なリング（SRPT）にトンネルするため、エッジノードのサブリングとアシスタントエッジノードを接続する必要があります。これらのサブリングのエッジノードの Edge-Hello パケットは、同じリンクを通ってアシスタントエッジノードへ転送されます。

エッジノードで設定された RRPP リンググループはエッジノード RRPP リンググループです。アシスタントエッジノードで設定された RRPP リンググループはアシスタントエッジノード RRPP リンググループです。エッジノード RRPP リンググループの中の 1 つのサブリングのみが、Edge-Hello パケットを送信することができます。

4.1.2 RRPPDU

サブリングの RRPPDU はプライマリリングのデータパケットとして転送され、プライマリリングの RRPPDU のみがプライマリリング内に転送することができます。

表 4-1 RRPPDU タイプと機能

タイプ	説明
Hello	マスタノードはHelloパケット（Healthパケットして知られます）を送信し、ネットワークのリングが正常であるかを確認します。
Link-Down	リンクに障害が発生した場合、トランジットノード、エッジノード、アシスタントエッジノードのポートはLink-Downパケットを送信し、リングが解除されたことをマスタノードに通知します。
Common-Flush-FDB	RRPPリングがDisconnect状態になった場合、マスタノードはCommon-Flush-FDBパケットをトランジットノードに対して送信し、MACアドレスエントリとARPエントリを更新するように通知します。(FDBはForwarding Databaseを示します)
Complete-Flush-FDB	RRPPリングがHealth状態になった場合、マスタノードはComplete-Flush-FDBパケットを以下のために送信します。 • トランジットノードに対して送信し、MACアドレスエントリとARPエントリを更新します。 • ポートのブロックを一時的に解除します。
Edge-Hello	エッジノードはEdge-Helloパケットを送信し、エッジノードとアシスタントエッジノード間のSRPTを確認します。

タイプ	説明
Major-Fault	エッジノードとアシスタントエッジノード間のSRPTが切断された場合、アシスタントエッジノードはMajor-Faultパケットを送信し、障害をエッジノードに通知します。

4.1.3 RRPP タイマ

RRPP はリングの状態を決定するとき、以下のタイマを使用します。

- **Hello タイマ**－マスタノードのプライマリポートから送信する Hello パケットの送信間隔です。
- **Fail タイマ**－セカンダリポートがマスタノードからの Hello パケットを受信する最大遅延時間（タイムアウト時間）です。もし Fail タイマが終了する前に、セカンダリポートがローカルのマスタノードによって送信された Hello パケットを受信した場合、リングは Health 状態となります。受信しない場合、リングは Disconnect 状態となります。

4.1.4 RRPP の動作

I. ポーリングメカニズム

ポーリングメカニズムはリングネットワークの Health 状態を確認するために、RRPP のマスタノードによって使用されます。

マスタノードはプライマリポートから Hello パケットを定期的に送信します。Hello パケットはリング上の各トランジットノードを順番に通過します。

- リングが正常な場合、マスタノードのセカンダリポートは Fail タイマの期限が切れる前に Hello パケットを受信し、マスタノードはセカンダリポートをブロック状態に維持します。
- リングが切断されている場合、マスタノードのセカンダリポートは Fail タイマの期限が切れる前に Hello パケットを受信することができません。これにより、マスタノードはセカンダリポートがプロテクト VLAN をブロックするのを解除して、Common-Flush-FDB を送信してすべてのトランジットノードに MAC アドレスエントリと ARP エントリの更新を通知します。

II. ロードバランシング

リングネットワークにおいて、複数の VLAN からのトラフィックは同時に転送される可能性があります。RRPP は異なるパスに沿って異なる VLAN からトラフィックを転送することでロードバランシング（負荷分散）を行うことができます。

リングネットワークの複数の RRPP ドメインを設定することができます。各 RRPP ドメインは指定した VLAN（プロテクト VLAN）からトラフィックを転送します。異なる VLAN からのトラフィックは、負荷分散用のリングネットワークの異なるトポロジにしたがって転送されます。

図 4-6に示すように、Ring 1 はプロテクト VLAN として設定された Domain 1、Domain 2 のプライマリリングです。Device A は Domain 1 の Ring 1 のマスタノードです。Device B は Domain 2 の Ring 1 のマスタノードです。この設定を行うことによって、異なる VLAN からのトラフィックがシングルリングネットワーク上でロードバランシングの異なるリンクに転送することができます。

III. LinkDown アラームメカニズム

RRPP において、トランジットノード、エッジノード、アシスタントエッジノードは RRPP ドメインに属するいずれかのポートがダウンしたことを検出すると、すぐにマスタノードへ Link-Down パケットを送信します。Link-Down パケットを受信すると、マスタノードは以下のアクションを行います。

- セカンダリポートのプロテクト VLAN のブロック状態を解除します。
- Common-Flush-FDB パケットを送信し、すべてのトランジットノード、エッジノード、アシスタントエッジノードに MAC アドレスエントリと ARP エントリを更新するように通知します。

各ノードがエントリを更新した後、トラフィックは通常のリンクに転送されます。

IV. リングの復旧

RRPP ドメインのトランジットノード、エッジノード、アシスタントエッジノードに所属するポートが再度アップするとき、リングは復旧します。しかしマスタノードは一定時間後にリングの復旧を認識する可能性があります。この間、プロテクト VLAN で一時的にループが発生することがあります。この結果、ブロードキャストストームが発生します。

一時的なループを防ぐために、マスタノード以外のノードはリングに接続するポートが再度アップしたことを検出するとすぐにそのポートをブロックします。コントロール VLAN のパケットの通過のみ許可します。ノードがポートでループが発生しないことを確認したときのみ、ブロック状態のポートのブロックが解除されます。

V. SRPT 障害時のマルチホームサブリングのブロードキャストストーム抑制メカニズム

図 4-5に示すように、Ring 1 はプライマリリング、Ring 2 と Ring 3 はサブリングです。エッジノードとアシスタントエッジノード間の 2 つのリンク（SRPT）がダウンした場合、Ring 2 と Ring 3 のマスタノードはそれぞれセカンダリポートのブロック状態を解除します。そしてこれにより Device B と Device C と Device E と Device F の間でループが作られます。この結果、ブロードキャストストームが発生します。

この場合、ループの発生を防ぐためにエッジノードはエッジポートを一時的にブロック状態にします。エッジノードがエッジポートでループが発生しないことを確認したときのみ、ブロック状態のエッジポートのブロックが解除されます。

VI. RRPP リンググループ

エッジノード RRPP リンググループでは、最小のドメイン ID とリング ID を持つアクティブなサブリングのみが Edge-Hello パケットを送信することができます。アシスタントエッジノード RRPP リンググループでは、Edge-Hello パケットを受信したいずれかのアクティブなサブリングがそのパケットを他のアクティブなサブリングに転送します。エッジノード RRPP リンググループとアシスタントエッジノード RRPP リンググループが設定されるとき、以下の理由により CPU の負荷が軽減します。

- エッジノードの 1 つのサブリングのみが Edge-Hello パケットを送信します。
- アシスタントエッジノードの 1 つのサブリングのみが Edge-Hello パケットを受信します。

図 4-5に示すように、Device B は Ring 2 と Ring 3 のエッジノードです。Device C は Ring 2 と Ring 3 のアシスタントエッジノードです。Device B と Device C は Edge-Hello パケットを頻繁に送信または受信します。より多くのサブリングが設定されたり、より多くのドメインによるロードバランシングが行われたりする場合、Device B と Device C は多くの Edge-Hello パケットを送信または受信することになります。

Edge-Hello パケットのトラフィックを削減するため、以下のことを行います。

- エッジノードの Device B 上で Ring 2 と Ring 3 を RRPP リンググループに割り当てます。
- アシスタントエッジノードの Device C 上で Ring 2 と Ring 3 を RRPP リンググループに割り当てます。

すべてのリングがアクティブな場合、Device B の Ring 2 のみが Edge-Hello パケットを送信します。

4.1.5 RRPP の典型的なネットワーク

🕮 **メモ：**

障害時のすばやい通信復旧を実現するために、リング内は RRPP を設定した装置のみで構成することを推奨します。

I. シングルリング

図 4-2にシングルリングのネットワークトポロジを示します。RRPP ドメインのみ定義することができます。

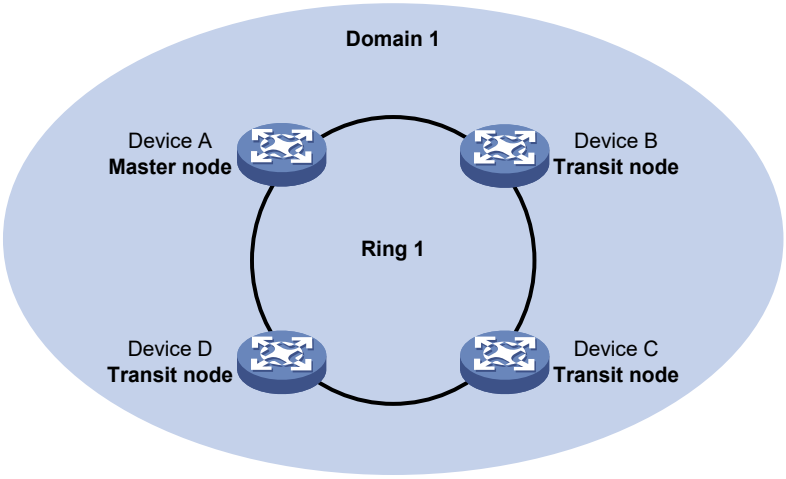


図 4-2 シングルリングのネットワークトポロジ

II. タンジェントリング（接面リング、トランジットリング）

図 4-3にタンジェントリングのネットワークトポロジを示します。2 つ以上のリングが存在します。リング間に 1 つの共通ノードがあります。各リングに RRPP ドメインを定義する必要があります。

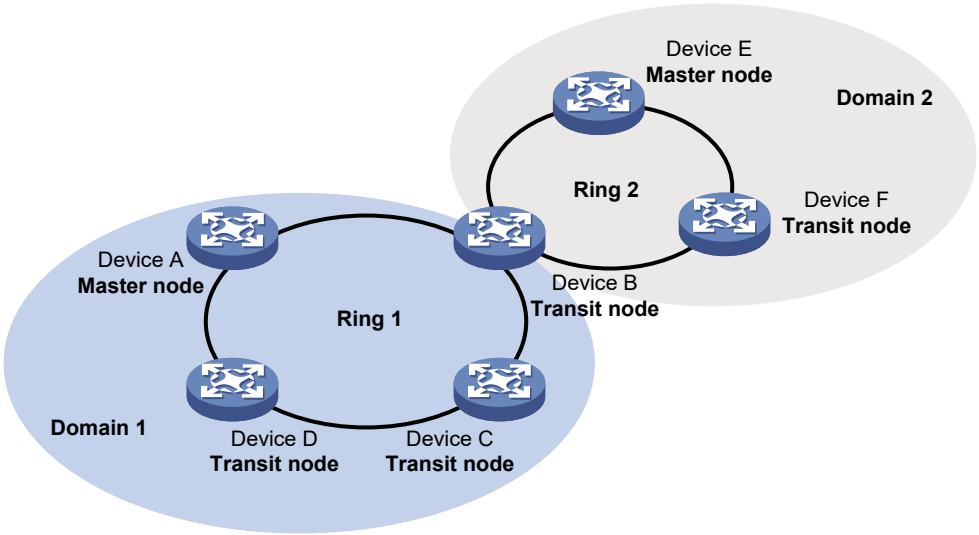


図 4-3 タンジェントリングのネットワークトポロジ

III. 交差リング（Intersecting リング、マルチリング）

図 4-4に交差リングのネットワークトポロジを示します。2 つ以上のリングが存在します。リング間に 2 つの共通ノードがあります。各リングに RRPP ドメインを定義し、1 つのプライマリリング、それ以外のサブリングを設定する必要があります。

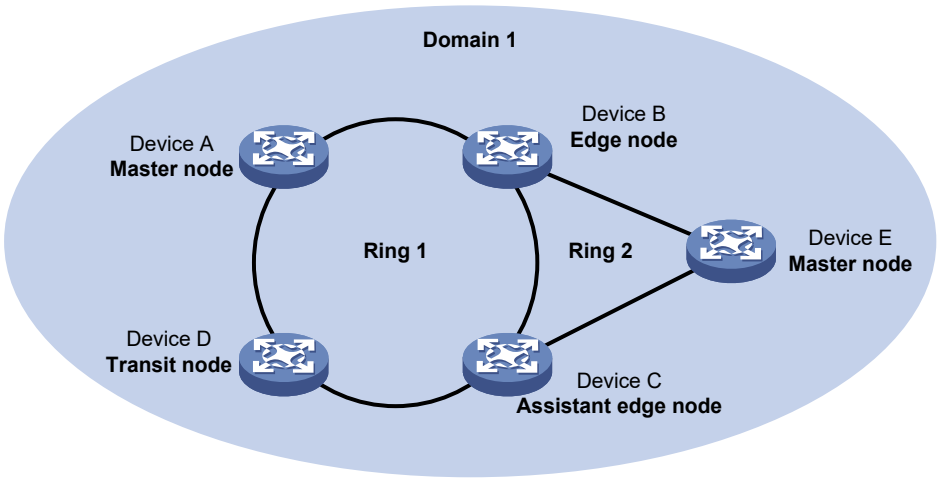


図 4-4 交差リングのネットワークトポロジ

IV. デュアルホームリング

図 4-5にデュアルホームリングのネットワークトポロジを示します。2 つ以上のリングが存在します。リング間に 2 つの類似した共通ノードがあります。各リングに RRPP ドメインを定義し、1 つのプライマリリング、それ以外のサブリングを設定する必要があります。

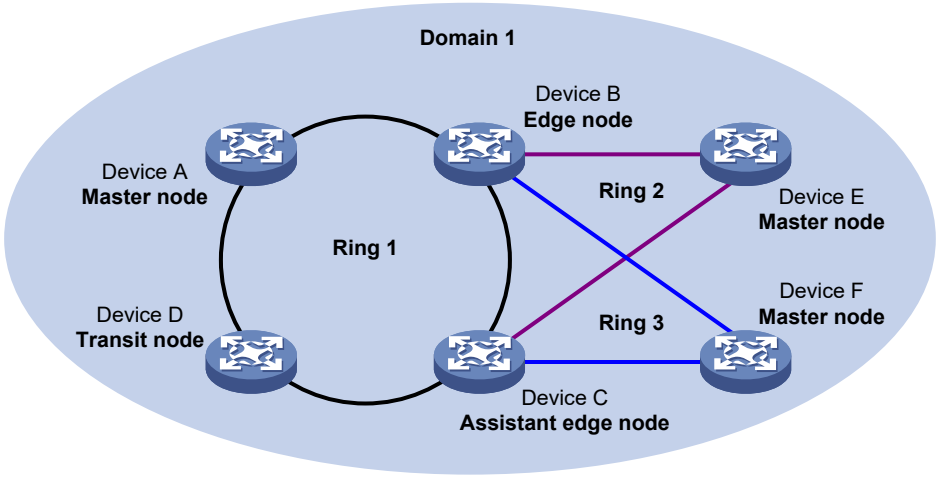


図 4-5 デュアルホームリングのネットワークトポロジ

V. シングルリングロードバランシング

図 4-6にシングルリングロードバランシングのネットワークトポロジを示します。複数のドメインを設定することでロードバランシングを構成することができます。

- Ring 1 を Domain 1、Domain 2 の両方のプライマリリングとして設定します。
- Domain 1、Domain 2 は異なるプロテクト VLAN に設定します。
- Domain 1 では Device A は Ring 1 のマスタノードとして設定します。

- Domain 2 では Device B は Ring 1 のマスタノードとして設定します。

VLAN にもとづいて異なるリンクをブロックさせ、シングルリングロードバランシングを構成するようにリングを設定します。

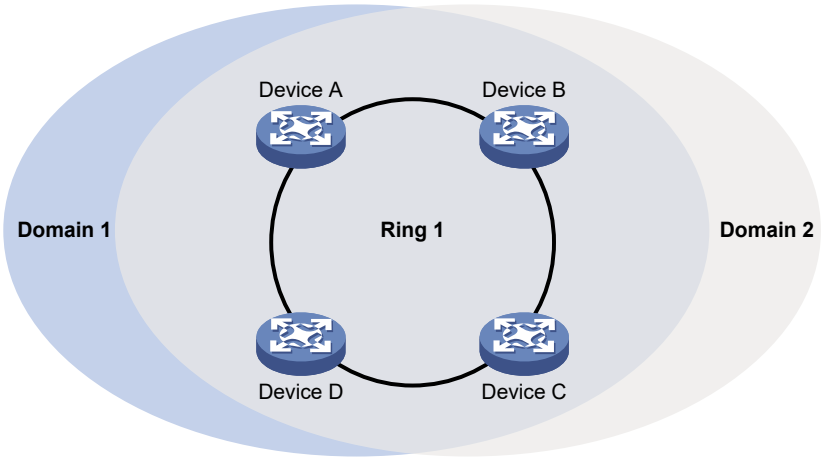


図 4-6 シングルリングロードバランシングのネットワークトポロジ

VI. 交差リング（Intersecting リング、マルチリング）ロードバランシング

図 4-7に交差リングロードバランシングのネットワークトポロジを示します。複数のドメインを設定することでロードバランシングを構成することができます。

- Ring 1 は Domain 1、Domain 2 のプライマリリング、Ring 2 は Domain 1、Domain 2 のサブリングとして設定します。
- Domain 1、Domain 2 は異なるプロテクト VLAN に設定します。
- Domain 1 では Device A は Ring 1 のマスタノードとして設定します。
- Domain 2 では Device D は Ring 1 のマスタノードとして設定します。
- Device E は Domain 1、Domain 2 の Ring 2 のマスタノードとして設定します。しかし Domain 1、Domain 2 の Device E の他のポートはブロックします。

異なる VLAN からサブリングとプライマリリングの異なるパスを越えて交差リングロードバランシングを構成するようにリングを設定します。

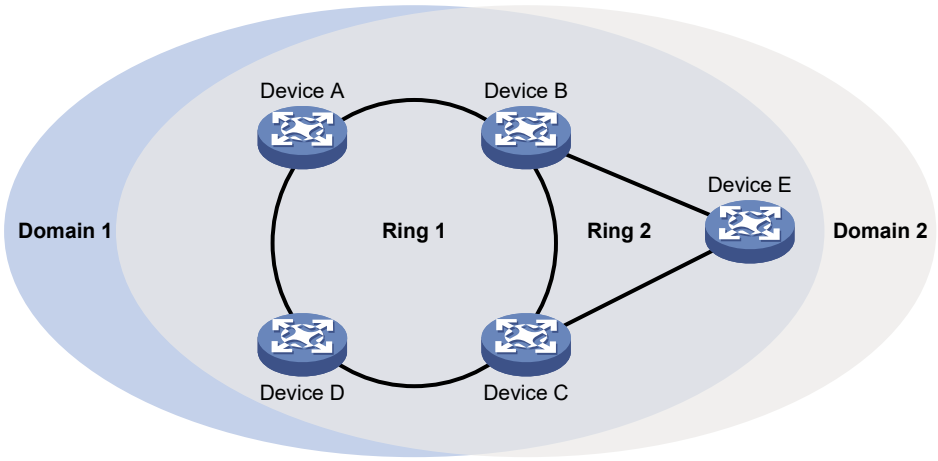


図 4-7 交差リング（Intersecting リング、マルチリング）ロードバランシング

4.2 RRPPの設定作業リスト

- サービスの計画にもとづいて RRPP ドメインを作成してください。
- 各 RRPP ドメインのコントロール VLAN、プロテクト VLAN を指定してください。
- 各 RRPP ドメインのトラフィックパスにもとづいてリングの役割、ノードの役割を定義してください。

RRPP は自動選択メカニズムがありません。リングネットワークをモニタし、保護するため、RRPP の各ノードを正しく設定してください。

RRPP を設定する前に、物理的にリング状の Ethernet トポロジを構成してください。

RRPP を設定するには次の作業を行ってください。

作業	補足
（必須設定項目）RRPP ドメインの作成	RRPP ドメインのすべてのノード上でこのタスクを実行してください。
（必須設定項目）コントロールVLANの設定	RRPP ドメインのすべてのノード上でこのタスクを実行してください。
（必須設定項目）プロテクトVLANの設定	RRPP ドメインのすべてのノード上でこのタスクを実行してください。
（必須設定項目）RRPP リングの設定 • RRPPポートの設定 • RRPPノードの設定	RRPP ドメインのすべてのノード上でこのタスクを実行してください。
（必須設定項目）RRPP ドメインの有効化	RRPP ドメインのすべてのノード上でこのタスクを実行してください。
（オプション設定項目）RRPPタイマの設定	RRPP ドメインのマスタノード上でこのタスクを実行してください。
（オプション設定項目）RRPPリンググループの設定	RRPP ドメインのエッジノード、およびアシスタントエッジノードでこのタスクを実行してください。
（オプション設定項目）RRPPに関するSNMP notificationの有効化	—

注意：

- RRPP ポートに 1000BASE-T-SFP トランシーバモジュールを使用した場合、リンクダウン検知に 1 秒程度かかります。RRPP リングを構成する際は、標準のポートや光ファイバトランシーバモジュールを使用することを推奨します。
- RRPP とループ検知機能を併用する場合は、RRPP リングを構成する各ノードのプライマリポートとセカンダリポートでループ保護アクションを設定しないで下さい。プライマリポートとセカンダリポートでループ保護アクションを設定すると、RRPP のノード上のどこかでループが発生したとき、ループ検知の保護アクションにより RRPP の Hello パケットが途切れて、マスタノードのセカンダリポートのブロックが解除されます。それにより、ループ検知の保護アクションが発生したノードのもう一方の RRPP ポートでも保護アクションが動作して自動復旧できなくなります。

4.3 RRPPドメインの作成

RRPP ドメインを作成するとき、RRPP ドメインに固有の RRPP ドメイン ID を指定してください。同じ RRPP ドメイン内のすべての装置は、同じ RRPP ドメイン ID で構成する必要があります。

以下に RRPP ドメインを作成する設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	–
2． RRPP ドメインを作成し、RRPP domain view に移行する	**rrpp domain** *domain-id*	デフォルト：設定なし

4.4 コントロールVLANの設定

RRPP ドメインで RRPP リングを設定する前に RRPP ドメインのすべてのノードに同じコントロール VLAN を設定してください。RRPP ドメインにプライマリコントロール VLAN のみを設定してください。システムは自動でセカンダリコントロール VLAN を設定します。セカンダリコントロール VLAN ID はプライマリコントロール VLAN ID に 1 を追加したものを使用します。コントロール VLAN を正常に設定するため、2 つのコントロール VLAN の ID が連続しており、既存の ID でないことを確認してください。

コントロール VLAN を設定するとき、以下のガイドラインに従ってください。

- コントロール VLAN として RRPP リングにアクセスするポートのデフォルト VLAN を設定しないでください。コントロール VLAN で QinQ、VLAN マッピングを有効にしないでください。有効にした場合、RRPPDU を正常に転送することができません。
- RRPP ドメインの RRPP リングを設定した後、ドメインのプライマリコントロール VLAN を削除あるいは修正することはできません。**undo control-vlan** コマンドを使用してプライマリコントロール VLAN を削除のみすることができます。

- RRPP が設定されていない装置で透過的に RRPPDU を転送するため、RRPP リングにアクセスする 2 つのポートのみ、コントロール VLAN からのパケットを許可できるようにしてください。そうでない場合、他の VLAN からのパケットはトランスペアレント転送モードのコントロール VLAN に入り、RRPP リングと衝突する可能性があります。

RRPP ドメインのすべてのノードで以下の設定を行ってください。

操作	コマンド	補足
1． system view に移行する	**system-view**	–
2． RRPP domain view に移行する	**rrpp domain** *domain-id*	–
3． RRPP ドメインのプライマリコントロール VLAN を設定する	**control-vlan** *vlan-id*	デフォルト：設定なし

4.5 プロテクトVLANの設定

RRPP ドメインで RRPP リングを設定する前に、最初に RRPP ドメインのすべてのノードに同じプロテクト VLAN を設定してください。 RRPP ポートが割り当てられるすべての VLAN は、RRPP ドメインによって保護されていなければなりません。

MSTI（Multiple Spanning Tree Instances）を参照してプロテクト VLAN を設定できます。プロテクト VLAN の設定方法はスパニングツリーモードによって異なります。

- STP、RSTP、MSTP モードの場合、VLAN と MSTI 間のマッピングを手動で設定してください。
- PVST モードの場合、装置は自動で各 VLAN を MSTI にマッピングします。スパニングツリーがグローバルで無効の場合、すべての VLAN は自動で MSTI 0 にマッピングされます。

スパニングツリーの詳細はオペレーションマニュアルのセクション 3 *アクセス”STP”*を参照してください。

⚠ **重要**：
ロードバランシングを設定するとき、異なる RRPP ドメインに異なるプロテクト VLAN を設定してください。

RRPP ドメインのすべてのノードで、設定を行ってください。

以下にプロテクト VLAN の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	–

操作	コマンド	補足
2. MST region view に移行する	**stp region-configuration**	装置がPVSTモードで動作する場合必要ありません。 コマンドの詳細はコマンドマニュアルのセクション 3 *アクセス”STP”*を参照してください。
3. VLAN-to instance マッピングテーブルを設定する	• 方法1： **instance** *instance-id* **vlan** *vlan-id-list* • 方法2： **vlan-mapping modulo** *modulo*	いずれか一方の設定を使用してください。 デフォルト：MSTのすべてのVLANはMSTI0(CIST)にマッピングされます。 装置がPVSTモードで動作する場合必要ありません。 コマンドの詳細はコマンドマニュアルのセクション 3 *アクセス”STP”*を参照してください。
4. MST region 設定を手動で有効化する	**active region-configuration**	装置がPVSTモードで動作する場合必要ありません。 コマンドの詳細はコマンドマニュアルのセクション 3 *アクセス”STP”*を参照してください。
5. （オプション設定項目）現在有効な MST region の設定情報を表示する	**display stp region-configuration**	すべてのviewで実行できます。 コマンドの出力にはVLAN-インスタンスマッピングが含まれます。 コマンドの詳細はコマンドマニュアルのセクション 3 *アクセス”STP”*を参照してください。
6. system view に戻る	**quit**	装置がPVSTモードで動作する場合必要ありません。
7. RRPP domain view に移行する	**rrpp domain** *domain-id*	ー
8. RRPP ドメインのプロテクト VLAN を設定する	**protected-vlan reference-instance** *instance-id-list*	デフォルト：設定なし

4.6 RRPPリングの設定

RRPP リングを設定する場合、ノードを設定する前に、各ノードを RRPP リングに接続しているポートを設定してください。

4.6.1 RRPP ポートの設定

RRPP ポートを設定するとき、以下のガイドラインに従ってください。

- RRPP ポートで OAM リモートループバック機能を有効にしないでください。一時的なブロードキャストストームを引き起こす恐れがあります。
- トポロジの収束を加速するため、RRPP ポートでリンクダウンの通知を抑制する **link-delay** コマンドを使用することを推奨します。**link-delay** コマンドは、物理状態の変更を通知するリンクダウンの抑制の時間を 0 秒に変更します。**link-delay** コマンドの詳細は、コマンドマニュアルのセクション 3 *アクセス*”*STP*”を参照してください。

RRPP リングにアクセスする各ノードのポートで設定してください。

以下に RRPP ポートの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Layer 2 Ethernet interface view または aggregation interface view へ移行する	**interface** *interface-type interface-number*	―
3. インタフェースのリンクタイプをトランクに設定する	**port link-type trunk**	デフォルト：アクセス コマンドの詳細はコマンドマニュアルのセクション 3 *アクセス*”*STP*”を参照してください。
4. トランクポートを RRPP ドメインのプロテクト VLAN に割り当てる	**port trunk permit vlan** { *vlan-id-list* | **all** }	デフォルト：VLAN1パケットのみ許可します。 RRPPポートはコントロールVLANからのパケットを許可します。 コマンドの詳細はコマンドマニュアルのセクション 3 *アクセス*”*STP*”を参照してください。
5. スパニングツリーを無効にする	**undo stp enable**	デフォルト：有効 コマンドの詳細はコマンドマニュアルのセクション 3 *アクセス*”*STP*”を参照してください。

4.6.2 RRPP ノードの設定

装置が RRPP ドメインで複数の RRPP リングを運ぶ場合、サブリングのエッジノードあるいはアシスタントエッジノードでのみできます。

I. マスタノードの指定

以下にマスタノードの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. RRPP domain view に移行する	**rrpp domain** *domain-id*	―

操作	コマンド	補足
3. 装置をマスタノードに設定し、プライマリポート、セカンダリポートを設定する	**ring** *ring-id* **node-mode master** [**primary-port** *interface-type interface-number*] [**secondary-port** *interface-type interface-number*] **level** *level-value*	デフォルト：設定なし

II. トランジットノードの指定

以下にトランジットノードの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. RRPP domain view に移行する	**rrpp domain** *domain-id*	―
3. 装置をトランジットノードに指定し、プライマリポート、セカンダリポートを指定する	**ring** *ring-id* **node-mode transit** [**primary-port** *interface-type interface-number*] [**secondary-port** *interface-type interface-number*] **level** *level-value*	デフォルト：設定なし

III. エッジノードの指定

エッジノードを設定する際、サブリングを設定する前にプライマリリングを最初に設定してください。

以下にエッジノードの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. RRPP domain view に移行する	**rrpp domain** *domain-id*	―
3. 装置をプライマリリングのマスタノードあるいはトランジットノードに指定し、プライマリポート、セカンダリポートを指定する	**ring** *ring-id* **node-mode** { **master** | **transit** } [**primary-port** *interface-type interface-number*] [**secondary-port** *interface-type interface-number*] **level** *level-value*	デフォルト：設定なし
4. 装置をサブリングのエッジノードに指定し、エッジポートを指定する	**ring** *ring-id* **node-mode edge** [**edge-port** *interface-type interface-number*]	デフォルト：設定なし

IV. アシスタントエッジノードの指定

アシスタントエッジノードを設定する際、サブリングを設定する前にプライマリリングを最初に設定してください。

以下にアシスタントエッジノードの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―

操作	コマンド	補足
2． RRPP domain view に移行する	**rrpp domain** *domain-id*	―
3． 装置をプライマリリングのマスタノードあるいはトランジットノードに指定し、プライマリポート、セカンダリポートを指定する	**ring** *ring-id* **node-mode** { **master** | **transit** } [**primary-port** *interface-type interface-number*] [**secondary-port** *interface-type interface-number*] **level** *level-value*	デフォルト：設定なし
4． 装置をサブリングのアシスタントエッジノードに指定し、エッジポートを指定する	**ring** *ring-id* **node-mode assistant-edge** [**edge-port** *interface-type interface-number*]	デフォルト：設定なし

4.7 RRPPドメインの有効化

装置で RRPP ドメインを有効にする前、装置の RRPP ドメインの RRPP プロトコルと RRPP リングを有効にしてください。

RRPP ドメインを有効にするとき、以下のガイドラインに従ってください。

- 装置でサブリングを有効にする前にプライマリリングを有効にしてください。装置でプライマリリングを無効にする前に、すべてのサブリングを無効にしてください。そうでない場合、システムは画面にエラー表示を行います。
- サブリングの Hello パケットがプライマリリングでループすることを防止するため、最初にマスタノードでプライマリリングを有効にしてください。そして別のマスタノードでサブリングを有効にしてください。

RRPP ドメインのすべてのノードで設定してください。

以下に RRPP ドメインを有効にする設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． RRPP を有効にする	**rrpp enable**	デフォルト：無効
3． RRPP domain view に移行する	**rrpp domain** *domain-id*	―
4． 指定した RRPP リングを有効にする	**ring** *ring-id* **enable**	デフォルト：無効

4.8 RRPPタイマの設定

Fail タイマは Hello タイマの 3 倍以上の値である必要があります。

デュアルホームリングネットワークにおいて、サブリングのマスタノードの Fail タイマとプライマリリングのマスタノードの Fail タイマの差分が、サブリングのマスタノードの Hello タイマの 2 倍以上であることを確認してください。そうでない場合プライマリリングで障害が発生したときに一時的なループが発生します。

RRPP ドメインのマスタノードで設定してください。

以下に RRPP タイマの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． RRPP domain view に移行する	**rrpp domain** *domain-id*	―
3． RRPP ドメインの Hello タイマと Fail タイマを設定する	**timer hello-timer** *hello-value* **fail-timer** *fail-value*	デフォルト： Helloタイマ：1秒 Failタイマ：3秒

4.9 RRPPリンググループの設定

Edge-Hello パケットのトラフィックを減らすために、RRPP リンググループに同じエッジノード、アシスタントエッジノードでサブリングを割り当てます。RRPP リンググループのメカニズムを適用します。RRPP リンググループは、エッジノードとアシスタントエッジノードの両方で設定する必要があります。RRPP リンググループは、エッジノードとアシスタントエッジノードにのみ設定することができます。

RRPP リンググループを設定するとき、以下のガイドラインに従ってください。

- 1 つの RRPP リンググループにのみサブリングを割り当てることができます。エッジノードで設定された RRPP リンググループと、アシスタントエッジノードで設定された RRPP リンググループが同じサブリングに含まれていることを確認してください。同じサブリングに含まれていない場合、RRPP リンググループは正常に動作することができません。
- RRPP リンググループのサブリングが同じエッジノードとアシスタントエッジノードを共有していること、エッジノードとアシスタントエッジノードが同じ SRPT を持っていることを確認してください。
- 装置が RRPP リンググループのサブリングでエッジノードあるいはアシスタントエッジノードであることを確認してください。
- エッジノード上の RRPP リンググループとアシスタントエッジノード上の RRPP リンググループは、同じ設定で同じ動作状態であることを確認してください。
- RRPP リンググループ内のすべてのサブリングが同じ SRPT を持っていることを確認してください。これらのサブリングの SRPT の設定が異なる場合、RRPP リンググループは正常に動作することができません。

RRPP ドメインのエッジノードとアシスタントエッジノードの両方で設定してください。

以下に RRPP リンググループの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． RRPP domain view に移行する	**rrpp domain** *domain-id*	デフォルト：設定なし
3． 指定したサブリングを RRPP リンググループに割り当てる	**domain** *domain-id* **ring** *ring-id-list*	デフォルト：設定なし

4.10 RRPPに関するSNMP notificationの有効化

SNMP notification を有効にすることで、RRPP に関する重要なイベントを NMS に通知します。NMS は設定された出力ルールにしたがって notification を出力する方法を決定します。SNMP notification の詳細は、オペレーションマニュアルのセクション 11 *システム管理*“*SNMP*”を参照してください。

以下に RRPP に関する SNMP notification の有効化の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． RRPP に関する SNMP notification を有効にする	**snmp-agent trap enable rrpp** [**major-fault** | **multi-master** | **ring-fail** | **ring-recover**] *	デフォルト：無効

4.11 RRPPの表示と維持

すべての view で **display** コマンドを実行でき、user view で **reset** コマンドを実行できます。

操作	コマンド
RRPPの概要情報を表示する	**display rrpp brief**
RRPPグループの設定情報を表示する	**display rrpp ring-group** [*ring-group-id*]
RRPPDUの統計情報を表示する	**display rrpp statistics domain** *domain-id* [**ring** *ring-id*]
RRPPの詳細情報を表示する	**display rrpp verbose domain** *domain-id* [**ring** *ring-id*]
RRPPDUの統計情報を削除する	**reset rrpp statistics domain** *domain-id* [**ring** *ring-id*]

4.12 RRPPの設定例

4.12.1 シングルリング設定例

I. ネットワーク要件

- Device A、Device B、Device C、Device D、Device E は RRPP ドメイン 1 を構成します。VLAN4092 を RRPP ドメイン 1 のプライマリコントロール VLAN に指定します。RRPP ドメイン 1 のプロテクト VLAN に VLAN1～VLAN 30 を設定します。
- Device A、Device B、Device C、Device D はプライマリリング 1 を構成します。
- Device A をプライマリリング 1 のマスタノードに指定し、GigabitEthernet 1/0/1 をプライマリポート、GigabitEthernet 1/0/2 をセカンダリポートに指定します。
- Device B と Device C と Device D をプライマリリング 1 のトランジットノードに指定します。各装置の GigabitEthernet 1/0/1 をプライマリポート、GigabitEthernet 1/0/2 をセカンダリポートに指定します。

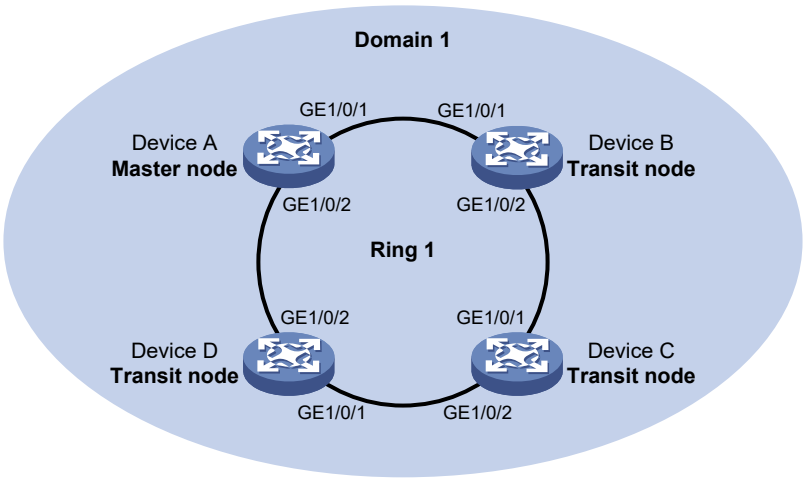


図 4-8 ネットワーク図

II. 設定手順

1)　Device A を設定します。

VLAN 1～VLAN 30 を作成します。

```
<DeviceA> system-view
[DeviceA] vlan 1 to 30
```

MSTI インスタンス 1 に VLAN をマッピングします。

```
[DeviceA] stp region-configuration
[DeviceA-mst-region] instance 1 vlan 1 to 30
```

MST region の設定を有効にします。

```
[DeviceA-mst-region] active region-configuration
[DeviceA-mst-region] quit
```

物理状態の変更があった場合、GigabitEthernet 1/0/1 のリンクダウンの通知を抑制する時間を 0 秒に設定します。

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] link-delay 0
```

ポートでスパニングツリー機能を無効にします。

```
[DeviceA-GigabitEthernet1/0/1] undo stp enable
```

ポートをトランクポートに設定します。

```
[DeviceA-GigabitEthernet1/0/1] port link-type trunk
```

VLAN 1～VLAN 30 にポートを割り当てます。

```
[DeviceA-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
```

```
[DeviceA-GigabitEthernet1/0/1] quit
```

GigabitEthernet 1/0/1 の設定と同様に GigabitEthernet 1/0/2 を設定します。

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] link-delay 0
[DeviceA-GigabitEthernet1/0/2] undo stp enable
[DeviceA-GigabitEthernet1/0/2] port link-type trunk
[DeviceA-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
[DeviceA-GigabitEthernet1/0/2] quit
```

RRPP ドメイン 1 を作成します。

```
[DeviceA] rrpp domain 1
```

RRPP ドメイン 1 のプライマリコントロール VLAN として VLAN 4092 を設定します。

```
[DeviceA-rrpp-domain1] control-vlan 4092
```

RRPP ドメイン 1 のプロテクト VLAN として MSTI 1 にマッピングした VLAN を設定します。

```
[DeviceA-rrpp-domain1] protected-vlan reference-instance 1
```

プライマリリング 1 のマスタノードとして Device A を設定します。プライマリポートを GigabitEthernet 1/0/1、セカンダリポートを GigabitEthernet 1/0/2 に設定します。リング 1 を有効にします。

```
[DeviceA-rrpp-domain1] ring 1 node-mode master primary-port gigabitethernet 1/0/1 secondary-port gigabitethernet 1/0/2 level 0
[DeviceA-rrpp-domain1] ring 1 enable
[DeviceA-rrpp-domain1] quit
```

RRPP を有効にします。

```
[DeviceA] rrpp enable
```

2) Device B を設定します。

VLAN 1～VLAN 30 を作成します。

```
<DeviceB> system-view
[DeviceB] vlan 1 to 30
```

MSTI 1 に VLAN をマッピングします。

```
[DeviceB] stp region-configuration
[DeviceB-mst-region] instance 1 vlan 1 to 30
```

MST region の設定を有効にします。

```
[DeviceB-mst-region] active region-configuration
[DeviceB-mst-region] quit
```

物理状態の変更があった場合、GigabitEthernet 1/0/1 のリンクダウンの通知を抑制する時間を 0 秒に設定します。

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] link-delay 0
```

ポートでスパニングツリー機能を無効にします。

```
[DeviceB-GigabitEthernet1/0/1] undo stp enable
```

ポートをトランクポートに設定します。

```
[DeviceB-GigabitEthernet1/0/1] port link-type trunk
```

VLAN 1～VLAN 30 にポートを割り当てます。

```
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceB-GigabitEthernet1/0/1] quit
```

GigabitEthernet 1/0/1 の設定と同様に GigabitEthernet 1/0/2 を設定します。

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] link-delay 0
[DeviceB-GigabitEthernet1/0/2] undo stp enable
[DeviceB-GigabitEthernet1/0/2] port link-type trunk
[DeviceB-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
[DeviceB-GigabitEthernet1/0/2] quit
```

RRPP ドメイン 1 を作成します。

```
[DeviceB] rrpp domain 1
```

RRPP ドメイン 1 のプライマリコントロール VLAN として VLAN 4092 を設定します。

```
[DeviceB-rrpp-domain1] control-vlan 4092
```

RRPP ドメイン 1 のプロテクト VLAN として MSTI 1 にマッピングした VLAN を設定します。

```
[DeviceB-rrpp-domain1] protected-vlan reference-instance 1
```

プライマリリング 1 のトランジットノードとして Device B を設定します。プライマリポートを GigabitEthernet 1/0/1、セカンダリポートを GigabitEthernet 1/0/2 に設定します。リング 1 を有効にします。

```
[DeviceB-rrpp-domain1] ring 1 node-mode transit primary-port gigabitethernet 1/0/1 secondary-port gigabitethernet 1/0/2 level 0
[DeviceB-rrpp-domain1] ring 1 enable
[DeviceB-rrpp-domain1] quit
```

RRPP を有効にします。

```
[DeviceB] rrpp enable
```

3) Device C を設定します。

Device B の設定と同様に Device C を設定します。

4)　Device D を設定します。

Device B の設定と同様に Device D を設定します。

III. 設定の確認

display コマンドを使用し、各 Device の RRPP 設定と動作情報を表示します。

4.12.2 交差リング（Intersecting リング、マルチリング）の設定例

I. ネットワーク要件

- Device A、Device B、Device C、Device D、Device E は RRPP ドメイン 1 を構成します。VLAN4092 を RRPP ドメイン 1 のプライマリコントロール VLAN に指定します。RRPP ドメイン 1 のプロテクト VLAN に VLAN1～VLAN 30 を設定します。
- Device A、Device B、Device C、Device D はプライマリリング 1 を構成します。Device B、Device C、Device E はサブリング 2 を構成します。
- Device A をプライマリリング 1 のマスタノードに指定し、GigabitEthernet 1/0/1 をプライマリポート、GigabitEthernet 1/0/2 をセカンダリポートに指定します。
- Device E をサブリング 2 のマスタノードに指定し、GigabitEthernet 1/0/1 をプライマリポート、GigabitEthernet 1/0/2 をセカンダリポートに指定します。
- Device B をプライマリリング 1 のトランジットノード、サブリング 2 のエッジノードに指定し、GigabitEthernet 1/0/3 をエッジポートに指定します。
- Device C をプライマリリング 1 のトランジットノード、サブリング 1 のアシスタントエッジノードに指定し、GigabitEthernet 1/0/3 をエッジポートに指定します。
- Device D をプライマリリング 1 のトランジットノードに指定し、GigabitEthernet 1/0/1 をプライマリポート、GigabitEthernet 1/0/2 をセカンダリポートに指定します。

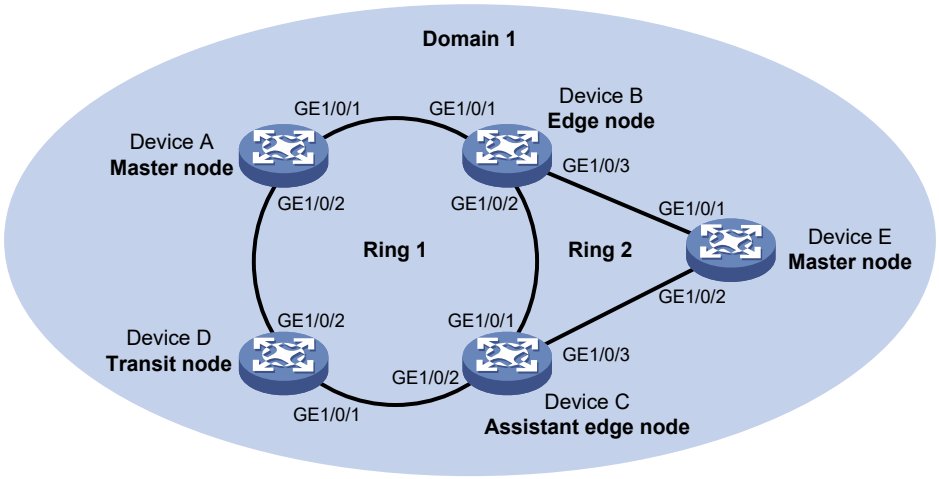


図 4-9 ネットワーク図

II. 設定手順

1)　Device A を設定します。

VLAN 1～VLAN 30 を作成します。

```
<DeviceA> system-view
[DeviceA] vlan 1 to 30
```

MSTI インスタンス 1 に VLAN をマッピングします。

```
[DeviceA] stp region-configuration
[DeviceA-mst-region] instance 1 vlan 1 to 30
```

MST region の設定を有効にします。

```
[DeviceA-mst-region] active region-configuration
[DeviceA-mst-region] quit
```

物理状態の変更があった場合、GigabitEthernet 1/0/1 のリンクダウンの通知を抑制する時間を 0 秒に設定します。

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] link-delay 0
```

ポートでスパニングツリー機能を無効にします。

```
[DeviceA-GigabitEthernet1/0/1] undo stp enable
```

ポートをトランクポートに設定します。

```
[DeviceA-GigabitEthernet1/0/1] port link-type trunk
```

VLAN 1～VLAN 30 にポートを割り当てます。

```
[DeviceA-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceA-GigabitEthernet1/0/1] quit
```

GigabitEthernet 1/0/1 の設定と同様に GigabitEthernet 1/0/2 を設定します。

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] link-delay 0
[DeviceA-GigabitEthernet1/0/2] undo stp enable
[DeviceA-GigabitEthernet1/0/2] port link-type trunk
[DeviceA-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
[DeviceA-GigabitEthernet1/0/2] quit
```

RRPP ドメイン 1 を作成します。

```
[DeviceA] rrpp domain 1
```

RRPP ドメイン 1 のプライマリコントロール VLAN として VLAN 4092 を設定します。

```
[DeviceA-rrpp-domain1] control-vlan 4092
```

RRPP ドメイン 1 のプロテクト VLAN として MSTI 1 にマッピングした VLAN を設定します。

```
[DeviceA-rrpp-domain1] protected-vlan reference-instance 1
```

プライマリリング 1 のマスタノードとして Device A を設定します。プライマリポートを GigabitEthernet 1/0/1、セカンダリポートを GigabitEthernet 1/0/2 に設定します。リング 1 を有効にします。

```
[DeviceA-rrpp-domain1] ring 1 node-mode master primary-port gigabitethernet 1/0/1 secondary-port gigabitethernet 1/0/2 level 0
[DeviceA-rrpp-domain1] ring 1 enable
[DeviceA-rrpp-domain1] quit
```

RRPP を有効にします。

```
[DeviceA] rrpp enable
```

2) Device B を設定します。

VLAN 1～VLAN 30 を作成します。

```
<DeviceB> system-view
[DeviceB] vlan 1 to 30
```

MSTI 1 に VLAN をマッピングします。

```
[DeviceB] stp region-configuration
[DeviceB-mst-region] instance 1 vlan 1 to 30
```

MST region の設定を有効にします。

```
[DeviceB-mst-region] active region-configuration
[DeviceB-mst-region] quit
```

物理状態の変更があった場合、GigabitEthernet 1/0/1 のリンクダウンの通知を抑制する時間を 0 秒に設定します。

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] link-delay 0
```

ポートでスパニングツリー機能を無効にします。

```
[DeviceB-GigabitEthernet1/0/1] undo stp enable
```

ポートをトランクポートに設定します。

```
[DeviceB-GigabitEthernet1/0/1] port link-type trunk
```

VLAN 1～VLAN 30 にポートを割り当てます。

```
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceB-GigabitEthernet1/0/1] quit
```

GigabitEthernet 1/0/1 の設定と同様に GigabitEthernet 1/0/2 を設定します。

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] link-delay 0
```

```
[DeviceB-GigabitEthernet1/0/2] undo stp enable
[DeviceB-GigabitEthernet1/0/2] port link-type trunk
[DeviceB-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
[DeviceB-GigabitEthernet1/0/2] quit
```

GigabitEthernet 1/0/1 の設定と同様に GigabitEthernet 1/0/3 を設定します。

```
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] link-delay 0
[DeviceB-GigabitEthernet1/0/3] undo stp enable
[DeviceB-GigabitEthernet1/0/3] port link-type trunk
[DeviceB-GigabitEthernet1/0/3] port trunk permit vlan 1 to 30
[DeviceB-GigabitEthernet1/0/3] quit
```

RRPP ドメイン 1 を作成します。

```
[DeviceB] rrpp domain 1
```

RRPP ドメイン 1 のプライマリコントロール VLAN として VLAN 4092 を設定します。

```
[DeviceB-rrpp-domain1] control-vlan 4092
```

RRPP ドメイン 1 のプロテクト VLAN として MSTI 1 にマッピングした VLAN を設定します。

```
[DeviceB-rrpp-domain1] protected-vlan reference-instance 1
```

プライマリリング 1 のトランジットノードとして Device B を設定します。プライマリポートを GigabitEthernet 1/0/1、セカンダリポートを GigabitEthernet 1/0/2 に設定します。リング 1 を有効にします。

```
[DeviceB-rrpp-domain1] ring 1 node-mode transit primary-port gigabitethernet 1/0/1 secondary-port gigabitethernet 1/0/2 level 0
[DeviceB-rrpp-domain1] ring 1 enable
```

サブリング 2 のエッジノードとして Device B を設定します。エッジポートを GigabitEthernet 1/0/3 に設定します。サブリング 2 を有効にします。

```
[DeviceB-rrpp-domain1] ring 2 node-mode edge edge-port gigabitethernet 1/0/3
[DeviceB-rrpp-domain1] ring 2 enable
[DeviceB-rrpp-domain1] quit
```

RRPP を有効にします。

```
[DeviceB] rrpp enable
```

3) Device C を設定します。

VLAN 1～VLAN 30 を作成します。

```
<DeviceC> system-view
[DeviceC] vlan 1 to 30
```

MSTI インスタンス 1 に VLAN をマッピングします。

```
[DeviceC] stp region-configuration
[DeviceC-mst-region] instance 1 vlan 1 to 30
```

MST region の設定を有効にします。

```
[DeviceC-mst-region] active region-configuration
[DeviceC-mst-region] quit
```

物理状態の変更があった場合、GigabitEthernet 1/0/1 のリンクダウンの通知を抑制する時間を 0 秒に設定します。

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] link-delay 0
```

ポートでスパニングツリー機能を無効にします。

```
[DeviceC-GigabitEthernet1/0/1] undo stp enable
```

ポートをトランクポートに設定します。

```
[DeviceC-GigabitEthernet1/0/1] port link-type trunk
```

VLAN 1～VLAN 30 にポートを割り当てます。

```
[DeviceC-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceC-GigabitEthernet1/0/1] quit
```

GigabitEthernet 1/0/1 の設定と同様に GigabitEthernet 1/0/2 を設定します。

```
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] link-delay 0
[DeviceC-GigabitEthernet1/0/2] undo stp enable
[DeviceC-GigabitEthernet1/0/2] port link-type trunk
[DeviceC-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
[DeviceC-GigabitEthernet1/0/2] quit
```

GigabitEthernet 1/0/1 の設定と同様に GigabitEthernet 1/0/3 を設定します。

```
[DeviceC] interface gigabitethernet 1/0/3
[DeviceC-GigabitEthernet1/0/3] link-delay 0
[DeviceC-GigabitEthernet1/0/3] undo stp enable
[DeviceC-GigabitEthernet1/0/3] port link-type trunk
[DeviceC-GigabitEthernet1/0/3] port trunk permit vlan 1 to 30
[DeviceC-GigabitEthernet1/0/3] quit
```

RRPP ドメイン 1 を作成します。

```
[DeviceC] rrpp domain 1
```

RRPP ドメイン 1 のプライマリコントロール VLAN として VLAN 4092 を設定します。

```
[DeviceC-rrpp-domain1] control-vlan 4092
```

RRPP ドメイン 1 のプロテクト VLAN として MSTI 1 にマッピングした VLAN を設定します。

```
[DeviceC-rrpp-domain1] protected-vlan reference-instance 1
```

プライマリリング 1 のトランジットノードとして Device C を設定します。プライマリポートを GigabitEthernet 1/0/1、セカンダリポートを GigabitEthernet 1/0/2 に設定します。リング 1 を有効にします。

```
[DeviceC-rrpp-domain1] ring 1 node-mode transit primary-port gigabitethernet 1/0/1 secondary-port gigabitethernet 1/0/2 level 0
[DeviceC-rrpp-domain1] ring 1 enable
```

サブリング 2 のアシスタントエッジノードとして Device C を設定します。エッジポートを GigabitEthernet 1/0/3 に設定します。サブリング 2 を有効にします。

```
[DeviceC-rrpp-domain1] ring 2 node-mode assistant-edge edge-port gigabitethernet 1/0/3
[DeviceC-rrpp-domain1] ring 2 enable
[DeviceC-rrpp-domain1] quit
```

RRPP を有効にします。

```
[DeviceC] rrpp enable
```

4) Device D を設定します。

VLAN 1～VLAN 30 を作成します。

```
<DeviceD> system-view
[DeviceD] vlan 1 to 30
```

MSTI インスタンス 1 に VLAN をマッピングします。

```
[DeviceD] stp region-configuration
[DeviceD-mst-region] instance 1 vlan 1 to 30
```

MST region の設定を有効にします。

```
[DeviceD-mst-region] active region-configuration
[DeviceD-mst-region] quit
```

物理状態の変更があった場合、GigabitEthernet 1/0/1 のリンクダウンの通知を抑制する時間を 0 秒に設定します。

```
[DeviceD] interface gigabitethernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] link-delay 0
```

ポートでスパニングツリー機能を無効にします。

```
[DeviceD-GigabitEthernet1/0/1] undo stp enable
```

ポートをトランクポートに設定します。

```
[DeviceD-GigabitEthernet1/0/1] port link-type trunk
```

VLAN 1～VLAN 30 にポートを割り当てます。

```
[DeviceD-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceD-GigabitEthernet1/0/1] quit
```

GigabitEthernet 1/0/1 の設定と同様に GigabitEthernet 1/0/2 を設定します。

```
[DeviceD] interface gigabitethernet 1/0/2
[DeviceD-GigabitEthernet1/0/2] link-delay 0
[DeviceD-GigabitEthernet1/0/2] undo stp enable
[DeviceD-GigabitEthernet1/0/2] port link-type trunk
[DeviceD-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
[DeviceD-GigabitEthernet1/0/2] quit
```

RRPP ドメイン 1 を作成します。

```
[DeviceD] rrpp domain 1
```

RRPP ドメイン 1 のプライマリコントロール VLAN として VLAN 4092 を設定します。

```
[DeviceD-rrpp-domain1] control-vlan 4092
```

RRPP ドメイン 1 のプロテクト VLAN として MSTI 1 にマッピングした VLAN を設定します。

```
[DeviceD-rrpp-domain1] protected-vlan reference-instance 1
```

プライマリリング 1 のトランジットノードとして Device D を設定します。プライマリポートを GigabitEthernet 1/0/1、セカンダリポートを GigabitEthernet 1/0/2 に設定します。リング 1 を有効にします。

```
[DeviceD-rrpp-domain1] ring 1 node-mode transit primary-port gigabitethernet 1/0/1 secondary-port gigabitethernet 1/0/2 level 0
[DeviceD-rrpp-domain1] ring 1 enable
[DeviceD-rrpp-domain1] quit
```

RRPP を有効にします。

```
[DeviceD] rrpp enable
```

5) Device E を設定します。

VLAN 1～VLAN 30 を作成します。

```
<DeviceE> system-view
[DeviceE] vlan 1 to 30
```

MSTI 1 に VLAN をマッピングします。

```
[DeviceE] stp region-configuration
[DeviceE-mst-region] instance 1 vlan 1 to 30
```

MST region の設定を有効にします。

```
[DeviceE-mst-region] active region-configuration
[DeviceE-mst-region] quit
```

物理状態の変更があった場合、GigabitEthernet 1/0/1 のリンクダウンの通知を抑制する時間を 0 秒に設定します。

```
[DeviceE] interface gigabitethernet 1/0/1
[DeviceE-GigabitEthernet1/0/1] link-delay 0
```

ポートでスパニングツリー機能を無効にします。

```
[DeviceE-GigabitEthernet1/0/1] undo stp enable
```

ポートをトランクポートに設定します。

```
[DeviceE-GigabitEthernet1/0/1] port link-type trunk
```

VLAN 1～VLAN 30 にポートを割り当てます。

```
[DeviceE-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceE-GigabitEthernet1/0/1] quit
```

GigabitEthernet 1/0/1 の設定と同様に GigabitEthernet 1/0/2 を設定します。

```
[DeviceE] interface gigabitethernet 1/0/2
[DeviceE-GigabitEthernet1/0/2] link-delay 0
[DeviceE-GigabitEthernet1/0/2] undo stp enable
[DeviceE-GigabitEthernet1/0/2] port link-type trunk
[DeviceE-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
[DeviceE-GigabitEthernet1/0/2] quit
```

RRPP ドメイン 1 を作成します。

```
[DeviceE] rrpp domain 1
```

RRPP ドメイン 1 のプライマリコントロール VLAN として VLAN 4092 を設定します。

```
[DeviceE-rrpp-domain1] control-vlan 4092
```

RRPP ドメイン 1 のプロテクト VLAN として MSTI 1 にマッピングした VLAN を設定します。

```
[DeviceE-rrpp-domain1] protected-vlan reference-instance 1
```

サブリング 2 のマスタノードとして Device E を設定します。プライマリポートを GigabitEthernet 1/0/1、セカンダリポートを GigabitEthernet 1/0/2 に設定します。サブリング 2 を有効にします。

```
[DeviceE-rrpp-domain1] ring 2 node-mode master primary-port gigabitethernet 1/0/1 secondary-port gigabitethernet 1/0/2 level 1
[DeviceE-rrpp-domain1] ring 2 enable
[DeviceE-rrpp-domain1] quit
```

RRPP を有効にします。

```
[DeviceE] rrpp enable
```

III. 設定の確認

display コマンドを使用し、各 Device の RRPP 設定と動作情報を表示します。

4.12.3 デュアルホームリングの設定例

I. ネットワーク要件

- Device A～Device H は RRPP ドメイン 1 を構成します。VLAN4092 を RRPP ドメイン 1 のプライマリコントロール VLAN に指定します。RRPP ドメイン 1 のプロテクト VLAN に VLAN1～VLAN 30 を設定します。
- Device A～Device D はプライマリリング 1 を構成します。Device A、Device B、Device E はサブリング 2 を構成します。Device A、Device B、Device F はサブリング 3 を構成します。Device C、Device D、Device G はサブリング 4 を構成します。Device C、Device D、Device H はサブリング 5 を構成します。
- Device A、Device E、Device F、Device G、Device H をそれぞれ Ring 1、Ring 2、Ring 3、Ring 4、Ring 5 のマスタノードに指定します。リングの GigabitEthernet 1/0/1 をプライマリポート、GigabitEthernet 1/0/2 をセカンダリポートに指定します。
- 接続されたサブリングのエッジノードとして Device A を指定します。GigabitEthernet 1/0/3、GigabitEthernet 1/0/4 をエッジポートに指定します。プライマリリングのトランジットノードと接続されたサブリングのエッジノードとして Device D を指定します。GigabitEthernet 1/0/3、GigabitEthernet 1/0/4 をエッジポートに指定します。プライマリリングのトランジットノードと接続されたサブリングのアシスタントエッジノードとして Device B、Device C を指定します。GigabitEthernet 1/0/3、GigabitEthernet 1/0/4 をエッジポートに指定します。

重要：

プロテクト VLAN がポートによって否定されるときに、他のプロトコルがまだ正しく動作するのを確かめるために、マスタノードの上の主要で、第 2 のポートを正しく設定してください。

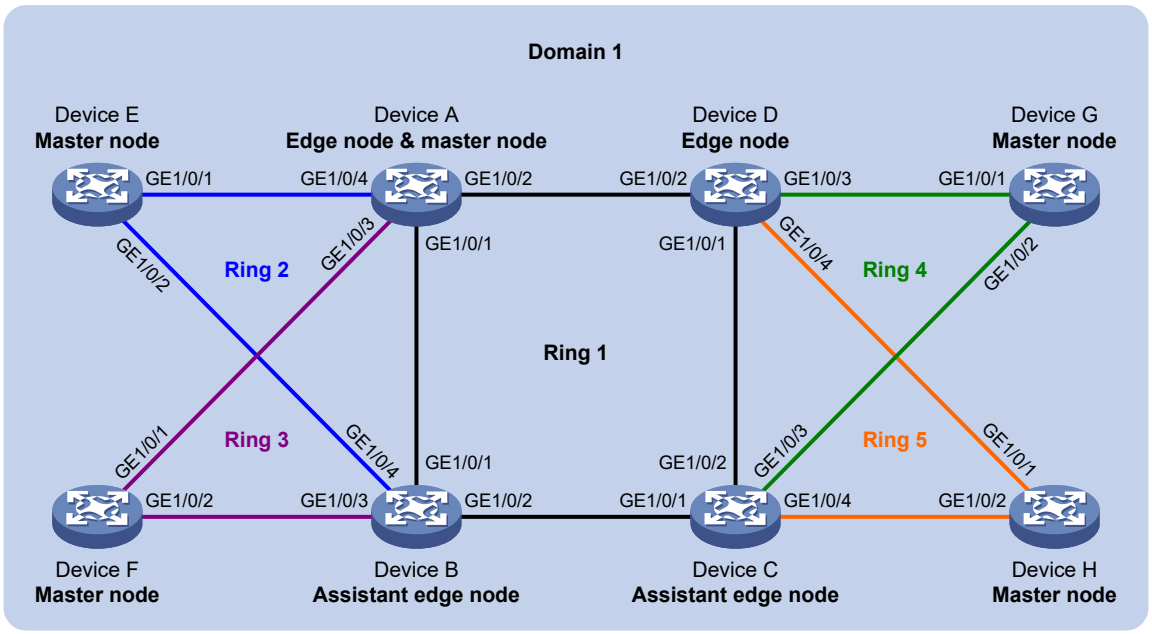


図 4-10 ネットワーク図

II. 設定手順

1)　Device A を設定します。

VLAN 1～VLAN 30 を作成します。

```
<DeviceA> system-view
[DeviceA] vlan 1 to 30
```

MSTI インスタンス 1 に VLAN をマッピングします。

```
[DeviceA] stp region-configuration
[DeviceA-mst-region] instance 1 vlan 1 to 30
```

MST region の設定を有効にします。

```
[DeviceA-mst-region] active region-configuration
[DeviceA-mst-region] quit
```

物理状態の変更があった場合、GigabitEthernet 1/0/1 のリンクダウンの通知を抑制する時間を 0 秒に設定します。

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] link-delay 0
```

ポートでスパニングツリー機能を無効にします。

```
[DeviceA-GigabitEthernet1/0/1] undo stp enable
```

ポートをトランクポートに設定します。

```
[DeviceA-GigabitEthernet1/0/1] port link-type trunk
```

VLAN 1～VLAN 30 にポートを割り当てます。

```
[DeviceA-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceA-GigabitEthernet1/0/1] quit
```

GigabitEthernet 1/0/1 の設定と同様に GigabitEthernet 1/0/2 を設定します。

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] link-delay 0
[DeviceA-GigabitEthernet1/0/2] undo stp enable
[DeviceA-GigabitEthernet1/0/2] port link-type trunk
[DeviceA-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
[DeviceA-GigabitEthernet1/0/2] quit
```

GigabitEthernet 1/0/1 の設定と同様に GigabitEthernet 1/0/3 を設定します。

```
[DeviceA] interface gigabitethernet 1/0/3
[DeviceA-GigabitEthernet1/0/3] link-delay 0
[DeviceA-GigabitEthernet1/0/3] undo stp enable
[DeviceA-GigabitEthernet1/0/3] port link-type trunk
[DeviceA-GigabitEthernet1/0/3] port trunk permit vlan 1 to 30
[DeviceA-GigabitEthernet1/0/3] quit
```

GigabitEthernet 1/0/1 の設定と同様に GigabitEthernet 1/0/4 を設定します。

```
[DeviceA] interface gigabitethernet 1/0/4
[DeviceA-GigabitEthernet1/0/4] link-delay 0
[DeviceA-GigabitEthernet1/0/4] undo stp enable
[DeviceA-GigabitEthernet1/0/4] port link-type trunk
[DeviceA-GigabitEthernet1/0/4] port trunk permit vlan 1 to 30
[DeviceA-GigabitEthernet1/0/4] quit
```

RRPP ドメイン 1 を作成します。

```
[DeviceA] rrpp domain 1
```

RRPP ドメイン 1 のプライマリコントロール VLAN として VLAN 4092 を設定します。

```
[DeviceA-rrpp-domain1] control-vlan 4092
```

RRPP ドメイン 1 のプロテクト VLAN として MSTI 1 にマッピングした VLAN を設定します。

```
[DeviceA-rrpp-domain1] protected-vlan reference-instance 1
```

プライマリリング 1 のマスタノードとして Device A を設定します。プライマリポートを GigabitEthernet 1/0/1、セカンダリポートを GigabitEthernet 1/0/2 に設定します。リング 1 を有効にします。

```
[DeviceA-rrpp-domain1] ring 1 node-mode master primary-port gigabitethernet 1/0/1 secondary-port gigabitethernet 1/0/2 level 0
[DeviceA-rrpp-domain1] ring 1 enable
```

サブリング 2 のエッジノードとして Device A を設定します。エッジポートを GigabitEthernet 1/0/4 に設定します。サブリング 2 を有効にします。

```
[DeviceA-rrpp-domain1] ring 2 node-mode edge edge-port gigabitethernet 1/0/4
[DeviceA-rrpp-domain1] ring 2 enable
```

サブリング 3 のエッジノードとして Device A を設定します。エッジポートを GigabitEthernet 1/0/3 に設定します。サブリング 3 を有効にします。

```
[DeviceA-rrpp-domain1] ring 3 node-mode edge edge-port gigabitethernet 1/0/3
[DeviceA-rrpp-domain1] ring 3 enable
[DeviceA-rrpp-domain1] quit
```

RRPP を有効にします。

```
[DeviceA] rrpp enable
```

2) Device B を設定します。

VLAN 1～VLAN 30 を作成します。

```
<DeviceB> system-view
[DeviceB] vlan 1 to 30
```

MSTI インスタンス 1 に VLAN をマッピングします。

```
[DeviceB] stp region-configuration
[DeviceB-mst-region] instance 1 vlan 1 to 30
```

MST region の設定を有効にします。

```
[DeviceB-mst-region] active region-configuration
[DeviceB-mst-region] quit
```

物理状態の変更があった場合、GigabitEthernet 1/0/1 のリンクダウンの通知を抑制する時間を 0 秒に設定します。

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] link-delay 0
```

ポートでスパニングツリー機能を無効にします。

```
[DeviceB-GigabitEthernet1/0/1] undo stp enable
```

ポートをトランクポートに設定します。

```
[DeviceB-GigabitEthernet1/0/1] port link-type trunk
```

VLAN 1～VLAN 30 にポートを割り当てます。

```
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceB-GigabitEthernet1/0/1] quit
```

GigabitEthernet 1/0/1 の設定と同様に GigabitEthernet 1/0/2 を設定します。

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] link-delay 0
[DeviceB-GigabitEthernet1/0/2] undo stp enable
[DeviceB-GigabitEthernet1/0/2] port link-type trunk
[DeviceB-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
[DeviceB-GigabitEthernet1/0/2] quit
```

GigabitEthernet 1/0/1 の設定と同様に GigabitEthernet 1/0/3 を設定します。

```
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] link-delay 0
[DeviceB-GigabitEthernet1/0/3] undo stp enable
[DeviceB-GigabitEthernet1/0/3] port link-type trunk
[DeviceB-GigabitEthernet1/0/3] port trunk permit vlan 1 to 30
[DeviceB-GigabitEthernet1/0/3] quit
```

GigabitEthernet 1/0/1 の設定と同様に GigabitEthernet 1/0/4 を設定します。

```
[DeviceB] interface gigabitethernet 1/0/4
[DeviceB-GigabitEthernet1/0/4] link-delay 0
[DeviceB-GigabitEthernet1/0/4] undo stp enable
[DeviceB-GigabitEthernet1/0/4] port link-type trunk
[DeviceB-GigabitEthernet1/0/4] port trunk permit vlan 1 to 30
[DeviceB-GigabitEthernet1/0/4] quit
```

RRPP ドメイン 1 を作成します。

```
[DeviceB] rrpp domain 1
```

RRPP ドメイン 1 のプライマリコントロール VLAN として VLAN 4092 を設定します。

```
[DeviceB-rrpp-domain1] control-vlan 4092
```

RRPP ドメイン 1 のプロテクト VLAN として MSTI 1 にマッピングした VLAN を設定します。

```
[DeviceB-rrpp-domain1] protected-vlan reference-instance 1
```

プライマリリング 1 のトランジットノードとして Device B を設定します。プライマリポートを GigabitEthernet 1/0/1、セカンダリポートを GigabitEthernet 1/0/2 に設定します。リング 1 を有効にします。

```
[DeviceB-rrpp-domain1] ring 1 node-mode transit primary-port gigabitethernet 1/0/1 secondary-port gigabitethernet 1/0/2 level 0
[DeviceB-rrpp-domain1] ring 1 enable
```

サブリング 2 のアシスタントエッジノードとして Device B を設定します。エッジポートを GigabitEthernet 1/0/4 に設定します。サブリング 2 を有効にします。

```
[DeviceB-rrpp-domain1] ring 2 node-mode assistant-edge edge-port gigabitethernet 1/0/4
[DeviceB-rrpp-domain1] ring 2 enable
```

サブリング 3 のアシスタントエッジノードとして Device B を設定します。エッジポートを GigabitEthernet 1/0/3 に設定します。サブリング 3 を有効にします。

```
[DeviceB-rrpp-domain1] ring 3 node-mode assistant-edge edge-port gigabitethernet 1/0/3
[DeviceB-rrpp-domain1] ring 3 enable
[DeviceB-rrpp-domain1] quit
```

RRPP を有効にします。

```
[DeviceB] rrpp enable
```

3) Device C を設定します。

VLAN 1～VLAN 30 を作成します。

```
<DeviceC> system-view
[DeviceC] vlan 1 to 30
```

MSTI インスタンス 1 に VLAN をマッピングします。

```
[DeviceC] stp region-configuration
[DeviceC-mst-region] instance 1 vlan 1 to 30
```

MST region の設定を有効にします。

```
[DeviceC-mst-region] active region-configuration
[DeviceC-mst-region] quit
```

物理状態の変更があった場合、GigabitEthernet 1/0/1 のリンクダウンの通知を抑制する時間を 0 秒に設定します。

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] link-delay 0
```

ポートでスパニングツリー機能を無効にします。

```
[DeviceC-GigabitEthernet1/0/1] undo stp enable
```

ポートをトランクポートに設定します。

```
[DeviceC-GigabitEthernet1/0/1] port link-type trunk
```

VLAN 1～VLAN 30 にポートを割り当てます。

```
[DeviceC-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
```

```
[DeviceC-GigabitEthernet1/0/1] quit
```

GigabitEthernet 1/0/1 の設定と同様に GigabitEthernet 1/0/2 を設定します。

```
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] link-delay 0
[DeviceC-GigabitEthernet1/0/2] undo stp enable
[DeviceC-GigabitEthernet1/0/2] port link-type trunk
[DeviceC-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
[DeviceC-GigabitEthernet1/0/2] quit
```

GigabitEthernet 1/0/1 の設定と同様に GigabitEthernet 1/0/3 を設定します。

```
[DeviceC] interface gigabitethernet 1/0/3
[DeviceC-GigabitEthernet1/0/3] link-delay 0
[DeviceC-GigabitEthernet1/0/3] undo stp enable
[DeviceC-GigabitEthernet1/0/3] port link-type trunk
[DeviceC-GigabitEthernet1/0/3] port trunk permit vlan 1 to 30
[DeviceC-GigabitEthernet1/0/3] quit
```

GigabitEthernet 1/0/1 の設定と同様に GigabitEthernet 1/0/4 を設定します。

```
[DeviceC] interface gigabitethernet 1/0/4
[DeviceC-GigabitEthernet1/0/4] link-delay 0
[DeviceC-GigabitEthernet1/0/4] undo stp enable
[DeviceC-GigabitEthernet1/0/4] port link-type trunk
[DeviceC-GigabitEthernet1/0/4] port trunk permit vlan 1 to 30
[DeviceC-GigabitEthernet1/0/4] quit
```

RRPP ドメイン 1 を作成します。

```
[DeviceC] rrpp domain 1
```

RRPP ドメイン 1 のプライマリコントロール VLAN として VLAN 4092 を設定します。

```
[DeviceC-rrpp-domain1] control-vlan 4092
```

RRPP ドメイン 1 のプロテクト VLAN として MSTI 1 にマッピングした VLAN を設定します。

```
[DeviceC-rrpp-domain1] protected-vlan reference-instance 1
```

プライマリリング 1 のトランジットノードとして Device C を設定します。プライマリポートを GigabitEthernet 1/0/1、セカンダリポートを GigabitEthernet 1/0/2 に設定します。リング 1 を有効にします。

```
[DeviceC-rrpp-domain1] ring 1 node-mode transit primary-port gigabitethernet 1/0/1 secondary-port gigabitethernet 1/0/2 level 0
```

```
[DeviceC-rrpp-domain1] ring 1 enable
```

サブリング 4 のアシスタントエッジノードとして Device C を設定します。エッジポートを GigabitEthernet 1/0/3 に設定します。サブリング 4 を有効にします。

```
[DeviceC-rrpp-domain1] ring 4 node-mode assistant-edge edge-port gigabitethernet 1/0/3
[DeviceC-rrpp-domain1] ring 4 enable
```

サブリング 5 のアシスタントエッジノードとして Device C を設定します。エッジポートを GigabitEthernet 1/0/4 に設定します。サブリング 5 を有効にします。

```
[DeviceC-rrpp-domain1] ring 5 node-mode assistant-edge edge-port gigabitethernet 1/0/4
[DeviceC-rrpp-domain1] ring 5 enable
[DeviceC-rrpp-domain1] quit
```

RRPP を有効にします。

```
[DeviceC] rrpp enable
```

4)　Device D を設定します。

VLAN 1～VLAN 30 を作成します。

```
<DeviceD> system-view
[DeviceD] vlan 1 to 30
```

MSTI インスタンス 1 に VLAN をマッピングします。

```
[DeviceD] stp region-configuration
[DeviceD-mst-region] instance 1 vlan 1 to 30
```

MST region の設定を有効にします。

```
[DeviceD-mst-region] active region-configuration
[DeviceD-mst-region] quit
```

物理状態の変更があった場合、GigabitEthernet 1/0/1 のリンクダウンの通知を抑制する時間を 0 秒に設定します。

```
[DeviceD] interface gigabitethernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] link-delay 0
```

ポートでスパニングツリー機能を無効にします。

```
[DeviceD-GigabitEthernet1/0/1] undo stp enable
```

ポートをトランクポートに設定します。

```
[DeviceD-GigabitEthernet1/0/1] port link-type trunk
```

VLAN 1～VLAN 30 にポートを割り当てます。

```
[DeviceD-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceD-GigabitEthernet1/0/1] quit
```

GigabitEthernet 1/0/1 の設定と同様に GigabitEthernet 1/0/2 を設定します。

```
[DeviceD] interface gigabitethernet 1/0/2
[DeviceD-GigabitEthernet1/0/2] link-delay 0
[DeviceD-GigabitEthernet1/0/2] undo stp enable
[DeviceD-GigabitEthernet1/0/2] port link-type trunk
[DeviceD-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
[DeviceD-GigabitEthernet1/0/2] quit
```

GigabitEthernet 1/0/1 の設定と同様に GigabitEthernet 1/0/3 を設定します。

```
[DeviceD] interface gigabitethernet 1/0/3
[DeviceD-GigabitEthernet1/0/3] link-delay 0
[DeviceD-GigabitEthernet1/0/3] undo stp enable
[DeviceD-GigabitEthernet1/0/3] port link-type trunk
[DeviceD-GigabitEthernet1/0/3] port trunk permit vlan 1 to 30
[DeviceD-GigabitEthernet1/0/3] quit
```

GigabitEthernet 1/0/1 の設定と同様に GigabitEthernet 1/0/4 を設定します。

```
[DeviceD] interface gigabitethernet 1/0/4
[DeviceD-GigabitEthernet1/0/4] link-delay 0
[DeviceD-GigabitEthernet1/0/4] undo stp enable
[DeviceD-GigabitEthernet1/0/4] port link-type trunk
[DeviceD-GigabitEthernet1/0/4] port trunk permit vlan 1 to 30
[DeviceD-GigabitEthernet1/0/4] quit
```

RRPP ドメイン 1 を作成します。

```
[DeviceD] rrpp domain 1
```

RRPP ドメイン 1 のプライマリコントロール VLAN として VLAN 4092 を設定します。

```
[DeviceD-rrpp-domain1] control-vlan 4092
```

RRPP ドメイン 1 のプロテクト VLAN として MSTI 1 にマッピングした VLAN を設定します。

```
[DeviceD-rrpp-domain1] protected-vlan reference-instance 1
```

プライマリリング 1 のトランジットノードとして Device D を設定します。プライマリポートを GigabitEthernet 1/0/1、セカンダリポートを GigabitEthernet 1/0/2 に設定します。リング 1 を有効にします。

```
[DeviceD-rrpp-domain1] ring 1 node-mode transit primary-port gigabitethernet 1/0/1 secondary-port gigabitethernet 1/0/2 level 0
[DeviceD-rrpp-domain1] ring 1 enable
```

サブリング 4 のエッジノードとして Device D を設定します。エッジポートを GigabitEthernet 1/0/3 に設定します。サブリング 4 を有効にします。

```
[DeviceD-rrpp-domain1] ring 4 node-mode edge edge-port gigabitethernet 1/0/3
[DeviceD-rrpp-domain1] ring 4 enable
```

サブリング 5 のエッジノードとして Device D を設定します。エッジポートを GigabitEthernet 1/0/4 に設定します。サブリング 5 を有効にします。

```
[DeviceD-rrpp-domain1] ring 5 node-mode edge edge-port gigabitethernet 1/0/4
[DeviceD-rrpp-domain1] ring 5 enable
[DeviceD-rrpp-domain1] quit
```

RRPP を有効にします。

```
[DeviceD] rrpp enable
```

5) Device E を設定します。

VLAN 1～VLAN 30 を作成します。

```
<DeviceE> system-view
[DeviceE] vlan 1 to 30
```

MSTI インスタンス 1 に VLAN をマッピングします。

```
[DeviceE] stp region-configuration
[DeviceE-mst-region] instance 1 vlan 1 to 30
```

MST region の設定を有効にします。

```
[DeviceE-mst-region] active region-configuration
[DeviceE-mst-region] quit
```

物理状態の変更があった場合、GigabitEthernet 1/0/1 のリンクダウンの通知を抑制する時間を 0 秒に設定します。

```
[DeviceE] interface gigabitethernet 1/0/1
[DeviceE-GigabitEthernet1/0/1] link-delay 0
```

ポートでスパニングツリー機能を無効にします。

```
[DeviceE-GigabitEthernet1/0/1] undo stp enable
```

ポートをトランクポートに設定します。

```
[DeviceE-GigabitEthernet1/0/1] port link-type trunk
```

VLAN 1～VLAN 30 にポートを割り当てます。

```
[DeviceE-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceE-GigabitEthernet1/0/1] quit
```

GigabitEthernet 1/0/1 の設定と同様に GigabitEthernet 1/0/2 を設定します。

```
[DeviceE] interface gigabitethernet 1/0/2
[DeviceE-GigabitEthernet1/0/2] link-delay 0
[DeviceE-GigabitEthernet1/0/2] undo stp enable
```

```
[DeviceE-GigabitEthernet1/0/2] port link-type trunk
[DeviceE-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
[DeviceE-GigabitEthernet1/0/2] quit
```

RRPP ドメイン 1 を作成します。

```
[DeviceE] rrpp domain 1
```

RRPP ドメイン 1 のプライマリコントロール VLAN として VLAN 4092 を設定します。

```
[DeviceE-rrpp-domain1] control-vlan 4092
```

RRPP ドメイン 1 のプロテクト VLAN として MSTI 1 にマッピングした VLAN を設定します。

```
[DeviceE-rrpp-domain1] protected-vlan reference-instance 1
```

サブリング 2 のマスタノードとして Device E を設定します。プライマリポートを GigabitEthernet 1/0/1、セカンダリポートを GigabitEthernet 1/0/2 に設定します。サブリング 2 を有効にします。

```
[DeviceE-rrpp-domain1] ring 2 node-mode master primary-port gigabitethernet 1/0/1 secondary-port gigabitethernet 1/0/2 level 1
[DeviceE-rrpp-domain1] ring 2 enable
[DeviceE-rrpp-domain1] quit
```

RRPP を有効にします。

```
[DeviceE] rrpp enable
```

6) Device F を設定します。

VLAN 1～VLAN 30 を作成します。

```
<DeviceF> system-view
[DeviceF] vlan 1 to 30
```

MSTI インスタンス 1 に VLAN をマッピングします。

```
[DeviceF] stp region-configuration
[DeviceF-mst-region] instance 1 vlan 1 to 30
```

MST region の設定を有効にします。

```
[DeviceF-mst-region] active region-configuration
[DeviceF-mst-region] quit
```

物理状態の変更があった場合、GigabitEthernet 1/0/1 のリンクダウンの通知を抑制する時間を 0 秒に設定します。

```
[DeviceF] interface gigabitethernet 1/0/1
[DeviceF-GigabitEthernet1/0/1] link-delay 0
```

ポートでスパニングツリー機能を無効にします。

```
[DeviceF-GigabitEthernet1/0/1] undo stp enable
```

ポートをトランクポートに設定します。

```
[DeviceF-GigabitEthernet1/0/1] port link-type trunk
```

VLAN 1～VLAN 30 にポートを割り当てます。

```
[DeviceF-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceF-GigabitEthernet1/0/1] quit
```

GigabitEthernet 1/0/1 の設定と同様に GigabitEthernet 1/0/2 を設定します。

```
[DeviceF] interface gigabitethernet 1/0/2
[DeviceF-GigabitEthernet1/0/2] link-delay 0
[DeviceF-GigabitEthernet1/0/2] undo stp enable
[DeviceF-GigabitEthernet1/0/2] port link-type trunk
[DeviceF-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
[DeviceF-GigabitEthernet1/0/2] quit
```

RRPP ドメイン 1 を作成します。

```
[DeviceF] rrpp domain 1
```

RRPP ドメイン 1 のプライマリコントロール VLAN として VLAN 4092 を設定します。

```
[DeviceF-rrpp-domain1] control-vlan 4092
```

RRPP ドメイン 1 のプロテクト VLAN として MSTI 1 にマッピングした VLAN を設定します。

```
[DeviceF-rrpp-domain1] protected-vlan reference-instance 1
```

サブリング 3 のマスタノードとして Device F を設定します。プライマリポートを GigabitEthernet 1/0/1、セカンダリポートを GigabitEthernet 1/0/2 に設定します。サブリング 3 を有効にします。

```
[DeviceF-rrpp-domain1] ring 3 node-mode master primary-port gigabitethernet 1/0/1 secondary-port gigabitethernet 1/0/2 level 1
[DeviceF-rrpp-domain1] ring 3 enable
[DeviceF-rrpp-domain1] quit
```

RRPP を有効にします。

```
[DeviceF] rrpp enable
```

7) Device G を設定します。

VLAN 1～VLAN 30 を作成します。

```
<DeviceG> system-view
[DeviceG] vlan 1 to 30
```

MSTI 1 に VLAN をマッピングします。

```
[DeviceG] stp region-configuration
[DeviceG-mst-region] instance 1 vlan 1 to 30
```

MST region の設定を有効にします。

```
[DeviceG-mst-region] active region-configuration
[DeviceG-mst-region] quit
```

物理状態の変更があった場合、GigabitEthernet 1/0/1 のリンクダウンの通知を抑制する時間を 0 秒に設定します。

```
[DeviceG] interface gigabitethernet 1/0/1
[DeviceG-GigabitEthernet1/0/1] link-delay 0
```

ポートでスパニングツリー機能を無効にします。

```
[DeviceG-GigabitEthernet1/0/1] undo stp enable
```

ポートをトランクポートに設定します。

```
[DeviceG-GigabitEthernet1/0/1] port link-type trunk
```

VLAN 1～VLAN 30 にポートを割り当てます。

```
[DeviceG-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceG-GigabitEthernet1/0/1] quit
```

GigabitEthernet 1/0/1 の設定と同様に GigabitEthernet 1/0/2 を設定します。

```
[DeviceG] interface gigabitethernet 1/0/2
[DeviceG-GigabitEthernet1/0/2] link-delay 0
[DeviceG-GigabitEthernet1/0/2] undo stp enable
[DeviceG-GigabitEthernet1/0/2] port link-type trunk
[DeviceG-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
[DeviceG-GigabitEthernet1/0/2] quit
```

RRPP ドメイン 1 を作成します。

```
[DeviceG] rrpp domain 1
```

RRPP ドメイン 1 のプライマリコントロール VLAN として VLAN 4092 を設定します。

```
[DeviceG-rrpp-domain1] control-vlan 4092
```

RRPP ドメイン 1 のプロテクト VLAN として MSTI 1 にマッピングした VLAN を設定します。

```
[DeviceG-rrpp-domain1] protected-vlan reference-instance 1
```

サブリング 4 のマスタノードとして Device G を設定します。プライマリポートを GigabitEthernet 1/0/1、セカンダリポートを GigabitEthernet 1/0/2 に設定します。サブリング 4 を有効にします。

```
[DeviceG-rrpp-domain1] ring 4 node-mode master primary-port gigabitethernet 1/0/1 secondary-port gigabitethernet 1/0/2 level 1
[DeviceG-rrpp-domain1] ring 4 enable
[DeviceG-rrpp-domain1] quit
```

RRPP を有効にします。

```
[DeviceG] rrpp enable
```

8) Device H を設定します。

VLAN 1～VLAN 30 を作成します。

```
<DeviceH> system-view
[DeviceH] vlan 1 to 30
```

MSTI 1 に VLAN をマッピングします。

```
[DeviceH] stp region-configuration
[DeviceH-mst-region] instance 1 vlan 1 to 30
```

MST region の設定を有効にします。

```
[DeviceH-mst-region] active region-configuration
[DeviceH-mst-region] quit
```

物理状態の変更があった場合、GigabitEthernet 1/0/1 のリンクダウンの通知を抑制する時間を 0 秒に設定します。

```
[DeviceH] interface gigabitethernet 1/0/1
[DeviceH-GigabitEthernet1/0/1] link-delay 0
```

ポートでスパニングツリー機能を無効にします。

```
[DeviceH-GigabitEthernet1/0/1] undo stp enable
```

ポートをトランクポートに設定します。

```
[DeviceH-GigabitEthernet1/0/1] port link-type trunk
```

VLAN 1～VLAN 30 にポートを割り当てます。

```
[DeviceH-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceH-GigabitEthernet1/0/1] quit
```

GigabitEthernet 1/0/1 の設定と同様に GigabitEthernet 1/0/2 を設定します。

```
[DeviceH] interface gigabitethernet 1/0/2
[DeviceH-GigabitEthernet1/0/2] link-delay 0
[DeviceH-GigabitEthernet1/0/2] undo stp enable
[DeviceH-GigabitEthernet1/0/2] port link-type trunk
[DeviceH-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
[DeviceH-GigabitEthernet1/0/2] quit
```

RRPP ドメイン 1 を作成します。

```
[DeviceH] rrpp domain 1
```

RRPP ドメイン 1 のプライマリコントロール VLAN として VLAN 4092 を設定します。

```
[DeviceH-rrpp-domain1] control-vlan 4092
```

RRPP ドメイン 1 のプロテクト VLAN として MSTI 1 にマッピングした VLAN を設定します。

```
[DeviceH-rrpp-domain1] protected-vlan reference-instance 1
```

サブリング 5 のマスタノードとして Device H を設定します。プライマリポートを GigabitEthernet 1/0/1、セカンダリポートを GigabitEthernet 1/0/2 に設定します。サブリング 5 を有効にします。

```
[DeviceH-rrpp-domain1] ring 5 node-mode master primary-port gigabitethernet 1/0/1 secondary-port gigabitethernet 1/0/2 level 1
[DeviceH-rrpp-domain1] ring 5 enable
[DeviceH-rrpp-domain1] quit
```

RRPP を有効にします。

```
[DeviceH] rrpp enable
```

III. 設定の確認

display コマンドを使用し、各 Device の RRPP 設定と動作情報を表示します。

4.12.4 交差リング（Intersecting リング、マルチリング）ロードバランシングの設定例

I. ネットワーク要件

- Device A、Device B、Device C、Device D、Device F は RRPP ドメイン 1 を構成します。VLAN 100 を RRPP ドメイン 1 のプライマリコントロール VLAN に指定します。Device A はプライマリリング Ring 1 のマスタノードです。Device D はプライマリリング Ring 1 のトランジットノードです。Device F はサブリング Ring 3 のマスタノードです。Device C はサブリング Ring 3 のエッジノードです。Device B はサブリング Ring 3 のアシスタントエッジノードです。
- Device A、Device B、Device C、Device D、Device E は RRPP ドメイン 2 を構成します。VLAN 105 を RRPP ドメイン 2 のプライマリコントロール VLAN に指定します。Device A はプライマリリング Ring 1 のマスタノードです。Device D はプライマリリング Ring 1 のトランジットノードです。Device E はサブリング Ring 2 のマスタノードです。Device C はサブリング Ring 2 のエッジノードです。Device B はサブリング Ring 2 のアシスタントエッジノードです。
- RRPP ドメイン 1 のプロテクト VLAN に VLAN11 を設定します。RRPP ドメイン 2 のプロテクト VLAN に VLAN12 を設定します。リング Ring1 で VLAN ベースのロードバランシングを行います。
- Ring 2、Ring 3 は同一エッジノードと同一アシスタントエッジノードを持ちます。2 つのサブリングは同じ SRPT を持ちます。Edge-Hello トラフィックを削減させるため、RRPP リンググループに Ring 2、Ring 3 を追加します。

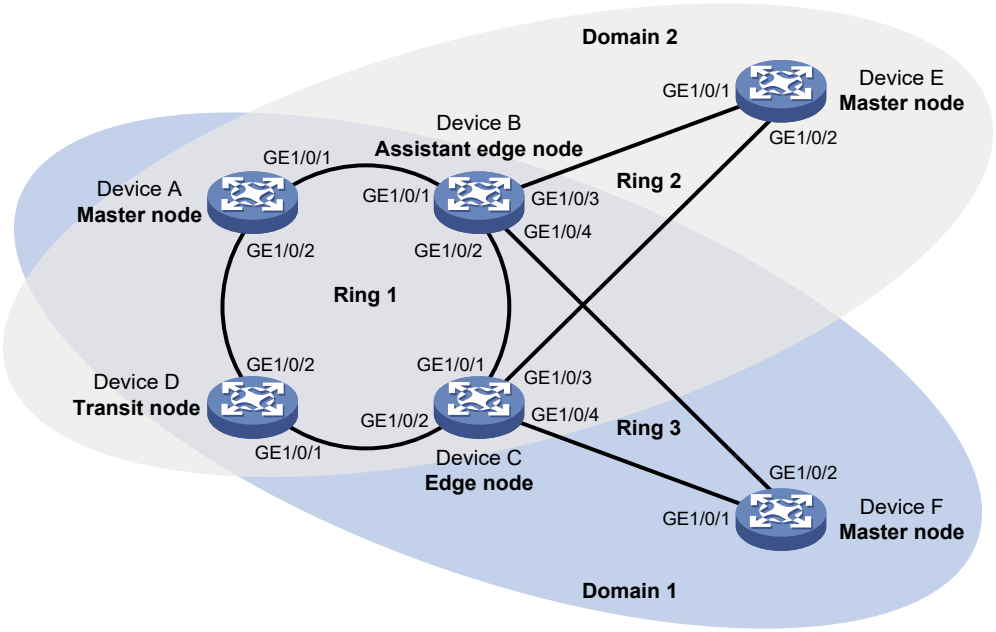


図 4-11 ネットワーク図

II. 設定手順

1)　Device A を設定します。

VLAN 11、VLAN 12 を作成します。

```
<DeviceA> system-view
[DeviceA] vlan 11 to 12
```

MSTI 1 に VLAN 11、MSTI 2 に VLAN 12 をマッピングします。

```
[DeviceA] stp region-configuration
[DeviceA-mst-region] instance 1 vlan 11
[DeviceA-mst-region] instance 2 vlan 12
```

MST region の設定を有効にします。

```
[DeviceA-mst-region] active region-configuration
[DeviceA-mst-region] quit
```

物理状態の変更があった場合、GigabitEthernet 1/0/1 のリンクダウンの通知を抑制する時間を 0 秒に設定します。

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] link-delay 0
```

ポートでスパニングツリー機能を無効にします。

```
[DeviceA-GigabitEthernet1/0/1] undo stp enable
```

ポートをトランクポートに設定します。

```
[DeviceA-GigabitEthernet1/0/1] port link-type trunk
```

VLAN 1 からポートを削除し、VLAN 11、VLAN 12 に削除したポートを割り当てます。

```
[DeviceA-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[DeviceA-GigabitEthernet1/0/1] port trunk permit vlan 11 12
```

デフォルト VLAN として VLAN 11 を設定します。

```
[DeviceA-GigabitEthernet1/0/1] port trunk pvid vlan 11
[DeviceA-GigabitEthernet1/0/1] quit
```

GigabitEthernet 1/0/1 の設定と同様に GigabitEthernet 1/0/2 を設定します。

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] link-delay 0
[DeviceA-GigabitEthernet1/0/2] undo stp enable
[DeviceA-GigabitEthernet1/0/2] port link-type trunk
[DeviceA-GigabitEthernet1/0/2] undo port trunk permit vlan 1
[DeviceA-GigabitEthernet1/0/2] port trunk permit vlan 11 12
[DeviceA-GigabitEthernet1/0/2] port trunk pvid vlan 11
[DeviceA-GigabitEthernet1/0/2] quit
```

RRPP ドメイン 1 を作成します。

```
[DeviceA] rrpp domain 1
```

RRPP ドメイン 1 のプライマリコントロール VLAN として VLAN 100 を設定します。

```
[DeviceA-rrpp-domain1] control-vlan 100
```

RRPP ドメイン 1 のプロテクト VLAN として MSTI 1 にマッピングした VLAN を設定します。

```
[DeviceA-rrpp-domain1] protected-vlan reference-instance 1
```

プライマリリング 1 のマスタノードとして Device A を設定します。プライマリポートを GigabitEthernet 1/0/1、セカンダリポートを GigabitEthernet 1/0/2 に設定します。リング 1 を有効にします。

```
[DeviceA-rrpp-domain1] ring 1 node-mode master primary-port gigabitethernet 1/0/1 secondary-port gigabitethernet 1/0/2 level 0
[DeviceA-rrpp-domain1] ring 1 enable
[DeviceA-rrpp-domain1] quit
```

RRPP ドメイン 2 を作成します。

```
[DeviceA] rrpp domain 2
```

RRPP ドメイン 2 のプライマリコントロール VLAN として VLAN 105 を設定します。

```
[DeviceA-rrpp-domain2] control-vlan 105
```

RRPP ドメイン 2 のプロテクト VLAN として MSTI 2 にマッピングした VLAN を設定します。

```
[DeviceA-rrpp-domain2] protected-vlan reference-instance 2
```

プライマリリング 1 のマスタノードとして Device A を設定します。プライマリポートを GigabitEthernet 1/0/2、セカンダリポートを GigabitEthernet 1/0/1 に設定します。リング 1 を有効にします。

```
[DeviceA-rrpp-domain2] ring 1 node-mode master primary-port gigabitethernet 1/0/2 secondary-port gigabitethernet 1/0/1 level 0
[DeviceA-rrpp-domain2] ring 1 enable
[DeviceA-rrpp-domain2] quit
```

RRPP を有効にします。

```
[DeviceA] rrpp enable
```

2) Device B を設定します。

VLAN 11、VLAN 12 を作成します。

```
<DeviceB> system-view
[DeviceB] vlan 11 to 12
```

MSTI 1 に VLAN 11、MSTI 2 に VLAN 12 をマッピングします。

```
[DeviceB] stp region-configuration
[DeviceB-mst-region] instance 1 vlan 11
[DeviceB-mst-region] instance 2 vlan 12
```

MST region の設定を有効にします。

```
[DeviceB-mst-region] active region-configuration
[DeviceB-mst-region] quit
```

物理状態の変更があった場合、GigabitEthernet 1/0/1 のリンクダウンの通知を抑制する時間を 0 秒に設定します。

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] link-delay 0
```

ポートでスパニングツリー機能を無効にします。

```
[DeviceB-GigabitEthernet1/0/1] undo stp enable
```

ポートをトランクポートに設定します。

```
[DeviceB-GigabitEthernet1/0/1] port link-type trunk
```

VLAN 1 からポートを削除し、VLAN 11、VLAN 12 に削除したポートを割り当てます。

```
[DeviceB-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 11 12
```

デフォルト VLAN として VLAN 11 を設定します。

```
[DeviceB-GigabitEthernet1/0/1] port trunk pvid vlan 11
[DeviceB-GigabitEthernet1/0/1] quit
```

GigabitEthernet 1/0/1 の設定と同様に GigabitEthernet 1/0/2 を設定します。

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] link-delay 0
[DeviceB-GigabitEthernet1/0/2] undo stp enable
[DeviceB-GigabitEthernet1/0/2] port link-type trunk
[DeviceB-GigabitEthernet1/0/2] undo port trunk permit vlan 1
[DeviceB-GigabitEthernet1/0/2] port trunk permit vlan 11 12
[DeviceB-GigabitEthernet1/0/2] port trunk pvid vlan 11
[DeviceB-GigabitEthernet1/0/2] quit
```

物理状態の変更があった場合、GigabitEthernet 1/0/3 のリンクダウンの通知を抑制する時間を 0 秒に設定します。

```
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] link-delay 0
```

ポートでスパニングツリー機能を無効にします。

```
[DeviceB-GigabitEthernet1/0/3] undo stp enable
```

ポートをトランクポートに設定します。

```
[DeviceB-GigabitEthernet1/0/3] port link-type trunk
```

VLAN 1 からポートを削除し、VLAN 12 に削除したポートを割り当てます。

```
[DeviceB-GigabitEthernet1/0/3] undo port trunk permit vlan 1
[DeviceB-GigabitEthernet1/0/3] port trunk permit vlan 12
```

デフォルト VLAN として VLAN 12 を設定します。

```
[DeviceB-GigabitEthernet1/0/3] port trunk pvid vlan 12
[DeviceB-GigabitEthernet1/0/3] quit
```

物理状態の変更があった場合、GigabitEthernet 1/0/4 のリンクダウンの通知を抑制する時間を 0 秒に設定します。

```
[DeviceB] interface gigabitethernet 1/0/4
[DeviceB-GigabitEthernet1/0/4] link-delay 0
```

ポートでスパニングツリー機能を無効にします。

```
[DeviceB-GigabitEthernet1/0/4] undo stp enable
```

ポートをトランクポートに設定します。

```
[DeviceB-GigabitEthernet1/0/4] port link-type trunk
```

VLAN 1 からポートを削除し、VLAN 11 に削除したポートを割り当てます。

```
[DeviceB-GigabitEthernet1/0/4] undo port trunk permit vlan 1
[DeviceB-GigabitEthernet1/0/4] port trunk permit vlan 11
```

デフォルト VLAN として VLAN 11 を設定します。

```
[DeviceB-GigabitEthernet1/0/4] port trunk pvid vlan 11
[DeviceB-GigabitEthernet1/0/4] quit
```

RRPP ドメイン 1 を作成します。

```
[DeviceB] rrpp domain 1
```

RRPP ドメイン 1 のプライマリコントロール VLAN として VLAN 100 を設定します。

```
[DeviceB-rrpp-domain1] control-vlan 100
```

RRPP ドメイン 1 のプロテクト VLAN として MSTI 1 にマッピングした VLAN を設定します。

```
[DeviceB-rrpp-domain1] protected-vlan reference-instance 1
```

RRPP ドメイン 1 のプライマリリング 1 のトランジットノードとして Device B を設定します。プライマリポートを GigabitEthernet 1/0/1、セカンダリポートを GigabitEthernet 1/0/2 に設定します。リング 1 を有効にします。

```
[DeviceB-rrpp-domain1] ring 1 node-mode transit primary-port gigabitethernet 1/0/1 secondary-port gigabitethernet 1/0/2 level 0
[DeviceB-rrpp-domain1] ring 1 enable
```

RRPP ドメイン 1 のサブリング 3 のアシスタントエッジノードとして Device B を設定します。エッジポートを GigabitEthernet 1/0/4 に設定します。サブリング 3 を有効にします。

```
[DeviceB-rrpp-domain1] ring 3 node-mode assistant-edge edge-port gigabitethernet 1/0/4
[DeviceB-rrpp-domain1] ring 3 enable
[DeviceB-rrpp-domain1] quit
```

RRPP ドメイン 2 を作成します。

```
[DeviceB] rrpp domain 2
```

RRPP ドメイン 2 のプライマリコントロール VLAN として VLAN 105 を設定します。

```
[DeviceB-rrpp-domain2] control-vlan 105
```

RRPP ドメイン 2 のプロテクト VLAN として MSTI 2 にマッピングした VLAN を設定します。

```
[DeviceB-rrpp-domain2] protected-vlan reference-instance 2
```

プライマリリング 1 のトランジットノードとして Device B を設定します。プライマリポートを GigabitEthernet 1/0/1、セカンダリポートを GigabitEthernet 1/0/2 に設定します。リング 1 を有効にします。

```
[DeviceB-rrpp-domain2] ring 1 node-mode transit primary-port gigabitethernet 1/0/1 secondary-port gigabitethernet 1/0/2 level 0
```

```
[DeviceB-rrpp-domain2] ring 1 enable
```

サブリング 2 のアシスタントエッジノードとして Device B を設定します。エッジポートを GigabitEthernet 1/0/3 に設定します。サブリング 2 を有効にします。

```
[DeviceB-rrpp-domain2] ring 2 node-mode assistant-edge edge-port gigabitethernet 1/0/3
[DeviceB-rrpp-domain2] ring 2 enable
[DeviceC-rrpp-domain2] quit
```

RRPP を有効にします。

```
[DeviceB] rrpp enable
```

3) Device C を設定します。

VLAN 11、VLAN 12 を作成します。

```
<DeviceC> system-view
[DeviceC] vlan 11 to 12
```

MSTI 1 に VLAN 11、MSTI 2 に VLAN 12 をマッピングします。

```
[DeviceC] stp region-configuration
[DeviceC-mst-region] instance 1 vlan 11
[DeviceC-mst-region] instance 2 vlan 12
```

MST region の設定を有効にします。

```
[DeviceC-mst-region] active region-configuration
[DeviceC-mst-region] quit
```

物理状態の変更があった場合、GigabitEthernet 1/0/1 のリンクダウンの通知を抑制する時間を 0 秒に設定します。

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] link-delay 0
```

ポートでスパニングツリー機能を無効にします。

```
[DeviceC-GigabitEthernet1/0/1] undo stp enable
```

ポートをトランクポートに設定します。

```
[DeviceC-GigabitEthernet1/0/1] port link-type trunk
```

VLAN 1 からポートを削除し、VLAN 11、VLAN 12 に削除したポートを割り当てます。

```
[DeviceC-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[DeviceC-GigabitEthernet1/0/1] port trunk permit vlan 11 12
```

デフォルト VLAN として VLAN 11 を設定します。

```
[DeviceC-GigabitEthernet1/0/1] port trunk pvid vlan 11
[DeviceC-GigabitEthernet1/0/1] quit
```

GigabitEthernet 1/0/1 の設定と同様に GigabitEthernet 1/0/2 を設定します。

```
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] link-delay 0
[DeviceC-GigabitEthernet1/0/2] undo stp enable
[DeviceC-GigabitEthernet1/0/2] port link-type trunk
[DeviceC-GigabitEthernet1/0/2] undo port trunk permit vlan 1
[DeviceC-GigabitEthernet1/0/2] port trunk permit vlan 11 12
[DeviceC-GigabitEthernet1/0/2] port trunk pvid vlan 11
[DeviceC-GigabitEthernet1/0/2] quit
```

物理状態の変更があった場合、GigabitEthernet 1/0/3 のリンクダウンの通知を抑制する時間を 0 秒に設定します。

```
[DeviceC] interface gigabitethernet 1/0/3
[DeviceC-GigabitEthernet1/0/3] link-delay 0
```

ポートでスパニングツリー機能を無効にします。

```
[DeviceC-GigabitEthernet1/0/3] undo stp enable
```

ポートをトランクポートに設定します。

```
[DeviceC-GigabitEthernet1/0/3] port link-type trunk
```

VLAN 1 からポートを削除し、VLAN 11、VLAN 12 に削除したポートを割り当てます。

```
[DeviceC-GigabitEthernet1/0/3] undo port trunk permit vlan 1
[DeviceC-GigabitEthernet1/0/3] port trunk permit vlan 12
```

デフォルト VLAN として VLAN 12 を設定します。

```
[DeviceC-GigabitEthernet1/0/3] port trunk pvid vlan 12
[DeviceC-GigabitEthernet1/0/3] quit
```

物理状態の変更があった場合、GigabitEthernet 1/0/4 のリンクダウンの通知を抑制する時間を 0 秒に設定します。

```
[DeviceC] interface gigabitethernet 1/0/4
[DeviceC-GigabitEthernet1/0/4] link-delay 0
```

ポートでスパニングツリー機能を無効にします。

```
[DeviceC-GigabitEthernet1/0/4] undo stp enable
```

ポートをトランクポートに設定します。

```
[DeviceC-GigabitEthernet1/0/4] port link-type trunk
```

VLAN 1 からポートを削除し、VLAN 11 に削除したポートを割り当てます。

```
[DeviceC-GigabitEthernet1/0/4] undo port trunk permit vlan 1
[DeviceC-GigabitEthernet1/0/4] port trunk permit vlan 11
```

デフォルト VLAN として VLAN 11 を設定します。

```
[DeviceC-GigabitEthernet1/0/4] port trunk pvid vlan 11
[DeviceC-GigabitEthernet1/0/4] quit
```

RRPP ドメイン 1 を作成します。

```
[DeviceC] rrpp domain 1
```

RRPP ドメイン 1 のプライマリコントロール VLAN として VLAN 100 を設定します。

```
[DeviceC-rrpp-domain1] control-vlan 100
```

RRPP ドメイン 1 のプロテクト VLAN として MSTI 1 にマッピングした VLAN を設定します。

```
[DeviceC-rrpp-domain1] protected-vlan reference-instance 1
```

プライマリリング 1 のトランジットノードとして Device C を設定します。プライマリポートを GigabitEthernet 1/0/1、セカンダリポートを GigabitEthernet 1/0/2 に設定します。リング 1 を有効にします。

```
[DeviceC-rrpp-domain1] ring 1 node-mode transit primary-port gigabitethernet 1/0/1 secondary-port gigabitethernet 1/0/2 level 0
[DeviceC-rrpp-domain1] ring 1 enable
```

サブリング 3 のエッジノードとして Device C を設定します。エッジポートを GigabitEthernet 1/0/4 に設定します。サブリング 3 を有効にします。

```
[DeviceC-rrpp-domain1] ring 3 node-mode edge edge-port gigabitethernet 1/0/4
[DeviceC-rrpp-domain1] ring 3 enable
[DeviceC-rrpp-domain1] quit
```

RRPP ドメイン 2 を作成します。

```
[DeviceC] rrpp domain 2
```

RRPP ドメイン 2 のプライマリコントロール VLAN として VLAN 105 を設定します。

```
[DeviceC-rrpp-domain2] control-vlan 105
```

RRPP ドメイン 2 のプロテクト VLAN として MSTI 2 にマッピングした VLAN を設定します。

```
[DeviceC-rrpp-domain2] protected-vlan reference-instance 2
```

RRPP ドメイン 2 のプライマリリング 1 のトランジットノードとして Device C を設定します。プライマリポートを GigabitEthernet 1/0/1、セカンダリポートを GigabitEthernet 1/0/2 に設定します。リング 1 を有効にします。

```
[DeviceC-rrpp-domain2] ring 1 node-mode transit primary-port gigabitethernet 1/0/1 secondary-port gigabitethernet 1/0/2 level 0
[DeviceC-rrpp-domain2] ring 1 enable
```

RRPP ドメイン 2 のサブリング 2 のエッジノードとして Device C を設定します。エッジポートを GigabitEthernet 1/0/3 に設定します。サブリング 2 を有効にします。

```
[DeviceC-rrpp-domain2] ring 2 node-mode edge edge-port gigabitethernet 1/0/3
```

```
[DeviceC-rrpp-domain2] ring 2 enable
[DeviceC-rrpp-domain2] quit
```

RRPP を有効にします。

```
[DeviceC] rrpp enable
```

4) Device D を設定します。

VLAN 11、VLAN 12 を作成します。

```
<DeviceD> system-view
[DeviceD] vlan 11 to 12
```

MSTI 1 に VLAN 11、MSTI 2 に VLAN 12 をマッピングします。

```
[DeviceD] stp region-configuration
[DeviceD-mst-region] instance 1 vlan 11
[DeviceD-mst-region] instance 2 vlan 12
```

MST region の設定を有効にします。

```
[DeviceD-mst-region] active region-configuration
[DeviceD-mst-region] quit
```

物理状態の変更があった場合、GigabitEthernet 1/0/1 のリンクダウンの通知を抑制する時間を 0 秒に設定します。

```
[DeviceD] interface gigabitethernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] link-delay 0
```

ポートでスパニングツリー機能を無効にします。

```
[DeviceD-GigabitEthernet1/0/1] undo stp enable
```

ポートをトランクポートに設定します。

```
[DeviceD-GigabitEthernet1/0/1] port link-type trunk
```

VLAN 1 からポートを削除し、VLAN 11、VLAN 12 に削除したポートを割り当てます。

```
[DeviceD-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[DeviceD-GigabitEthernet1/0/1] port trunk permit vlan 11 12
```

デフォルト VLAN として VLAN 11 を設定します。

```
[DeviceD-GigabitEthernet1/0/1] port trunk pvid vlan 11
[DeviceD-GigabitEthernet1/0/1] quit
```

GigabitEthernet 1/0/1 の設定と同様に GigabitEthernet 1/0/2 を設定します。

```
[DeviceD] interface gigabitethernet 1/0/2
[DeviceD-GigabitEthernet1/0/2] link-delay 0
[DeviceD-GigabitEthernet1/0/2] undo stp enable
```

```
[DeviceD-GigabitEthernet1/0/2] port link-type trunk
[DeviceD-GigabitEthernet1/0/2] undo port trunk permit vlan 1
[DeviceD-GigabitEthernet1/0/2] port trunk permit vlan 11 12
[DeviceD-GigabitEthernet1/0/2] port trunk pvid vlan 11
[DeviceD-GigabitEthernet1/0/2] quit
```

RRPP ドメイン 1 を作成します。

```
[DeviceD] rrpp domain 1
```

RRPP ドメイン 1 のプライマリコントロール VLAN として VLAN 100 を設定します。

```
[DeviceD-rrpp-domain1] control-vlan 100
```

RRPP ドメイン 1 のプロテクト VLAN として MSTI 1 にマッピングした VLAN を設定します。

```
[DeviceD-rrpp-domain1] protected-vlan reference-instance 1
```

プライマリリング 1 のトランジットノードとして Device D を設定します。プライマリポートを GigabitEthernet 1/0/1、セカンダリポートを GigabitEthernet 1/0/2 に設定します。リング 1 を有効にします。

```
[DeviceD-rrpp-domain1] ring 1 node-mode transit primary-port gigabitethernet 1/0/1 secondary-port gigabitethernet 1/0/2 level 0
[DeviceD-rrpp-domain1] ring 1 enable
[DeviceD-rrpp-domain1] quit
```

RRPP ドメイン 1 を作成します。

```
[DeviceD] rrpp domain 2
```

RRPP ドメイン 1 のプライマリコントロール VLAN として VLAN 105 を設定します。

```
[DeviceD-rrpp-domain2] control-vlan 105
```

RRPP ドメイン 2 のプロテクト VLAN として MSTI 2 にマッピングした VLAN を設定します。

```
[DeviceD-rrpp-domain2] protected-vlan reference-instance 2
```

プライマリリング 1 のトランジットノードとして Device D を設定します。プライマリポートを GigabitEthernet 1/0/1、セカンダリポートを GigabitEthernet 1/0/2 に設定します。リング 1 を有効にします。

```
[DeviceD-rrpp-domain2] ring 1 node-mode transit primary-port gigabitethernet 1/0/1 secondary-port gigabitethernet 1/0/2 level 0
[DeviceD-rrpp-domain2] ring 1 enable
[DeviceD-rrpp-domain2] quit
```

RRPP を有効にします。

```
[DeviceD] rrpp enable
```

5) Device E を設定します。

VLAN 12 を作成します。

```
<DeviceE> system-view
[DeviceE] vlan 12
```

MSTI 2 に VLAN 12 をマッピングします。

```
[DeviceE-vlan12] quit
[DeviceE] stp region-configuration
[DeviceE-mst-region] instance 2 vlan 12
```

MST region の設定を有効にします。

```
[DeviceE-mst-region] active region-configuration
[DeviceE-mst-region] quit
```

物理状態の変更があった場合、GigabitEthernet 1/0/1 のリンクダウンの通知を抑制する時間を 0 秒に設定します。

```
[DeviceE] interface gigabitethernet 1/0/1
[DeviceE-GigabitEthernet1/0/1] link-delay 0
```

ポートでスパニングツリー機能を無効にします。

```
[DeviceE-GigabitEthernet1/0/1] undo stp enable
```

ポートをトランクポートに設定します。

```
[DeviceE-GigabitEthernet1/0/1] port link-type trunk
```

VLAN 1 からポートを削除し、VLAN 12 に削除したポートを割り当てます。

```
[DeviceE-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[DeviceE-GigabitEthernet1/0/1] port trunk permit vlan 12
```

デフォルト VLAN として VLAN 12 を設定します。

```
[DeviceE-GigabitEthernet1/0/1] port trunk pvid vlan 12
[DeviceE-GigabitEthernet1/0/1] quit
```

GigabitEthernet 1/0/1 の設定と同様に GigabitEthernet 1/0/2 を設定します。

```
[DeviceE] interface gigabitethernet 1/0/2
[DeviceE-GigabitEthernet1/0/2] link-delay 0
[DeviceE-GigabitEthernet1/0/2] undo stp enable
[DeviceE-GigabitEthernet1/0/2] port link-type trunk
[DeviceE-GigabitEthernet1/0/2] undo port trunk permit vlan 1
[DeviceE-GigabitEthernet1/0/2] port trunk permit vlan 12
[DeviceE-GigabitEthernet1/0/2] port trunk pvid vlan 12
[DeviceE-GigabitEthernet1/0/2] quit
```

RRPP ドメイン 2 を作成します。

```
[DeviceE] rrpp domain 2
```

RRPP ドメイン 2 のプライマリコントロール VLAN として VLAN 105 を設定します。

```
[DeviceE-rrpp-domain2] control-vlan 105
```

RRPP ドメイン 2 のプロテクト VLAN として MSTI 2 にマッピングした VLAN を設定します。

```
[DeviceE-rrpp-domain2] protected-vlan reference-instance 2
```

RRPP ドメイン 2 のサブリング 2 のマスタノードとして Device E を設定します。プライマリポートを GigabitEthernet 1/0/1、セカンダリポートを GigabitEthernet 1/0/2 に設定します。リング 2 を有効にします。

```
[DeviceE-rrpp-domain2] ring 2 node-mode master primary-port gigabitethernet 1/0/2 secondary-port gigabitethernet 1/0/1 level 1
[DeviceE-rrpp-domain2] ring 2 enable
[DeviceE-rrpp-domain2] quit
```

RRPP を有効にします。

```
[DeviceE] rrpp enable
```

6) Device F を設定します。

VLAN 11 を作成します。

```
<DeviceF> system-view
[DeviceF] vlan 11
[DeviceF-vlan11] quit
```

MSTI 1 に VLAN 11 をマッピングします。

```
[DeviceF] stp region-configuration
[DeviceF-mst-region] instance 1 vlan 11
```

MST region の設定を有効にします。

```
[DeviceF-mst-region] active region-configuration
[DeviceF-mst-region] quit
```

物理状態の変更があった場合、GigabitEthernet 1/0/1 のリンクダウンの通知を抑制する時間を 0 秒に設定します。

```
[DeviceF] interface gigabitethernet 1/0/1
[DeviceF-GigabitEthernet1/0/1] link-delay 0
```

ポートでスパニングツリー機能を無効にします。

```
[DeviceF-GigabitEthernet1/0/1] undo stp enable
```

ポートをトランクポートに設定します。

```
[DeviceF-GigabitEthernet1/0/1] port link-type trunk
```

VLAN 1 からポートを削除し、VLAN 11 に削除したポートを割り当てます。

```
[DeviceF-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[DeviceF-GigabitEthernet1/0/1] port trunk permit vlan 11
```

デフォルト VLAN として VLAN 11 を設定します。

```
[DeviceF-GigabitEthernet1/0/1] port trunk pvid vlan 11
[DeviceF-GigabitEthernet1/0/1] quit
```

GigabitEthernet 1/0/1 の設定と同様に GigabitEthernet 1/0/2 を設定します。

```
[DeviceF] interface gigabitethernet 1/0/2
[DeviceF-GigabitEthernet1/0/2] link-delay 0
[DeviceF-GigabitEthernet1/0/2] undo stp enable
[DeviceF-GigabitEthernet1/0/2] port link-type trunk
[DeviceF-GigabitEthernet1/0/2] undo port trunk permit vlan 1
[DeviceF-GigabitEthernet1/0/2] port trunk permit vlan 11
[DeviceF-GigabitEthernet1/0/2] port trunk pvid vlan 11
[DeviceF-GigabitEthernet1/0/2] quit
```

RRPP ドメイン 1 を作成します。

```
[DeviceF] rrpp domain 1
```

RRPP ドメイン 1 のプライマリコントロール VLAN として VLAN 100 を設定します。

```
[DeviceF-rrpp-domain1] control-vlan 100
```

RRPP ドメイン 1 のプロテクト VLAN として MSTI 1 にマッピングした VLAN を設定します。

```
[DeviceF-rrpp-domain1] protected-vlan reference-instance 1
```

RRPP ドメイン 1 のサブリング 3 のマスタノードとして Device F を設定します。プライマリポートを GigabitEthernet 1/0/1、セカンダリポートを GigabitEthernet 1/0/2 に設定します。サブリング 3 を有効にします。

```
[DeviceF-rrpp-domain1] ring 3 node-mode master primary-port gigabitethernet 1/0/1 secondary-port gigabitethernet 1/0/2 level 1
[DeviceF-rrpp-domain1] ring 3 enable
[DeviceF-rrpp-domain1] quit
```

RRPP を有効にします。

```
[DeviceF] rrpp enable
```

7) Device B、Device C で RRPP リンググループを設定します。

Device B で RRPP リンググループ 1 を作成し、RRPP リンググループにサブリング 2、サブリング 3 を追加します。

```
[DeviceB] rrpp ring-group 1
```

```
[DeviceB-rrpp-ring-group1] domain 2 ring 2
[DeviceB-rrpp-ring-group1] domain 1 ring 3
```

Device C で RRPP リンググループ 1 を作成し、RRPP リンググループにサブリング 2、サブリング 3 を追加します。

```
[DeviceC] rrpp ring-group 1
[DeviceC-rrpp-ring-group1] domain 2 ring 2
[DeviceC-rrpp-ring-group1] domain 1 ring 3
```

III. 設定の確認

display コマンドを使用し、各 Device の RRPP 設定と動作情報を表示します。

4.13 RRPPのトラブルシューティング

I. 症状

リンクの状態が正常なとき、マスタノードが Hello パケットを受信できず、マスタノードがセカンダリポートのブロック状態を解除しました。

II. 分析

問題の原因は以下のものが考えられます。

- RRPP リング内のいくつかのノードで RRPP が有効になっていません。
- RRPP リング内のノードにドメイン ID またはプライマリコントロール VLAN-ID が他のノードと異なっているノードがあります。
- ポートに異常があります。

III. 解決策

問題を解決する場合、以下を行ってください。

- **display rrpp brief** コマンドで、すべてのノードで RRPP が有効かどうかを確認してください。RRPP が有効になっていないノードがある場合、そのノードで **rrpp enable** コマンドと **ring enable** コマンドを使用して RRPP と RRPP リングを有効にしてください。
- **display rrpp brief** コマンドで、すべてのノードでドメイン ID とプライマリコントロール VLAN の ID が同じかどうかを確認してください。ドメイン ID またはプライマリコントロール VLAN の ID が異なるノードがある場合、そのノードの設定を他のノードと同じドメイン ID とプライマリコントロール VLAN の ID に変更してください。
- **display rrpp verbose** コマンドで、各リングの各ポートのリンク状態を確認してください。
- **debugging rrpp** コマンドで、各ノードで Hello パケットを送受信しているかどうかを確認してください。

目次

このセクションのページは **10-x-x** です。

5章 Smart Link 5-1
5.1 概要 5-1
5.1.1 用語の説明 5-2
5.1.2 Smart Linkの動作メカニズム 5-3
5.1.3 Smart LinkとMonitor Linkのコラボレーション 5-4
5.2 Smart Lin設定作業リスト 5-4
5.3 Smart Link装置の設定 5-5
5.3.1 設定要件 5-5
5.3.2 Smart Linkグループのプロテクトvlanの設定 5-5
5.3.3 Smart Linkグループのメンバポートの設定 5-7
5.3.4 Smart Linkグループのrole preemptionの設定 5-8
5.3.5 flushメッセージの送信の有効化 5-8
5.3.6 Smart とTrackのコラボレーションの設定 5-9
5.4 関連装置の設定 5-9
5.4.1 設定要件 5-9
5.4.2 flushメッセージの受信の有効化 5-9
5.5 Smart Linkの表示と維持 5-10
5.6 Smart Linkの設定例 5-10
5.6.1 単一Smart Link groupグループの設定例 5-10
5.6.2 複数Smart Linkグループの負荷分散の設定例 5-16

5章 Smart Link

5.1 概要

ネットワークの信頼性を保障するために、図 5-1に示すようにアップリンクの装置とダウンリンクの装置を 2 重で接続する冗長構成のネットワークを築きます。

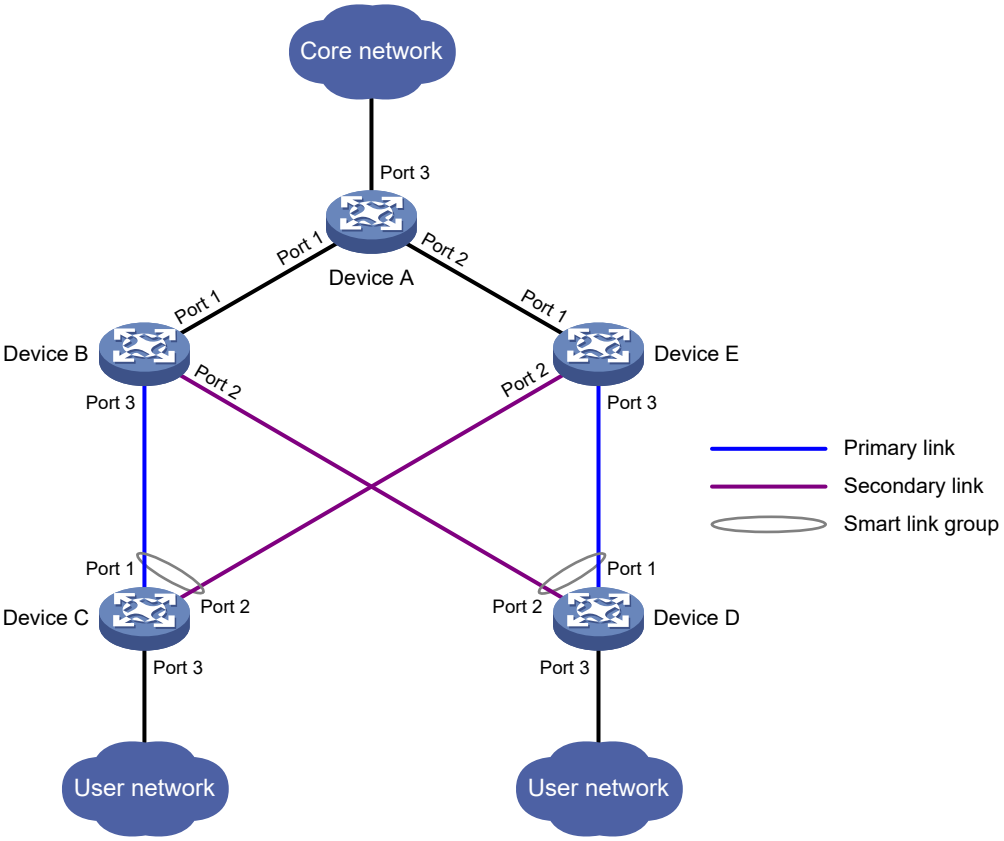


図 5-1 2 つのアップリンクを持つネットワーク

冗長構成のネットワークでループを回避するには、スパニングツリープロトコルや RRPP（Rapid Ring Protection Protocol）を使用します。しかし、スパニングツリープロトコルは収束時間が長く、収束速度に高い要求を持つユーザに適していないという問題があります。RRPP は収束速度についての要求に満足しますが、複雑なネットワーク構成を含み、主にリング状のネットワークで使用されます。

スパニングツリープロトコルの詳細は、オペレーションマニュアルのセクション 3 *アクセス* "*STP*"を参照してください。RRPP の詳細は、オペレーションマニュアルのセクション 10 *高可用性* "*RRPP*"を参照してください。

Smart Link は、STP の収束が遅いという問題に対処するために開発された機能です。プライマリリンクで障害が発生した場合に、ただちにバックアップリンクに切り替えるため、ネットワークの高速な収束を提供します。

装置は Flush メッセージを転送するため、Smart link グループと制御 VLAN を転送するように Smart link の設定を行います。図 5-1の Device C、Device D は Smart link の装置です。

関連装置は Smart link をサポートし、指定された制御 VLAN から Flush メッセージを受信します。図 5-1の Device A、Device B、Device E は関連装置です。

5.1.1 用語の説明

I. Smart link グループ

Smart link グループは、primary と secondary の 2 つのポートで構成されています。1 ポートだけが active になり転送可能になります。もう一方のポートはブロックされ、standby 状態になります。リンク障害や片方向リンクで active ポートがシャットダウンした場合、active ポートがブロックされた状態になり、standby ポートが active になります。

図 5-1では、Device C の Port1 と Port2 が、Smart Link グループを形成し、Device D の Port1 と Port2 が、別の Smart Link グループを形成します。Port1 が active で、Port2 は standby 状態です。

II. Primary/secondary ポート

Smart link グループには primary ポートと secondary ポートの 2 種類のポートがあります。Smart Link グループの両方のポートが UP しているときには、primary ポートが優先的に転送状態になり、secondary ポートは standby 状態になります。primary ポートで障害が発生した場合、secondary ポートは、トラフィックを転送するために active になります。図 5-1では、Device C の Port1 と Device D の Port1 を primary ポートとして、Device C の Port2 と Device D の Port2 を secondary ポートとして設定しています。

III. Primary/secondary リンク

Smart link グループの primary ポートをつなぐリンクが primary リンクです。secondary ポートをつなぐリンクが secondary リンクです。

IV. Flush メッセージ

Flush メッセージは、リンクの切り替えが Smart link グループで発生したときに、MAC アドレス転送エントリと ARP/ND エントリをリフレッシュするよう他の装置に通知するために使用されます。Flush メッセージは、共通のマルチキャストデータパケットであり、ブロックされた受信ポートによって廃棄されます

V. プロテクト VLAN

Smart link グループは、プロテクト VLAN の転送状態を制御します。異なる Smart link グループのポートは、異なるプロテクト VLAN を制御します。プロテクト VLAN のポートの状態は、Smart link グループのポートの状態によって決まります。

VI. 送信制御 VLAN

送信制御 VLAN は、Flush メッセージの送信を制御します。リンクの切り替えが発生した場合、装置（図 5-1では Device C と Device D）は送信制御 VLAN を使用して Flush メッセージを送信します。

VII. 受信制御 VLAN

受信制御 VLAN は Flush メッセージを受信し、処理します。リンクの切り替えが発生した場合、装置（図 5-1では、Device A、Device B、Device E）は受信制御 VLAN の Flush メッセージの処理を行い、MAC アドレス転送エントリと ARP/ND エントリをリフレッシュさせます。

5.1.2 Smart Link の動作メカニズム

I. リンクバックアップ

図 5-1で示すように、Device C の Port1 のリンクは primary link です。Device C の Port2 のリンクは secondary link です。通常、Port1 が active 状態の時、Port2 は standby 状態になります。primary link で障害が発声した場合、Port2 がトラフィックを転送するために standby から active に切り替わります。Port1 はブロックされ、standby 状態になります。

ポートの状態が変化した際にポートの状態変化をユーザに通知するために、ログを出力します。

II. トポロジ変更

リンク切り替えは、すべての装置の MAC アドレス転送エントリと ARP/ND エントリを無効化してしまうため、正常な通信を保証するために転送エントリアップデートメカニズムを必要とします。以下のアップデートメカニズムが提供されます。

- **アップリンクのトラフィックをトリガとした MAC アドレスの学習**－アップデートはアップリンクトラフィックによって発生します。このメカニズムは、他のベンダの装置など、Smart Link をサポートしていない装置を使用する環境に適切です。
- **フラッシュアップデート**－Smart Link 対応装置がアップリンクの装置へバックアップリンク上の flush メッセージを送信することで、flush の情報をアップデートします。このメカニズムは、アップリンクの装置が MAC アドレス転送エントリと ARP/ND エントリをアップデートする Smart Link flush メッセージを認識できる必要があります。

III. preemption モード

図 5-1では、Device C の Port1 のリンクは primary link です。Device C の Port2 のリンクは secondary link です。primary link で障害が発生すると、Port1 は自動的にブロッキングされ standby 状態になります。そして、Port2 がトラフィックを転送するよう standby から active に切り替わります。primary link が復旧するとシステムは、以下の 1 つの動作を行います。

- Smart Link グループに Role preemption が設定されない場合、トラフィック転送状態を維持するために、リンク障害でブロッキングされた port1 は、active に切り替わりません。port2 でリンク障害が発生したときに、port1 は active に切り替わります。

- Smart Link グループに Role preemption を設定した場合、port1 のリンクが復旧するとすぐに active に切り替わります。port2 は自動的にブロッキングされ standby 状態になります。

IV. 負荷分散

リング構成のネットワークは複数の VLAN のトラフィックを転送します。Smart Link は、Smart Link グループ毎に異なる VLAN でトラフィックを転送させ、負荷分散を行います。

負荷分散を行うために、ポートを複数の Smart Link グループに割り当てます。それぞれ異なるプロテクト VLAN の各グループに設定してください。Smart Link グループからのトラフィックが異なる経路で転送できるように、Smart Link グループでポートが異なることを確認してください。

MSTI（Multiple Spanning Tree Instances）を参照することで、Smart Link グループのプロテクト VLAN を設定することができます。MSTI の詳細は、オペレーションマニュアルのセクション 3 *アクセス* "*STP*"を参照してください。

5.1.3 Smart Link と Monitor Link のコラボレーション

Smart Link は、アップリンクで障害が発生したときや障害が復旧したとき、リンクの状態変化を検出できません。アップリンクのリンク状態を監視するために、アップリンクポートを監視する Monitor Link を設定することができます。Monitor Link は、ダウンリンクの装置上でリンクの切り替えを実行する Smart Link をトリガにし、ダウンリンクポートのアップ/ダウンの状態をアップリンクポートのアップ/ダウン状態に適応させます。Monitor Link の詳細は、オペレーションマニュアルのセクション 10 *高可用性” Monitor Link*"を参照してください。

5.2 Smart Lin設定作業リスト

作業リスト
Smart Link装置の設定： ● （必須設定項目） Smart Linkグループのプロテクトvlanの設定 ● （必須設定項目） Smart Linkグループのメンバポートの設定 ● （オプション設定項目） Smart Linkグループのrole preemptionの設定 ● （オプション設定項目） flushメッセージの送信の有効化 ● （オプション設定項目）Smart とTrackのコラボレーションの設定
関連装置の設定 ● （必須設定項目） flushメッセージの受信の有効化

5.3 Smart Link装置の設定

5.3.1 設定要件

Smart link 装置の設定を行う前に、以下の作業を完了してください。

- ループを防ぐため、Smart Link グループのメンバポートの設定をする前に、ポートをシャットダウンしてください。Smart Link グループの設定を完了したのち、ポートをリンクアップさせてください。
- Smart Link グループに追加するポートは、スパニングツリー機能と RRPP を無効にしてください。

🕮 **メモ：**

- スパニングツリー機能を無効にしたとき、Smart Link 機能をポートで有効するまではネットワークでループが発生する可能性があります。
- アグリゲーショングループメンバと Smart Link メンバの両方を設定したとき、アグリゲーショングループの設定が適用されます。ポートは **display smart-link group** コマンドで表示することができません。Smart Link グループの設定は、アグリゲーショングループからポートを削除したのち、適用されます。

5.3.2 Smart Link グループのプロテクト VLAN の設定

MSTI を参照することにより、Smart Link グループにプロテクト VLAN を設定できます。プロテクト VLAN 設定は、スパニングツリープロトコルによります。

STP、RSTP あるいは MSTP モードでは、VALN と MSTI 間のマッピングを手動で設定しなければなりません。

PVST モードでは、VLAN と MSTI のマッピングを自動で行います。スパニングツリープロトコルが無効の場合は、VLAN は MSTI0 にマッピングされます。

以下に Smart Link グループのプロテクト VLAN の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． MST region view に移行する	**stp region-configuration**	PVSTモードで動作する場合省略します。 コマンドの詳細は、コマンドマニュアルのセクション3 *アクセス "STP"*を参照してください。

操作	コマンド	補足
3. VLAN-インスタンスマッピングテーブルを設定する	• 方法1： **instance** *instance-id* **vlan** *vlan-id-list* • 方法2： **vlan-mapping modulo** *modulo*	PVSTモードで動作する場合省略します。 デフォルト：MST regionのすべてのVLANはCIST（MSTI0）にマッピングされます。 コマンドの詳細は、コマンドマニュアルのセクション3 *アクセス* "*STP*"を参照してください。
4. MST region 設定を手動でアクティブにする	**active region-configuration**	PVSTモードで動作する場合省略します。 コマンドの詳細は、コマンドマニュアルのセクション3 *アクセス* "*STP*"を参照してください。
5. （オプション設定項目）現在のアクティブな MST region の設定情報を表示する	**display stp region-configuration**	すべてのviewで実行できます。 コマンドの出力はVLAN-インスタンスマッピング情報が含まれます。 コマンドの詳細は、コマンドマニュアルのセクション3 *アクセス* "*STP*"を参照してください。
6. system view に戻る	**quit**	PVSTモードで動作する場合省略します。
7. Smart Link グループを作成し、smart link group view に移行する	**smart-link group** *group-id*	―
8. Smart Link グループのプロテクト VLAN を設定する	**protected-vlan reference-instance** *instance-id-list*	デフォルト：設定なし

重要：

pvst mode を設定している装置で Smart Link を使用する場合は、以下の通りに **protected-vlan reference-instance** コマンドを指定してください。**reference-instance** の値が正しく指定されていない場合は、Smart Link の STANDBY ポートがパケットを転送します。

・**stp global enable** コマンド設定なし
　protected-vlan reference-instance 0 コマンドを設定します。
・**stp global enable** コマンド設定あり

VLAN の個数が 128 個までは、VLAN ID＝インスタンス ID でマッピングされます。129 個目以降の VLAN は全て、インスタンス 0 にマッピングされます。

例）vlan 1, 3, 5, 200 を定義している場合、以下のように自動的にマッピングされます。

Instance	VLANs Mapped
0	2, 4, 6 to 199, 201 to 4094 （未定義の VLAN、または、129 個目以降の VLAN は 0 にマッピングされる）
1	1
3	3
5	5
200	200

注）display stp region-configuration は、MSTP モード時しか利用できず、
　　PVST モード時は、実際の MSTI マッピング状態を確認できません。

Smart Link の対象となる vlan の ID が、VLAN ID＝インスタンス ID でマッピングされた vlan の場合は、**protected-vlan reference-instance** に該当する vlan と同じ ID を instance に設定します。Smart Link の対象となる vlan の ID が、インスタンス 0 にマッピングされている場合は、**protected-vlan reference-instance 0** を設定します。

たとえば、VLAN 100 を使用する場合は、**protected-vlan reference-instance 100** を設定します。しかし、VLAN 200 を使用する場合は、定義された VLAN の数により、vlan と同じ ID または 0 のどちらを指定すべきか判断する必要があります。

5.3.3 Smart Link グループのメンバポートの設定

Smart Link グループのメンバポートを smart link group view か interface view のどちらかで設定できます。2 つの view で行った設定は同じ効果を持ちます。

I. smart link group view でメンバポートの設定

以下に smart link group view で Smart Link グループのメンバポートの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Smart Link グループを作成し、smart link group view に移行する	**smart-link group** *group-id*	―
3. Smart Link グループのメンバポートを設定する	**port** *interface-type interface-number* { **primary** | **secondary** }	デフォルト：設定なし

II. interface view でメンバポートの設定

以下に interface view で Smart Link グループのメンバポートの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. interface view または aggregate interface view に移行する	**interface** *interface-type interface-number*	ー
3. Smart Link グループのメンバポートを設定する	**port smart-link group** *group-id* { **primary** | **secondary** }	デフォルト：設定なし

5.3.4 Smart Link グループの role preemption の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. smart link group view に移行する	**smart-link group** *group-id*	ー
3. role preemption を有効にする	**preemption mode role**	デフォルト：無効
4. preemption delay を設定する	**preemption delay** *delay*	デフォルト：1秒 preemption delayの設定は、role preemptionを有効にした後にのみ適用されます。

5.3.5 flush メッセージの送信の有効化

Flush メッセージの送信を有効にする設定を行うとき、以下のガイドラインに従ってください。

- Smart link グループで設定された制御 VLAN は、他の smart link グループに設定された制御 VLAN と異なるようにしてください。
- 制御 VLAN がすでに存在することを確認し、Smart link グループのメンバポートを制御 VLAN に割り当ててください。
- Smart Link グループの制御 VLAN は、プロテクト VLAN にしてください。制御 VLAN を削除しないでください。制御 VLAN を削除すると、flush メッセージを正しく送信できなくなります。

以下に Flush メッセージの送信を有効にする設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. smart link group view に移行する	**smart-link group** *group-id*	ー
3. Flush メッセージの送信を有効にする	**flush enable** [**control-vlan** *vlan-id*]	デフォルト：有効 VLAN 1は制御VLANです。

5.3.6 Smart と Track のコラボレーションの設定

I. Smart Link と Track のコラボレーションの設定

リンク検出を行うため、Track エントリを通して、CFD の CC 機能と Smart link のコラボレーションを行います。

II. 設定要件

ポートで Smart link と Track 間のコラボレーションの設定を行う前に、ポートを指定した Smart link グループに追加されていることを確認してください。

III. 設定手順

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． Ethernet interface view あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	―
3． ポートで Smart Link と CFD の CC 機能とのコラボレーションを設定する	**port smart-link group** *group-id* **track** *track-entry-number*	デフォルト：設定なし

5.4 関連装置の設定

5.4.1 設定要件

Smart Link グループのメンバポートに接続している、関連する装置のポートのスパニングツリー機能を無効にしてください。スパニングツリーが有効になっている場合、トポロジーが変更されたときに転送ステートにいない場合、ポートは flush メッセージを破棄します。

5.4.2 flush メッセージの受信の有効化

flush メッセージを受信するため、関連づけられた装置ですべてのポートを有効にする必要はありません。Smart Link 装置と宛先装置間の primary と secondary のリンク上のポートのすべての制御 VLAN でのみ、有効にする必要があります。

Flush メッセージの受信を有効にする設定を行う前に、以下の作業を完了してください。

- flush メッセージを処理する制御 VLAN を指定していない場合、装置は flush メッセージを処理せずに転送します。
- Smart Link 装置において、受信制御 VLAN と送信制御 VLAN が同じ VLAN であることを確認してください。 送受信する制御 VLAN が同じでない場合、関連装置は、受信した flush メッセージを処理せずに転送します。

- 制御 VLAN を削除しないでください。制御 VLAN を削除すると、flush メッセージを正しく送信できなくなります。
- 制御 VLAN が既存の VLAN であることを確認してください。制御 VLAN に flush メッセージが受信できるポートを割り当ててください。

以下に Flush メッセージの受信を有効にする設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． interface view または aggregate interface view に移行する	**interface** *interface-type interface-number*	—
3． Flush メッセージを受信する制御 VLAN を設定する	**smart-link flush enable** [**control-vlan** *vlan-id-list*]	デフォルト：設定なし

5.5 Smart Linkの表示と維持

すべての view で **display** コマンドを実行でき、user view で **reset** コマンドを実行できます。

操作	コマンド
受信したFlushメッセージの情報を表示する	**display smart-link flush**
Smart linkグループの情報を表示する	**display smart-link group** { *group-id* | **all** }
Flushメッセージの統計情報をクリアする	**reset smart-link statistics**

5.6 Smart Linkの設定例

5.6.1 単一 Smart Link group グループの設定例

I. ネットワーク要件

図 5-2に示すようなネットワークで設定します。

- Device C、Device D は Smart link 装置です。Device A、Device B、Device E は関連装置です。Device C の VLAN 1～VLAN 30 のトラフィックが Device A に 2 重アップリンクされます。
- 2 重アップリンクのバックアップ用に Device C と Device D で Smart link を設定します。

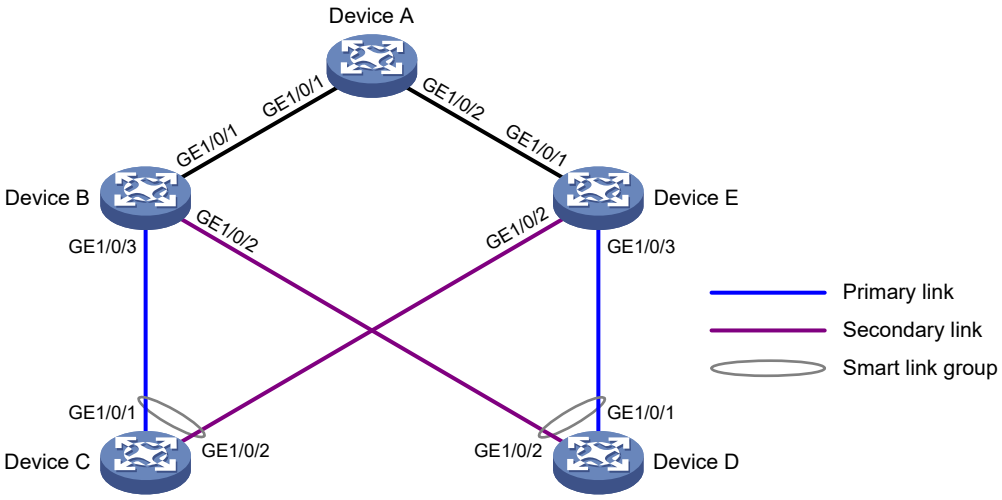


図 5-2 ネットワーク図

II. 設定手順

1)　Device C を設定します。

VLAN 1～VLAN 30 を作成します。MSTI1 にマッピングし、MST region 設定を動作させます。

```
<DeviceC> system-view
[DeviceC] vlan 1 to 30
[DeviceC] stp region-configuration
[DeviceC-mst-region] instance 1 vlan 1 to 30
[DeviceC-mst-region] active region-configuration
[DeviceC-mst-region] quit
```

GigabitEthernet 1/0/1 と GigabitEthernet 1/0/2 をシャットダウンします。GigabitEthernet 1/0/1 と GigabitEthernet 1/0/2 上のスパニングツリー機能を無効にします。トランクポートとして設定し、VLAN 1～VLAN 30 に割り当てます。

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] shutdown
[DeviceC-GigabitEthernet1/0/1] undo stp enable
[DeviceC-GigabitEthernet1/0/1] port link-type trunk
[DeviceC-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceC-GigabitEthernet1/0/1] quit
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] shutdown
```

```
[DeviceC-GigabitEthernet1/0/2] undo stp enable
[DeviceC-GigabitEthernet1/0/2] port link-type trunk
[DeviceC-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
[DeviceC-GigabitEthernet1/0/2] quit
```

Smart Link グループ 1 を作成し、すべての VLAN をプロテクト VLAN として MSTI 1 にマッピングします。

```
[DeviceC] smart-link group 1
[DeviceC-smlk-group1] protected-vlan reference-instance 1
```

Smart Link グループ 1 の primary ポートとして GigabitEthernet 1/0/1 を設定し、secondary ポートとして GigabitEthernet 1/0/2 を設定します。

```
[DeviceC-smlk-group1] port gigabitethernet 1/0/1 primary
[DeviceC-smlk-group1] port gigabitethernet 1/0/2 secondary
```

Smart Link グループ 1 で flush メッセージの送信を有効にし、送信制御 VLAN として VLAN 10 を設定します。

```
[DeviceC-smlk-group1] flush enable control-vlan 10
[DeviceC-smlk-group1] quit
```

GigabitEthernet 1/0/1 と GigabitEthernet 1/0/2 を再度アップにします。

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] undo shutdown
[DeviceC-GigabitEthernet1/0/1] quit
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] undo shutdown
[DeviceC-GigabitEthernet1/0/2] quit
```

2)　Device D を設定します。

VLAN 1～VLAN 30 を作成します。MSTI1 にマッピングし、MST region 設定を動作させます。

```
<DeviceD> system-view
[DeviceD] vlan 1 to 30
[DeviceD] stp region-configuration
[DeviceD-mst-region] instance 1 vlan 1 to 30
[DeviceD-mst-region] active region-configuration
[DeviceD-mst-region] quit
```

GigabitEthernet 1/0/1 と GigabitEthernet 1/0/2 をシャットダウンします。GigabitEthernet 1/0/1 と GigabitEthernet 1/0/2 上のスパニングツリー機能を無効にします。トランクポートとして設定し、VLAN 1～VLAN 30 に割り当てます。

```
[DeviceD] interface gigabitethernet 1/0/1
```

```
[DeviceD-GigabitEthernet1/0/1] shutdown
[DeviceD-GigabitEthernet1/0/1] undo stp enable
[DeviceD-GigabitEthernet1/0/1] port link-type trunk
[DeviceD-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceD-GigabitEthernet1/0/1] quit
[DeviceD] interface gigabitethernet 1/0/2
[DeviceD-GigabitEthernet1/0/2] shutdown
[DeviceD-GigabitEthernet1/0/2] undo stp enable
[DeviceD-GigabitEthernet1/0/2] port link-type trunk
[DeviceD-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
[DeviceD-GigabitEthernet1/0/2] quit
```

Smart Link グループ 1 を作成し、すべての VLAN をプロテクト VLAN として MSTI 1 にマッピングします。

```
[DeviceD] smart-link group 1
[DeviceD-smlk-group1] protected-vlan reference-instance 1
```

Smart Link グループ 1 の primary ポートとして GigabitEthernet 1/0/1 を設定し、secondary ポートとして GigabitEthernet 1/0/2 を設定します。

```
[DeviceD-smlk-group1] port gigabitethernet 1/0/1 primary
[DeviceD-smlk-group1] port gigabitethernet 1/0/2 secondary
```

Smart Link グループ 1 で flush メッセージの送信を有効にし、送信制御 VLAN として VLAN20 を設定します。

```
[DeviceD-smlk-group1] flush enable control-vlan 20
[DeviceD-smlk-group1] quit
```

GigabitEthernet 1/0/1 と GigabitEthernet 1/0/2 を再度アップにします。

```
[DeviceD] interface gigabitethernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] undo shutdown
[DeviceD-GigabitEthernet1/0/1] quit
[DeviceD] interface gigabitethernet 1/0/2
[DeviceD-GigabitEthernet1/0/2] undo shutdown
[DeviceD-GigabitEthernet1/0/2] quit
```

3)　Device B を設定します。

VLAN 1～VLAN 30 を作成します。

```
<DeviceB> system-view
[DeviceB] vlan 1 to 30
```

GigabitEthernet 1/0/1 をトランクポートとして設定し、VLAN 1～VLAN 30 に割り付けます。flush メッセージの受信を有効にし、VLAN 10 と VLAN 20 を受信制御 VLAN として設定します。

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port link-type trunk
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceB-GigabitEthernet1/0/1] smart-link flush enable control-vlan 10 20
[DeviceB-GigabitEthernet1/0/1] quit
```

GigabitEthernet 1/0/2 をトランクポートとして設定し、VLAN 1～VLAN 30 に割り付けます。スパニングツリー機能を無効にします。flush メッセージの受信を有効にします。VLAN 20 を受信制御 VLAN として設定します。

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] port link-type trunk
[DeviceB-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
[DeviceB-GigabitEthernet1/0/2] undo stp enable
[DeviceB-GigabitEthernet1/0/2] smart-link flush enable control-vlan 20
[DeviceB-GigabitEthernet1/0/2] quit
```

GigabitEthernet 1/0/3 をトランクポートとして設定し、VLAN 1～VLAN 30 に割り付けます。スパニングツリー機能を無効にします。flush メッセージの受信を有効にします。VLAN 10 を受信制御 VLAN として設定します。

```
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] port link-type trunk
[DeviceB-GigabitEthernet1/0/3] port trunk permit vlan 1 to 30
[DeviceB-GigabitEthernet1/0/3] undo stp enable
[DeviceB-GigabitEthernet1/0/3] smart-link flush enable control-vlan 10
[DeviceB-GigabitEthernet1/0/3] quit
```

4) Device E を設定します。

VLAN 1～VLAN 30 を作成します。

```
<DeviceE> system-view
[DeviceE] vlan 1 to 30
```

GigabitEthernet 1/0/1 をトランクポートとして設定し、VLAN 1～VLAN 30 に割り付けます。スパニングツリー機能を無効にします。flush メッセージの受信を有効にします。VLAN 10 と VLAN20 を受信制御 VLAN として設定します。

```
[DeviceE] interface gigabitethernet 1/0/1
[DeviceE-GigabitEthernet1/0/1] port link-type trunk
[DeviceE-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceE-GigabitEthernet1/0/1] smart-link flush enable control-vlan 10 20
```

```
[DeviceE-GigabitEthernet1/0/1] quit
```

GigabitEthernet 1/0/2 をトランクポートとして設定し、VLAN 1～VLAN 30 に割り付けます。スパニングツリー機能を無効にします。flush メッセージの受信を有効にします。VLAN 10 を受信制御 VLAN として設定します。

```
[DeviceE] interface gigabitethernet 1/0/2
[DeviceE-GigabitEthernet1/0/2] port link-type trunk
[DeviceE-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
[DeviceE-GigabitEthernet1/0/2] undo stp enable
[DeviceE-GigabitEthernet1/0/2] smart-link flush enable control-vlan 10
[DeviceE-GigabitEthernet1/0/2] quit
```

GigabitEthernet 1/0/3 をトランクポートとして設定し、VLAN 1～VLAN 30 に割り付けます。スパニングツリー機能を無効にします。flush メッセージの受信を有効にします。VLAN 20 を受信制御 VLAN として設定します。

```
[DeviceE] interface gigabitethernet 1/0/3
[DeviceE-GigabitEthernet1/0/3] port link-type trunk
[DeviceE-GigabitEthernet1/0/3] port trunk permit vlan 1 to 30
[DeviceE-GigabitEthernet1/0/3] undo stp enable
[DeviceE-GigabitEthernet1/0/3] smart-link flush enable control-vlan 20
[DeviceE-GigabitEthernet1/0/3] quit
```

5) Device A を設定します。

VLAN 1～VLAN 30 を作成します。

```
<DeviceA> system-view
[DeviceA] vlan 1 to 30
```

GigabitEthernet 1/0/1 と GigabitEthernet 1/0/2 をトランクポートとして設定し、VLAN 1～VLAN 30 に割り付けます。flush メッセージの受信を有効にし、VLAN 10 と VLAN 20 を受信制御 VLAN として設定します。

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-type trunk
[DeviceA-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceA-GigabitEthernet1/0/1] smart-link flush enable control-vlan 10 20
[DeviceA-GigabitEthernet1/0/1] quit
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port link-type trunk
[DeviceA-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
[DeviceA-GigabitEthernet1/0/2] smart-link flush enable control-vlan 10 20
[DeviceA-GigabitEthernet1/0/2] quit
```

III. 設定の確認

display smart-link group コマンドを使用し、デバイス上の Smart Link グループの設定を表示します。

Device C 上の Smart Link グループの設定を表示します。

```
[DeviceC] display smart-link group 1
Smart link group 1 information:
  Device ID       : 000f-e23d-5af0
  Preemption mode : NONE
  Preemption delay: 1(s)
  Control VLAN    : 10
  Protected VLAN  : Reference Instance 1

  Member                  Role      State   Flush-count     Last-flush-time

--------------------------------------------------------------------------------
  GE1/0/1                PRIMARY   ACTIVE  5               16:45:20 2014/04/21

  GE1/0/2                SECONDARY STANDBY 1               16:37:20 2014/04/21
```

display smart-link flush コマンドを使用し、デバイスが受信した flush メッセージを表示します。

Device B 上で受信した flush メッセージを表示します。

```
[DeviceB] display smart-link flush
 Received flush packets                              : 5
 Receiving interface of the last flush packet        : GigabitEthernet1/0/3
 Receiving time of the last flush packet             : 16:50:21 2014/04/21
 Device ID of the last flush packet                  : 000f-e23d-5af0
 Control VLAN of the last flush packet               : 10
```

5.6.2 複数 Smart Link グループの負荷分散の設定例

I. ネットワーク要件

図 5-3に示すようなネットワークで設定します。

- Device C は Smart Link 装置です。Device A、Device B、Device D は関連装置です。Device C 上の VLAN 1～VLAN 200 のトラフィックは、Device B と Device D によって Device A に 2 重にアップリンクされています。
- Device C のアップリンクのバックアップと負荷分散を実装します。VLAN 1～VLAN 100 のトラフィックは、Device B によって Device A にアップリンクされ、VLAN 101～VLAN 200 のトラフィックは、Device D によって Device A にアップリンクされています。

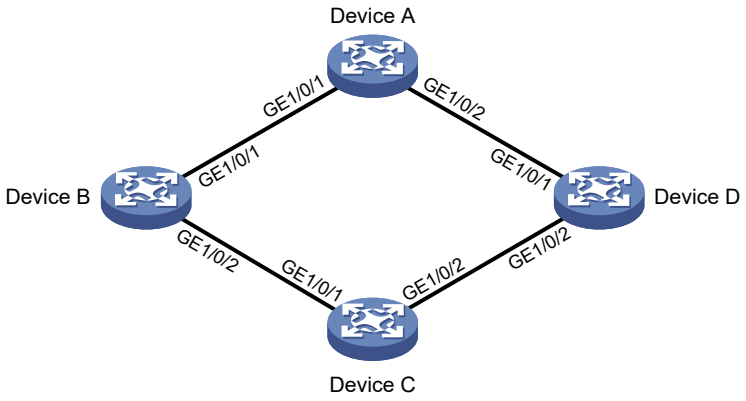


図 5-3 ネットワーク図

II. 設定手順

1)　Device C を設定します。

VLAN 1～VLAN 200 を作成します。VLAN 1～ VLAN 100 を MSTI 1 にマッピングします。VLAN 101～VLAN 200 を MSTI 2 にマッピングします。MST region 設定をアクティブにします。

```
<DeviceC> system-view
[DeviceC] vlan 1 to 200
[DeviceC] stp region-configuration
[DeviceC-mst-region] instance 1 vlan 1 to 100
[DeviceC-mst-region] instance 2 vlan 101 to 200
[DeviceC-mst-region] active region-configuration
[DeviceC-mst-region] quit
```

GigabitEthernet 1/0/1 と GigabitEthernet 1/0/2 をシャットダウンします。GigabitEthernet 1/0/1 と GigabitEthernet 1/0/2 上のスパニングツリー機能を無効にします。トランクポートとして設定し、VLAN 1～VLAN 200 に割り当てます。

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] shutdown
[DeviceC-GigabitEthernet1/0/1] undo stp enable
[DeviceC-GigabitEthernet1/0/1] port link-type trunk
[DeviceC-GigabitEthernet1/0/1] port trunk permit vlan 1 to 200
[DeviceC-GigabitEthernet1/0/1] quit
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] shutdown
```

```
[DeviceC-GigabitEthernet1/0/2] undo stp enable
[DeviceC-GigabitEthernet1/0/2] port link-type trunk
[DeviceC-GigabitEthernet1/0/2] port trunk permit vlan 1 to 200
[DeviceC-GigabitEthernet1/0/2] quit
```

Smart Link グループ 1 を作成し、すべての VLAN を Smart Link グループ 1 のプロテクト VLAN として MSTI 1 にマッピングします。

```
[DeviceC] smart-link group 1
[DeviceC-smlk-group1] protected-vlan reference-instance 1
```

Smart Link グループ 1 の primary ポートとして GigabitEthernet 1/0/1 を設定し、secondary ポートとして GigabitEthernet 1/0/2 を設定します。

```
[DeviceC-smlk-group1] port gigabitethernet 1/0/1 primary
[DeviceC-smlk-group1] port gigabitethernet 1/0/2 secondary
```

Smart Link グループ 1 で role preemption を有効にし、flush メッセージの送信を有効にします。送信制御 VLAN として VLAN 10 を設定します。

```
[DeviceC-smlk-group1] preemption mode role
[DeviceC-smlk-group1] flush enable control-vlan 10
[DeviceC-smlk-group1] quit
```

Smart Link グループ 2 を作成し、すべての VLAN を Smart Link グループ 2 のプロテクト VLAN として MSTI 2 にマッピングします。

```
[DeviceC] smart-link group 2
[DeviceC-smlk-group2] protected-vlan reference-instance 2
```

Smart Link グループ 2 の secondary ポートとして GigabitEthernet 1/0/1 を設定し、primary ポートとして GigabitEthernet 1/0/2 を設定します。

```
[DeviceC-smlk-group2] port gigabitethernet 1/0/2 primary
[DeviceC-smlk-group2] port gigabitethernet 1/0/1 secondary
```

Smart Link グループ 2 で role preemption を有効にします。flush メッセージの送信を有効にします。送信制御 VLAN として VLAN 110 を設定します。

```
[DeviceC-smlk-group2] preemption mode role
[DeviceC-smlk-group2] flush enable control-vlan 110
[DeviceC-smlk-group2] quit
```

GigabitEthernet 1/0/1 と GigabitEthernet 1/0/2 を再度アップにします。

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] undo shutdown
[DeviceC-GigabitEthernet1/0/1] quit
[DeviceC] interface gigabitethernet 1/0/2
```

```
[DeviceC-GigabitEthernet1/0/2] undo shutdown
[DeviceC-GigabitEthernet1/0/2] quit
```

2)　Device B を設定します。

VLAN 1～VLAN 200 を作成します。

```
<DeviceB> system-view
[DeviceB] vlan 1 to 200
```

GigabitEthernet 1/0/1 をトランクポートとして設定し、VLAN 1～VLAN 200 に割り付けます。flush メッセージの受信を有効にし、VLAN 10 と VLAN 110 を GigabitEthernet 1/0/1 の受信制御 VLAN として設定します。

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port link-type trunk
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 1 to 200
[DeviceB-GigabitEthernet1/0/1] smart-link flush enable control-vlan 10 110
[DeviceB-GigabitEthernet1/0/1] quit
```

GigabitEthernet 1/0/2 をトランクポートとして設定し、VLAN 1～VLAN 200 に割り付けます。スパニングツリー機能を無効にします。flush メッセージの受信を有効にします。VLAN 10 と VLAN 110 を受信制御 VLAN として設定します。

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] port link-type trunk
[DeviceB-GigabitEthernet1/0/2] port trunk permit vlan 1 to 200
[DeviceB-GigabitEthernet1/0/2] undo stp enable
[DeviceB-GigabitEthernet1/0/2] smart-link flush enable control-vlan 10 110
[DeviceB-GigabitEthernet1/0/2] quit
```

3)　Device D を設定します。

VLAN 1～VLAN 200 を作成します。

```
<DeviceD> system-view
[DeviceD] vlan 1 to 200
```

GigabitEthernet 1/0/1 をトランクポートとして設定し、VLAN 1～VLAN 200 に割り付けます。flush メッセージの受信を有効にし、VLAN 10 と VLAN 110 を GigabitEthernet 1/0/1 の受信制御 VLAN として設定します。

```
[DeviceD] interface gigabitethernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] port link-type trunk
[DeviceD-GigabitEthernet1/0/1] port trunk permit vlan 1 to 200
[DeviceD-GigabitEthernet1/0/1] smart-link flush enable control-vlan 10 110
[DeviceD-GigabitEthernet1/0/1] quit
```

GigabitEthernet 1/0/2 をトランクポートとして設定し、VLAN 1～VLAN 200 に割り付けます。スパニングツリー機能を無効にします。flush メッセージの受信を有効にします。VLAN 10 と VLAN 110 を受信制御 VLAN として設定します。

```
[DeviceD] interface gigabitethernet 1/0/2
[DeviceD-GigabitEthernet1/0/2] port link-type trunk
[DeviceD-GigabitEthernet1/0/2] port trunk permit vlan 1 to 200
[DeviceD-GigabitEthernet1/0/2] undo stp enable
[DeviceD-GigabitEthernet1/0/2] smart-link flush enable control-vlan 10 110
[DeviceD-GigabitEthernet1/0/2] quit
```

4) Device A を設定します。

VLAN 1～VLAN 200 を作成します。

```
<DeviceA> system-view
[DeviceA] vlan 1 to 200
```

GigabitEthernet 1/0/1 と GigabitEthernet 1/0/2 をトランクポートとして設定し、VLAN 1～VLAN 200 に割り付けます。flush メッセージの受信を有効にし、VLAN 10 と VLAN 110 をポートの受信制御 VLAN として設定します。

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-type trunk
[DeviceA-GigabitEthernet1/0/1] port trunk permit vlan 1 to 200
[DeviceA-GigabitEthernet1/0/1] smart-link flush enable control-vlan 10 110
[DeviceA-GigabitEthernet1/0/1] quit
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port link-type trunk
[DeviceA-GigabitEthernet1/0/2] port trunk permit vlan 1 to 200
[DeviceA-GigabitEthernet1/0/2] smart-link flush enable control-vlan 10 110
[DeviceA-GigabitEthernet1/0/2] quit
```

III. 設定の確認

display smart-link group コマンドを使用し、デバイス上の Smart Link グループの設定を表示します。

Device C 上の Smart Link グループの設定を表示します。

```
[DeviceC] display smart-link group all
Smart link group 1 information:
  Device ID       : 000f-e23d-5af0
  Preemption mode : ROLE
  Preemption delay: 1(s)
  Control VLAN    : 10
  Protected VLAN  : Reference Instance 1

  Member                  Role      State   Flush-count     Last-flush-time

--------------------------------------------------------------------------------
```

```
  GE1/0/1                PRIMARY   ACTIVE  5              16:45:20 2014/04/21

  GE1/0/2                SECONDARY STANDBY 1              16:37:20 2014/04/21

Smart link group 2 information:
  Device ID       : 000f-e23d-5af0
  Preemption mode : ROLE
  Preemption delay: 1(s)
  Control VLAN    : 110
  Protected VLAN  : Reference Instance 2

  Member                  Role      State   Flush-count     Last-flush-time

--------------------------------------------------------------------------------
  GE1/0/2                PRIMARY   ACTIVE  5              16:45:20 2014/04/21

  GE1/0/1                SECONDARY STANDBY 1              16:37:20 2014/04/21
```

display smart-link flush コマンドを使用し、デバイスが受信した flush メッセージを表示することができます。

Device B 上で受信した flush メッセージを表示します。

```
[DeviceB] display smart-link flush
 Received flush packets                              : 5
 Receiving interface of the last flush packet        : GigabitEthernet1/0/2
 Receiving time of the last flush packet             : 16:25:21 2014/04/21
 Device ID of the last flush packet                  : 000f-e23d-5af0
 Control VLAN of the last flush packet               : 10
```

目次

このセクションのページは **10-x-x** です。

6 章 Monitor Link 6-1
6.1 概要 6-1
6.2 設定の制限とガイドライン 6-2
6.3 Monitor Link の設定作業リスト 6-2
6.4 Monitor Link グループの作成 6-2
6.5 Monitor Link グループメンバインタフェースの設定 6-2
6.5.1 monitor link group view での設定 6-3
6.5.2 interface view での設定 6-3
6.6 Monitor Link の表示と維持 6-3
6.7 Monitor Link の設定例 6-4

6章 Monitor Link

6.1 概要

Monitor Link はダウンリンクインタフェースの状態を Monitor Link グループのアップリンクインタフェースの状態に関連づけます。アップリンクが故障したため、Monitor Link がダウンリンクインタフェースをシャットダウンする場合、下流の装置が別のリンクに接続を変更します。

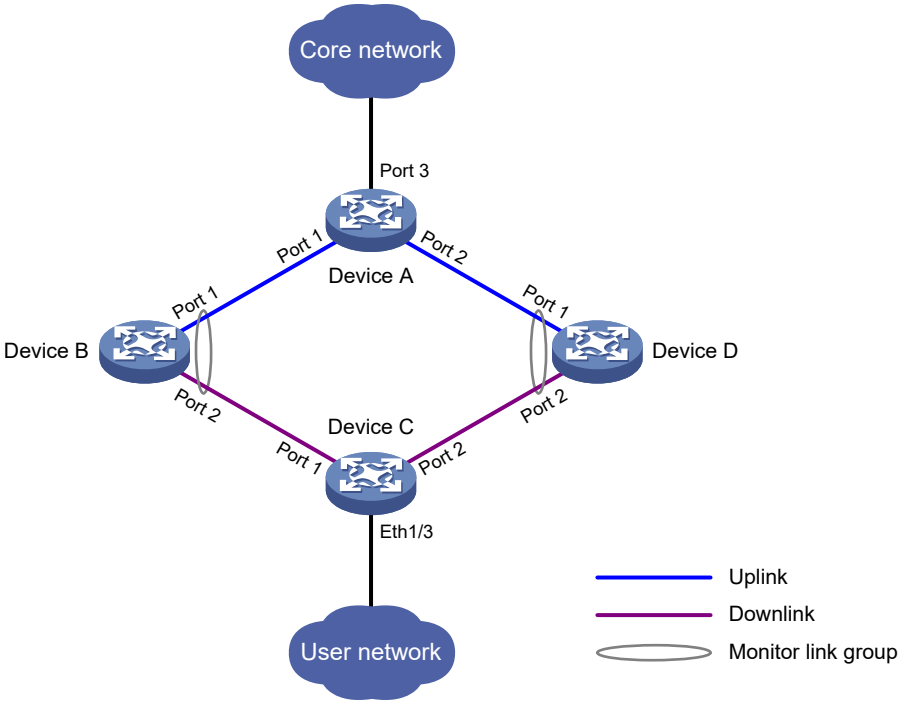


図 6-1 Monitor Link アプリケーションシナリオ

Monitor Link グループはアップリンクインタフェースとダウンリンクインタフェースが含まれます。インタフェースは 1 つの Monitor Link グループにのみ所属します。

- アップリンクインタフェースは監視されるインタフェースです。Monitor Link グループの状態は、そのメンバアップリンクインタフェースの状態と関連します。Monitor Link グループ内のアップ状態にあるアップリンクインタフェースの数が指定されたしきい値より小さい場合、Monitor Link グループはダウンとなりダウンリンクインタフェースはシャットダウンします。アップ状態にあるアップリンクインタフェースの数がしきい値に戻ると、Monitor Link グループはアップしダウンリンクインタフェースもアップになります。
- ダウンリンクインタフェースは監視するインタフェースです。ダウンインタフェースの状態は Monitor Link グループの状態と関連します。Monitor Link グループの状態が変化すると、メンバダウンリンクインタフェースの状態がグループ状態に一致するように変更します。

図 6-1は以下のような構成となります。

- Device B の Port 1 と Port 2 が Monitor Link グループとなります。
- Device D の Port 1 と Port 2 が別の Monitor Link グループとなります。
- Port 1 は両方の Device のアップリンクインタフェースで、Port 2 は両方の Device のダウンリンクインタフェースです。

Monitor Link グループの動作は、他の Monitor Link グループの動作と独立しています。Monitor Link グループ内のアップ状態にあるアップリンクインタフェースの数が指定されたしきい値より小さい場合、Monitor Link グループはダウンとなりダウンリンクインタフェースはシャットダウンします。アップ状態にあるアップリンクインタフェースの数がしきい値に戻ると、Monitor Link グループはアップしダウンリンクインタフェースもアップになります。

6.2 設定の制限とガイドライン

Monitor Link を設定するとき、以下の制限とガイドラインに従ってください。

- Monitor Link グループのダウンリンクインタフェースを手動でシャットダウンあるいはアップさせないでください。

6.3 Monitor Linkの設定作業リスト

作業リスト
（必須設定項目）Monitor Linkグループの作成
（必須設定項目）Monitor Linkグループメンバインタフェースの設定

6.4 Monitor Linkグループの作成

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. Monitor Link グループを作成し monitor link group view に移行する	**monitor-link group** *group-id*	デフォルト：設定なし

6.5 Monitor Linkグループメンバインタフェースの設定

Monitor Link グループのメンバインタフェースを monitor link group view か interface view のどちらかで設定することができます。2 つの view で行った設定は同じ効果を持ちます。以下のインタフェースは Monitor Link グループのメンバインタフェースの設定として設定することができます。

- レイヤ 2 イーサネットインタフェース、アグリゲートインタフェース
- アグリゲーショングループのメンバポート

Monitor Link グループメンバインタフェースを設定するとき、以下のガイドラインに従ってください。

- ダウンリンクインタフェースでダウン/アップ状態が頻繁に変更することをさけるため、ダウンリンクインタフェースを設定する前にアップリンクインタフェースを設定してください。
- Monitor link による中断を防ぐため、同じ Monitor link グループにアグリゲートインタフェース、アグリゲーショングループのメンバポートを割り当てないでください。
- インタフェースは 1 つの Monitor link グループのみ割り当てることができます。

6.5.1 monitor link group view での設定

以下に monitor link group view で Monitor Link グループのメンバインタフェースの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. monitor link group view に移行する	**monitor-link group** *group-id*	―
3. Monitor Link グループのメンバインタフェースを設定する	**port** *interface-type interface-number* { **downlink** | **uplink** }	デフォルト：設定なし

6.5.2 interface view での設定

以下に interface view で Monitor Link グループのメンバインタフェースの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. interface view に移行する	**interface** *interface-type interface-number*	―
3. Monitor Link グループのメンバとして現在のインタフェースを設定する	**port monitor-link group** *group-id* { **downlink** | **uplink** }	デフォルト：設定なし

6.6 Monitor Linkの表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
Monitor linkグループの情報を表示する	**display monitor-link group** { *group-id* | **all** }

6.7 Monitor Linkの設定例

I. ネットワーク要件

図 6-2に示すようなネットワークで設定します。

- Device C は Smart link 装置で、Device A、Device B、Device D は関連装置です。Device C 上の VLAN 1～VLAN 30 のトラフィックは Smart Link グループを介して Device A にデュアルアップリンクされます。
- Device C はデュアルアップリンクのバックアップを実装します。Device A と Device B（または Device D）間でリンク障害が発生した際に、Device C はリンク障害を察知し、Smart Link グループ内でリンク切り替えを行います。

Smart Link の詳細はオペレーションマニュアルのセクション 10 *高可用性* "*Smart Link*"を参照してください。

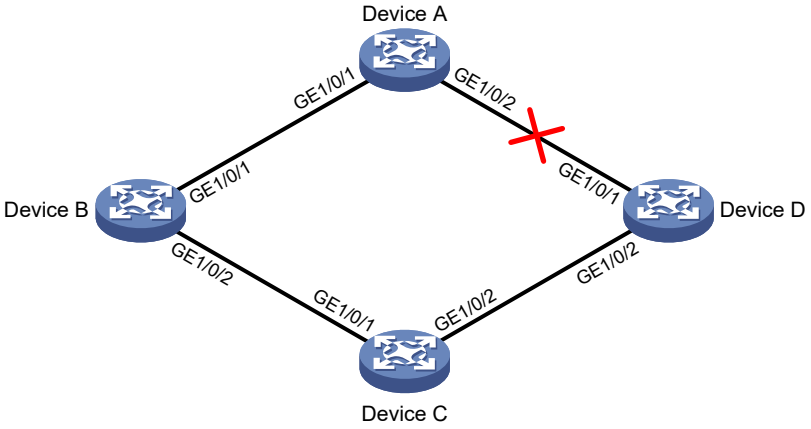


図 6-2 ネットワーク図

II. 設定手順

1)　Device C を設定します。

VLAN 1～VLAN 30 を作成します。

```
<DeviceC> system-view
[DeviceC] vlan 1 to 30
```

MSTI 1 に VLAN をマッピングします。

```
[DeviceC] stp region-configuration
[DeviceC-mst-region] instance 1 vlan 1 to 30
```

MST region 設定を動作させます。

```
[DeviceC-mst-region] active region-configuration
[DeviceC-mst-region] quit
```

GigabitEthernet 1/0/1 をシャットダウンします。

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] shutdown
```

インタフェースでスパニングツリー機能を無効にします。

```
[DeviceC-GigabitEthernet1/0/1] undo stp enable
```

トランクポートとしてインタフェースを設定します。

```
[DeviceC-GigabitEthernet1/0/1] port link-type trunk
```

インタフェースを VLAN 1～VLAN 30 に割り当てます。

```
[DeviceC-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceC-GigabitEthernet1/0/1] quit
```

GigabitEthernet 1/0/1 の設定と同様に GigabitEthernet 1/0/2 を設定します。

```
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] shutdown
[DeviceC-GigabitEthernet1/0/2] undo stp enable
[DeviceC-GigabitEthernet1/0/2] port link-type trunk
[DeviceC-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
[DeviceC-GigabitEthernet1/0/2] quit
```

Smart Link グループ 1 を作成し、プロテクト VLAN として MSTI 1 にすべての VLAN をマッピングします。

```
[DeviceC] smart-link group 1
[DeviceC-smlk-group1] protected-vlan reference-instance 1
```

Smart Link グループ 1 の primary ポートとして GigabitEthernet 1/0/1 を設定し、secondary ポートとして GigabitEthernet 1/0/2 を設定します。

```
[DeviceC-smlk-group1] port gigabitethernet 1/0/1 primary
[DeviceC-smlk-group1] port gigabitethernet 1/0/2 secondary
```

Smart Link グループで flush メッセージの送信を有効にします。

```
[DeviceC-smlk-group1] flush enable
[DeviceC-smlk-group1] quit
```

GigabitEthernet 1/0/1 と GigabitEthernet 1/0/2 を再度リンクアップにします。

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] undo shutdown
[DeviceC-GigabitEthernet1/0/1] quit
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] undo shutdown
```

```
[DeviceC-GigabitEthernet1/0/2] quit
```

2)　Device A を設定します。

VLAN 1～VLAN 30 を作成します。

```
<DeviceA> system-view
[DeviceA] vlan 1 to 30
```

GigabitEthernet 1/0/1 を設定します。

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-type trunk
```

インタフェースに VLAN 1～VLAN 30 を割り当てます。

```
[DeviceA-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
```

インタフェースで flush メッセージの受信を有効にします。

```
[DeviceA-GigabitEthernet1/0/1] smart-link flush enable
[DeviceA-GigabitEthernet1/0/1] quit
```

GigabitEthernet 1/0/1 の設定と同様に GigabitEthernet 1/0/2 を設定します。

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port link-type trunk
[DeviceA-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
[DeviceA-GigabitEthernet1/0/2] smart-link flush enable
[DeviceA-GigabitEthernet1/0/2] quit
```

3)　Device B を設定します。

VLAN 1～VLAN 30 を作成します。

```
<DeviceB> system-view
[DeviceB] vlan 1 to 30
```

トランクポートとして GigabitEthernet 1/0/1 を設定します。

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port link-type trunk
```

インタフェースに VLAN 1～VLAN 30 を割り当てます。

```
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
```

インタフェースで flush メッセージの受信を有効にします。

```
[DeviceB-GigabitEthernet1/0/1] smart-link flush enable
[DeviceB-GigabitEthernet1/0/1] quit
```

GigabitEthernet 1/0/2 でスパニングツリー機能を無効にします。

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] undo stp enable
```

トランクポートとしてインタフェースを設定します。

```
[DeviceB-GigabitEthernet1/0/2] port link-type trunk
```

インタフェースに VLAN 1～VLAN 30 を割り当てます。

```
[DeviceB-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
```

インタフェースで flush メッセージの受信を有効にします。

```
[DeviceB-GigabitEthernet1/0/2] smart-link flush enable
[DeviceB-GigabitEthernet1/0/2] quit
```

Monitor Link グループ 1 を作成します。

```
[DeviceB] monitor-link group 1
```

Monitor Link グループ 1 のアップリンクインタフェースとして GigabitEthernet 1/0/1 を設定します。

```
[DeviceB-mtlk-group1] port gigabitethernet 1/0/1 uplink
```

Monitor Link グループ 1 のダウンリンクインタフェースとして GigabitEthernet 1/0/2 を設定します。

```
[DeviceB-mtlk-group1] port gigabitethernet 1/0/2 downlink
[DeviceB-mtlk-group1] quit
```

4)　Device D を設定します。

VLAN 1～VLAN 30 を作成します。

```
<DeviceD> system-view
[DeviceD] vlan 1 to 30
```

トランクポートとして GigabitEthernet 1/0/1 を設定します。

```
[DeviceD] interface gigabitethernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] port link-type trunk
```

インタフェースに VLAN 1～VLAN 30 を割り当てます。

```
[DeviceD-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
```

インタフェースで flush メッセージの受信を有効にします。

```
[DeviceD-GigabitEthernet1/0/1] smart-link flush enable
[DeviceD-GigabitEthernet1/0/1] quit
```

GigabitEthernet 1/0/2 でスパニングツリー機能を無効にします。

```
[DeviceD] interface gigabitethernet 1/0/2
[DeviceD-GigabitEthernet1/0/2] undo stp enable
```

トランクポートとしてインタフェースを設定します。

```
[DeviceD-GigabitEthernet1/0/2] port link-type trunk
```

インタフェースに VLAN 1～VLAN 30 を割り当てます。

```
[DeviceD-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
```

インタフェースで flush メッセージの受信を有効にします。

```
[DeviceD-GigabitEthernet1/0/2] smart-link flush enable
[DeviceD-GigabitEthernet1/0/2] quit
```

Monitor Link グループ 1 を作成します。

```
[DeviceD] monitor-link group 1
```

Monitor Link グループ 1 のアップリンクインタフェースとして GigabitEthernet 1/0/1 を設定します。

```
[DeviceD-mtlk-group1] port gigabitethernet 1/0/1 uplink
```

Monitor Link グループ 1 のダウンリンクインタフェースとして GigabitEthernet 1/0/2 を設定します。

```
[DeviceD-mtlk-group1] port gigabitethernet 1/0/2 downlink
[DeviceD-mtlk-group1] quit
```

III. 設定の確認

リンク障害のため、Device A 上の GigabitEthernet 1/0/2 がダウンしたとき、Device B の Monitor Link グループ 1 の情報を確認します。

```
[DeviceB] display monitor-link group 1
 Monitor link group 1 information:
  Group status     : UP
  Downlink up-delay: 0(s)
  Last-up-time     : 16:38:26 2014/4/21
  Last-down-time   : 16:37:20 2014/4/21
  Up-port-threshold: 1

  Member                    Role       Status
  ------------------------------------------
  GE1/0/1                  UPLINK     UP
  GE1/0/2                  DOWNLINK   UP
```

Device D の Monitor Link グループ 1 の情報を確認します。

```
[DeviceD] display monitor-link group 1
Monitor link group 1 information:
  Group status     : DOWN
  Downlink up-delay: 0(s)
  Last-up-time     : 16:37:20 2014/4/21
  Last-down-time   : 16:38:26 2014/4/21
  Up-port-threshold: 1

  Member                    Role       Status
  ------------------------------------------
  GE1/0/1                  UPLINK     DOWN
  GE1/0/2                  DOWNLINK   DOWN
```

目次

このセクションのページは **10-x-x** です。

7 章 VRRP 7-1
7.1 概要 7-1
7.2 VRRP standard モード 7-2
7.2.1 VRRP ネットワーク 7-2
7.2.2 仮想 IP アドレスと IP アドレスオーナ 7-2
7.2.3 VRRP グループのルータ優先度 7-2
7.2.4 動作モード 7-3
7.2.5 認証方式 7-3
7.2.6 VRRP タイマ 7-3
7.2.7 マスタの選定 7-4
7.2.8 VRRP トラッキング 7-4
7.2.9 VRRP アプリケーション 7-5
7.3 プロトコルと標準 7-6
7.4 IPv4 VRRP の設定 7-6
7.4.1 制限とガイドライン 7-6
7.4.2 IPv4 VRRP 設定作業リスト 7-6
7.4.3 IPv4 VRRP バージョンの指定 7-6
7.4.4 IPv4 VRRP グループの設定 7-6
7.4.5 IPv4 VRRP パケット属性の設定 7-8
7.4.6 VRRP に関する SNMP notification の有効化 7-9
7.4.7 IPv4 VRRP の表示と維持 7-9
7.5 IPv6 VRRP の設定 7-10
7.5.1 制限とガイドライン 7-10
7.5.2 IPv6 VRRP 設定作業リスト 7-10
7.5.3 IPv6 VRRP グループの設定 7-10
7.5.4 IPv6 VRRP パケット属性の設定 7-12
7.5.5 IPv6 VRRP の表示と維持 7-13
7.6 IPv4 VRRP 設定例 7-13
7.6.1 VRRP グループが 1 組の場合の設定例 7-13
7.6.2 VRRP グループが複数の場合の設定例 7-16
7.7 IPv6 VRRP 設定例 7-19
7.7.1 VRRP グループが 1 組の場合の設定例 7-19
7.7.2 VRRP グループが複数の場合の設定例 7-22
7.8 VRRP のトラブルシューティング 7-26
7.8.1 エラーメッセージが表示される 7-26
7.8.2 VRRP グループで複数のマスタが現れる 7-27
7.8.3 VRRP の状態が頻繁に遷移する 7-27

7章 VRRP

7.1 概要

一般的に、LAN 上のホストは、デフォルトゲートウェイを設定します。他のネットワーク宛てのパケットはすべてデフォルトゲートウェイに送信されます。図 7-1に示すように、デフォルトゲートウェイが故障したとき、ホストは外部のネットワークと通信することができません。

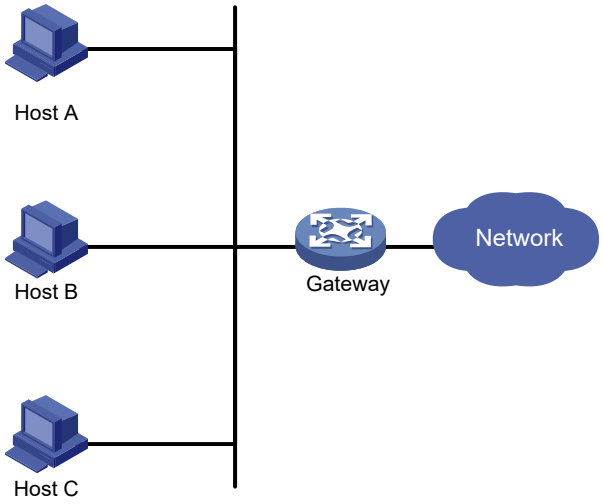


図 7-1 LAN ネットワーク

デフォルトゲートウェイを使用する方法は設定が容易ですが、高い可用性も同時に必要となります。システムの信頼性を高める一般的な方法は、より多くのゲートウェイを使って、ルーティングの問題を複数のゲートウェイ間で解決することです。

VRRP(Virtual Router Redundancy Protocol)はこの問題の対処が可能です。VRRP は VRRP グループへネットワークゲートウェイとなるルータを追加します。これは、仮想ルータと呼ばれます。VRRP グループは 1 つのマスタと複数のバックアップで構成されます。これらの VRRP グループは 1 つの仮想 IP アドレスを持ちます。サブネット上のホストは外部ネットワークと通信するために、デフォルトゲートウェイとして仮想ルータを設定するのみで可能となります。

VRRP は 1 箇所が故障しても他の箇所がカバーすることができ、ホストの設定を簡単にします。マルチキャストあるいはブロードキャスト LAN(Ethernet ネットワークなど)で VRRP グループのマスタが故障しても、ダイナミックルート再計算、ルート再検出、ホストでのゲートウェイの再設定を変更せずに、VRRP グループの別のルータがマスタとして動作することができ、トラフィックの中断を防ぐことができます。

VRRP は以下のモードで動作します。

Standard モード – RFC を元に実装されています。詳細は、オペレーションマニュアルのセクション 10 *高可用性 "VRRP"の" VRRP standard モード"* を参照してください。

VRRP には、VRRPv2 と VRRPv3 の 2 つのバージョンがあります。VRRPv2 は IPv4 VRRP をサポートし、VRRPv3 は IPv4 VRRP と IPv6 VRRP をサポートしています。

7.2 VRRP standardモード

7.2.1 VRRP ネットワーク

図 7-2に示すように、Router A、Router B、Router C は自身の IP アドレスを持つ仮想ルータを形成しています。サブネット上のホストは、デフォルトのゲートウェイとして仮想ルータを使用します。

もっとも優先度が高いルータがマスタに選出されてゲートウェイとなり、他の 2 台はバックアップとなります。VRRP グループのマスタのみがゲートウェイサービスを提供することができます。マスタが故障すると、ゲートウェイサービスを中断させないために、バックアップルータは新しいマスタを選出し、故障したマスタに代わって動作します。

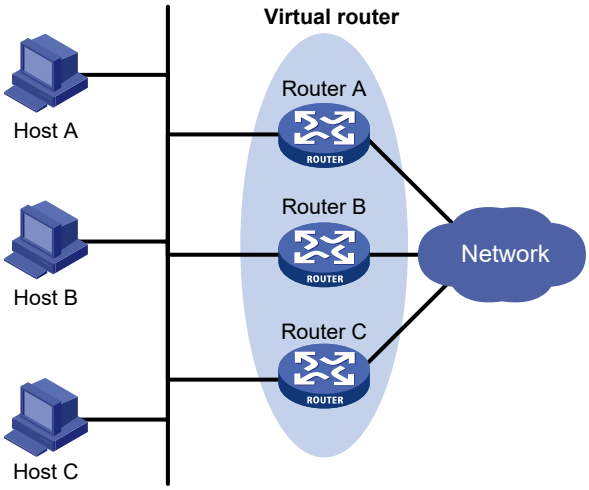


図 7-2 VRRP ネットワーク

7.2.2 仮想 IP アドレスと IP アドレスオーナ

仮想ルータの仮想 IP アドレスは以下の IP アドレスのどちらかを使用できます。

VRRP グループが存在するサブネットで使用されていない IP アドレス
VRRP グループのルータのインタフェースの IP アドレス

後者の場合、ルータは IP アドレスオーナと呼ばれます。VRRP グループは 1 つの IP アドレスオーナのみ持つことができます。

7.2.3 VRRP グループのルータ優先度

VRRP は、優先度によって、VRRP グループの各ルータの役割 (マスタまたはバックアップ) を決定します。優先度が高いほど、マスタになる機会が多くなります。

VRRP の優先度は、0 から 255 の範囲で設定します。大きい数字ほど、優先度が高くなり、1 から 254 の値が設定可能です。0 は特別な用途向けに予約されており、255 は IP アドレ

スオーナ用です。IP アドレスオーナとして機能しているとき、そのルータの優先度は 255 になり設定は変更できません。つまり、IP アドレスオーナは正常に稼働している限り、マスタとして機能します。

7.2.4 動作モード

VRRP グループのルータは、以下のいずれかのモードで動作します。

Non-preemptive モード – VRRP グループのルータが一度マスタになると、その後バックアップルータがより高い優先度を割り当てられた場合でも、正常に動作している限りマスタとして稼動します。Non-preemptive モードはマスタとバックアップルータが頻繁に切り替わることを避けることができます。

Preemptive モード – 優先度が稼働中のマスタルータよりも高いことを検出したバックアップルータは、VRRP グループで新しいマスタルータの選出を開始し、マスタになります。Preemptive モードは VRRP グループのもっとも高い優先度のルータが常にマスタとして動作します。

7.2.5 認証方式

許可されていないユーザからの攻撃を防御するため、VRRP マスタルータは、お互いを認証するため、VRRP パケットに認証キーを追加します。VRRP は以下の認証方式を提供します。

Simple 認証

送信ルータは VRRP パケットに認証キーを追加し、受信ルータは受信した認証キーとローカル認証キーを比較します。もし 2 つの認証キーがマッチする場合、受信した VRRP パケットは正式なパケットとなります。もしマッチしない場合、受信したパケットは不正なパケットとして廃棄されます。

MD5 認証

送信ルータは、認証キーと MD5 アルゴリズムを使用して送信されるパケットを暗号化し、結果を VRRP パケットの認証ヘッダに保存します。パケットを受信したルータは、認証キーでパケットを復号化し、パケットが正式かどうかをチェックします。マッチしない場合、不正なパケットを廃棄します。

セキュアなネットワークでは、認証モードを設定する必要はありません。

🕮 **メモ：**

IP4 VRRPv3 と IPv6 VRRPv3 は VRRP パケット認証をサポートしていません。

7.2.6 VRRP タイマ

I. Skew_Time

Skew_Time は VRRP グループのマスタルータが故障したとき、同時に複数のバックアップルータがマスタルータになることを防ぎます。

Skew_Time は設定不可能で、VRRP のバージョンに依存した値となります。

VRRPv2 (RFC 3768 に記載されています。)

Skew_Time ＝ (256 － ルータ優先度) ／ 256

VRRPv3 (RFC 5798 に記載されています。)

Skew_Time ＝ ((256 － ルータ優先度) × VRRP アドバタイズメント間隔) ／ 256

II. VRRP advertisement interval(VRRP アドバタイズメント間隔)

VRRP グループのマスタルータは、定期的に VRRP アドバタイズメントを送り、VRRP グループ内の他のルータに、正常に稼働していることを通知します。

VRRP advertisement interval タイマを設定することで、VRRP アドバタイズメントの送信間隔を調節できます。バックアップルータが、タイマ(送信間隔の 3 倍＋ Skew_Time)の間にアドバタイズメントを受け取らなければ、マスタが故障したとみなし、バックアップルータは自身がマスタに切り替わります。

III. VRRP preemption delay タイマ

VRRP preemption delay タイマは以下の目的のために設定することができます。

VRRP グループのメンバ間で頻繁に状態が変更されることを防ぎます。

バックアップルータがルーティング情報などの情報を収集するのに十分な時間を提供します。

preempt モードでは、バックアップルータは、ローカル優先度よりも低い優先度のアドバタイズメントを受信した後、すぐにマスタルータになりません。マスタに変わる前に、preemption delay ＋ Skew_Time の期間、経過した後にマスタルータに切り替わります。

7.2.7 マスタの選定

VRRP グループのルータは優先度によって役割を決めます。ルータが VRRP に加入したとき、役割はバックアップとなります。ルータの役割は以下の状況にしたがって変更します。

バックアップルータがタイマ(3 × アドバタイズメント間隔 ＋ Skew_Time)が終了したとき、マスタルータになります。

タイマ(3 × アドバタイズメント間隔 ＋ Skew_Time)の時間内に、バックアップルータが高いあるいは同一の優先度の VRRP アドバタイズメントを受信したとき、バックアップルータのままとなります。

タイマ(3 × アドバタイズメント間隔 ＋ Skew_Time)の時間内に、バックアップルータが低い優先度の VRRP アドバタイズメントを受信したとき、以下の結果となります。

- non-preemptive モードではバックアップルータのままとなります。
- preemptive モードではマスタルータとなります。

選定されたマスタルータは、VRRP アドバタイズメント間隔を開始し、マスタルータが正常に動作していることを通知するため、周期的に VRRP アドバタイズメントをバックアップルータに送信します。各バックアップルータはマスタからのアドバタイズメントを待つタイマを開始します。

VRRP グループの複数のルータが、ネットワークの問題によって、マスタと宣言したとき、もっとも高い優先度のルータがマスタルータとなります。もし 2 つのルータが同一の優先度を持つとき、もっとも高い IP アドレスを持つルータがマスタルータとなります。

7.2.8 VRRP トラッキング

VRRP トラッキング機能はマスタあるいは上流リンクの状態をモニタするため、NQA（network quality analyzer）あるいは BFD（bidirectional forwarding detection）を使用し

ます。トラック機能を通した VRRP 装置の状態と NQA 間のコラボレーション、あるいは VRRP 装置の状態と BFD 間のコラボレーションは以下の機能を確立します。

上流のリンクをモニタし、リンクの状態にしたがってルータの優先度を変更します。上流のリンクが故障したとき、サブネットのホストはルータを通して外部ネットワークにアクセスできません。トラックエントリの状態は Negative になります。マスタの優先度は指定された値に減少し、VRRP グループのもっとも高い優先度を持つルータがマスタになります。この切り替えによって、サブネットのホストと外部ネットワーク間での通信を中断しません。

バックアップのマスタの状態をモニタします。マスタが故障したとき、バックアップは通信を中断しないようにするため、即座にマスタに切り替わります。

トラックエントリが Negative から Positive あるいは Notready に変更したとき、ルータは自動的に優先度を回復します。トラックエントリの詳細は、オペレーションマニュアルのセクション 10 *高可用性* "*Track*"を参照してください。

VRRP トラッキング機能を有効にする場合、最初に VRRP グループ内のルータを preemptive モードに設定しておく必要があります。もっとも高い優先順位を持つルータが常にパケット転送のためのマスタとして動作できるようにします。

7.2.9 VRRP アプリケーション

I. マスタ／バックアップ

マスタ／バックアップモードでは、図 7-3に示すようにマスタのみがパケットを転送します。マスタルータが故障すると新しいマスタルータがバックアップルータから選定されます。このモードでは 1 つの VRRP グループのみが必要で、グループの各ルータは異なる優先度を持ちます。もっとも高い優先度を持つルータがマスタになります。

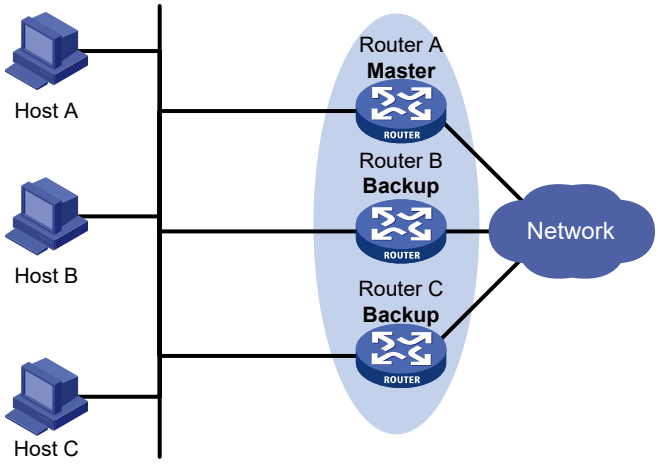


図 7-3 マスタ／バックアップモードの VRRP

Router A が外部ネットワークにパケットを転送するためマスタルータとして動作し、Router B と Router C が listening 状態のバックアップルータであると仮定します。Router A が故障したとき、サブネット上のホストのパケットを転送するため、Router B と Router C は新しいマスタルータを選択します。

7.3 プロトコルと標準

RFC 3768, Virtual Router Redundancy Protocol (VRRP)
RFC 5798, *Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6*

7.4 IPv4 VRRPの設定

7.4.1 制限とガイドライン

IPv4 VRRP はアグリゲーショングループのメンバポートでは適用されません。
IPv4 VRRP グループのルータの設定は一致している必要があります。

7.4.2 IPv4 VRRP 設定作業リスト

作業リスト
(オプション設定項目) IPv4 VRRPバージョンの指定
(必須設定項目) VRRPグループの設定
(オプション設定項目) IPv4 VRRPパケット属性の設定
(オプション設定項目) VRRPに関するSNMP notificationの有効化

7.4.3 IPv4 VRRP バージョンの指定

I. IPv4 VRRP バージョン

IPv4 VRRP は VRRPv2、VRRPv3 を使用します。

II. 制限とガイドライン

IPv4 VRRP グループのすべてのルータの VRRP バージョンは同一にする必要があります。

III. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. interface view に移行する	**interface** *interface-type interface-number*	―
3. VRRP のバージョンを指定する	**vrrp version** *version-number*	デフォルト：VRRPv3

7.4.4 IPv4 VRRP グループの設定

I. IPv4 VRRP グループ

VRRP グループは、作成後に正しく動作し、1 つ以上の仮想 IP アドレスを割り当てることができます。インタフェース上の VRRP グループに複数の仮想 IP アドレスを設定して、異なるサブネット上のルータバックアップ用の複数のサブネットに接続できます。

IPv4 VRRP グループを無効にすると、VRRP グループは **Initialize** 状態になり、VRRP グループ上の既存の設定は変更されません。 VRRP グループの設定を変更できます。 変更は、VRRP グループを再度有効にすることで変更されます。

II. 制限とガイドライン

項目	備考
仮想IPアドレス	VRRPグループの仮想IPアドレスは次のいずれかのアドレスになります。 ● VRRPグループが存在するサブネットで未使用のIPアドレス ● VRRPグループのルータのインタフェースのIPアドレス 設定されている仮想IPアドレスを持たないIPv4 VRRPグループは、他の設定(優先順位とpreemptionモードなど)が利用可能になっている装置でのみ有効です。このようなVRRPグループはinactive状態で、動作しません。 サブネット内のホストが外部ネットワークにアクセスする場合、同一サブネットに以下のアドレスを設定する必要があります。 ● IPv4 VRRPグループの仮想IPアドレス ● VRRPグループメンバの下流インタフェースのIPアドレス
IPアドレスオーナ	ルータがVRRPグループのIPアドレスオーナである場合、ネイバとの接続を確立するため、VRRPグループの仮想IPアドレスを所有するインタフェースで**network**コマンドを使用してOSPFを有効にしないでください。あるいはVRRPグループの仮想IPアドレスを使用しないでください。**network**コマンドについての詳細は、コマンドマニュアルのセクション5 *ルーティングプロトコル "OSPF"* を参照してください。 IPアドレスオーナのVRRPグループの削除は、IPアドレスコリジョンの原因となります。コリジョンを防ぐため、インタフェースからVRRPグループを削除する前に、IPアドレスオーナのインタフェースでIPアドレスを変更してください。 IPアドレスオーナの優先度は常に255です。設定する必要はありません。 IPアドレスオーナは常にpreemptiveモードで動作します。 IPアドレスオーナで**vrrp vrid track priority reduced**コマンドあるいは**vrrp vrid track switchover**コマンドを設定した場合、設定はルータがIPアドレスオーナでなくなるまで有効になりません
VRRPとtrackエントリの関連づけ	TrackエントリがNegativeからPositiveまたはNotreadyに変更されると、ルータは自動的に優先度をもとに戻し、失敗したマスタルータは再びマスタになります。

III. VRRP グループの作成と仮想 IP アドレスの割り当て

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. interface view に移行する	**interface** *interface-type interface-number*	—
3. VRRP グループを作成し、仮想 IP アドレスを設定する	**vrrp vrid** *virtual-router-id* **virtual-ip** *virtual-address*	—

IV. IPv4 VRRP グループの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. interface view に移行する	**interface** *interface-type interface-number*	—

操作	コマンド	補足
3. VRRP グループのルータの優先度を設定する	**vrrp vrid** *virtual-router-id* **priority** *priority-value*	デフォルト：100
4. VRRP グループのルータの preemptive モードを有効にし、preemption delay タイマを設定する	**vrrp vrid** *virtual-router-id* **preempt-mode** [**delay** *delay-value*]	デフォルト：ルータは preemptive モードで動作し、preemption delay タイマは0秒で、切り替えはすぐに発生します。
5. VRRP グループを Track エントリに関連づける	**vrrp vrid** *virtual-router-id* **track** *track-entry-number* { **forwarder-switchover member-ip** *ip-address* | **priority reduced** [*priority-reduced*] | **switchover** | **weight reduced** [*weight-reduced*]] }	デフォルト：設定なし

7.4.5 IPv4 VRRP パケット属性の設定

I. 制限とガイドライン

インタフェースの VRRP グループに異なる認証モードと認証キーを設定することができます。しかし同じグループのメンバは同じ認証モードと認証キーを使用する必要があります。

VRRPv2 では、VRRP グループのすべてのルータは同じアドバタイズメント間隔を持つ必要があります。

VRRPv3 では、認証モードと認証キーの設定は適用されません。

VRRPv3 では、IPv4 VRRP グループのルータは異なるアドバタイズメント間隔を設定することができます。VRRP グループのマスタは指定した間隔で VRRP アドバタイズメントを送信します(アドバタイズメントには設定した間隔が記載されています)。バックアップルータがアドバタイズメントを受信した後、アドバタイズメントの間隔を記録します。もしタイマ(3 × 記録した間隔 + Skew_Time)が終了したときに、マスタから新しい VRRP アドバタイズメントを受信しない場合、マスタが故障したと認識し、新しいマスタに切り替わります。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. interface view に移行する	**interface** *interface-type interface-number*	—
3. IPv4 VRRP グループの VRRP パケットの送受信を行う VRRP グループの認証モードと認証キーを設定する	**vrrp vrid** *virtual-router-id* **authentication-mode** { **md5** | **simple** } { **cipher** | **plain** } *key*	デフォルト：認証は無効です。
4. IPv4 VRRP グループのマスタが VRRP アドバタイズメントを送信する間隔を設定する	**vrrp vrid** *virtual-router-id* **timer advertise** *adver-interval*	デフォルト：1秒(100センチ秒) VRRPアドバタイズメント間隔は1秒よりも大きい値に設定することを推奨します。そうでない場合、システムは安定しません。

操作	コマンド	補足
5. VRRP パケットを送受信するための送信元インタフェースを指定する	**vrrp vrid** *virtual-router-id* **source-interface** *interface-type interface-number*	デフォルトでは、VRRPパケットを送受信する送信元インタフェースは指定されていません。VRRPグループが存在するインタフェースは、VRRPパケットを送受信します。
6. IPv4 VRRP パケットの TTL チェックを有効にする	**vrrp check-ttl enable**	デフォルト：有効
7. system view に戻る	**quit**	ー
8. VRRP パケットの DSCP 値を設定する	**vrrp dscp** *dscp-value*	デフォルト：48 DSCP値はパケットの優先度レベルを指定し、パケットの優先度に影響します。

7.4.6 VRRP に関する SNMP notification の有効化

I. VRRP に関する SNMP notification の有効化

SNMP notification を有効にすることで、VRRP に関する重要なイベントを NMS に通知します。NMS は設定された出力ルールにしたがって notification を出力する方法を決定します。SNMP notifications についての詳細は、オペレーションマニュアルのセクション 11 *システム管理* "*SNMP*"を参照してください。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. VRRP に関する SNMP notification を有効にする	**snmp-agent trap enable vrrp** [**auth-failure** | **new-master**]	デフォルト：有効

7.4.7 IPv4 VRRP の表示と維持

すべての view で **display** コマンドを実行でき、user view で **reset** コマンドを実行できます。

操作	コマンド
IPv4 VRRPグループの状態を表示する	**display vrrp** [**interface** *interface-type interface-number* [**vrid** *virtual-router-id*]] [**verbose**]
IPv4 VRRPグループの統計情報を表示する	**display vrrp statistics** [**interface** *interface-type interface-number* [**vrid** *virtual-router-id*]]
IPv4 VRRPグループの統計情報を削除する	**reset vrrp statistics** [**interface** *interface-type interface-number* [**vrid** *virtual-router-id*]]

7.5 IPv6 VRRPの設定

7.5.1 制限とガイドライン

IPv6 VRRP はアグリゲーショングループのメンバポートでは適用されません。
IPv6 VRRP グループのルータの設定は一致している必要があります。

7.5.2 IPv6 VRRP 設定作業リスト

作業リスト
(必須設定項目) IPv6 VRRPグループの設定
(オプション設定項目) IPv6 VRRPパケット属性の設定

7.5.3 IPv6 VRRP グループの設定

I. IPv6 VRRP グループ

VRRP グループは、作成後に正しく動作し、1 つ以上の仮想 IPv6 アドレスを割り当てることができます。インタフェース上の VRRP グループに複数の仮想 IPv6 アドレスを設定して、異なるサブネット上のルータバックアップ用の複数のサブネットに接続できます。

IPv6 VRRP グループを無効にすると、VRRP グループは **Initialize** 状態になり、VRRP グループ上の既存の設定は変更されません。 VRRP グループの設定を変更できます。 変更は、VRRP グループを再度有効にすることで変更されます。

II. 制限とガイドライン

項目	備考
仮想IPv6アドレス	設定されている仮想IPv6アドレスを持たないIPv6 VRRPグループは、他の設定(優先順位とpreemptionモードなど)が利用可能になっている装置でのみ有効です。このようなVRRPグループはinactive状態で、動作しません。 サブネット内のホストが外部ネットワークにアクセスする場合、同一サブネットに以下のアドレスを設定する必要があります。 ● IPv6 VRRPグループの仮想IPv6アドレス ● VRRPグループメンバの下流インタフェースのIPv6アドレス

項目	備考
IPアドレスオーナ	ルータがVRRPグループのIPアドレスオーナである場合、ネイバとの接続を確立するため、VRRPグループの仮想IPv6アドレスを所有するインタフェースで**ospfv3 area**コマンドを使用してOSPFを有効にしないでください。あるいはVRRPグループの仮想IPアドレスを使用しないでください。**ospfv3 area**コマンドについての詳細は、コマンドマニュアルのセクション5 *ルーティングプロトコル* "*OSPFv3*"を参照してください。 IPアドレスオーナのVRRPグループの削除は、IPアドレスコリジョンの原因となります。コリジョンを防ぐため、インタフェースからVRRPグループを削除する前に、IPv6アドレスオーナのインタフェースでIPv6アドレスを変更してください。 IPアドレスオーナの優先度は常に255です。設定する必要はありません。 IPアドレスオーナは常にpreemptiveモードで動作します。 IPアドレスオーナで**vrrp ipv6 vrid track priority reduced**コマンドあるいは**vrrp ipv6 vrid track switchover**コマンドを設定した場合、設定はルータがIPアドレスオーナでなくなるまで有効になりません。 IPアドレスオーナで、VRRPが設定されているインタフェースの重複アドレス検出、Duplicate Address Detection(DAD)を無効にしてください。DADを無効にするには、**ipv6 nd dad attempts**コマンドのintervalを0に設定します。このコマンドの詳細については、コマンドマニュアルのセクション4 *IP サービス* "*IPv6の基本*"を参照してください。
VRRPとtrackエントリの関連づけ	TrackエントリがNegativeからPositiveまたはNotreadyに変更されると、ルータは自動的に優先度をもとに戻し、失敗したマスタルータは再びマスタになります。

III. VRRP グループの作成と仮想 IPv6 アドレスの割り当て

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. interface view に移行する	**interface** *interface-type interface-number*	―
3. IPv6 VRRP グループを作成し、リンクローカルアドレスの仮想 IPv6 アドレスを設定する	**vrrp ipv6 vrid** *virtual-router-id* **virtual-ip** *virtual-address* **link-local**	デフォルト：VRRPグループは存在しません。 VRRPグループの最初の仮想IPv6アドレスは、リンクローカルアドレスでなければなりません。 IPv6 VRRPグループを削除する場合、最後にIPv6アドレスを削除してください。 1つのVRRPグループには1つのリンクローカルアドレスを割り当てることができます。

IV. IPv6 VRRP グループの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. interface view に移行する	**interface** *interface-type interface-number*	―

操作	コマンド	補足
3. グローバルユニキャストアドレスである仮想 IPv6 アドレスを割り当てる	**vrrp ipv6 vrid** *virtual-router-id* **virtual-ip** *virtual-address*	デフォルトでは、グローバルユニキャストアドレスはIPv6 VRRPグループに割り当てられません。
4. IPv6 VRRP グループのルータの優先度を設定する	**vrrp ipv6 vrid** *virtual-router-id* **priority** *priority-value*	デフォルト：100
5. IPv6 VRRP グループのルータの preemptive モードを有効にし、preemption delay タイマを設定する	**vrrp ipv6 vrid** *virtual-router-id* **preempt-mode** [**delay** *delay-value*]	デフォルト：ルータは preemptiveモードで動作し、preemption delayタイマは0秒で、切り替えはすぐに発生します。
6. VRRP グループを Track エントリに関連づける	**vrrp ipv6 vrid** *virtual-router-id* **track** *track-entry-number* { **forwarder-switchover member-ip** *ipv6-address* | **priority reduced** [*priority-reduced*] | **switchover** | **weight reduced** [*weight-reduced*] }	デフォルト：設定なし

7.5.4 IPv6 VRRP パケット属性の設定

I. 制限とガイドライン

IPv6 VRRP グループのルータは異なるアドバタイズメント間隔を設定することができます。IPv6 VRRP グループのマスタは指定した間隔で VRRP アドバタイズメントを送信します(アドバタイズメントには設定した間隔が記載されています)。バックアップルータがアドバタイズメントを受信した後、アドバタイズメントの間隔を記録します。もしタイマ(3 × 記録した間隔＋Skew_Time)が終了する前に、マスタから新しい VRRP アドバタイズメントを受信しない場合、マスタが故障したと認識し、新しいマスタに切り替わります。

ネットワークのトラフィックが高いとき、バックアップルータは、指定した時間内に、マスタから VRRP アドバタイズメントを受信するのに失敗することがあります。その結果、予期しないマスタの切り替えが発生します。この問題を解決するため、アドバタイズメントを送信する間隔は大きい値に設定してください。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. interface view に移行する	**interface** *interface-type interface-number*	―
3. IPv6 VRRP アドバタイズメントを送信する間隔を設定する	**vrrp ipv6 vrid** *virtual-router-id* **timer advertise** *adver-interval*	デフォルト：1秒(100センチ秒) VRRPアドバタイズメント間隔は1秒より大きい値に設定することを推奨します。そうでない場合、システムは安定しません。
4. system view に戻る	**quit**	―

操作	コマンド	補足
5. IPv6 VRRP パケットの DSCP 値を設定する	**vrrp ipv6 dscp** *dscp-value*	デフォルト：56 DSCP値はパケットの優先度レベルを指定し、パケットの優先度に影響します。

7.5.5 IPv6 VRRP の表示と維持

すべての view で **display** コマンドを実行でき、user view で **reset** コマンドを実行できます。

操作	コマンド
IPv6 VRRP グループの状態を表示する	**display vrrp ipv6** [**interface** *interface-type interface-number* [**vrid** *virtual-router-id*]] [**verbose**]
IPv6 VRRP グループの統計情報を表示する	**display vrrp ipv6 statistics** [**interface** *interface-type interface-number* [**vrid** *virtual-router-id*]]
IPv6 VRRP グループの統計情報をクリアする	**reset vrrp ipv6 statistics** [**interface** *interface-type interface-number* [**vrid** *virtual-router-id*]]

7.6 IPv4 VRRP設定例

7.6.1 VRRP グループが 1 組の場合の設定例

I. ネットワーク要件

図 7-4に示すように、Switch A と Switch B は VRRP グループを形成し、Host A があるサブネット用にゲートウェイサービスを提供するために仮想 IP アドレス 10.1.1.111/24 を使用します。

マスタとして Switch A が動作し、Host A から Host B にパケットを転送します。Switch A が故障したとき、Switch B が Host A のパケットを転送するため、マスタに切り替わります。

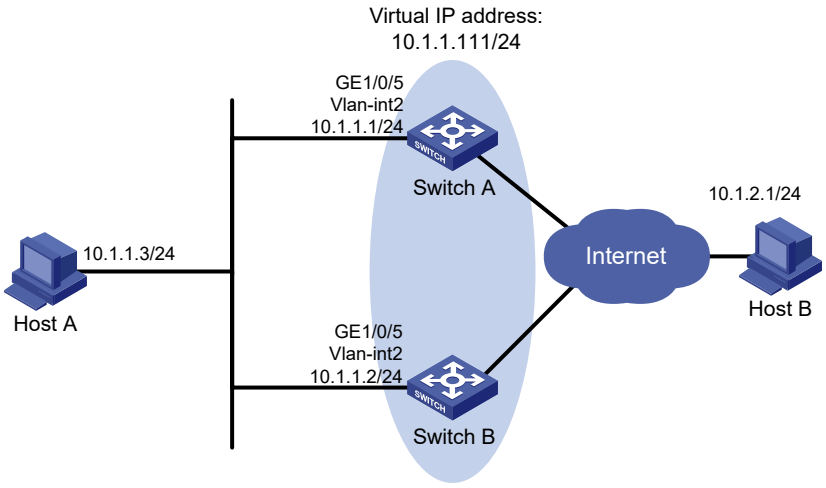


図 7-4 ネットワーク図

II. 設定手順

1)　Switch A を設定します

VLAN 2 を設定します。

```
<SwitchA> system-view
[SwitchA] vlan 2
[SwitchA-vlan2] port gigabitethernet 1/0/5
[SwitchA-vlan2] quit
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ip address 10.1.1.1 255.255.255.0
```

VLAN インタフェース 2 で VRRP グループ 1 を作成し、仮想 IP アドレス 10.1.1.111 を設定します。

```
[SwitchA-Vlan-interface2] vrrp vrid 1 virtual-ip 10.1.1.111
```

Switch A がマスタになるように VRRP グループ 1 の Switch A の優先度を Switch B よりも高い値に割り当てます。

```
[SwitchA-Vlan-interface2] vrrp vrid 1 priority 110
```

いつでも適切にマスタに切り替わることができるように、Switch A を preemptive モードで動作するように設定します。Switch の切り替えが頻繁に発生しないように preemption delay タイマを 5000 センチ秒に設定します。

```
[SwitchA-Vlan-interface2] vrrp vrid 1 preempt-mode delay 5000
```

2)　Switch B を設定します

VLAN 2 を設定します。

```
<SwitchB> system-view
[SwitchB] vlan 2
```

```
[SwitchB-Vlan2] port gigabitethernet 1/0/5
[SwitchB-vlan2] quit
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] ip address 10.1.1.2 255.255.255.0
```

VLAN インタフェース 2 で VRRP グループ 1 を作成し、仮想 IP アドレス 10.1.1.111 を設定します。

```
[SwitchB-Vlan-interface2] vrrp vrid 1 virtual-ip 10.1.1.111
```

VRRP グループ 1 の Switch B の優先度を 100 に設定します。

```
[SwitchB-Vlan-interface2] vrrp vrid 1 priority 100
```

Switch B を preemptive モードで動作するように設定し、preemption delay タイマを 5000 センチ秒に設定します。

```
[SwitchB-Vlan-interface2] vrrp vrid 1 preempt-mode delay 5000
```

III. 設定の確認

Host A から Host B に ping を行います。(詳細は省略します)

Switch A の VRRP グループ 1 の詳細情報を表示します。

```
[SwitchA-Vlan-interface2] display vrrp verbose
IPv4 Virtual Router Information:
 Running Mode      : Standard
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID             : 1                  Adver Timer  : 100
     Admin Status     : Up                 State        : Master
     Config Pri       : 110                Running Pri  : 110
     Preempt Mode     : Yes                Delay Time   : 5000
     Auth Type        : None
     Virtual IP       : 10.1.1.111
     Virtual MAC      : 0000-5e00-0101
     Master IP        : 10.1.1.1
```

Switch B の VRRP グループ 1 の詳細情報を表示します。

```
[SwitchB-Vlan-interface2] display vrrp verbose
IPv4 Virtual Router Information:
 Running Mode      : Standard
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID             : 1                  Adver Timer  : 100
     Admin Status     : Up                 State        : Backup
     Config Pri       : 100                Running Pri  : 100
     Preempt Mode     : Yes                Delay Time   : 5000
     Become Master    : 401ms left
     Auth Type        : None
     Virtual IP       : 10.1.1.111
     Master IP        : 10.1.1.1
```

出力は、Host A から Host B へパケットを転送するため、VRRP グループ 1 のマスタとして Switch A が動作していることを示します。

Host A と Switch A 間のリンクを切断し、Host A が Host B に ping できることを確認します。(詳細は省略します)

Switch B の VRRP グループ 1 の詳細情報を表示します。

```
[SwitchB-Vlan-interface2] display vrrp verbose
IPv4 Virtual Router Information:
 Running Mode       : Standard
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID             : 1                    Adver Timer  : 100
     Admin Status     : Up                   State        : Master
     Config Pri       : 100                  Running Pri  : 100
     Preempt Mode     : Yes                  Delay Time   : 5000
     Auth Type        : None
     Virtual IP       : 10.1.1.111
     Virtual MAC      : 0000-5e00-0101
     Master IP        : 10.1.1.2
```

出力は、Switch A が故障したとき、Host A から Host B のパケットを転送するため、Switch B に切り替わったことを示します。

Host A と Switch A 間のリンクを復旧させ、Switch A の VRRP グループ 1 の詳細情報を表示します。

```
[SwitchA-Vlan-interface2] display vrrp verbose
IPv4 Virtual Router Information:
 Running Mode       : Standard
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID             : 1                    Adver Timer  : 100
     Admin Status     : Up                   State        : Master
     Config Pri       : 110                  Running Pri  : 110
     Preempt Mode     : Yes                  Delay Time   : 5000
     Auth Type        : None
     Virtual IP       : 10.1.1.111
     Virtual MAC      : 0000-5e00-0101
     Master IP        : 10.1.1.1
```

出力は、Switch A が正常動作に戻ったとき、Host A から Host B にパケットを転送するため、Switch A がマスタになることを示します。

7.6.2 VRRP グループが複数の場合の設定例

I. ネットワーク要件

図 7-5に示すように、Switch A と Switch B は 2 つの VRRP グループを形成します。VLAN2 のホストにゲートウェイサービスを提供するため、VRRP グループ 1 は仮想 IP アドレス 10.1.1.100/25 を使用します。VLAN3 のホストにゲートウェイサービスを提供するため、VRRP グループ 2 は仮想 IP アドレス 10.1.1.200/25 を使用します。

2 つの Switch 間で VLAN2 と VLAN3 からのトラフィックを分散させるため、VRRP グループ 1 の Switch A の優先度は Switch B よりも高い値に割り当て、VRRP グループ 2 の Switch A の優先度は Switch B よりも低い値に割り当てます。一方の Switch が故障したとき、正常な Switch が両方の VLAN のゲートウェイサービスを提供します。

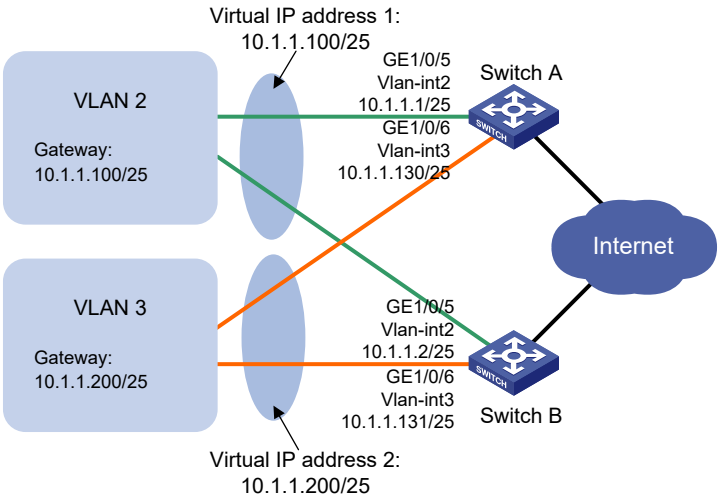


図 7-5 ネットワーク図

II. 設定手順

1)　Switch A を設定します

VLAN 2 を設定します。

```
<SwitchA> system-view
[SwitchA] vlan 2
[SwitchA-vlan2] port gigabitethernet 1/0/5
[SwitchA-vlan2] quit
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ip address 10.1.1.1 255.255.255.128
```

VRRP グループ 1 を作成し、仮想 IP アドレス 10.1.1.100 を設定します。

```
[SwitchA-Vlan-interface2] vrrp vrid 1 virtual-ip 10.1.1.100
```

Switch A がグループでマスタになるように VRRP グループ 1 の Switch A の優先度を Switch B よりも高い値に割り当てます。

```
[SwitchA-Vlan-interface2] vrrp vrid 1 priority 110
[SwitchA-Vlan-interface2] quit
```

VLAN 3 を設定します。

```
[SwitchA] vlan 3
[SwitchA-vlan3] port gigabitethernet 1/0/6
[SwitchA-vlan3] quit
[SwitchA] interface vlan-interface 3
[SwitchA-Vlan-interface3] ip address 10.1.1.130 255.255.255.128
```

VRRP グループ 2 を作成し、仮想 IP アドレス 10.1.1.200 を設定します。

```
[SwitchA-Vlan-interface3] vrrp vrid 2 virtual-ip 10.1.1.200
```

2)　Switch B を設定します。

VLAN 2 を設定します。

```
<SwitchB> system-view
[SwitchB] vlan 2
[SwitchB-vlan2] port gigabitethernet 1/0/5
[SwitchB-vlan2] quit
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] ip address 10.1.1.2 255.255.255.128
```

VRRP グループ 1 を作成し、仮想 IP アドレス 10.1.1.100 を設定します。

```
[SwitchB-Vlan-interface2] vrrp vrid 1 virtual-ip 10.1.1.100
[SwitchB-Vlan-interface2] quit
```

VLAN 3 を設定します。

```
[SwitchB] vlan 3
[SwitchB-vlan3] port gigabitethernet 1/0/6
[SwitchB-vlan3] quit
[SwitchB] interface vlan-interface 3
[SwitchB-Vlan-interface3] ip address 10.1.1.131 255.255.255.128
```

VRRP グループ 2 を作成し、仮想 IP アドレス 10.1.1.200 を設定します。

```
[SwitchB-Vlan-interface3] vrrp vrid 2 virtual-ip 10.1.1.200
```

Switch B がマスタとなるように VRRP グループ 2の Switch B の優先度を Switch A よりも高い値に割り当てます。

```
[SwitchB-Vlan-interface3] vrrp vrid 2 priority 110
```

III. 設定の確認

Switch A の VRRP グループの詳細情報を表示します。

```
[SwitchA-Vlan-interface3] display vrrp verbose
IPv4 Virtual Router Information:
 Running Mode      : Standard
 Total number of virtual routers : 2
   Interface Vlan-interface2
     VRID             : 1                  Adver Timer  : 100
     Admin Status     : Up                 State        : Master
     Config Pri       : 110                Running Pri  : 110
     Preempt Mode     : Yes                Delay Time   : 0
     Auth Type        : None
     Virtual IP       : 10.1.1.100
     Virtual MAC      : 0000-5e00-0101
     Master IP        : 10.1.1.1

   Interface Vlan-interface3
     VRID             : 2                  Adver Timer  : 100
     Admin Status     : Up                 State        : Backup
```

```
    Config Pri       : 100                  Running Pri  : 100
    Preempt Mode     : Yes                  Delay Time   : 0
    Become Master    : 203ms left
    Auth Type        : None
    Virtual IP       : 10.1.1.200
    Master IP        : 10.1.1.131
```

Switch B の VRRP グループの詳細情報を表示します。

```
[SwitchB-Vlan-interface3] display vrrp verbose
IPv4 Virtual Router Information:
 Running Mode      : Standard
 Total number of virtual routers : 2
   Interface Vlan-interface2
     VRID             : 1                  Adver Timer  : 100
     Admin Status     : Up                 State        : Backup
     Config Pri       : 100                Running Pri  : 100
     Preempt Mode     : Yes                Delay Time   : 0
     Become Master    : 211ms left
     Auth Type        : None
     Virtual IP       : 10.1.1.100
     Master IP        : 10.1.1.1

   Interface Vlan-interface3
     VRID             : 2                  Adver Timer  : 100
     Admin Status     : Up                 State        : Master
     Config Pri       : 110                Running Pri  : 110
     Preempt Mode     : Yes                Delay Time   : 0
     Auth Type        : None
     Virtual IP       : 10.1.1.200
     Virtual MAC      : 0000-5e00-0102
     Master IP        : 10.1.1.131
```

出力は、以下のことを示します。

ホストがデフォルトゲートウェイ 10.1.1.100/25 を使用し、インタネットトラフィックを転送するため、Switch A が VRRP グループ 1 でマスタとして動作しています。

ホストがデフォルトゲートウェイ 10.1.1.200/25 を使用し、インタネットトラフィックを転送するため、Switch B が VRRP グループ 2 でマスタとして動作しています。

7.7 IPv6 VRRP設定例

7.7.1 VRRP グループが 1 組の場合の設定例

I. ネットワーク要件

図 7-6に示すように、Switch A と Switch B は VRRP グループを形成し、Host A があるサブネット用にゲートウェイサービスを提供するために仮想 IPv6 アドレス 1::10/64、FE80::10 を使用します。

Host A は Switch によって送信された RA メッセージからデフォルトゲートウェイとして 1::10/64 を学習します。

マスタとして Switch A が動作し、Host A から Host B にパケットを転送します。Switch A が故障したとき、Switch B が Host A のパケットを転送するため、マスタに切り替わります。

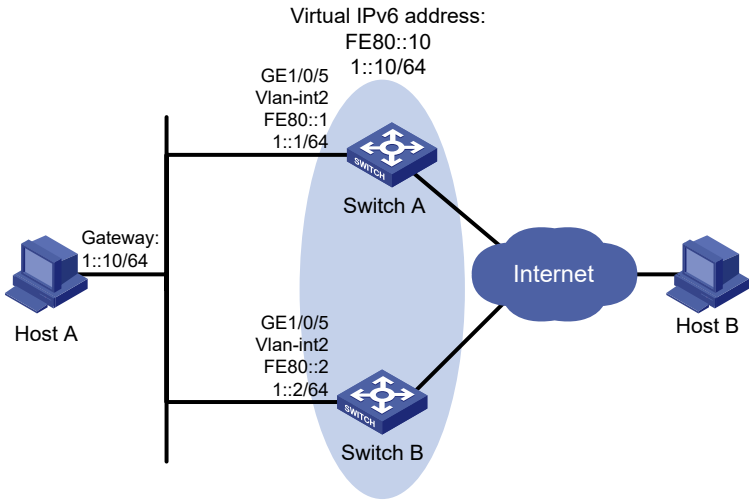


図 7-6 ネットワーク図

II. 設定手順

1)　Switch A を設定します。

VLAN 2 を設定します。

```
<SwitchA> system-view
[SwitchA] vlan 2
[SwitchA-vlan2] port gigabitethernet 1/0/5
[SwitchA-vlan2] quit
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ipv6 address fe80::1 link-local
[SwitchA-Vlan-interface2] ipv6 address 1::1 64
```

VRRP グループ 1 を作成し、仮想 IPv6 アドレス FE80::10、1::10 を設定します。

```
[SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local
[SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip 1::10
```

Switch A がマスタになるように VRRP グループ 1 の Switch A の優先度を Switch B よりも高い値に割り当てます。

```
[SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 priority 110
```

いつでも適切にマスタに切り替わることができるように、Switch A を preemptive モードで動作するように設定します。Switch の切り替えが頻繁に発生しないように preemption delay タイマを 500 センチ秒に設定します。

```
[SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 preempt-mode delay 5000
```

Host A がデフォルトゲートウェイアドレスを学習できるように、Switch A が RA メッセージを送信するようにします。

```
[SwitchA-Vlan-interface2] undo ipv6 nd ra halt
```

2)　Switch B を設定します。

VLAN 2 を設定します。

```
<SwitchB> system-view
[SwitchB] vlan 2
[SwitchB-vlan2] port gigabitethernet 1/0/5
[SwitchB-vlan2] quit
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] ipv6 address fe80::2 link-local
[SwitchB-Vlan-interface2] ipv6 address 1::2 64
```

VRRP グループ 1 を作成し、仮想 IPv6 アドレス FE80::10、1::10 を設定します。

```
[SwitchB-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local
[SwitchB-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip 1::10
```

Switch B を preemptive モードで動作するように設定し、preemption delay タイマを 5000 センチ秒に設定します。

```
[SwitchB-Vlan-interface2] vrrp ipv6 vrid 1 preempt-mode delay 5000
```

Host A がデフォルトゲートウェイアドレスを学習できるように、Switch B が RA メッセージを送信するようにします。

```
[SwitchB-Vlan-interface2] undo ipv6 nd ra halt
```

III. 設定の確認

Host A から Host B に ping を行います。(詳細は省略します)

Switch A の VRRP グループ 1 の詳細情報を表示します。

```
[SwitchA-Vlan-interface2] display vrrp ipv6 verbose
IPv6 Virtual Router Information:
 Running Mode       : Standard
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID             : 1                  Adver Timer  : 100
     Admin Status     : Up                 State        : Master
     Config Pri       : 110                Running Pri  : 110
     Preempt Mode     : Yes                Delay Time   : 5000
     Auth Type        : None
     Virtual IP       : FE80::10
                        1::10
     Virtual MAC      : 0000-5e00-0201
     Master IP        : FE80::1
```

Switch B の VRRP グループ 1 の詳細情報を表示します。

```
[SwitchB-Vlan-interface2] display vrrp ipv6 verbose
IPv6 Virtual Router Information:
 Running Mode         : Standard
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID             : 1                  Adver Timer  : 100
     Admin Status     : Up                 State        : Backup
     Config Pri       : 100                Running Pri  : 100
     Preempt Mode     : Yes                Delay Time   : 5000
```

```
    Become Master    : 403ms left
    Auth Type        : None
    Virtual IP       : FE80::10
                       1::10
    Master IP        : FE80::1
```

出力は、Host A から Host B へパケットを転送するため、VRRP グループ 1 のマスタとして Switch A が動作していることを示します。

Host A と Switch A 間のリンクを切断し、Host A が Host B に ping できることを確認してください。(詳細は省略します)

Switch B の VRRP グループ 1 の詳細情報を表示します。

```
[SwitchB-Vlan-interface2] display vrrp ipv6 verbose
IPv6 Virtual Router Information:
 Running Mode      : Standard
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID             : 1                  Adver Timer  : 100
     Admin Status     : Up                 State        : Master
     Config Pri       : 100                Running Pri  : 100
     Preempt Mode     : Yes                Delay Time   : 5000
     Auth Type        : None
     Virtual IP       : FE80::10
                        1::10
     Virtual MAC      : 0000-5e00-0201
     Master IP        : FE80::2
```

出力は、Switch A が故障したとき、Host A から Host B のパケットを転送するため、Switch B に切り替わったことを示します。

Host A と Switch A 間のリンクを復旧させ、Switch A の VRRP グループ 1 の詳細情報を表示します。

```
[SwitchA-Vlan-interface2] display vrrp ipv6 verbose
IPv6 Virtual Router Information:
 Running Mode      : Standard
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID             : 1                  Adver Timer  : 100
     Admin Status     : Up                 State        : Master
     Config Pri       : 110                Running Pri  : 110
     Preempt Mode     : Yes                Delay Time   : 5000
     Auth Type        : None
     Virtual IP       : FE80::10
                        1::10
     Virtual MAC      : 0000-5e00-0201
     Master IP        : FE80::1
```

出力は、Switch A が正常動作に戻ったとき、Host A から Host B にパケットを転送するため、Switch A がマスタになることを示します。

7.7.2 VRRP グループが複数の場合の設定例

I. ネットワーク要件

図 7-7に示すように、Switch A と Switch B は 2 つの VRRP グループを形成します。VLAN2 のホストにゲートウェイサービスを提供するため、VRRP グループ 1 は仮想 IPv6 アドレス 1::10/64、FE80::10 を使用します。VLAN3 のホストにゲートウェイサービスを提供するため、VRRP グループ 2 は仮想 IPv6 アドレス 2::10/64、FE90::10 を使用します。

VLAN2 のホストは、Switch によって送信された RA メッセージからデフォルトゲートウェイとして 1::10/64 を学習します。VLAN3 のホストは、Switch によって送信された RA メッセージからデフォルトゲートウェイとして 2::10/64 を学習します。

2 つの Switch 間で VLAN2 と VLAN3 からのトラフィックを分散させるため、VRRP グループ 1 の Switch A の優先度は Switch B よりも高い値に割り当て、VRRP グループ 2 の Switch A の優先度は Switch B よりも低い値に割り当てます。一方の Switch が故障したとき、正常な Switch が両方の VLAN のゲートウェイサービスを提供します。

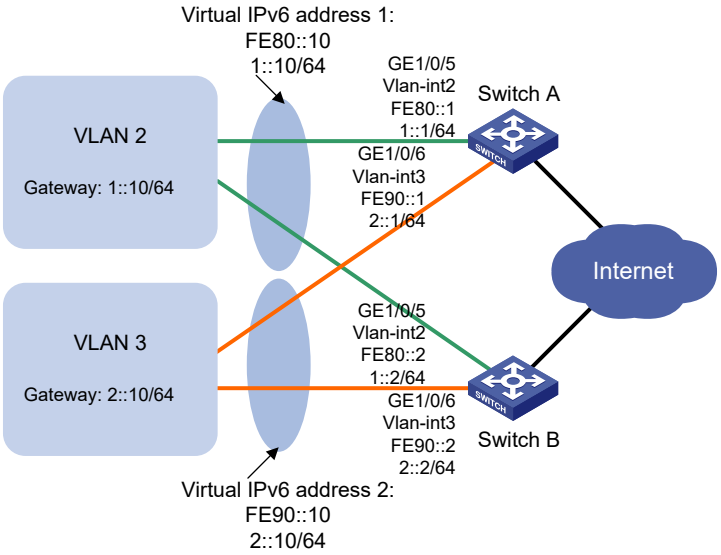


図 7-7 ネットワーク図

II. 設定手順

1)　Switch A を設定します。

VLAN 2 を設定します。

```
<SwitchA> system-view
[SwitchA] vlan 2
[SwitchA-vlan2] port gigabitethernet 1/0/5
[SwitchA-vlan2] quit
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ipv6 address fe80::1 link-local
[SwitchA-Vlan-interface2] ipv6 address 1::1 64
```

VRRP グループ 1 を作成し、仮想 IPv6 アドレス FE80::10、1::10 を設定します。

```
[SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local
[SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip 1::10
```

Switch A がグループでマスタになるように VRRP グループ 1 の Switch A の優先度を Switch B よりも高い値に割り当てます。

```
[SwitchA-Vlan-interface2] vrrp ipv6 vrid 1 priority 110
```

VLAN2 の Host がデフォルトゲートウェイアドレスを学習できるように、Switch A が RA メッセージを送信するようにします。

```
[SwitchA-Vlan-interface2] undo ipv6 nd ra halt
[SwitchA-Vlan-interface2] quit
```

VLAN 3 を設定します。

```
[SwitchA] vlan 3
[SwitchA-vlan3] port gigabitethernet 1/0/6
[SwitchA-vlan3] quit
[SwitchA] interface vlan-interface 3
[SwitchA-Vlan-interface3] ipv6 address fe90::1 link-local
[SwitchA-Vlan-interface3] ipv6 address 2::1 64
```

VRRP グループ 2 を作成し、仮想 IPv6 アドレス FE90::10、2::10 を設定します。

```
[SwitchA-Vlan-interface3] vrrp ipv6 vrid 2 virtual-ip fe90::10 link-local
[SwitchA-Vlan-interface3] vrrp ipv6 vrid 2 virtual-ip 2::10
```

VLAN3 の Host がデフォルトゲートウェイアドレスを学習できるように、Switch A が RA メッセージを送信するようにします。

```
[SwitchA-Vlan-interface3] undo ipv6 nd ra halt
```

2) Switch B を設定します。

VLAN 2 を設定します。

```
<SwitchB> system-view
[SwitchB-vlan2] port gigabitethernet 1/0/5
[SwitchB-vlan2] quit
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] ipv6 address fe80::2 link-local
[SwitchB-Vlan-interface2] ipv6 address 1::2 64
```

VRRP グループ 1 を作成し、仮想 IPv6 アドレス FE80::10、1::10 を設定します。

```
[SwitchB-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local
[SwitchB-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip 1::10
```

VLAN2 の Host がデフォルトゲートウェイアドレスを学習できるように、Switch B が RA メッセージを送信するようにします。

```
[SwitchB-Vlan-interface2] undo ipv6 nd ra halt
[SwitchB-Vlan-interface2] quit
```

VLAN 3 を設定します。

```
[SwitchB] vlan 3
```

```
[SwitchB-vlan3] port gigabitethernet 1/0/6
[SwitchB-vlan3] quit
[SwitchB] interface vlan-interface 3
[SwitchB-Vlan-interface3] ipv6 address fe90::2 link-local
[SwitchB-Vlan-interface3] ipv6 address 2::2 64
```

VRRP グループ 2 を作成し、仮想 IPv6 アドレス FE90::10、2::10 を設定します。

```
[SwitchB-Vlan-interface3] vrrp ipv6 vrid 2 virtual-ip fe90::10 link-local
[SwitchB-Vlan-interface3] vrrp ipv6 vrid 2 virtual-ip 2::10
```

Switch B がグループでマスタになるように VRRP グループ 2 の Switch B の優先度を Switch A よりも高い値に割り当てます。

```
[SwitchB-Vlan-interface3] vrrp ipv6 vrid 2 priority 110
```

VLAN3 の Host がデフォルトゲートウェイアドレスを学習できるように、Switch B が RA メッセージを送信するようにします。

```
[SwitchB-Vlan-interface3] undo ipv6 nd ra halt
```

III. 設定の確認

Switch A の VRRP グループの詳細情報を表示します。

```
[SwitchA-Vlan-interface3] display vrrp ipv6 verbose
IPv6 Virtual Router Information:
 Running Mode      : Standard
 Total number of virtual routers : 2
   Interface Vlan-interface2
     VRID             : 1                  Adver Timer  : 100
     Admin Status     : Up                 State        : Master
     Config Pri       : 110                Running Pri  : 110
     Preempt Mode     : Yes                Delay Time   : 0
     Auth Type        : None
     Virtual IP       : FE80::10
                        1::10
     Virtual MAC      : 0000-5e00-0201
     Master IP        : FE80::1

   Interface Vlan-interface3
     VRID             : 2                  Adver Timer  : 100
     Admin Status     : Up                 State        : Backup
     Config Pri       : 100                Running Pri  : 100
     Preempt Mode     : Yes                Delay Time   : 0
     Become Master    : 402ms left
     Auth Type        : None
     Virtual IP       : FE90::10
                        2::10
     Master IP        : FE90::2
```

Switch B の VRRP グループの詳細情報を表示します。

```
[SwitchB-Vlan-interface3] display vrrp ipv6 verbose
IPv6 Virtual Router Information:
 Running Mode      : Standard
 Total number of virtual routers : 2
   Interface Vlan-interface2
     VRID             : 1                  Adver Timer  : 100
     Admin Status     : Up                 State        : Backup
```

```
    Config Pri       : 100                  Running Pri  : 100
    Preempt Mode     : Yes                  Delay Time   : 0
    Become Master    : 401ms left
    Auth Type        : None
    Virtual IP       : FE80::10
                       1::10
    Master IP        : FE80::1

  Interface Vlan-interface3
    VRID             : 2                    Adver Timer  : 100
    Admin Status     : Up                   State        : Master
    Config Pri       : 110                  Running Pri  : 110
    Preempt Mode     : Yes                  Delay Time   : 0
    Auth Type        : None
    Virtual IP       : FE90::10
                       2::10
    Virtual MAC      : 0000-5e00-0202
    Master IP        : FE90::2
```

出力は、以下のことを示します。

ホストがデフォルトゲートウェイ 1::10/64 を使用し、インタネットトラフィックを転送するため、Switch A が VRRP グループ 1 でマスタとして動作しています。

ホストがデフォルトゲートウェイ 2::10/64 を使用し、インタネットトラフィックを転送するため、Switch B が VRRP グループ 2 でマスタとして動作しています。

7.8 VRRPのトラブルシューティング

7.8.1 エラーメッセージが表示される

I. 症状

設定中に、"The virtual router detected a VRRP configuration error."のエラーメッセージが表示されます。

II. 分析

問題の原因は以下のものが考えられます。

パケットの VRRP アドバタイズメント間隔が、現在の VRRP グループ(VRRPv2 のみ)の VRRP アドバタイズメント間隔と異なります。

パケットの仮想 IP アドレス数が、現在の VRRP グループの仮想 IP アドレス数と異なります。

仮想 IP アドレスリストが、現在の VRRP グループの仮想 IP アドレスリストと異なります。

VRRP グループの装置が不正な VRRP パケットを受信しています。例えば IP アドレスオーナが優先度 255 の VRRP パケットを受信しています。

III. 解決策

問題を解決する場合、以下を行ってください。

1) VRRP グループのルータの設定を正しい値に修正します。
2) 潜在的な脅威を除去するため、故障箇所を特定し攻撃に対して防御を行います。
3) 問題が解決しない場合、NEC に問い合わせてください。

7.8.2 VRRP グループで複数のマスタが現れる

I. 症状

VRRP グループで複数のマスタが現れます。

II. 分析

問題の原因は以下のものが考えられます。

VRRP グループに短時間、複数のマスタが存在することは正常動作です。この状況においては、何らかの処理を行う必要はありません。

VRRP グループに長時間、複数のマスタが存在する場合、以下の状態を確認してください。

マスタが互いにアドバタイズメントを受信できていません。
不正なアドバタイズメントを受信しています。

III. 解決策

問題を解決する場合、以下を行ってください。

1) マスタ間で ping を行い、以下の確認を行ってください。
   - □ ping に失敗したとき、ネットワークの接続を確認してください。
   - □ ping が成功したとき、仮想 IP アドレス数、仮想 IP アドレス、認証が矛盾していないか設定を確認してください。IPv4 VRRP では、VRRP グループのすべてのルータで VRRP バージョンが一致していることを確認してください。VRRPv2 を使用している場合、VRRP グループのルータに設定された VRRP アドバタイズメント間隔が正しいか確認してください。
2) 問題が解決しない場合、NEC に問い合わせてください。

7.8.3 VRRP の状態が頻繁に遷移する

I. 症状

VRRP の状態が頻繁に遷移します。

II. 分析

VRRP アドバタイズメント間隔の設定が短すぎます。

III. 解決策

問題を解決する場合、以下を行ってください。

1) VRRP アドバタイズメントの送信間隔を長くするか、preemption delay タイマを設定してください。
2) 問題が解決しない場合、NEC に問い合わせてください。

目次

このセクションのページは **10-x-x** です。

8 章 BFD 8-1
8.1 BFD の概要 8-1
8.1.1 BFD セッションの確立 8-1
8.1.2 BFD セッションモードと動作モード 8-2
8.1.3 サポート機能 8-3
8.1.4 プロトコルと標準 8-3
8.2 BFD の基本機能の設定 8-3
8.2.1 エコーパケットモードの設定 8-3
8.2.2 コントロールパケットモードの設定 8-4
8.3 BFD の表示と維持 8-6

8章 BFD

8.1 BFDの概要

双方向フォワーディング検出（BFD）は、汎用性を有し、標準的で、中規模ネットワークに向き、プロトコルに依存しない高速な障害検出メカニズムを提供します。BFD では、通信障害検出するため、IP での接続状態を監視・検出することができます。これにより、素早く障害対策を実施でき、ネットワークの可用性を高め、サービスの継続性を確保することができます。

BFD は、ルーティングプロトコルとして位置づけられる上位層プロトコルのための 2 つのデバイス間の双方向の転送パスの障害を均一かつ迅速に検出することができます。BFD は、ミリ秒単位での検出結果の提供ができますが、上位層プロトコルによって使用される hello メカニズムは、リンク障害を検出するのに数秒を必要とします。

BFD はシングル Hop 検出とマルチ Hop 検出の双方を使用することができます。

- **シングル Hop検出**－2つの直接に接続されたシステムの間の IP 接続性を検出します。
- **マルチ Hop検出**－2つのシステムの間のどのようなパスでも検出します。 これらのパスは複数の Hop を持ち、重複する可能性があります。

8.1.1 BFD セッションの確立

I. BFD セッションの確立

BFD はネイバ発見メカニズムを提供しません。BFD を提供するプロトコル群は、セッションを確立する必要のあるルータの BFD に通知します。

BFD セッションの確立プロセスについて以下に記載します。

1) プロトコルはネイバの発見とネイバ関係の確立のために Hello メッセージを送信します。
2) ネイバ関係を確立した後、プロトコルは BFD に宛先と送信元アドレスを含むネイバ情報を報告します。
3) BFD は BFD セッションを確立するために情報を使用します。

II. BFD セッションの終了

BFD の障害検出プロセスについて以下に記載します。

1) BFD はセッションをクリアします。
2) BFD は障害をプロトコルに報告します。
3) プロトコルはリンク上のネイバ関係を終了させます。
4) バックアップリンクを利用できる場合、プロトコルはバックアップリンクをパケットの転送に使用します。

8.1.2 BFD セッションモードと動作モード

BFD セッションは以下のタイプのパケットを使用します。

- **エコーパケット**－ポート番号 3785 で UDP パケットにカプセル化されているパケット
- **コントロールパケット**– シングル Hop 検出用にポート番号 3784、マルチ Hop 検出用にポート番号 4784 で UDP パケットにカプセル化されているパケット

I. エコーパケットモード

リンクのローカルエンドが BFD セッションを確立して、リンクの状態を監視するためのエコーパケットを送信します。ピアエンドは BFD セッションを確立せず、パケットを発信側に戻すために転送するだけとなります。

エコーモードでは、BFD はシングル Hop 検出のみをサポートし、BFD セッションは動作モードとは無関係となります。

II. コントロールパケットモード

リンク状態を監視するため、BFD はリンクの両端で BFD コントロールパケットを交換します。

BFD セッションが確立される前に、BFD には 2 つの動作モード（Active、Passive）があります。

- **Active モード**－ピアから BFD コントロールパケットを受信したかどうかに関係なく、BFD コントロールパケットを自発的に送信します。
- **Passive モード**－ピアから BFD コントロールパケットを受信するまで BFD コントロールパケットを送信しません。

少なくとも 1 つの装置は BFD セッションを確立するために Active モードで動作する必要があります。

BFD セッションが確立された後、両端で BFD の動作モードのいずれかを動作させる必要があります。

- **Asynchronous モード**－装置が互いに定期的に BFD コントロールパケットを送信します。BFD は指定した時間内に BFD コントロールパケットを受信しない場合、セッションがダウンしたとみなします。
- **Demand モード**– 装置は定期的に BFD コントロールパケットを送信します。片端が Asynchronous モードである場合（デフォルト）、片端は BFD コントロールパケットの送信を停止します。片端が Demand モードである場合、両端は BFD コントロールパケットの送信を停止します。別のシステムに接続していることを明示する必要がある場合、システムはネゴシエートした送信間隔で Poll（P）ビットがセットされた BFD コントロールパケットを送信します。検出時間内に応答がない場合、セッションがダウンしたとみなします。接続していると認識した場合、次のコマンドが送信されるまで BFD コントロールパケットを送信しません。

加えてリンクの両端で BFD セッションを維持するため BFD コントロールパケットを交換でき、リンクの片端がリンク状態をモニタリングするためエコーパケットを送信します。

8.1.3 サポート機能

- スタティックルーティング。詳細は、オペレーションマニュアルのセクション 5 *ルーティングプロトコル "スタティックルーティング"*を参照してください。
- IPv6 スタティックルーティング。詳細は、オペレーションマニュアルのセクション 5 *ルーティングプロトコル "IPv6 スタティックルーティング"*を参照してください。
- リンクアグリゲーション。詳細は、オペレーションマニュアルのセクション 3 *アクセス "リンクアグリゲーション"*を参照してください。

8.1.4 プロトコルと標準

- RFC 5880, *Bidirectional Forwarding Detection (BFD)*
- RFC 5881, *Bidirectional Forwarding Detection (BFD) for IPv4 and IPv6 (Single Hop)*
- RFC 5882, *Generic Application of Bidirectional Forwarding Detection (BFD)*
- RFC 5883, *Bidirectional Forwarding Detection (BFD) for Multihop Paths*
- RFC 7130, Bidirectional Forwarding Detection (BFD) *on Link Aggregation Group (LAG) Interfaces*

8.2 BFDの基本機能の設定

BFD 基本機能の設定を行う前に、当該機器が隣接装置とネットワークレイヤで通信できるようにインタフェースに IP アドレスを設定してください。

BFD セッションが確立した後、両端で BFD 関連の以下のようなパラメータを取り決めます。最小受信間隔です。両端は現在のセッションに影響を及ぼすことなく、取り決めたパラメータを使用します。

BDF セッションのばたつきがメンバーポートのアグリゲートインタフェースで発生する場合があります。BFD パケットの送受信をするマスター装置が再起動した場合、下位装置はただちに引き継がないかもしれません。たとえば、下位装置は検出時間が短かったり大量の BFD セッションを持っていると引き継げないでしょう。

初期状態では、BFD バージョン 1 で動作し、BFD バージョン 0 と互換性があります。コマンドにより BFD バージョンを 0 に変更することはできません。接続装置が BFD バージョン 0 で動作する場合、自装置は自動的にバージョン 0 に切り替わります。

8.2.1 エコーパケットモードの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―

操作	コマンド	補足
2. エコーパケットの送信元 IP アドレスを設定する	• エコーパケットの送信元IPアドレスを設定する **bfd echo-source-ip** *ip-address* • エコーパケットの送信元IPv6アドレスを設定する **bfd echo-source-ipv6** *ipv6-address*	• デフォルト：設定なし 送信元IPv4アドレスをローカルインタフェースのIPv4アドレスと同じネットワークセグメント上に配置しないでください。そうでないと、大量のICMPリダイレクトパケットがピアから送信され、リンク輻輳が生じる可能性があります。 • デフォルト：設定なし エコーパケットの送信元IPv6アドレスは、グローバルユニキャストアドレスだけにすることができます。
3. （オプション設定項目）エコーパケットモードパラメータを設定する	• interface viewに移行する **interface** *interface-type interface-number* • エコーパケットの最小受信間隔を設定する **bfd min-echo-receive-interval** *interval* • 検出時間乗数を設定する **bfd detect-multiplier** *value*	（最小受信間隔） デフォルト：400ミリ秒 （検出時間乗数） デフォルト：5

8.2.2 コントロールパケットモードの設定

以下にシングル Hop 検出のコントロールパケットモードの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. BFD セッションを確立するモードを指定する	**bfd session init-mode** { **active** | **passive** }	デフォルト：active BFDバージョン0ではこのコマンドは未サポートです。設定は無効となります。
3. interface view に移行する	**interface** *interface-type interface-number*	―
4. シングル Hop コントロールパケットの認証モードを設定する	**bfd authentication-mode** { **md5** | **sha1** | **simple** } *key-id* { **cipher** *cipher-string* | **plain** *plain-string* }	デフォルト：認証なし BFDバージョン0ではこのコマンドは未サポートです。設定は無効となります。
5. Demand モードを有効にする	**bfd demand enable**	デフォルト:Asynchronousモード BFDバージョン0ではこのコマンドは未サポートです。設定は無効となります。

操作	コマンド	補足
6. エコーパケットモードを有効にする	**bfd echo enable**	デフォルト：無効 BFDバージョン0ではこのコマンドは未サポートです。設定は無効となります。 コントロールパケットが送信され、BFDセッションがUPになる間に、エコーパケットモードを有効にした場合、リンク接続を検出し、コントロールパケットの受信レートを減らすため、BFDは定期的にエコーパケットを送信します。
7. シングル Hop コントロールパケットを転送する最小間隔を設定する	**bfd min-transmit-interval** *value*	デフォルト：400ミリ秒
8. シングル Hop コントロールパケットを受信する最小間隔を設定する	**bfd min-receive-interval** *value*	デフォルト：400ミリ秒
9. シングル Hop 検出時間の乗数を設定する	**bfd detect-multiplier** *value*	デフォルト：5

以下にマルチ Hop 検出のコントロールパケットモードの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. BFD セッションを確立するモードを指定する	**bfd session init-mode** { **active** | **passive** }	デフォルト：active BFDバージョン0ではこのコマンドは未サポートです。設定は無効となります。
3. シングル Hop コントロールパケットの認証モードを設定する	**bfd multi-hop authentication-mode** { **md5** | **sha1** | **simple** } *key-id* { **cipher** *cipher-string* | **plain** *plain-string* }	デフォルト：認証なし BFDバージョン0ではこのコマンドは未サポートです。設定は無効となります。
4. マルチ Hop BFD コントロールパケットの宛先ポート番号を設定する	**bfd multi-hop destination-port** *port-number*	デフォルト： 4784
5. マルチ Hop 検出時間の乗数を設定する	**bfd multi-hop detect-multiplier** *value*	デフォルト： 5
6. マルチ Hop コントロールパケットを受信する最小間隔を設定する	**bfd multi-hop min-receive-interval** *value*	デフォルト：400ミリ秒
7. マルチ Hop コントロールパケットを送信する最小間隔を設定する	**bfd multi-hop min-transmit-interval** *value*	デフォルト：400ミリ秒

8.3 BFDの表示と維持

すべての view で **display** コマンドを実行でき、user view で **reset** コマンドを実行できます。

操作	コマンド
BFDセッション情報を表示する	**display bfd session** [**discriminator** *value* | **verbose**]
BFDセッション統計情報を削除する	**reset bfd session statistics**

目次

このセクションのページは **10-x-x** です。

9章 Track 9-1
9.1 概要 9-1
9.1.1 コラボレーションメカニズム 9-1
9.1.2 サポート検出モジュール 9-2
9.1.3 サポートアプリケーションモジュール 9-2
9.2 制限とガイドライン 9-2
9.3 コラボレーションアプリケーション例 9-2
9.4 Track設定作業リスト 9-3
9.5 Trackモジュールと検出モジュールの関連づけ 9-3
9.5.1 TrackとNQAの関連づけ 9-3
9.5.2 TrackとBFDの関連づけ 9-4
9.5.3 TrackとCFDの関連付け 9-5
9.5.4 TrackとPoEの関連づけ 9-5
9.6 Trackモジュールとアプリケーションモジュールの関連づけ 9-6
9.6.1 設定要件 9-6
9.6.2 TrackとVRRPの関連付け 9-6
9.6.3 Trackとスタティックルーティングの関連づけ 9-8
9.6.4 TrackとPBRの関連づけ 9-11
9.6.5 TrackとSmart linkの関連づけ 9-12
9.7 Trackの表示と維持 9-13
9.8 Track設定例 9-13
9.8.1 VRRP-Track-NQAコラボレーション設定例 9-13
9.8.2 マスタを監視するVRRPバックアップ用BFDの設定例 9-17
9.8.3 アップリンクを監視するVRRPマスタ用BFDの設定例 9-20
9.8.4 スタティックルーティング-Track-NQAコラボレーション設定例 9-23
9.8.5 スタティックルーティング-Track-BFDコラボレーション設定例 9-28
9.8.6 VRRP-Track-インタフェースマネジメントコラボレーション設定例 9-32

9章 Track

9.1 概要

トラックモジュールはアプリケーションと検出モジュール間で動作します。アプリケーションモジュールから、さまざまな検出モジュール間の相違点を保護します。

9.1.1 コラボレーションメカニズム

トラックモジュールはアプリケーションと検出モジュールと連携します。

図 9-1に示すように検出モジュールとアプリケーションモジュールの Track モジュールを連携した後、コラボレーションが有効となります。以下のことを行います。

1) 検出モジュールは、インタフェース状態、リンク状態、ネットワークの接続性、ネットワーク性能のような指定したオブジェクトを調査し、検出結果を Track モジュールに通知します。
2) Track モジュールは関連したアプリケーションモジュールに検出結果を送信します。
3) Track オブジェクトの変更を通知したとき、アプリケーションモジュールは通信の中断とネットワーク性能の低下を防ぐため、結果に対して対応することができます。

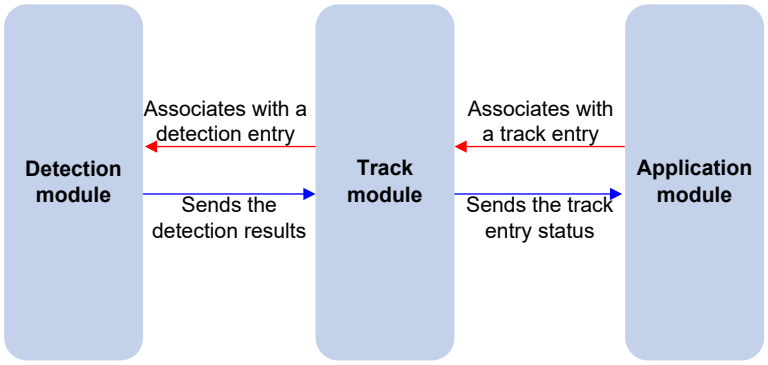


図 9-1 Track モジュールを介したコラボレーション

II. Track モジュールと検出モジュール間のコラボレーション

検出モジュールは、関連した Track 対象オブジェクトの検出結果を Track 対象モジュールに送信します。結果に依存して、Track モジュールは以下のように Track エントリの状態を変更します。

- Track 対象オブジェクト機能が正常の場合、Track エントリの状態は Positive になります。たとえば、以下のいずれかの状況の Track エントリの状態は Positive です。
  - □ ターゲットインタフェースがアップです。
  - □ ターゲットネットワークが到達可能です。
- Track 対象オブジェクト機能が正常の場合、Track エントリの状態は Negative になります。たとえば、以下のいずれかの状況の Track エントリの状態は Negative です。

- ターゲットインタフェースがダウンです。
- ターゲットネットワークが到達不可能です。

- 検出結果が有効でない場合、Track エントリの状態は、NotReady になります。たとえば Track エントリに関連した NQA テストグループが存在しない場合、NotReady になります。

III. Track モジュールとアプリケーションモジュール間のコラボレーション

トラックモジュールはアプリケーションモジュールにトラックエントリの状態変化を報告します。そして、アプリケーションモジュールは通信の中断とネットワークの性能低下を防ぐため、正しいアクションを行うことができます。

9.1.2 サポート検出モジュール

以下の検出モジュールが Track モジュールに関連づけることができます。

- NQA
- BFD
- CFD
- インタフェース管理モジュール
- ルート管理モジュール
- LLDP

9.1.3 サポートアプリケーションモジュール

以下のアプリケーションモジュールが Track モジュールに関連づけることができます。

- VRRP
- スタティックルーティング
- PBR
- Smart Link
- EAA
- ERPS

9.2 制限とガイドライン

アプリケーションモジュールの Track エントリを設定するとき、状態の変化をすぐに通知することを防ぐため、通知する前に遅延時間を設定することができます。

遅延時間を設定することで、ルートの収束がリンク状態の変更通知よりも遅いとき、通信が失敗することを防ぎます。たとえば、VRRP グループでマスタは Track モジュールを通してアップリンクインタフェースを監視します。Track モジュールはマスタに優先度を下げるように通知します。高い優先度を持つバックアップがマスタとなります。故障したアップリンクインタフェースが回復したとき、Track モジュールは元のマスタに優先度を戻し、トラフィックを転送するように通知します。もしアップリンクが回復していない場合、転送は失敗します。

9.3 コラボレーションアプリケーション例

以下に NQA、Track、スタティックルーティング間のコラボレーションの例を示します。

装置でネクストホップ 192.168.0.88 のスタティックルートを設定します。ネクストホップが到達可能なとき、スタティックルートは有効です。もしネクストホップが到達不可能

となったとき、スタティックルートは無効となります。このため、NQA、Track、スタティックルーティングモジュール間のコラボレーションを設定します。

1) IP アドレス 192.168.0.88 の到達可能性を監視するため、NQA テストグループを作成します。
2) Track エントリを作成し、NQA テストグループに関連づけます。
   - □ ネクストホップ 192.168.0.88 が到達可能であるとき、Track エントリは Positive 状態となります。
   - □ ネクストホップが到達不能になったとき、Track エントリは Negative 状態となります。
3) スタティックルートに Track エントリを関連づけます。
   - □ Track エントリが Positive 状態になったとき、スタティックルートが有効となります。
   - □ Track エントリが Negative 状態になったとき、スタティックルートが無効となります。

9.4 Track設定作業リスト

コラボレーション機能を動作させるため、Track モジュールと検出モジュール、および Track モジュールとアプリケーションモジュールを関連づけます。

作業リスト
(必須設定項目) Trackモジュールと検出モジュールの関連づけ ● TrackとNQAの関連づけ ● TrackとBFDの関連づけ ● TrackとPoEの関連づけ
(必須設定項目) Trackモジュールとアプリケーションモジュールの関連づけ: ● TrackとVRRPの関連づけ ● Trackとスタティックルーティングの関連づけ ● TrackとPBRの関連づけ ● TrackとSmart Linkの関連づけ

9.5 Trackモジュールと検出モジュールの関連づけ

9.5.1 Track と NQA の関連づけ

I. Track と NQA の関連づけ

NQA は、ネットワークのパフォーマンス、サービス、サービス品質を解析するために複数のテストタイプをサポートしています。たとえば、NQA テストでは、宛先へ到達可能かどうか、あるいは TCP サーバへ TCP 接続がアップであるかどうかを定期的に検出することができます。

NQA テストグループは、Track エントリに関連づけられている場合、以下のように機能します。

- エラーが連続して指定のしきい値に達した場合、NQA モジュールは、Track モジュールに Track 対象オブジェクトの異常を通知します。その後、Track モジュールは、Track エントリの状態を Negative に変更します。
- 指定したしきい値に達していない場合、NQA モジュールは、Track 対象オブジェクトが正常に機能していることを Track モジュールに通知します。Track モジュールは、Track エントリの状態を Positive に変更します。

NQA の詳細は、オペレーションマニュアルのセクション 11 *システム管理* "*NQA*"を参照してください。

II. 制限とガイドライン

指定した NQA テストグループあるいは Track エントリのリアクションエントリが存在しない場合、Track エントリの状態は NotReady となります。

III. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. Track エントリを生成し、NQA リアクションエントリと関連づけを行う	**track** *track-entry-number* **nqa entry** *admin-name operation-tag* **reaction** *item-number*	ー

9.5.2 Track と BFD の関連づけ

I. Track と BFD の関連づけ

Track エントリはエコーモード BFD と関連づけることができます。Track エントリはエコーモード BFD セッションのみと関連づけることができます。BFD の詳細はオペレーションマニュアルのセクション 10 *高可用性* "*BFD*"を参照してください。

Track エントリが BFD に関連づけられているとき、以下のように動作します。

- BFD がリンク故障を検出したとき、リンク故障を Track エントリに通知します。Track モジュールは Track エントリの状態を Negative にします。
- BFD がリンクの正常動作を検出したとき、Track モジュールは Track エントリの状態を Positive にします。

II. 制限とガイドライン

BFD セッションのローカルあるいはリモートアドレスとして VRRP グループの仮想 IP アドレスを設定しないでください。

III. 設定要件

Track と BFD を関連づける前に、BFD エコーパケットの送信元 IP アドレスを設定してください。詳細はオペレーションマニュアルのセクション 10 *高可用性* "*BFD*"を参照してください。

IV. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Track エントリを生成し、BFD セッションと関連づけを行う	**track** *track-entry-number* **bfd echo interface** *interface-type interface-number* **remote ip** *remote-ip* **local ip** *local-ip*	―

9.5.3 Track と CFD の関連付け

I. Track と CFD の関連づけ

関連するトラックと CFD は次のように動作します。

- CFD はリンク障害を検出すると、Track モジュールにリンク障害を通知します。次に、Track モジュールは Track エントリを Negative に設定します。
- リンクが正常に動作していることを CFD が検出すると、Track モジュールは Track エントリを Positive に設定します。

CFD の詳細は、オペレーションマニュアルのセクション 10 *高可用性 "CFD"*を参照してください。

II. 設定要件

Track を CFD に関連付ける前に、CFD を有効にして MEP を作成します。詳細は、オペレーションマニュアルのセクション 10 *高可用性 "CFD"*を参照してください。

III. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Track エントリを生成し、CFD に関連づけを行う	**track** *track-entry-number* **cfd cc service-instance** *instance-id* **mep** *mep-id*	―

9.5.4 Track と PoE の関連づけ

🕮 **メモ：**

Track と PoE の関連づけは、Version 7.4.61 を含む以降のソフトウェアからサポートしています。

Track と PoE の関連づけ

PoE モジュールは Track モジュールと連携して、デバイスと PD 間のリンクステータスを監視できます。たとえば、PD が NQA ICMP エコーテストをサポートしている場合、NQA に関連付けられた Track エントリを指定して、PD の到達可能性をテストできます。NQA ICMP エコーテストは、レイヤ 3 インタフェースで設定する必要があります。PI はレイヤ

2 インタフェースです。ICMP エコーテスト用の VLAN インタフェースを作成し、その VLAN に PI を割り当てる必要があります。

Track モジュールは、次のモニタリング結果を PoE モジュールに通知します。

- Positive:監視対象オブジェクトに到達可能です。
- Negative:監視対象オブジェクトに到達不能です。
- NotReady:トラックエントリに関連付けられた NQA グループが存在しないなどの理由により、監視結果の準備ができていません。

トラックモジュールはリンクの障害を検出すると、トラックエントリの状態を正から負に変更します。これにより、PoE モジュールは次のアクションを実行します。

- alarm-only:SNMP 通知とログを出力します。
- alarm-reboot-pd:SNMP 通知とログを出力し、PI に接続されている PD を再起動します。
- NotReady:トラックエントリに関連付けられた NQA グループが存在しないなどの理由により、監視結果の準備ができていません。

I. 設定手順

操作	コマンド	補足
3． system view に移行する	**system-view**	—
4． PI view に移行する	**interface** *interface-type interface-number*	—
5． PI とトラックエントリを関連付ける	**poe track** *track-entry-number* **action** { **alarm** | **alarm-reboot-pd** }	デフォルト：PIはトラックエントリに関連付けられていません。

9.6 Trackモジュールとアプリケーションモジュールの関連づけ

Track モジュールとアプリケーションモジュールを関連づける前に、Track エントリが作成されていることを確認してください。

9.6.1 設定要件

アプリケーションモジュールと関連付ける前に Track エントリを作成してください。

関連づけられた Track エントリが存在しない場合、アプリケーションモジュールは間違った Track エントリ状態の情報を取得する可能性があります。

9.6.2 Track と VRRP の関連付け

I. Track と VRRP の関連付け

VRRP が標準モードまたはロードバランスモードで動作している場合、Track モジュールを VRRP グループに関連付けて、以下のアクションを実装してください。

- アップリンクの状態に応じて、ルータの優先順位を変更します。ルータのアップリンク上で障害が発生した場合、VRRP グループはアップリンクの障害を認識していません。ルータがマスタである場合、LAN 内のホストは外部ネットワークにアクセスすることはできません。この問題は、Track と VRRP グループの関連づけを確立することで解決することができます。検出モジュールを使ってルータのアップリンクの状態を監視し、検出モジュール、Track モジュール、VRRP の間でコラボレーションを確立します。
  アップリンクに障害が発生した場合、検出モジュールは、監視した Track エントリのステータスを Negative に変更するよう Track モジュールに通知します。マスタの優先度は指定した値に低下し、VRRP グループ内の優先順位の高いルータがマスタになることを可能にします。
- バックアップのマスタを監視します。マスタで障害が発生した場合、スイッチオーバモードで動作しているバックアップは、正常な通信を維持するために即座にマスタを切り替えます。

VRRP がロードバランスモードで動作している場合、次の機能を実装するために、Track モジュールを VRRP VF に関連付けます。

- アップリンクの状態に応じて AVF の優先度を変更します。AVF のアップリンクに障害が発生すると、Track エントリは Negative 状態に変わります。AVF の重みはユーザが指定した値だけ減少します。優先度の高い VF がパケットを転送する新しい AVF になります。
- LVF から AVF ステータスを監視します。AVF が失敗すると、切り替えモードで動作している LVF が新しい AVF になり、継続的な転送が保証されます。

VRRP の設定の詳細については、オペレーションマニュアルのセクション 10 *高可用性* "*VRRP*"を参照してください。

II. 制限とガイドライン

- **vrrp vrid track priority reduced** コマンドあるいは **vrrp vrid track switchover** コマンドは IP アドレスのオーナーに適用されません。ルータが IP アドレスのオーナーとして動作しないとき、このコマンドが適用されます。IP アドレスのオーナーは、VRRP グループの仮想 IP アドレスとして使用されるインタフェースの IP アドレスを持つルータです。
- Track エントリのステータスが Negative から Positive または NotReady に変化するとき、関連したルータまたは VF が自動で優先度を戻します。

III. Track と VRRP グループの関連づけ

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. interface view に移行する	**interface** *interface-type interface-number*	—
3. Track エントリと VRRP グループを関連づける	**vrrp** [**ipv6**] **vrid** *virtual-router-id* **track** *track-entry-number* { **forwarder-switchover member-ip** *ip-address* | **priority reduced** [*priority-reduced*] | **switchover** | **weight reduced** [*weight-reduced*]] }	デフォルト：設定なし

IV. Track と VRRP VF の関連づけ

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． interface view に移行する	**interface** *interface-type interface-number*	―
3． Track エントリと VRRP VR を関連づける	**vrrp** [**ipv6**] **vrid** *virtual-router-id* **track** *track-entry-number* { **forwarder-switchover member-ip** *ip-address* | **priority reduced** [*priority-reduced*] | **switchover** | **weight reduced** [*weight-reduced*]] }	デフォルト：設定なし このコマンドは、VRRPが標準モードまたはロードバランスモードで動作している場合に設定可能です。ただし、設定はVRRPがロードバランスモードで動作している場合にのみ有効になります。

9.6.3 Track とスタティックルーティングの関連づけ

I. Track とスタティックルーティングの関連づけ

スタティックルートは手動でルートを設定します。スタティックルートについての詳細は、オペレーションマニュアルのセクション 5 *ルーティングプロトコル”スタティックルーティング*”を参照してください。

スタティックルートの欠点は、ネットワークトポロジの変化に適応できないことです。そのため、ネットワークの障害やトポロジの変化が発生すると、ターゲットとの通信ができなくなることがあります。

この問題を回避するために、スタティックルートのバックアップをする別のルートを設定します。スタティックが到達可能であるとき、パケットはスタティックルートを通して転送されます。スタティックルートが到達不可能であるとき、パケットはバックアップルートを通して転送されます。

リアルタイムでスタティックルートの到達可能性をチェックする場合、Track とスタティックルート間の関連づけを行います。

スタティックルートを設定するときに、出力インタフェースでなくネクストホップを指定すると、スタティックルート、Track モジュール、宛先モジュール間でのコラボレーションを確立することができます。これにより、Track エントリの状態でスタティックルートの到達可能性をチェックすることができます。

- Track エントリの状態が Positive の場合、以下の状況となります。
  - □ スタティックルートのネクストホップが到達可能です。
  - □ 設定されたスタティックルートが有効です。
- Track エントリの状態が Negative の場合、以下の状況となります。
  - □ スタティックルートのネクストホップが到達不可能です。
  - □ 設定されたスタティックルートが無効です。
- Track エントリの状態が NotReady の場合、以下の状況となります。
  - □ スタティックルートのネクストホップの到達可能性が不明です。
  - □ スタティックルートが有効です。

II. 制限とガイドライン

スタティックルート、Track モジュール、宛先モジュール間でのコラボレーションを行う場合、NQA 用に同一の VPN インスタンスとスタティックルートのネクストホップを設定してください。そうでない場合アクセス検出は正しく動作しません。

スタティックルートのルートを復旧させる場合、関連する Track エントリはスタティックルートではなく復旧ルートのネクストホップを監視させる必要があります。そうでなければルートは無効とみなされます。

III. 設定手順

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． ネクストホップの到達可能性をチェックするためにスタティックルーティングと Track エントリを関連づける	• パブリックネットワーク: **ip route-static** { *dest-address* { *mask-length* | *mask* } | **group** *group-name* } { *interface-type interface-number* [*next-hop-address*] [**backup-interface** *interface-type interface-number* [**backup-nexthop** *backup-nexthop-address*] [**permanent**] | **bfd** { **control-packet** | **echo-packet** } | **permanent** | **track** *track-entry-number*] | *next-hop-address* [**recursive-lookup host-route**] [**bfd control-packet bfd-source** *ip-address* | **permanent** | **track** *track-entry-number*] | **vpn-instance** *d-vpn-instance-name next-hop-address* [**recursive-lookup host-route**] [**bfd control-packet bfd-source** *ip-address* | **permanent** | **track** *track-entry-number*] } [**preference** *preference*] [**tag** *tag-value*] [**description** *text*] • VPN: **ip route-static vpn-instance** *s-vpn-instance-name* { *dest-address* { *mask-length* | *mask* } | **group** *group-name* } { *interface-type interface-number* [*next-hop-address*] [**backup-interface** *interface-type interface-number* [**backup-nexthop** *backup-nexthop-address*] [**permanent**] | **bfd** { **control-packet** | **echo-packet** } | **permanent** | **track** *track-entry-number*] | *next-hop-address* [**recursive-lookup host-route**] [**public**] [**bfd control-packet bfd-source** *ip-address* | **permanent** | **track** *track-entry-number*] | **vpn-instance** *d-vpn-instance-name next-hop-address* [**recursive-lookup host-route**] [**bfd control-packet bfd-source** *ip-address* | **permanent** | **track** *track-entry-number*] } [**preference** *preference*] [**tag** *tag-value*] [**description** *text*]	デフォルト：設定なし

9.6.4 Track と PBR の関連づけ

I. Track と PBR の関連づけ

PBR は、ACL のような基準にマッチするパケットの VPN インスタンス、ネクストホップを指定します。PBR の詳細は、オペレーションマニュアルのセクション 5 *ルーティングプロトコル”ポリシーベースルーティング*”を参照してください。

PBR はパケットの動作が有効であるかどうかを検出することはできません。ネクストホップが故障したとき、検出が有効でないとき、パケットが廃棄される可能性があります。たとえば、故障した PBR にネクストホップが指定されている場合、PBR は故障と認識することができず、ネクストホップにマッチするパケットを転送し続けます。

この問題は Track に PBR を関連づけることによって解決することができます。PBR アプリケーションの柔軟性を高めて､PBRがトポロジの変化を感知することを可能にします。

Track エントリを apply 項と関連づけた後、Track エントリと関連づけられた検出モジュールは、Track されたオブジェクトの有効性の検出結果を送信します。

- Track エントリの状態が Positive の場合､オブジェクトは有効で､apply は有効です。
- Track エントリの状態が Negative の場合、オブジェクトは有効でなく、apply は無効です。
- Track エントリの状態が NotReady の場合、apply は有効です。

現在のソフトウェアバージョンでは、PBR ポリシでパケットを一致させるためのネクストホップだけを指定できます。

II. 設定要件

Track と PBR を関連づける前に、ポリシあるいはポリシノードを作成し、同様にマッチング基準を設定してください。

III. Track と PBR の関連づけ

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. ポリシあるいはポリシノードを作成し、PBR policy node view に移行する	**policy-based-route** *policy-name* [**deny** | **permit**] **node** *node-number*	―
3. ACL マッチング基準を定義する	**if-match acl** { *acl-number* | **name** *acl-name* }	デフォルト：設定なし ACL一致条件がレイヤ2情報と一致しません。 ACLの照合基準では、**permit**または**deny**アクションと、指定されたACLの時間範囲を使用してパケットを照合しません。

操作	コマンド	補足
4. パケットを照合するネクストホップを設定し、ネクストホップを Track エントリに関連付づける	• ネクストホップを設定し、Trackエントリと関連づける: **apply next-hop** [**vpn-instance** *vpn-instance-name* | **inbound-vpn**] { *ip-address* [**direct**] [**track** *track-entry-number*] [**weight** *weight-value*] }&<1-n>	デフォルト：設定なし

IV. Track と IPv6 PBR の関連づけ

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. ポリシあるいはポリシノードを作成し、PBR policy node view に移行する	**ipv6 policy-based-route** *policy-name* [**deny** | **permit**] **node** *node-number*	ー
3. ACL マッチング基準を定義する	**if-match acl** { *ipv6-acl-number* | **name** *ipv6-acl-name* }	デフォルト：設定なし ACL一致条件がレイヤ2情報と一致しません。 ACLの照合基準では、**permit** または**deny**アクションと、指定されたACLの時間範囲を使用してパケットを照合しません。
4. パケットを照合するネクストホップを設定し、ネクストホップを Track エントリに関連付づける	• ネクストホップを設定し、Trackエントリと関連づける: **apply next-hop** [**vpn-instance** *vpn-instance-name* | **inbound-vpn**] { *ipv6-address* [**direct**] [**track** *track-entry-number*] [**weight** *weight-value*] } &<1-n>	デフォルト：設定なし

9.6.5 Track と Smart link の関連づけ

I. Track と Smart link の関連づけ

Smart Link は、中間装置またはネットワークパス上で障害（たとえば、単方向リンク、誤接続、およびパケット損失）が発生したときや障害が復旧したとき、リンク状態を検出できません。また故障が解決したときも検出することができません。リンク状態を監視するために Smart Link のポートは、リンク検出プロトコルを使用する必要があります。障害が検出あるいは復旧すると、リンク検出プロトコルは、リンクを切り替えるために Smart Link に通知します。

Smart Link グループメンバポートで Smart Link と Track 間のコラボレーションを設定することができます。Smart Link は、ポートのリンク状態を検出するため、Track エントリを通して CFD の CC 機能とコラボレーションを行います。

- Track エントリが Positive 状態の場合、リンクは通常状態です。Smart Link は Smart Link グループのリンクの切り替えを行いません。
- Track エントリが Negative 状態の場合、リンクは故障状態です。Smart Link は Smart Link グループに設定されたリンクの preemption モードとポート役割に従い、リンクの切り替えを行うかどうか決定します。
- Track エントリが NotReady 状態の場合、ポートの状態は変更しません。

Smart link の詳細はオペレーションマニュアルのセクション 10 *高可用性*”*Smart link*”を参照してください。

II. 制限とガイドライン

Smart Link とコラボレーションに使用される Track エントリは CFD の CC 機能と関連付けられている必要があります。

III. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Layer 2 Ethernet interface view あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	―
3. ポートの Smart Link と Track のコラボレーションを設定する	**port smart-link group** *group-id* **track** *track-entry-number*	デフォルト：設定なし

9.7 Trackの表示と維持

すべての view で **display** コマンドを表示することができます。

操作	コマンド
Trackエントリの情報を表示する	**display track** { *track-entry-number* | **all** [**negative** | **positive**] } [**brief**]

9.8 Track設定例

9.8.1 VRRP-Track-NQA コラボレーション設定例

I. ネットワーク要件

図 9-2に示すように設定します。

- Host A はインタネットの Host B にアクセスします。Host A のデフォルトゲートウェイは 10.1.1.10/24 です。
- Switch A と Switch B は仮想 IP アドレスが 10.1.1.10 の VRRP グループ 1 に属します。

- マスタのアップリンクをモニタし、以下の要件に適用するために、VRRP-Track-NQA コラボレーションを設定します。
- Switch A が正常に動作するとき、Host A から Host B のパケットは Switch A を通して転送されます。
- NQA によって Switch A のアップリンクが故障したと認識したとき、Host A から Host B へのパケットは Switch B を通して転送されます。

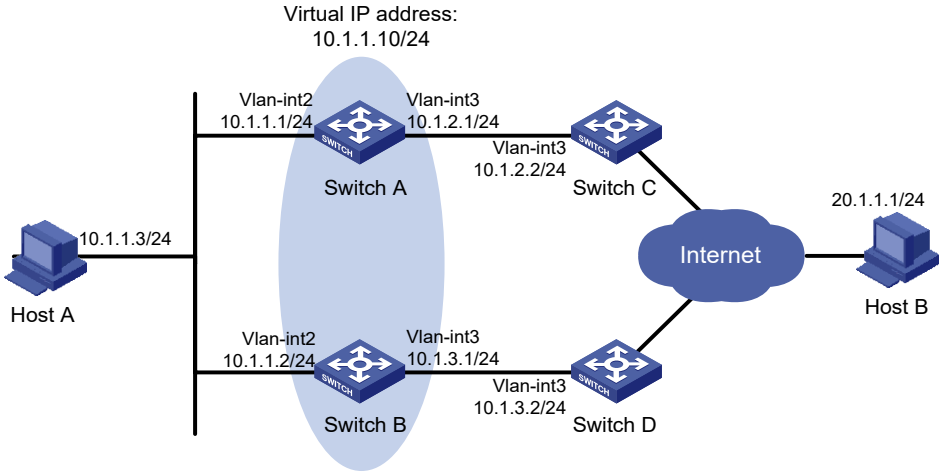


図 9-2 ネットワーク図

II. 設定手順

1) VLAN を作成し、対応するポートを割り当てます。図 9-2に示すように各 VLAN インタフェースの IP アドレスを割り当てます。(詳細は省略します)
2) Switch A で NQA テストグループを設定します。

管理者 **admin**、オペレーションタグ **test** の NQA オペレーションを作成します。

```
<SwitchA> system-view
[SwitchA] nqa entry admin test
```

ICMP エコーとしてオペレーションタイプを設定します。

```
[SwitchA-nqa-admin-test] type icmp-echo
```

ICMP エコーリクエストの宛先アドレスを 10.1.2.2 に設定します。

```
[SwitchA-nqa-admin-test-icmp-echo] destination ip 10.1.2.2
```

ICMP エコーオペレーションのテスト間隔を 100ms に設定します。

```
[SwitchA-nqa-admin-test-icmp-echo] frequency 100
```

リアクションエントリ 1 を設定し、Track モジュールのトリガを 5 回連続して失敗するように指定します。

```
[SwitchA-nqa-admin-test-icmp-echo] reaction 1 checked-element probe-fail threshold-type consecutive 5 action-type trigger-only
[SwitchA-nqa-admin-test-icmp-echo] quit
```

NQA オペレーションを開始します。

```
[SwitchA] nqa schedule admin test start-time now lifetime forever
```

3) Switch A で Track エントリ 1 を設定し、NQA オペレーショングループに割り当てます。

```
[SwitchA] track 1 nqa entry admin test reaction 1
```

4) Switch A で VRRP を設定します。

VLAN インタフェース 2 で VRRPv2 を指定します。

```
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] vrrp version 2
```

VRRP グループ 1 を作成し、グループの仮想 IP アドレス 10.1.1.10 を設定します。

```
[SwitchA-Vlan-interface2] vrrp vrid 1 virtual-ip 10.1.1.10
```

VRRP グループ 1 の Switch A の優先度を 110 に設定します。

```
[SwitchA-Vlan-interface2] vrrp vrid 1 priority 110
```

VRRP グループ 1 の認証モードを **simple**、認証キーを **hello** に設定します。

```
[SwitchA-Vlan-interface2] vrrp vrid 1 authentication-mode simple hello
```

500 センチ秒間隔で VRRP パケットを送信するようにマスタを設定します。

```
[SwitchA-Vlan-interface2] vrrp vrid 1 timer advertise 500
```

preemptive モードで Switch A を動作するように設定し、preemption delay タイマを 5000 センチ秒に設定します。

```
[SwitchA-Vlan-interface2] vrrp vrid 1 preempt-mode timer delay 5000
```

Track エントリ 1 をモニタするように設定し、Track エントリ 1 の状態を Negative に変更するときのルータの優先度を 30 に減少させます。

```
[SwitchA-Vlan-interface2] vrrp vrid 1 track 1 priority reduced 30
```

5) Switch B で VRRP を設定します。

VLAN インタフェース 2 で VRRPv2 を指定します。

```
<SwitchB> system-view
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] vrrp version 2
```

VRRP グループ 1 を作成し、グループの仮想 IP アドレス 10.1.1.10 を設定します。

```
[SwitchB-Vlan-interface2] vrrp vrid 1 virtual-ip 10.1.1.10
```

VRRP グループ 1 の認証モードを **simple**、認証キーを **hello** に設定します。

```
[SwitchB-Vlan-interface2] vrrp vrid 1 authentication-mode simple hello
```

500 センチ秒間隔で VRRP パケットを送信するようにマスタを設定します。

```
[SwitchB-Vlan-interface2] vrrp vrid 1 timer advertise 500
```

preemptive モードで Switch B を動作するように設定し、preemption delay タイマを 5000 センチ秒に設定します。

```
[SwitchB-Vlan-interface2] vrrp vrid 1 preempt-mode timer delay 5000
```

III. 設定の確認

Host A から Host B に ping を行い、Host B が到達可能であることを確認します。（詳細は省略します）

Switch A の VRRP グループ 1 の詳細情報を表示します。

```
[SwitchA-Vlan-interface2] display vrrp verbose
IPv4 Virtual Router Information:
 Running Mode      : Standard
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID             : 1               Adver Timer  : 500
     Admin Status     : Up              State        : Master
     Config Pri       : 110             Running Pri  : 110
     Preempt Mode     : Yes             Delay Time   : 5000
     Auth Type        : Simple          Key          : ******
     Virtual IP       : 10.1.1.10
     Virtual MAC      : 0000-5e00-0101
     Master IP        : 10.1.1.1
   VRRP Track Information:
     Track Object   : 1             State : Positive          Pri Reduced : 30
```

Switch B の VRRP グループ 1 の詳細情報を表示します。

```
[SwitchB-Vlan-interface2] display vrrp verbose
IPv4 Virtual Router Information:
 Running Mode      : Standard
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID             : 1               Adver Timer  : 500
     Admin Status     : Up              State        : Backup
     Config Pri       : 100             Running Pri  : 100
     Preempt Mode     : Yes             Delay Time   : 5000
     Become Master    : 2200ms left
     Auth Type        : Simple          Key          : ******
     Virtual IP       : 10.1.1.10
     Master IP        : 10.1.1.1
```

出力は、VRRP グループ 1 の Switch A がマスタで、Switch B がバックアップであることを示します。Host A から Host B へのパケットは Switch A を通して転送されます。

Switch A と Switch C 間のリンクを切断し、Host A から Host B への ping が成功していることを確認します。（詳細は省略します）

Switch A の VRRP グループ 1 の詳細情報を表示します。

```
[SwitchA-Vlan-interface2] display vrrp verbose
IPv4 Virtual Router Information:
 Running Mode      : Standard
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID             : 1               Adver Timer  : 500
     Admin Status     : Up              State        : Backup
     Config Pri       : 110             Running Pri  : 80
     Preempt Mode     : Yes             Delay Time   : 5000
     Become Master    : 2200ms left
     Auth Type        : Simple          Key          : ******
     Virtual IP       : 10.1.1.10
     Master IP        : 10.1.1.2
   VRRP Track Information:
     Track Object   : 1             State : Negative          Pri Reduced : 30
```

Switch B の VRRP グループ 1 の詳細情報を表示します。

```
[SwitchB-Vlan-interface2] display vrrp verbose
IPv4 Virtual Router Information:
 Running Mode      : Standard
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID             : 1               Adver Timer  : 500
     Admin Status     : Up              State        : Master
     Config Pri       : 100             Running Pri  : 100
     Preempt Mode     : Yes             Delay Time   : 5000
     Auth Type        : Simple          Key          : ******
     Virtual IP       : 10.1.1.10
     Virtual MAC      : 0000-5e00-0101
     Master IP        : 10.1.1.2
```

出力は、Switch A がバックアップになり、Switch B がマスタになることを示します。Host A から Host B へのパケットは Switch B を通して転送されます。

9.8.2 マスタを監視する VRRP バックアップ用 BFD の設定例

I. ネットワーク要件

図 9-3に示すように設定します。

- Switch A と Switch B は VRRP グループ 1 に属しています。仮想 IP アドレスは 192.168.0.10 です。
- LAN の Host のデフォルトゲートウェイは 192.168.0.10 です。
- バックアップのマスタをモニタし、以下の要件に適用するために、VRRP-Track-BFD コラボレーションを設定します。
- Switch A が正常に動作しているとき、LAN 上の Host は Switch A を通してインタネットにアクセスします。
- Switch A が故障したとき、バックアップ(Switch B)は BFD を通してマスタの状態変更を早急に検出し、新しいマスタになります。LAN の Host は Switch B を通してインタネットにアクセスします。

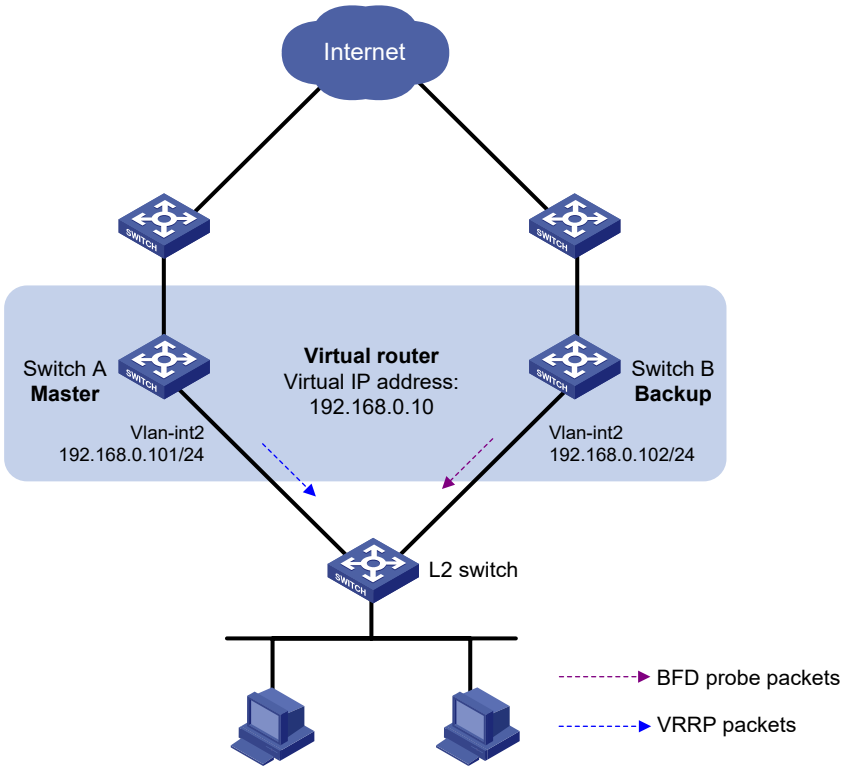


図 9-3 ネットワーク図

II. 設定手順

1) VLAN を作成し、対応するポートを割り当てます。図 9-3に示すように各 VLAN インタフェースの IP アドレスを割り当てます。(詳細は省略します)
2) Switch A を設定します。

VRRP グループ 1 を作成し、グループの仮想 IP アドレスを 192.168.0.10 に設定します。

```
<SwitchA> system-view
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] vrrp vrid 1 virtual-ip 192.168.0.10
```

VRRP グループ 1 の Switch A の優先度を 110 に設定します。

```
[SwitchA-Vlan-interface2] vrrp vrid 1 priority 110
[SwitchA-Vlan-interface2] return
```

3) Switch B を設定します。

BFD エコーパケットの送信元 IP アドレスを 10.10.10.10 に設定します。

```
<SwitchB> system-view
[SwitchB] bfd echo-source-ip 10.10.10.10
```

Track エントリを作成し、Switch A の到達可能性を確認するため、Switch B の BFD セッションに関連づけます。

```
[SwitchB] track 1 bfd echo interface vlan-interface 2 remote ip 192.168.0.101 local ip
```

```
192.168.0.102
```

VRRP グループ 1 を作成し、グループの仮想 IP アドレスを 192.168.0.10 に設定します。

```
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] vrrp vrid 1 virtual-ip 192.168.0.10
```

Track エントリ 1 の状態をモニタするため、VRRP グループ 1 を設定します。

```
[SwitchB-Vlan-interface2] vrrp vrid 1 track 1 switchover
[SwitchB-Vlan-interface2] return
```

III. 設定の確認

Switch A の VRRP グループ 1 の詳細情報を表示します。

```
<SwitchA> display vrrp verbose
IPv4 Virtual Router Information:
 Running Mode      : Standard
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID             : 1               Adver Timer  : 100
     Admin Status     : Up              State        : Master
     Config Pri       : 110             Running Pri  : 110
     Preempt Mode     : Yes             Delay Time   : 0
     Auth Type        : None
     Virtual IP       : 192.168.0.10
     Virtual MAC      : 0000-5e00-0101
     Master IP        : 192.168.0.101
```

Switch B の VRRP グループ 1 の詳細情報を表示します。

```
<SwitchB> display vrrp verbose
IPv4 Virtual Router Information:
 Running Mode      : Standard
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID             : 1               Adver Timer  : 100
     Admin Status     : Up              State        : Backup
     Config Pri       : 100             Running Pri  : 100
     Preempt Mode     : Yes             Delay Time   : 0
     Become Master    : 2200ms left
     Auth Type        : None
     Virtual IP       : 192.168.0.10
     Master IP        : 192.168.0.101
   VRRP Track Information:
     Track Object   : 1              State : Positive          Switchover
```

Switch B の Track エントリ 1 の情報を表示します。

```
<SwitchB> display track 1
Track ID: 1
  State: Positive
  Duration: 0 days 0 hours 0 minutes 32 seconds
  Notification delay: Positive 0, Negative 0 (in seconds)
  Tracked object:
    BFD session mode: Echo
    Outgoing interface: Vlan-interface2
    VPN instance name: --
    Remote IP: 192.168.0.101
    Local IP: 192.168.0.102
```

出力は、Track エントリの状態が Positive のとき、Switch A がマスタで Switch B がバックアップであることを示します。

Switch B で VRRP 状態、BFD イベント通知のデバッグを有効にします。

```
<SwitchB> terminal debugging
<SwitchB> terminal monitor
<SwitchB> debugging vrrp fsm
<SwitchB> debugging bfd ntfy
```

Switch A が故障したとき、Switch B に以下の出力が表示されます。

```
*Dec 17 14:44:34:142 2008 SwitchB BFD/7/DEBUG: Notify application:TRACK
State:DOWN
*Dec 17 14:44:34:144 2008 SwitchB VRRP4/7/FSM:
 IPv4 Vlan-interface2 | Virtual Router 1 : Backup --> Master  reason: The status
of the tracked object changed
```

Switch B の VRRP グループの詳細情報を表示します。

```
<SwitchB> display vrrp verbose
IPv4 Virtual Router Information:
 Running Mode      : Standard
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID             : 1               Adver Timer  : 100
     Admin Status     : Up              State        : Master
     Config Pri       : 100             Running Pri  : 100
     Preempt Mode     : Yes             Delay Time   : 0
     Auth Type        : None
     Virtual IP       : 192.168.0.10
     Virtual MAC      : 0000-5e00-0101
     Master IP        : 192.168.0.102
   VRRP Track Information:
     Track Object   : 1              State : Negative          Switchover
```

出力は、Switch A が故障したと BFD が検出したとき、Track モジュールは VRRP に、マスタになる Switch B の状態の変更を通知します。バックアップはアドバタイズメント間隔の 3 倍の期間＋Skew_Time を待つことなく、Switch B がマスタに切り替わります。

9.8.3 アップリンクを監視する VRRP マスタ用 BFD の設定例

I. ネットワーク要件

図 9-4に示すように設定します。

- Switch A と Switch B は VRRP グループ 1 に属します。仮想 IP アドレスを 192.168.0.10 に割り当てます。
- VLAN の Host のデフォルトゲートウェイは 192.168.0.10 です。
- マスタのアップリンクをモニタし、以下の要件に適用するために、VRRP-Track-BFD コラボレーションを設定します。
- Switch A が正常に動作しているとき、LAN 上の Host は Switch A を通してインタネットにアクセスします。
- Switch A が BFD を通してアップリンクダウンの故障を検出したとき、Switch B は新しいマスタになります。LAN の Host は Switch B を通してインタネットにアクセスします。

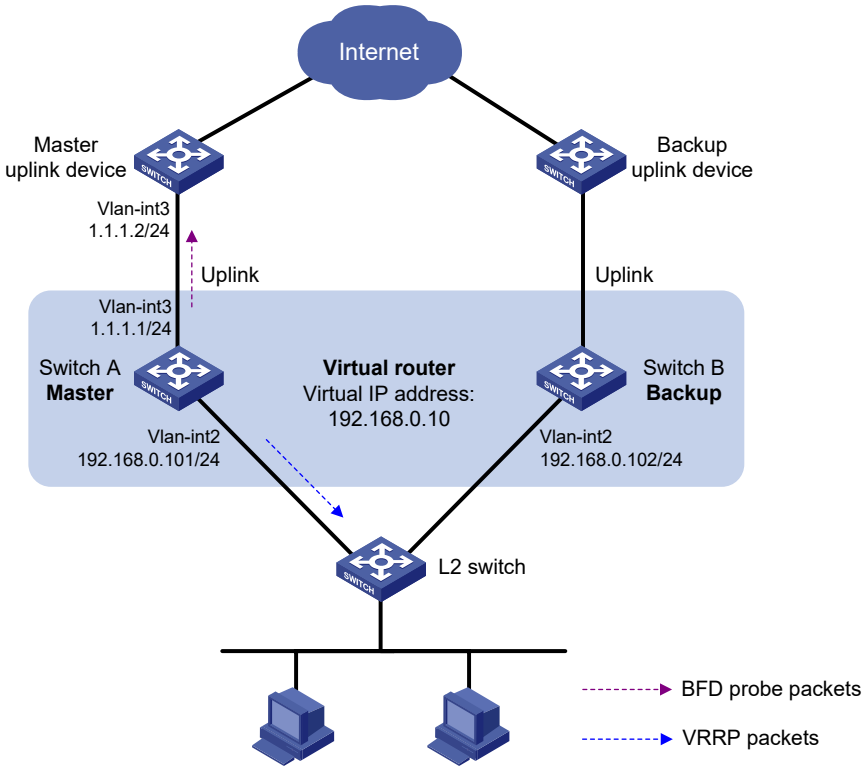


図 9-4 ネットワーク図

II. 設定手順

1) VLAN を作成し、対応するポートを割り当てます。図 9-4に示すように各 VLAN インタフェースの IP アドレスを割り当てます。(詳細は省略します)
2) Switch A を設定します。

BFD エコーパケットの送信元 IP アドレスを 10.10.10.10 に設定します。

```
<SwitchA> system-view
[SwitchA] bfd echo-source-ip 10.10.10.10
```

アップリンク装置（1.1.1.2）の到達可能性を確認するため、BFD セッションの Track エントリを作成します。

```
[SwitchA] track 1 bfd echo interface vlan-interface 3 remote ip 1.1.1.2 local ip 1.1.1.1
```

VRRP グループ 1 を設定し、仮想 IP アドレスを 192.168.0.10 として設定します。

```
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] vrrp vrid 1 virtual-ip 192.168.0.10
```

VRRP グループ 1 の Switch A の優先度を 110 として設定します。

```
[SwitchA-Vlan-interface2] vrrp vrid 1 priority 110
```

VRRP グループ 1 を Track エントリ 1 に関連づけます。Track エントリの状態が Negative になったとき、Switch A の優先度が 20 に減少します。

```
[SwitchA-Vlan-interface2] vrrp vrid 1 track 1 priority reduced 20
```

```
[SwitchA-Vlan-interface2] return
```

3) Switch B で、VRRP グループ 1 を設定し、仮想 IP アドレスを 192.168.0.10 として設定します。

```
<SwitchB> system-view
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] vrrp vrid 1 virtual-ip 192.168.0.10
[SwitchB-Vlan-interface2] return
```

III. 設定の確認

Switch A の VRRP グループの詳細情報を表示します。

```
<SwitchA> display vrrp verbose
           IPv4 Virtual Router Information:
 Running Mode      : Standard
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID              : 1               Adver Timer  : 100
     Admin Status      : Up              State        : Master
     Config Pri        : 110             Running Pri  : 110
     Preempt Mode      : Yes             Delay Time   : 0
     Auth Type         : None
     Virtual IP        : 192.168.0.10
     Virtual MAC       : 0000-5e00-0101
     Master IP         : 192.168.0.101
   VRRP Track Information:
     Track Object   : 1              State : Positive          Pri Reduced : 20
```

Switch A の Track エントリ 1 の情報を表示します。

```
<SwitchA> display track 1
Track ID: 1
  State: Positive
  Duration: 0 days 0 hours 0 minutes 32 seconds
  Notification delay: Positive 0, Negative 0 (in seconds)
  Tracked object:
    BFD session mode: Echo
    Outgoing interface: Vlan-interface2
    VPN instance name: --
    Remote IP: 1.1.1.2
    Local IP: 1.1.1.1
```

Switch B の VRRP グループの詳細情報を表示します。

```
<SwitchB> display vrrp verbose
IPv4 Virtual Router Information:
 Running Mode      : Standard
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID              : 1               Adver Timer  : 100
     Admin Status      : Up              State        : Backup
     Config Pri        : 100             Running Pri  : 100
     Preempt Mode      : Yes             Delay Time   : 0
     Become Master     : 2200ms left
     Auth Type         : None
     Virtual IP        : 192.168.0.10
     Master IP         : 192.168.0.101
```

出力は、Track エントリの状態が Positive のとき、Switch A がマスタで Switch B がバックアップであることを示します。

Switch A のアップリンクがダウンしたとき、Track エントリ 1 の情報を表示します。

```
<SwitchA> display track 1
Track ID: 1
  State: Negative
  Duration: 0 days 0 hours 0 minutes 32 seconds
  Notification delay: Positive 0, Negative 0 (in seconds)
  Tracked object:
    BFD session mode: Echo
    Outgoing interface: Vlan-interface2
    VPN instance name: --
    Remote IP: 1.1.1.2
    Local IP: 1.1.1.1
```

Switch A の VRRP グループ 1 の詳細情報を表示します。

```
<SwitchA> display vrrp verbose
IPv4 Virtual Router Information:
 Running Mode      : Standard
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID             : 1               Adver Timer  : 100
     Admin Status     : Up              State        : Backup
     Config Pri       : 110             Running Pri  : 90
     Preempt Mode     : Yes             Delay Time   : 0
     Become Master    : 2200ms left
     Auth Type        : None
     Virtual IP       : 192.168.0.10
     Master IP        : 192.168.0.102
   VRRP Track Information:
     Track Object   : 1             State : Negative          Pri Reduced : 20
```

Switch B の VRRP グループ 1 の詳細情報を表示します。

```
<SwitchB> display vrrp verbose
IPv4 Virtual Router Information:
 Running Mode      : Standard
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID             : 1               Adver Timer  : 100
     Admin Status     : Up              State        : Master
     Config Pri       : 100             Running Pri  : 100
     Preempt Mode     : Yes             Delay Time   : 0
     Auth Type        : None
     Virtual IP       : 192.168.0.10
     Virtual MAC      : 0000-5e00-0101
     Master IP        : 192.168.0.102
```

出力は、BFD を通してアップリンクが故障したと Switch A が検出したとき、Switch A の優先度が 20 に減少していることを示します。Switch B はマスタに切り替わります。

9.8.4 スタティックルーティング-Track-NQA コラボレーション設定例

I. ネットワーク要件

図 9-5に示すように設定します。

- Switch A はサブネット 20.1.1.0/24 内の Host のデフォルトゲートウェイです。
- Switch D はサブネット 30.1.1.0/24 内の Host のデフォルトゲートウェイです。
- 2 つのサブネット内の Host はスタティックルートを通して互いに通信します。

ネットワークの信頼性を保証するため、ルートのバックアップを設定し、以下のように Switch A と Switch D のスタティックルーティング-Track-NQA コラボレーションを設定します。

- Switch A 上で、高い優先度、ネクストホップが Switch B、宛先が 30.1.1.0/24 のスタティックルートを割り当てます。このルートがマスタルートです。ネクストホップが Switch C、宛先が 30.1.1.0/24 へのスタティックルートはバックアップルートとして動作します。Switch A は、Switch C を通して 30.1.1.0/24 にパケットを転送します。
- Switch D 上で、高い優先度、ネクストホップが Switch B、宛先が 20.1.1.0/24 のスタティックルートを割り当てます。このルートがマスタルートです。ネクストホップが Switch C、宛先が 20.1.1.0/24 へのスタティックルートはバックアップルートとして動作します。マスタルートが到達不能であるとき、バックアップルートが適用されます。Switch D は、Switch C を通して 20.1.1.0/24 にパケットを転送します。

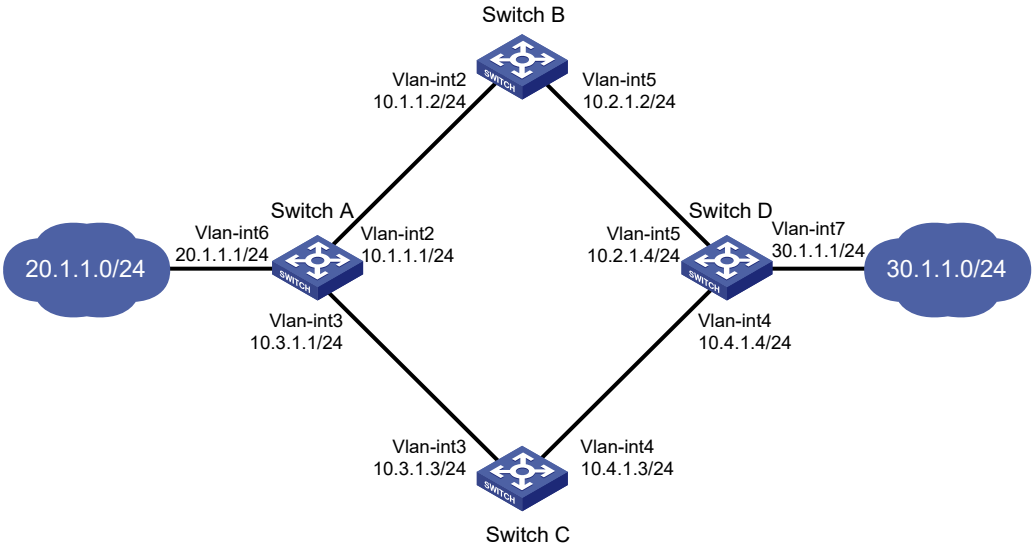


図 9-5 ネットワーク図

II. 設定手順

1) VLAN を作成し、対応するポートを割り当てます。図 9-5に示すように各 VLAN インタフェースの IP アドレスを割り当てます。(詳細は省略します)
2) Switch A を設定します。

ネクストホップのアドレスを 10.1.1.2、デフォルトの優先度を 60 のスタティックルート 30.1.1.0/24 を設定します。このスタティックルートを Track エントリ 1 に関連づけます。

```
<SwitchA> system-view
[SwitchA] ip route-static 30.1.1.0 24 10.1.1.2 track 1
```

ネクストホップのアドレスが 10.3.1.3、優先度を 80 のスタティックルート 30.1.1.0/24 を設定します。

```
[SwitchA] ip route-static 30.1.1.0 24 10.3.1.3 preference 80
```

ネクストホップのアドレスが 10.1.1.2 のスタティックルート 10.2.1.4 を設定します。

```
[SwitchA] ip route-static 10.2.1.4 24 10.1.1.2
```

管理者 **admin**、オペレータタグ **test** の NQA オペレーションを作成します。

```
[SwitchA] nqa entry admin test
```

オペレーションタイプを ICMP エコータイプとして設定します。

```
[SwitchA-nqa-admin-test] type icmp-echo
```

宛先アドレスを 10.2.1.4 に設定します。

```
[SwitchA-nqa-admin-test-icmp-echo] destination ip 10.2.1.4
```

ネクストホップのアドレスを 10.1.1.2 に設定します。

```
[SwitchA-nqa-admin-test-icmp-echo] next-hop ip 10.1.1.2
```

100 ミリ秒の間隔で繰り返す ICMP エコーオペレーションを設定します。

```
[SwitchA-nqa-admin-test-icmp-echo] frequency 100
```

リアクションエントリ 1 を設定し、Track モジュールのトリガを 5 回連続して失敗するように指定します。

```
[SwitchA-nqa-admin-test-icmp-echo] reaction 1 checked-element probe-fail threshold-type consecutive 5 action-type trigger-only
[SwitchA-nqa-admin-test-icmp-echo] quit
```

NQA オペレーションを開始します。

```
[SwitchA] nqa schedule admin test start-time now lifetime forever
```

Track エントリ 1 を設定し、NQA オペレーションのリアクションエントリ 1 に関連づけます。

```
[SwitchA] track 1 nqa entry admin test reaction 1
```

3) Switch B を設定します。

ネクストホップのアドレスが 10.2.1.4、宛先が 30.1.1.0/24 のスタティックルートを設定します。

```
<SwitchB> system-view
[SwitchB] ip route-static 30.1.1.0 24 10.2.1.4
```

ネクストホップのアドレスが 10.1.1.1、宛先が 20.1.1.0/24 のスタティックルートを設定します。

```
[SwitchB] ip route-static 20.1.1.0 24 10.1.1.1
```

4) Switch C を設定します。

ネクストホップのアドレスが 10.4.1.4、宛先が 30.1.1.0/24 のスタティックルートを設定します。

```
<SwitchC> system-view
[SwitchC] ip route-static 30.1.1.0 24 10.4.1.4
```

ネクストホップのアドレスが 10.3.1.1、宛先が 20.1.1.0/24 のスタティックルートを設定します。

```
[SwitchC] ip route-static 20.1.1.0 24 10.3.1.1
```

5) Switch D を設定します。

ネクストホップのアドレスが 10.2.1.2、宛先が 20.1.1.0/24 のスタティックルートを設定し、デフォルトの優先度を 60 に設定します。このスタティックルートを Track エントリ 1 に割り当てます。

```
<SwitchD> system-view
[SwitchD] ip route-static 20.1.1.0 24 10.2.1.2 track 1
```

ネクストホップのアドレスが 10.4.1.3、宛先が 20.1.1.0/24 のスタティックルートを設定し、デフォルトの優先度を 80 に設定します。

```
[SwitchD] ip route-static 20.1.1.0 24 10.4.1.3 preference 80
```

ネクストホップのアドレスが 10.2.1.2、宛先が 10.1.1.1/24 のスタティックルートを設定します。

```
[SwitchD] ip route-static 10.1.1.1 24 10.2.1.2
```

管理者 **admin**、オペレータタグ **test** の NQA オペレーションを作成します。

```
[SwitchD] nqa entry admin test
```

テストタイプを ICMP エコータイプとして設定します。

```
[SwitchD-nqa-admin-test] type icmp-echo
```

オペレーションの宛先 IP アドレスを 10.1.1.1 に設定します。

```
[SwitchD-nqa-admin-test-icmp-echo] destination ip 10.1.1.1
```

ネクストホップアドレスを 10.2.1.2 に設定します。

```
[SwitchD-nqa-admin-test-icmp-echo] next-hop ip 10.2.1.2
```

ICMP エコーオペレーションのテスト間隔を 100ms に設定します。

```
[SwitchD-nqa-admin-test-icmp-echo] frequency 100
```

リアクションエントリ 1 を設定し、Track モジュールのトリガを 5 回連続して失敗するように指定します。

```
[SwitchD-nqa-admin-test-icmp-echo] reaction 1 checked-element probe-fail threshold-type consecutive 5 action-type trigger-only
[SwitchD-nqa-admin-test-icmp-echo] quit
```

NQA オペレーションを開始します。

```
[SwitchD] nqa schedule admin test start-time now lifetime forever
```

Track エントリ 1 を設定し、NQA オペレーションのリアクションエントリ 1 に関連づけます。

```
[SwitchD] track 1 nqa entry admin test reaction 1
```

III. 設定の確認

Switch A の Track エントリの情報を表示します。

```
[SwitchA] display track all
Track ID: 1
  State: Positive
```

```
  Duration: 0 days 0 hours 0 minutes 32 seconds
  Notification delay: Positive 0, Negative 0 (in seconds)
  Tracked object:
    NQA entry: admin test
    Reaction: 1
    Remote IP/URL:--
    Local IP:--
    Interface:--
```

出力は、Track エントリの状態が Positive で、NQA オペレーションが成功し、マスタルートが有効であることを示します。

Switch A のルーティングテーブルを表示します。

```
[SwitchA] display ip routing-table

Destinations : 10       Routes : 10

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
10.1.1.0/24         Direct 0    0            10.1.1.1        Vlan2
10.1.1.1/32         Direct 0    0            127.0.0.1       InLoop0
10.2.1.0/24         Static 60   0            10.1.1.2        Vlan2
10.3.1.0/24         Direct 0    0            10.3.1.1        Vlan3
10.3.1.1/32         Direct 0    0            127.0.0.1       InLoop0
20.1.1.0/24         Direct 0    0            20.1.1.1        Vlan6
20.1.1.1/32         Direct 0    0            127.0.0.1       InLoop0
30.1.1.0/24         Static 60   0            10.1.1.2        Vlan2
127.0.0.0/8         Direct 0    0            127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0            127.0.0.1       InLoop0
```

出力では、Switch A は Switch B を通して 30.1.1.0/24 にパケットを転送しています。

Switch B で VLAN インタフェース 2 の IP アドレスを削除します。

```
<SwitchB> system-view

[SwitchB] interface vlan-interface 2

[SwitchB-Vlan-interface2] undo ip address
```

Switch A の Track エントリの情報を表示します。

```
[SwitchA] display track all
Track ID: 1
  State: Negative
  Duration: 0 days 0 hours 0 minutes 32 seconds
  Notification delay: Positive 0, Negative 0 (in seconds)
  Tracked object:
    NQA entry: admin test
    Reaction: 1
    Remote IP/URL:--
    Local IP:--
    Interface:--
```

出力では、Track エントリの状態が Negative で、NQA オペレーションが失敗し、マスタルートが無効であることを示します。

Switch A のルーティングテーブルを表示します。

```
[SwitchA] display ip routing-table

Destinations : 10       Routes : 10

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
10.1.1.0/24         Direct 0    0            10.1.1.1        Vlan2
10.1.1.1/32         Direct 0    0            127.0.0.1       InLoop0
10.2.1.0/24         Static 60   0            10.1.1.2        Vlan2
```

```
10.3.1.0/24          Direct 0    0           10.3.1.1        Vlan3
10.3.1.1/32          Direct 0    0           127.0.0.1       InLoop0
20.1.1.0/24          Direct 0    0           20.1.1.1        Vlan6
20.1.1.1/32          Direct 0    0           127.0.0.1       InLoop0
30.1.1.0/24          Static 80   0           10.3.1.3        Vlan3
127.0.0.0/8          Direct 0    0           127.0.0.1       InLoop0
127.0.0.1/32         Direct 0    0           127.0.0.1       InLoop0
```

出力では、Switch A は Switch C を通して 30.1.1.0/24 にパケットを転送しています。バックアップルートが適用されています。

マスタが故障したとき、20.1.1.0/24 内の Host が 30.1.1.0/24 内の Host と通信できることを確認してください。

```
[SwitchA] ping -a 20.1.1.1 30.1.1.1
Ping 30.1.1.1: 56  data bytes, press CTRL_C to break
Reply from 30.1.1.1: bytes=56 Sequence=1 ttl=254 time=2 ms
Reply from 30.1.1.1: bytes=56 Sequence=2 ttl=254 time=1 ms
Reply from 30.1.1.1: bytes=56 Sequence=3 ttl=254 time=1 ms
Reply from 30.1.1.1: bytes=56 Sequence=4 ttl=254 time=2 ms
Reply from 30.1.1.1: bytes=56 Sequence=5 ttl=254 time=1 ms

--- Ping statistics for 30.1.1.1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.00% packet loss
round-trip min/avg/max/std-dev = 1/1/2/1 ms
```

マスタが故障したとき、30.1.1.0/24 内の Host が 20.1.1.0/24 内の Host と通信できることを確認してください。

```
[SwitchB] ping -a 30.1.1.1 20.1.1.1
Ping 20.1.1.1: 56  data bytes, press CTRL_C to break
Reply from 20.1.1.1: bytes=56 Sequence=1 ttl=254 time=2 ms
Reply from 20.1.1.1: bytes=56 Sequence=2 ttl=254 time=1 ms
Reply from 20.1.1.1: bytes=56 Sequence=3 ttl=254 time=1 ms
Reply from 20.1.1.1: bytes=56 Sequence=4 ttl=254 time=1 ms
Reply from 20.1.1.1: bytes=56 Sequence=5 ttl=254 time=1 ms

--- Ping statistics for 20.1.1.1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.00% packet loss
round-trip min/avg/max/std-dev = 1/1/2/1 ms
```

9.8.5 スタティックルーティング-Track-BFD コラボレーション設定例

I. ネットワーク要件

図 9-6に示すように設定します。

- Switch A はサブネット 20.1.1.0/24 内の Host のデフォルトゲートウェイです。
- Switch D はサブネット 30.1.1.0/24 内の Host のデフォルトゲートウェイです。
- 2 つのサブネット内の Host はスタティックルートを通して互いに通信します。
- ネットワークの信頼性を保証するため、ルートのバックアップを設定し、以下のように Switch A と Switch B のスタティックルーティング-Track-BFD コラボレーションを設定します。
- Switch A 上で、高い優先度、ネクストホップが Switch B、宛先が 30.1.1.0/24 のスタティックルートを割り当てます。このルートがマスタルートです。ネクストホップが Switch C、宛先が 30.1.1.0/24 へのスタティックルートはバックアップルートとして動作します。マスタルートが故障したとき、バックアップルートを適用するため、BFD が早急にルートの故障を検出します。
- Switch B 上で、高い優先度、ネクストホップが Switch A、宛先が 20.1.1.0/24 のスタティックルートを割り当てます。このルートがマスタルートです。ネクストホップが Switch C、宛先が 20.1.1.0/24 へのスタティックルートはバックアップルートとして

動作します。マスタルートが故障したとき、バックアップルートを適用するため、BFD が早急にルートの故障を検出します。

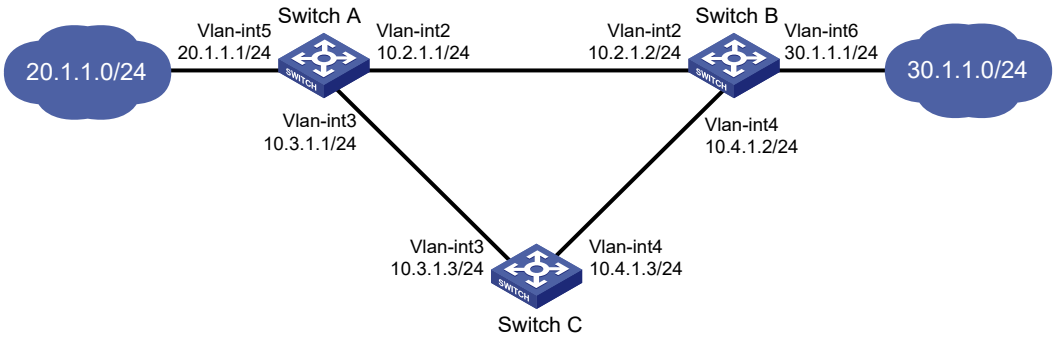


図 9-6 ネットワーク図

II. 設定手順

1) VLAN を作成し、対応するポートを割り当てます。図 9-6に示すように各 VLAN インタフェースの IP アドレスを割り当てます。(詳細は省略します)
2) Switch A を設定します。

ネクストホップのアドレスを 10.2.1.2、デフォルトの優先度を 60 のスタティックルート 30.1.1.0/24 を設定します。このスタティックルートを Track エントリ 1 に関連づけます。

```
<SwitchA> system-view
[SwitchA] ip route-static 30.1.1.0 24 10.2.1.2 track 1
```

ネクストホップのアドレスを 10.3.1.3、優先度を 80 のスタティックルート 30.1.1.0/24 を設定します。

```
[SwitchA] ip route-static 30.1.1.0 24 10.3.1.3 preference 80
```

BFD エコーパケットの送信元 IP アドレスを 10.10.10.10 に設定します。

```
[SwitchA] bfd echo-source-ip 10.10.10.10
```

Track エントリ 1 を設定し、Switch A と Switch B 間が通信可能かどうか確認するため、BFD セッションに関連づけます。

```
[SwitchA] track 1 bfd echo interface vlan-interface 2 remote ip 10.2.1.2 local ip 10.2.1.1
```

3) Switch B を設定します。

ネクストホップのアドレスを 10.2.1.1、デフォルトの優先度を 60 のスタティックルート 20.1.1.0/24 を設定します。このスタティックルートを Track エントリ 1 に関連づけます。

```
<SwitchB> system-view
[SwitchB] ip route-static 20.1.1.0 24 10.2.1.1 track 1
```

ネクストホップのアドレスを 10.4.1.3、優先度を 80 のスタティックルート 20.1.1.0/24 を設定します。

```
[SwitchB] ip route-static 20.1.1.0 24 10.4.1.3 preference 80
```

BFD エコーパケットの送信元 IP アドレスを 1.1.1.1 に設定します。

```
[SwitchB] bfd echo-source-ip 1.1.1.1
```

Track エントリ 1 を設定し、Switch A と Switch B 間が通信可能かどうか確認するため、BFD セッションに関連づけます。

```
[SwitchB] track 1 bfd echo interface vlan-interface 2 remote ip 10.2.1.1 local ip 10.2.1.2
```

4)　Switch C を設定します。

ネクストホップのアドレスを 10.4.1.2、スタティックルート 30.1.1.0/24 を設定します。

```
<SwitchC> system-view
[SwitchC] ip route-static 30.1.1.0 24 10.4.1.2
```

ネクストホップのアドレスを 10.3.1.1、スタティックルート 20.1.1.0/24 を設定します。

```
[SwitchB] ip route-static 20.1.1.0 24 10.3.1.1
```

III. 設定の確認

Switch A の Track エントリの情報を表示します。

```
[SwitchA] display track all
Track ID: 1
  State: Positive
  Duration: 0 days 0 hours 0 minutes 32 seconds
  Notification delay: Positive 0, Negative 0 (in seconds)
  Tracked object:
    BFD session mode: Echo
    Outgoing interface: Vlan-interface2
    Remote IP: 10.2.1.2
    Local IP: 10.2.1.1
```

出力は、Track エントリの状態が Positive で、ネクストホップ 10.2.1.2 が到達可能であることを示します。

Switch A のルーティングテーブルを表示します。

```
[SwitchA] display ip routing-table

Destinations : 9        Routes : 9

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
10.2.1.0/24         Direct 0    0            10.2.1.1        Vlan2
10.2.1.1/32         Direct 0    0            127.0.0.1       InLoop0
10.3.1.0/24         Direct 0    0            10.3.1.1        Vlan3
10.3.1.1/32         Direct 0    0            127.0.0.1       InLoop0
20.1.1.0/24         Direct 0    0            20.1.1.1        Vlan5
20.1.1.1/32         Direct 0    0            127.0.0.1       InLoop0
30.1.1.0/24         Static 60   0            10.2.1.2        Vlan2
127.0.0.0/8         Direct 0    0            127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0            127.0.0.1       InLoop0
```

出力では、Switch A は Switch B を通して 30.1.1.0/24 にパケットを転送しています。マスタルートが適用されています。

Switch B の VLAN インタフェース 2 の IP アドレスを削除します。

```
<SwitchB> system-view
[SwitchB] interface vlan-interface 2
```

```
[SwitchB-Vlan-interface2] undo ip address
```

Switch A の Track エントリの情報を表示します。

```
[SwitchA] display track all
Track ID: 1
  State: Negative
  Duration: 0 days 0 hours 0 minutes 32 seconds
  Notification delay: Positive 0, Negative 0 (in seconds)
  Tracked object:
    BFD session mode: Echo
    Outgoing interface: Vlan-interface2
    VPN instance name: --
    Remote IP: 10.2.1.2
    Local IP: 10.2.1.1
```

出力は、Track エントリの状態が Negative で、ネクストホップ 10.2.1.2 が到達不可能であることを示します。

Switch A のルーティングテーブルを表示します。

```
[SwitchA] display ip routing-table

Destinations : 9        Routes : 9

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
10.2.1.0/24         Direct 0    0            10.2.1.1        Vlan2
10.2.1.1/32         Direct 0    0            127.0.0.1       InLoop0
10.3.1.0/24         Direct 0    0            10.3.1.1        Vlan3
10.3.1.1/32         Direct 0    0            127.0.0.1       InLoop0
20.1.1.0/24         Direct 0    0            20.1.1.1        Vlan5
20.1.1.1/32         Direct 0    0            127.0.0.1       InLoop0
30.1.1.0/24         Static 80   0            10.3.1.3        Vlan3
127.0.0.0/8         Direct 0    0            127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0            127.0.0.1       InLoop0
```

出力では、Switch A は Switch C を通して 30.1.1.0/24 にパケットを転送しています。バックアップルートが適用されています。

マスタが故障したとき、20.1.1.0/24 内の Host が 30.1.1.0/24 内の Host と通信できることを確認してください。

```
[SwitchA] ping -a 20.1.1.1 30.1.1.1
Ping 30.1.1.1: 56  data bytes, press CTRL_C to break
Reply from 30.1.1.1: bytes=56 Sequence=1 ttl=254 time=2 ms
Reply from 30.1.1.1: bytes=56 Sequence=2 ttl=254 time=1 ms
Reply from 30.1.1.1: bytes=56 Sequence=3 ttl=254 time=1 ms
Reply from 30.1.1.1: bytes=56 Sequence=4 ttl=254 time=2 ms
Reply from 30.1.1.1: bytes=56 Sequence=5 ttl=254 time=1 ms

--- Ping statistics for 30.1.1.1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.00% packet loss
round-trip min/avg/max/std-dev = 1/1/2/1 ms
```

マスタが故障したとき、30.1.1.0/24 内の Host が 20.1.1.0/24 内の Host と通信できることを確認してください。

```
[SwitchB] ping -a 30.1.1.1 20.1.1.1
Ping 20.1.1.1: 56  data bytes, press CTRL_C to break
Reply from 20.1.1.1: bytes=56 Sequence=1 ttl=254 time=2 ms
Reply from 20.1.1.1: bytes=56 Sequence=2 ttl=254 time=1 ms
Reply from 20.1.1.1: bytes=56 Sequence=3 ttl=254 time=1 ms
Reply from 20.1.1.1: bytes=56 Sequence=4 ttl=254 time=1 ms
Reply from 20.1.1.1: bytes=56 Sequence=5 ttl=254 time=1 ms

--- Ping statistics for 20.1.1.1 ---
```

```
5 packet(s) transmitted, 5 packet(s) received, 0.00% packet loss
round-trip min/avg/max/std-dev = 1/1/2/1 ms
```

9.8.6 VRRP-Track-インタフェースマネジメントコラボレーション設定例

I. ネットワーク要件

図 9-7に示すように設定します。

- Host A はインタネットの Host B に接続する必要があります。Host A のデフォルトゲートウェイは 10.1.1.10/24 です。
- Switch A と Switch B は VRRP グループ 1 に属しています。仮想 IP アドレスを 10.1.1.10 に割り当てます。
- マスタのアップリンクインタフェースをモニタするため、VRRP-Track-インタフェースマネジメントコラボレーションを設定し、以下の要件に適用させます。
- Switch A が正常に動作しているとき、Host A から Host B のパケットは Switch A を通して転送されます。
- VRRP がインタフェース管理モジュールを通して Switch A のアップリンクインタフェースの故障を検出したとき、Host A から Host B のパケットは Switch B を通して転送されます。

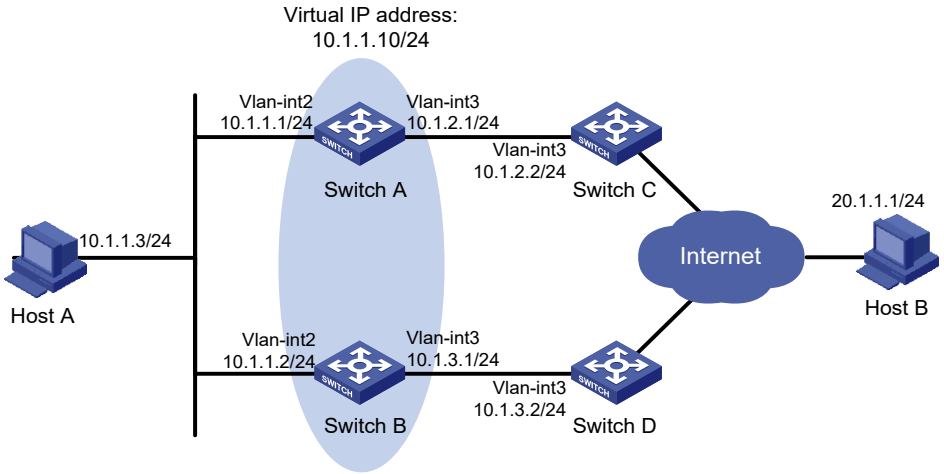


図 9-7 ネットワーク図

II. 設定手順

1) VLAN を作成し、対応するポートを割り当てます。図 9-7に示すように各 VLAN インタフェースの IP アドレスを割り当てます。(詳細は省略します)
2) Switch A を設定します。

Track エントリ 1 を設定し、VLAN インタフェース 3 のアップリンクインタフェースの物理状態に関連づけます。

```
[SwitchA] track 1 interface vlan-interface 3
```

VRRP グループ 1 を作成し、グループの仮想 IP アドレスを 10.1.1.10 に設定します。

```
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] vrrp vrid 1 virtual-ip 10.1.1.10
```

VRRP グループ 1 の Switch A の優先度を 110 に設定します。

```
[SwitchA-Vlan-interface2] vrrp vrid 1 priority 110
```

VRRP グループ 1 を Track エントリ 1 に関連づけ、Track エントリ 1 の状態が Negative に変更したとき、ルータの優先度を 30 に減少させます。

```
[SwitchA-Vlan-interface2] vrrp vrid 1 track 1 priority reduced 30
```

3) Switch B で VRRP グループ 1 を作成し、グループの仮想 IP アドレスを 10.1.1.10 に設定します。

```
<SwitchB> system-view
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] vrrp vrid 1 virtual-ip 10.1.1.10
```

III. 設定の確認

Host B が到達可能であることを確認するため、Host A から Host B に ping を行います。（詳細は省略します）

Switch A の VRRP グループ 1 の詳細情報を表示します。

```
[SwitchA-Vlan-interface2] display vrrp verbose
IPv4 Virtual Router Information:
 Running Mode       : Standard
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID             : 1               Adver Timer  : 100
     Admin Status     : Up              State        : Master
     Config Pri       : 110             Running Pri  : 110
     Preempt Mode     : Yes             Delay Time   : 0
     Auth Type        : None
     Virtual IP       : 10.1.1.10
     Virtual MAC      : 0000-5e00-0101
     Master IP        : 10.1.1.1
   VRRP Track Information:
     Track Object   : 1             State : Positive          Pri Reduced : 30
```

Switch B の VRRP グループ 1 の詳細情報を表示します。

```
[SwitchB-Vlan-interface2] display vrrp verbose
IPv4 Virtual Router Information:
 Running Mode       : Standard
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID             : 1               Adver Timer  : 100
     Admin Status     : Up              State        : Backup
     Config Pri       : 100             Running Pri  : 100
     Preempt Mode     : Yes             Delay Time   : 0
     Become Master    : 2200ms left
     Auth Type        : None
     Virtual IP       : 10.1.1.10
     Master IP        : 10.1.1.1
```

出力は、VRRP グループ 1 の Switch A がマスタで、Switch B がバックアップであることを示します。Host A から Host B のパケットは Switch A を通して転送されます。

Switch A の VLAN インタフェース 3 のアップリンクインタフェースをシャットダウンします。

```
[SwitchA-Vlan-interface2] interface vlan-interface 3
```

```
[SwitchA-Vlan-interface3] shutdown
```

Host B が到達可能であることを確認するため、Host A から Host B に ping を行います。（詳細は省略します）

Switch A の VRRP グループ 1 の詳細情報を表示します。

```
[SwitchA-Vlan-interface3] display vrrp verbose
IPv4 Virtual Router Information:
 Running Mode      : Standard
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID             : 1               Adver Timer  : 100
     Admin Status     : Up              State        : Backup
     Config Pri       : 110             Running Pri  : 80
     Preempt Mode     : Yes             Delay Time   : 0
     Become Master    : 2200ms left
     Auth Type        : None
     Virtual IP       : 10.1.1.10
     Master IP        : 10.1.1.2
   VRRP Track Information:
     Track Object   : 1             State : Negative          Pri Reduced : 30
```

Switch B の VRRP グループ 1 の詳細情報を表示します。

```
[SwitchB-Vlan-interface2] display vrrp verbose
IPv4 Virtual Router Information:
 Running Mode      : Standard
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID             : 1               Adver Timer  : 100
     Admin Status     : Up              State        : Master
     Config Pri       : 100             Running Pri  : 100
     Preempt Mode     : Yes             Delay Time   : 0
     Auth Type        : None
     Virtual IP       : 10.1.1.10
     Virtual MAC      : 0000-5e00-0101
     Master IP        : 10.1.1.2
```

出力は、Switch A がバックアップ、Switch B がマスタになります。Host A から Host B のパケットは Switch B を通して転送されることを示します。

QX-S5100G シリーズ Ethernet スイッチ

オペレーションマニュアル

11. システム管理

本マニュアルは以下に示す章で構成されています。

01-システムの保守とデバッグ
02-NQA
03-NTP
04-PoE
05-SNMP
06-RMON
07-NETCONF
08-プロセスモニタリングとメンテナンス
09-ポートミラーリング
10-トラフィックミラーリング
11-sFlow
12-Information Center
13-NetMeister

目次

このセクションのページは **11-x-x** です。

1 章 システムの保守とデバッグ 1-1
1.1 Ping 1-1
1.1.1 ping コマンドを使用したネットワークの接続試験 1-1
1.1.2 Ping 設定例 1-1
1.2 Tracert 1-3
1.2.1 設定要件 1-4
1.2.2 tracert コマンドを使用した故障の検出、ルートにあるすべてのノードの確認 1-4
1.2.3 Tracert 設定例 1-4
1.3 システムのデバッグ 1-6
1.3.1 スイッチのデバッグ情報の制御 1-6
1.3.2 システムデバッグの設定 1-7

1章 システムの保守とデバッグ

この章は ping、tracert を使用したシステムのデバッグ情報について記載します。

1.1 Ping

ping コマンドで、指定したアドレスに到達可能かどうかを確認したり、ネットワーク接続を試験したりすることができます。

ping は ICMP エコーリクエスト（ECHO-REQUEST）を宛先装置に送信します。リクエストを受信した、宛先リクエストは ICMP のリクエストに応答して送信元装置に ICMP エコーリプライ（ECHO-REPLY）を送信します。送信元装置は、パケット送信数、受信したパケットリプライ数、ラウンドトリップタイムの ping の統計情報を表示します。これらの統計情報を解析することによってネットワークの性能を測定することができます。

1.1.1 ping コマンドを使用したネットワークの接続試験

すべての view で **ping** コマンドを実行できます。

操作	コマンド	補足
指定したアドレスに到達可能かどうかを確認する	• IPv4ネットワーク： **ping** [**ip**] [**-a** *source-ip* | **-c** *count* | **-f** | **-h** *ttl* | *-i interface-type interface-number* | **-m** *interval* | **-n** | **-p** *pad* | **-q** | **-r** | **-s** *packet-size* | **-t** *timeout* | **-tos** *tos* | **-v**] * *host* • IPv6ネットワーク： **ping ipv6** [**-a** *source-ipv6* | **-c** *count* | **-i** *interface-type interface-number* | **-m** *interval* | **-q** | **-s** *packet-size* | **-t** *timeout* | **-v**] * *host*	低速ネットワークで**ping**コマンドを使用するとき、タイムアウトタイマの値を大きな値に設定してください。（コマンドの**-t**キーワードで示されます。）

1.1.2 Ping 設定例

I. ネットワーク要件

図 1-1に示すように、Device A と Device C 間で通信可能かどうか確認します。互いに通信可能である場合、Device A から Device C のルートについての詳細な情報を取得します。

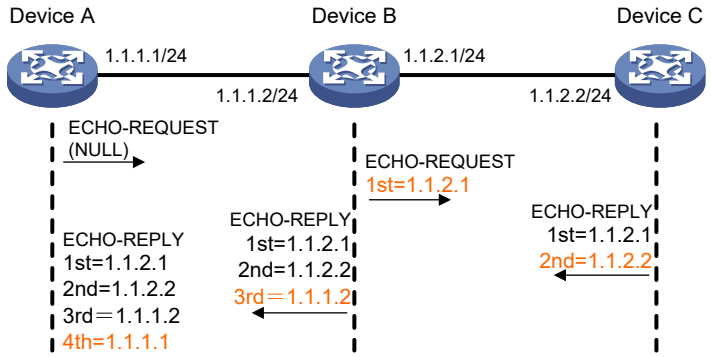


図 1-1 ネットワーク図

II. 設定手順

Device A で **ping** コマンドを使用し、Device C と通信可能かどうか確認します。

```
Ping 1.1.2.2 (1.1.2.2): 56 data bytes, press CTRL_C to break
56 bytes from 1.1.2.2: icmp_seq=0 ttl=254 time=2.137 ms
56 bytes from 1.1.2.2: icmp_seq=1 ttl=254 time=2.051 ms
56 bytes from 1.1.2.2: icmp_seq=2 ttl=254 time=1.996 ms
56 bytes from 1.1.2.2: icmp_seq=3 ttl=254 time=1.963 ms
56 bytes from 1.1.2.2: icmp_seq=4 ttl=254 time=1.991 ms

--- Ping statistics for 1.1.2.2 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.963/2.028/2.137/0.062 ms
```

出力は、以下の状態を示します。

- Device A が Device C に 5 つの ICMP パケットを送信し、Device A は ICMP パケットを受信します。
- パケットの送信失敗がありません。
- ルートが到達可能です。

Device A から Device C の詳細なルート情報を取得します。

```
<DeviceA> ping -r 1.1.2.2
Ping 1.1.2.2 (1.1.2.2): 56 data bytes, press CTRL_C to break
56 bytes from 1.1.2.2: icmp_seq=0 ttl=254 time=4.685 ms
RR:     1.1.2.1
        1.1.2.2
        1.1.1.2
        1.1.1.1
56 bytes from 1.1.2.2: icmp_seq=1 ttl=254 time=4.834 ms  (same route)
56 bytes from 1.1.2.2: icmp_seq=2 ttl=254 time=4.770 ms  (same route)
56 bytes from 1.1.2.2: icmp_seq=3 ttl=254 time=4.812 ms  (same route)
56 bytes from 1.1.2.2: icmp_seq=4 ttl=254 time=4.704 ms  (same route)

--- Ping statistics for 1.1.2.2 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 4.685/4.761/4.834/0.058 ms
```

図 1-1に示すように **ping - r** のテスト手順は以下となります。

1) 送信元（Device A）は RR オプションを空で ICMP エコーリクエストを宛先（Device C）に対して送信します。
2) 中間デバイス（Device B）は ICMP エコーリクエストの RR オプションに出力インタフェースの IP アドレス（1.1.2.1）を追加し、転送します。

3) リクエストを受信した宛先デバイスはリクエストの RR オプションをコピーし、RR オプションに出力インタフェースの IP アドレス（1.1.2.2）を追加します。ICMP エコーリプライを送信します。
4) 中間デバイスは ICMP エコーリプライの RR オプションに出力インタフェースの IP アドレス（1.1.1.2）を追加し、リプライを転送します。
5) リプライを受信した送信元デバイスは RR オプションにインタフェースの IP アドレス（1.1.1.1）を追加します。最後に、1.1.1.1 <-> {1.1.1.2; 1.1.2.1} <-> 1.1.2.2 という Device A～Device C 間の詳細な情報を取得します。

1.2 Tracert

Tracert（traceroute と呼ばれます）は、ネットワークが有効かどうか確認するために、送信元から宛先にパケットを伝送するレイヤ 3 デバイスの IP アドレスの追跡を行います。ネットワークに不具合があった場合に、tracert コマンドを使用して機能しなくなったノードを特定するのに有用です。

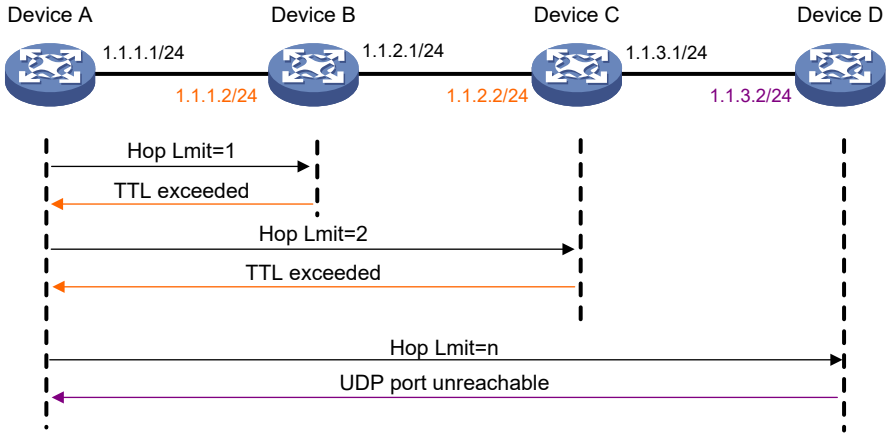


図 1-2 Tracert の動作

Tracert はデバイスの IP アドレスを取得するため、受信した ICMP エラーメッセージを使用します。図 1-2に示すように、tracert が動作します。

1) 送信元デバイス（Device A）が宛先デバイス（Device D）に TTL 値が 1 のパケットを送信します。パケットの UDP 番号は宛先のアプリケーションで使用されないポート番号です。
2) 最初のホップ（Device B）（パケットを最初に受信するレイヤ 3 デバイス）は、1.1.1.2 の IP アドレスがカプセル化された TTL-expired ICMP エラーメッセージを送信元に返します。このように、送信元デバイスは最初のレイヤ 3 デバイスのアドレス（1.1.1.2）を受信します。
3) 送信元デバイスが宛先のデバイスに TTL 値が 2 のパケットを送信します。
4) 2 番目のホップ（Device C）が TTL-expired ICMP エラーメッセージで応答し、これで送信元デバイスは 2 番目のレイヤ 3 デバイスのアドレス（1.1.2.2）を取得します。
5) このプロセスは、最終宛先のデバイスに到達するまで続きます。宛先のアプリケーションは UDP ポートを使用していません。宛先は IP アドレス 1.1.3.2 の到達不能 ICMP エラーメッセージのリプライをします。
6) 送信元デバイスは以下のことを認識します。

- 到達不能 ICMP エラーメッセージを受信したとき、宛先に届いたことを認識します。

- 宛先デバイスまでのパスは 1.1.1.2 から、1.1.2.2 から、1.1.3.2 であると認識します。

1.2.1 設定要件

tracert コマンドを使用する前に、以下の作業を行ってください。

IPv4 ネットワーク：

- 中間デバイス（送信元デバイスと宛先デバイスの間のデバイス）で ICMP タイムアウトパケットの送信を有効にします。もし中間デバイスが QX シリーズの場合、デバイスで **ip ttl-expires enable** コマンドを実行してください。このコマンドの詳細は、コマンドマニュアルのセクション 4 *IP サービス "IP パフォーマンスの最適化"*を参照してください。
- 中間デバイス（送信元デバイスと宛先デバイスの間のデバイス）で ICMP 宛先到達不能パケットの送信を有効にします。もし中間デバイスが QX シリーズの場合、デバイスで **ip unreachables enable** コマンドを実行してください。このコマンドの詳細は、コマンドマニュアルのセクション 4 *IP サービス "IP パフォーマンスの最適化"*を参照してください。

IPv6 ネットワーク：

- 中間デバイス（送信元デバイスと宛先デバイスの間のデバイス）で ICMPv6 タイムアウトパケットの送信を有効にします。もし中間デバイスが QX シリーズの場合、デバイスで **ipv6 hoplimit-expires enable** コマンドを実行してください。このコマンドの詳細は、コマンドマニュアルのセクション 4 *IP サービス "IPv6 の基本"*を参照してください。
- 中間デバイス（送信元デバイスと宛先デバイスの間のデバイス）で ICMPv6 宛先到達不能パケットの送信を有効にします。もし中間デバイスが QX シリーズの場合、デバイスで **ipv6 unreachables enable** コマンドを実行してください。このコマンドの詳細は、コマンドマニュアルのセクション 4 *IP サービス "IPv6 の基本"*を参照してください。

1.2.2 tracert コマンドを使用した故障の検出、ルートにあるすべてのノードの確認

すべての view で **tracert** コマンドを実行できます。

操作	コマンド
送信元から宛先のルートを表示する	• IPv4ネットワーク： **tracert** [**-a** *source-ip* | **-f** *first-ttl* | **-m** *max-ttl* | **-p** *port* | **-q** *packet-number* | **-w** *timeout*] * *host* • IPv6ネットワーク： **tracert ipv6** [**-f** *first-hop* | **-m** *max-hops* | **-p** *port* | **-q** *packet-number* | **-w** *timeout*] * *host*

1.2.3 Tracert 設定例

I. ネットワーク要件

図 1-3に示すように、Device A は Device C への Telnet が失敗しています。

Device A と Device C 間でネットワークの接続性を確認します。互いに通信できない場合、ネットワークの故障したノードを特定できます。

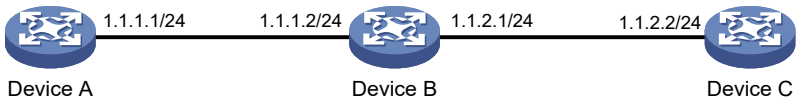


図 1-3 ネットワーク図

II. 設定手順

1) 図 1-3に示すように Device に IP アドレスを設定します。
2) Device A でスタティックルートを設定します。

```
<DeviceA> system-view
[DeviceA] ip route-static 0.0.0.0 0.0.0.0 1.1.1.2
[DeviceA] quit
```

3) **ping** コマンドを使用して Device A と Device C 間の接続性を確認します。

```
<DeviceA> ping 1.1.2.2
Ping 1.1.2.2(1.1.2.2): 56 -data bytes, press CTRL_C to break
Request time out
Request time out
Request time out
Request time out
Request time out

--- Ping statistics for 1.1.2.2 ---
5 packet(s) transmitted,0 packet(s) received,100.0% packet loss
```

出力は、Device A と Device C が通信不可能であることを示します。

4) **tracert** コマンドを使用して、故障したノードを特定します。

Device B で ICMP タイムアウトパケットの送信を有効にします。

```
<DeviceB> system-view
[DeviceB] ip ttl-expires enable
```

Device C で ICMP 到達不可能パケットの送信を有効にします。

```
<DeviceC> system-view
[DeviceC] ip unreachables enable
```

Device A で **tracert** コマンドを実行します。

```
<DeviceA> tracert 1.1.2.2
traceroute to 1.1.2.2 (1.1.2.2) 30 hops at most,40 bytes each packet, press CTRL_C
to break
 1  1.1.1.2 (1.1.1.2) 1 ms 2 ms 1 ms
 2  * * *
 3  * * *
 4  * * *
 5
<DeviceA>
```

出力は、Device A と Device C が互いに到達できず、Device A と Device B が到達でき、Device B と Device C 間の通信でエラーが発生していることを示します。

5)　問題を確認するため Device A と Device C で以下のコマンドを実行します。

- **debugging ip icmp** コマンドを使用して Device A と Device C で ICMP パケットの送受信ができるか確認を行います。
- **display ip routing-table** コマンドを使用して Device A と Device C のルートがあるか確認します。

1.3 システムのデバッグ

装置は、さまざまなデバッグ機能があります。サポートしているプロトコルおよび機能の大半に対し、システムはユーザのエラー診断に役立つデバッグ情報を提供しています。

1.3.1 スイッチのデバッグ情報の制御

次の 2 つのスイッチがデバッグ情報の表示を制御します。

- **モジュールデバッグスイッチ** － モジュール特有のデバッグ情報を制御します。
- **画面出力スイッチ** － 所定の画面にデバッグ情報を表示するかを制御します。出力する画面上で **terminal monitor** コマンド、**terminal logging level** コマンドを使用します。これらのコマンドの詳細は、コマンドマニュアルのセクション 11 *システム管理* "*Information center*"を参照してください。

図 1-4に示すように、モジュールデバッグスイッチと画面出力スイッチの関係を示したものです。デバイスは、デバッグ情報をモジュール 1、2、3 に出力できると仮定します。両方に電源が入っているときのみ情報は端末に出力されます。

デバッグ情報は通常、コンソールに表示されます。他の宛先にデバッグ情報を送信することができます。詳細は、オペレーションマニュアルのセクション 11 *システム管理* "*Information center*"を参照してください。

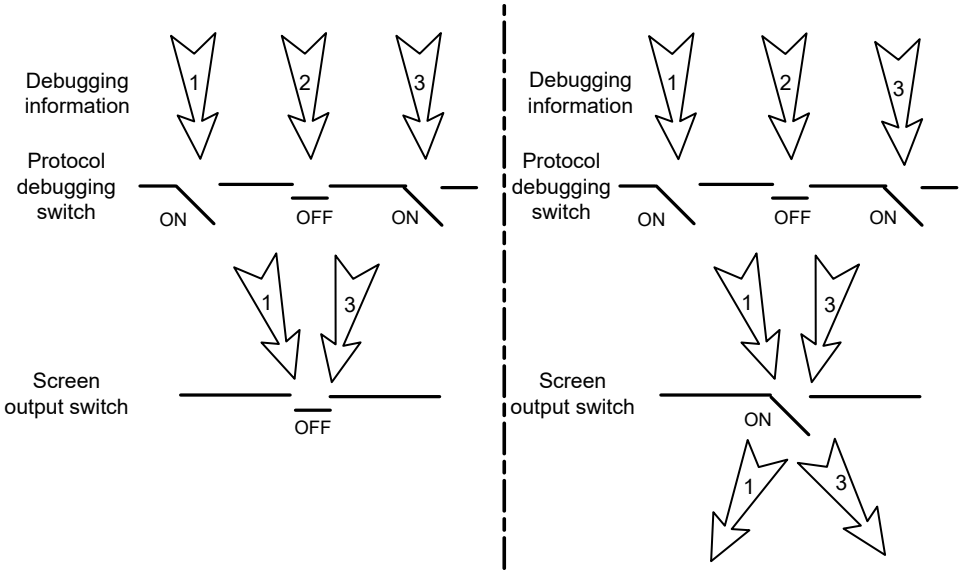


図 1-4 モジュールデバッグスイッチと画面出力スイッチの関係

1.3.2 システムデバッグの設定

デバッグコマンドの出力は、メモリ容量に影響します。システム性能を保証するため、異常な状況にあるプロトコルに関連したデバッグのみ有効にしてください。デバッグを行った後、**undo debugging all** コマンドを使用してすべてのデバッグ機能を無効にしてください。

以下にデバッグ機能の設定を示します。

操作	コマンド	補足
1. user view でプロトコルのデバッグを有効にする	**debugging** *module-name* [*option*]	デフォルト：無効
2. （オプション設定項目）すべての view で有効なデバッグ機能を表示する	**display debugging** [*module-name*]	—

目次

このセクションのページは **11-x-x** です。

2 章 NQA..... 2-1
2.1 概要..... 2-1
2.1.1 NQA のテストタイプ..... 2-1
2.1.2 しきい値監視機能..... 2-2
2.2 NQA 設定作業リスト..... 2-2
2.3 NQA サーバの設定..... 2-2
2.4 NQA クライアントの有効化..... 2-3
2.5 NQA クライアントの NQA テストの設定..... 2-4
2.5.1 NQA テストの設定作業リスト..... 2-4
2.5.2 ICMP エコーテストの設定..... 2-4
2.5.3 DHCP テストの設定..... 2-5
2.5.4 DNS テストの設定..... 2-6
2.5.5 FTP テストの設定..... 2-7
2.5.6 HTTP テストの設定..... 2-8
2.5.7 UDP ジッタテストの設定..... 2-9
2.5.8 SNMP テストの設定..... 2-10
2.5.9 TCP テストの設定..... 2-11
2.5.10 UDP エコーテストの設定..... 2-12
2.5.11 音声テストの設定..... 2-13
2.5.12 DLSw テストの設定..... 2-15
2.5.13 NQA テストのオプションパラメータの設定..... 2-16
2.5.14 しきい値監視機能の設定..... 2-17
2.5.15 NQA 統計情報収集機能の設定..... 2-18
2.5.16 NQA 履歴記録保存の設定..... 2-19
2.5.17 NQA クライアントにおける NQA テストのスケジューリング..... 2-19
2.6 NQA の表示と維持..... 2-20
2.7 NQA 設定例..... 2-20
2.7.1 ICMP エコーテスト設定例..... 2-20
2.7.2 DHCP テスト設定例..... 2-22
2.7.3 DNS テスト設定例..... 2-24
2.7.4 FTP テスト設定例..... 2-25
2.7.5 HTTP テスト設定例..... 2-26
2.7.6 UDP ジッタテスト設定例..... 2-28
2.7.7 SNMP テスト設定例..... 2-30
2.7.8 TCP テスト設定例..... 2-32
2.7.9 UDP エコーテスト設定例..... 2-33
2.7.10 音声テスト設定例..... 2-35
2.7.11 DLSw テスト設定例..... 2-37

2章 NQA

2.1 概要

NQA（Network quality analyzer）は、ネットワークの性能、IP サービスのサービスレベルとアプリケーションを確認し、ネットワークの問題を診断することができます。以下のタイプのテストをサポートしています。

- ICMP エコーテスト
- DHCP
- DLSw
- DNS
- FTP
- HTTP
- SNMP
- TCP
- UDP エコーテスト
- Voice
- UDP ジッタ

図 2-1に示すように、NQA 送信元装置（NQA クライアント）は、ネットワークパフォーマンスを測定するため、NQA 宛先装置に IP サービスとアプリケーションのシミュレーションを行うデータを送信します。取得した性能の測定基準は、1 方向の遅延、ジッタ、音声品質、アプリケーション性能、サーバ応答時間が含まれます。

NQA のすべてのタイプは NQA クライアントが必要ですが、TCP、UDP エコー、UDP ジッタ、音声は NQA サーバのみ必要です。FTP のように、すでに宛先装置でサービスが提供されている場合、NQA サーバは必要ではありません。

さまざまなテストのニーズを満たすため、特定の IP アドレスとポートをリスニングし、応答する NQA サーバを設定することができます。



図 2-1 ネットワーク図

2.1.1 NQA のテストタイプ

以下に異なる NQA テストタイプを示します。

- TCP あるいは DLSw テストは接続をセットアップします。
- UDP ジッタや音声テストは指定した数のプローブパケットを送信します。プローブパケット数は **probe packet-number** コマンドで設定可能です。
- FTP テストはファイルのアップロードあるいはダウンロードを行います。
- HTTP テストは Web ページを取得します。
- DHCP テストは DHCP を通して IP アドレスを取得します。

- DNS テストは IP アドレスにドメイン名を変換します。
- ICMP エコーテストは ICMP エコーリクエストを送信します。
- UDP エコーテストは UDP ペットを送信します。
- SNMP テストは SNMPv1 パケット、SNMPv2c パケット、SNMPv3 パケットを送信します。

2.1.2 しきい値監視機能

しきい値監視機能は、NQA が指定したしきい値を越えたとき、指定されたアクションを実行します。

表 2-1に監視対象とサポートするテストタイプの関係について示します。

表 2-1 監視対象とサポートするテストタイプの関係

監視対象	サポートするテストタイプ
プローブ期間	UDPジッタ、音声を除くすべてのNQAテスト
検査失敗回数	UDPジッタ、音声を除くすべてのNQAテスト
廃棄パケット数	UDPジッタ、音声テスト
1方向のジッタ（送信元から宛先、宛先から送信元）	UDPジッタ、音声テスト
1方向の遅延（送信元から宛先、宛先から送信元）	UDPジッタ、音声テスト
ICPIF（Calculated Planning Impairment Factor）（詳細はオペレーションマニュアルのセクション11 *システム管理"NQA"の"音声テストの設定"*を参照してください。）	音声テスト
MOS（Mean Opinion Scores）（詳細はオペレーションマニュアルのセクション11 *システム管理"NQA"の"音声テストの設定"*を参照してください。）	音声テスト

2.2 NQA設定作業リスト

作業リスト	補足
NQAサーバの設定	TCP、UDP、UDPジッタ、音声テストでは必須設定項目
（必須設定項目）NQAクライアントの有効化	ー
（必須設定項目） NQAクライアントのNQAテストの設定	ー

2.3 NQAサーバの設定

TCP、UDP エコー、UDP ジッタ、音声テストを実行するため、宛先装置で NQA サーバを有効にする必要があります。NQA サーバは。指定されたアドレスとポート番号で NQA クライアントからの要求に応答します。IP アドレスとポート番号は NQA クライアントが設定したものと一致する必要があります。また現在リスニングしているものとは別にする必要があります。

NQA サーバ上で、各 IP アドレスとポート番号に対応した複数の TCP、UDP リスニングサービスを設定することができます。リスニングサービスは NQA サーバで固有にする必要があります。IP アドレスとポート番号は NQA クライアントで設定された IP アドレスとポート番号と同一にする必要があります。

以下に NQA サーバの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. NQA サーバを有効にする	**nqa server enable**	デフォルト：無効
3. TCP、UDP リスニングサービスを設定する	● TCP リスニングサービスを設定する： **nqa server tcp-connect** *ip-address port-number* [**vpn-instance** *vpn-instance-name*] [**tos** *tos*] ● UDP リスニングサービスを設定する： **nqa server udp-echo** *ip-address port-number* [**vpn-instance** *vpn-instance-name*] [**tos** *tos*]	NQA サーバによって送信された応答パケットの IP パケットヘッダの ToS 値を指定することができます。 デフォルトの ToS 値：0

2.4 NQA クライアントの有効化

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. NQA クライアントを有効にする	**nqa agent enable**	デフォルト：有効 NQA クライアントを有効にしたのち NQA の設定が適用されます。

2.5 NQAクライアントのNQAテストの設定

2.5.1 NQA テストの設定作業リスト

作業リスト
（必須設定項目） 少なくとも1つを設定してください。 ● ICMPエコーテストの設定 ● DHCPテストの設定 ● DNSテストの設定 ● FTPテストの設定 ● HTTPテストの設定 ● UDPジッタテストの設定 ● SNMPテストの設定 ● TCPテストの設定 ● UDPエコーテストの設定 ● 音声テストの設定 ● DLSwテストの設定
（オプション設定項目） NQAテストのオプションパラメータの設定
（オプション設定項目） しきい値監視機能の設定
（オプション設定項目） NQA統計情報収集機能の設定
（オプション設定項目） NQA履歴記録保存の設定
（必須設定項目） NQAクライアントにおけるNQAスケジューリング

2.5.2 ICMP エコーテストの設定

ICMP エコーテストは宛先装置の到達可能性をテストします。ICMP エコーテストは **ping** コマンドと同等の機能ですが、さらに詳細な情報が得られます。送信元と宛先間で複数のパスがある場合、ICMP エコーテストでネクストホップを指定できます。

IPv6 ネットワークでは NQA ICMP エコーテストはサポートしていません。IPv6 アドレスの到達可能性をテストする場合には、**ping ipv6** コマンドを使用してください。詳細はコマンドマニュアルのセクション 11 *システム管理* "*システムの保守とデバッグ*"を参照してください。

以下に ICMP エコーテストの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. NQA テストを作成し、NQA operation view に移行する	**nqa entry** *admin-name operation-tag*	デフォルト：設定なし
3. ICMP エコータイプを指定し、その view に移行する	**type icmp-echo**	―
4. ICMP エコーリクエストの宛先アドレスを指定する	**destination ip** *ip-address*	デフォルト：設定なし

操作	コマンド	補足
5.　（オプション設定項目）各 ICMP エコーリクエストのペイロードサイズを指定する	**data-size** *size*	デフォルト：100バイト
6.　（オプション設定項目）各 ICMP エコーリクエストのペイロードに入る文字列を指定する	**data-fill** *string*	デフォルト：00102030405060708 09（16進数表示）
7.　（オプション設定項目）ICMP エコーリクエストの送信元 IP アドレスを指定する	● 送信元インタフェースを指定する： **source interface** *interface-type interface-number* ● 送信元IPアドレスを指定する： **source ip** *ip-address*	デフォルト：ICMPエコー要求パケットは送信元IPアドレスとして送信インタフェースのプライマリIPアドレスを使用します。 指定されていない場合、送信元IPアドレスとして出力インタフェースのプライマリIPアドレスが適用されます。 **source ip**コマンドと**source interface**コマンドの両方が設定された場合、最後に設定したコマンドが適用されます。 指定した送信元インタフェースはアップ状態でなくてはいけません。 送信元IPアドレスはローカルインタフェースのIPアドレスで、アップ状態でなくてはいけません。そうでなければICMPエコーテストに失敗します。
8.　（オプション設定項目）ICMP エコーリクエストのネクストホップを指定する	**next-hop** *ip-address*	デフォルト：設定なし

2.5.3 DHCP テストの設定

DHCP テストは、DHCP サーバが DHCP クライアントリクエストに応答できるかどうかをテストします。また DHCP サーバから IP アドレスを取得する時間を計測することができます。

NQA クライアントは、DHCP サーバから IP アドレスを取得するために DHCP リクエストを転送する DHCP リレーエージェントをテストします。DHCP テストを実行するインタフェースはインタフェースの IP アドレスを変更しません。DHCP テストを完了したとき、取得した IP アドレスを解放するため、NQA クライアントはパケットを送信します。

以下に DHCP テストの設定を示します。

操作	コマンド	補足
1.　system view に移行する	**system-view**	―

操作	コマンド	補足
2. NQA テストを作成し、NQA operation view に移行する	**nqa entry** *admin-name operation-tag*	デフォルト：設定なし
3. DHCP タイプを指定し、その view に移行する	**type dhcp**	―
4. DHCP パケットの宛先 IP アドレスとして DHCP サーバの IP アドレスを指定する	**destination ip** *ip-address*	デフォルト：設定なし
5. （オプション設定項目）DHCP リクエストパケットの送信元 IP アドレスを指定する	**source ip** *ip-address*	デフォルト : ICMPエコー要求パケットは送信元IPアドレスとして送信インタフェースのプライマリIPアドレスを使用します。 指定する送信元IPアドレスはローカルインタフェースのIPアドレスにする必要があります。またローカルインタフェースはアップ状態にする必要があります。そうでない場合、プローブパケットを送信できません。 NQAクライアントはDHCPサーバに送信するDHCP要求の**giaddr**フィールドに送信元IPアドレスを追加します。 詳細はオペレーションマニュアルのセクション4 *IP サービス "DHCP リレーエージェント"*を参照してください。

2.5.4 DNS テストの設定

DNS テストは DNS クライアントが DNS サーバを通してドメイン名を IP アドレスに変換する時間を測定します。

DNS テストは DNS 解決をテストします。取得した DNS エントリは保存しません。

以下に DNS テストの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. NQA テストを作成し、NQA operation view に移行する	**nqa entry** *admin-name operation-tag*	デフォルト：設定なし
3. DNS タイプを指定し、その view に移行する	**type dns**	―
4. DNS パケットの宛先アドレスとして DNS サーバの IP アドレスを指定する	**destination ip** *ip-address*	デフォルト：設定なし

操作	コマンド	補足
5. 変換に必要なドメイン名を指定する	**resolve-target** *domain-name*	デフォルト：設定なし

2.5.5 FTP テストの設定

FTP テストは NQA クライアントが FTP サーバからファイルを転送するかダウンロードする時間をテストします。

FTP テストを設定するとき、以下の制限とガイドラインに従ってください。

- **filename** コマンドが設定され、**put** オペレーションが行われるとき、NQA クライアントにファイルが存在することを確認してください。
- FTP サーバからファイルを取得するために **get** オペレーションを行う場合、FTP サーバの指定した URL にファイルが存在することを確認してください。
- NQA クライアントは FTP サーバから取得したファイルを保存しません。
- FTP テストを行う場合、小さいサイズのファイルを使用してください。大きいサイズのファイルは、タイムアウトでテストが失敗したり、ネットワークの帯域幅以上を独占して他のサービスに影響を与えたりする可能性があります。

以下に FTP テストの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. NQA テストを作成し、NQA operation view に移行する	**nqa entry** *admin-name operation-tag*	デフォルト：設定なし
3. FTP タイプを指定し、その view に移行する	**type ftp**	―
4. 宛先の FTP サーバの URL を指定する	**url** *url*	デフォルト：指定なし 以下のどちらかのフォーマットで URL を入力します。 ● ftp://*host*/*filename* ● ftp://*host*:*port*/*filename* **get** オペレーションを行うとき、ファイル名が必要です。
5. （オプション設定項目）FTP リクエストパケットの送信元 IP アドレスを指定する	**source ip** *ip-address*	デフォルト：ICMP エコー要求パケットは送信元 IP アドレスとして送信インタフェースのプライマリ IP アドレスを使用します。 送信元 IP アドレスはローカルインタフェースの IP アドレスにする必要があります。またローカルインタフェースはアップ状態にする必要があります。そうでない場合、FTP は送信できません。
6. FTP のオペレーションタイプを指定する	**operation** { **get** | **put** }	デフォルト：**get** FTP サーバからファイルを取得します。
7. FTP ログインユーザ名を指定する	**username** *username*	デフォルト：設定なし

操作	コマンド	補足
8. FTP ログインパスワードを指定する	**password** { **cipher** | **simple** } *string*	デフォルト：設定なし
9. （オプション設定項目）転送されるファイル名を指定する	**filename** *file-name*	デフォルト：設定なし この操作は**put**オペレーションが行われるときに必要です。

2.5.6 HTTP テストの設定

HTTP テストは NQA クライアントが HTTP サーバからデータを取得する時間をテストします。

以下に HTTP テストの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. NQA テストを作成し、NQA operation view に移行する	**nqa entry** *admin-name operation-tag*	デフォルト：設定なし
3. HTTP タイプを指定し、その view に移行する	**type http**	―
4. 宛先の HTTP サーバの URL を指定する	**url** *url*	デフォルト：指定なし 以下のどちらかのフォーマットでURLを入力します。 ● http://*host*/*resource* ● http://*host*:*port*/*resource*
5. HTTP ログインユーザ名を指定する	**username** *username*	デフォルト：設定なし
6. HTTP ログインパスワードを指定する	**password** { **cipher** | **simple** } *password*	デフォルト：設定なし
7. （オプション設定項目）リクエストパケットの送信元 IP アドレスを指定する	**source ip** *ip-address*	デフォルト：ICMPエコー要求パケットは送信元IPアドレスとして送信インタフェースのプライマリIPアドレスを使用します。 送信元IPアドレスはローカルインタフェースのIPアドレスにする必要があります。またローカルインタフェースはアップ状態にする必要があります。そうでない場合、リクエストは送信できません。
8. （オプション設定項目）HTTP オペレーションタイプを指定する	**operation** { **get** | **post** }	デフォルト：**get** HTTPサーバからファイルを取得します。
9. （オプション設定項目）HTTP バージョンを指定する	**version** { **v1.0** | **v1.1** }	デフォルト：HTTP 1.0

2.5.7 UDP ジッタテストの設定

⚠ **注意：**
UDP ジッタテストをポート番号 1～1023 で行わないでください。1～1023 を使用した場合 NQA テストは失敗するか、このポートに該当するサービスが動作しなくなります。

ジッタは相互のパケット遅延の変動値を意味します。UDP ジッタテストはネットワークで音声サービスやビデオサービスなどのジッタに敏感なリアルタイムサービスを行えるかどうか確認するため、片方向、双方向のジッタをテストします。

UDP ジッタテストは以下のように動作します。

1) NQA クライアントは通常の間隔で宛先ポートに UDP パケットを送信します。
2) 宛先装置は、受信した各パケットにタイムスタンプを追加し、NQA クライアントにパケットを送り返します。
3) 応答を受信すると、NQA クライアントは、タイムスタンプに従ってジッタを計算します。

UDP ジッタテストは、NQA サーバと NQA クライアントの両方が必要です。UDP ジッタテストを実行する前に、NQA サーバで UDP リスニングサービスの設定を行う必要があります。UDP リスニングサービスの詳細は、コマンドマニュアルのセクション 11 *システム管理* "*NQA*"の"*NQA サーバの設定*"を参照してください。

以下に UDP ジッタテストの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. NQA テストを作成し、NQA operation view に移行する	**nqa entry** *admin-name operation-tag*	デフォルト：設定なし
3. UDP ジッタタイプを指定し、その view に移行する	**type udp-jitter**	―
4. UDP パケットの宛先アドレスを指定する	**destination ip** *ip-address*	デフォルト：設定なし 宛先アドレスはNQAサーバでリスニングサービスを行っているIPアドレスと同一です。
5. UDP パケットの宛先ポートを指定する	**destination port** *port-number*	デフォルト：設定なし 宛先ポートはNQAサーバでリスニングサービスを行っているポートと同一です。

操作	コマンド	補足
6.　（オプション設定項目）UDP パケットの送信元 IP アドレスを指定する	**source ip** *ip-address*	デフォルト: ICMPエコー要求パケットは送信元IPアドレスとして送信インタフェースのプライマリIPアドレスを使用します。送信元IPアドレスはローカルインタフェースのIPアドレスにする必要があります。またローカルインタフェースはアップ状態にする必要があります。そうでない場合、UDPパケットは送信できません。
7.　（オプション設定項目）UDP パケットの送信元ポート番号を指定する	**source port** *port-number*	デフォルト：設定なし
8.　（オプション設定項目）各 UDP パケットのペイロードサイズを指定する	**data-size** *size*	デフォルト：100バイト
9.　（オプション設定項目）各 UDP パケットのペイロードで使われる文字列を指定する	**data-fill** *string*	デフォルト：00010203040506070809（16進数表示）
10.　（オプション設定項目）UDP ジッタテストで送信する UDP パケット数を指定する	**probe packet-number** *packet-number*	デフォルト：10
11.　（オプション設定項目）UDP パケットを送信する間隔を設定する	**probe packet-interval** *interval*	デフォルト：20ミリ秒
12.　（オプション設定項目）NQA クライアントの UDP パケットの受信待ち時間を指定する	**probe packet-timeout** *timeout*	デフォルト：3000ミリ秒

🕮 **メモ：**

display nqa result コマンドあるいは **display nqa statistics** コマンドを使用して UDP ジッタテストを確認してください。**display nqa history** コマンドは、UDP ジッタテストの結果や統計情報を表示しません。

2.5.8 SNMP テストの設定

SNMP テストは NQA クライアントが SNMP パケットを SNMP エージェントに送信し、SNMP エージェントから応答パケットを受信する時間を測定します。

以下に SNMP テストの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. NQA テストを作成し、NQA operation view に移行する	**nqa entry** *admin-name operation-tag*	デフォルト：設定なし
3. SNMP タイプを指定し、その view に移行する	**type snmp**	ー
4. SNMP パケットの宛先アドレスを指定する	**destination ip** *ip-address*	デフォルト：設定なし
5. （オプション設定項目）SNMP パケットの送信元ポート番号を指定する	**source port** *port-number*	デフォルト：設定なし
6. （オプション設定項目）SNMP パケットの送信元 IP アドレスを指定する	**source ip** *ip-address*	デフォルト: ICMPエコー要求パケットは送信元IPアドレスとして送信インタフェースのプライマリIPアドレスを使用します。 送信元IPアドレスはローカルインタフェースのIPアドレスにする必要があります。またローカルインタフェースはアップ状態にする必要があります。そうでない場合、SNMPパケットは送信できません。

2.5.9 TCP テストの設定

TCP テストは、NQA クライアントと NQA サーバ上のポート間で TCP 接続が確立される時間を測定するために使われます。これにより指定したサーバのポートの有効性と能力を判断します。

TCP テストは NQA サーバと NQA クライアントの両方が必要です。TCP テストを実行する前に、NQA サーバで TCP リスニングサービスの設定を行う必要があります。TCP リスニングサービスの詳細は、オペレーションマニュアルのセクション 11 *システム管理* "*NQA*"の"*NQA サーバの設定*"を参照してください。

以下に TCP テストの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. NQA テストを作成し、NQA operation view に移行する	**nqa entry** *admin-name operation-tag*	デフォルト：設定なし
3. TCP タイプを指定し、その view に移行する	**type tcp**	ー
4. TCP パケットの宛先アドレスを指定する	**destination ip** *ip-address*	デフォルト：設定なし 宛先アドレスはNQAサーバでリスニングサービスを行っているIPアドレスです。

操作	コマンド	補足
5. TCP パケットの宛先ポート番号を指定する	**destination port** *port-number*	デフォルト：設定なし 宛先ポート番号はNQAサーバでリスニングサービスを行っているポート番号です。
6. （オプション設定項目）TCP パケットの送信元 IP アドレスを指定する	**source ip** *ip-address*	デフォルト：ICMPエコー要求パケットは送信元IPアドレスとして送信インタフェースのプライマリIPアドレスを使用します。 送信元IPアドレスはローカルインタフェースのIPアドレスにする必要があります。またローカルインタフェースはアップ状態にする必要があります。そうでない場合、TCPパケットは送信できません。

2.5.10 UDP エコーテストの設定

UDP エコーテストはクライアントと NQA サーバの UDP ポート間のラウンドトリップ時間をテストします。

UDP エコーテストは、NQA サーバと NQA クライアントの両方が必要です。UDP エコーテストを行う前に、NQA サーバで UDP をリスニングするサービスを設定してください。UDP リスニングサービスの詳細は、コマンドマニュアルのセクション 11 *システム管理* "*NQA*"の"*NQA サーバの設定*"を参照してください。

以下に UDP エコーテストの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. NQA テストを作成し、NQA operation view に移行する	**nqa entry** *admin-name operation-tag*	デフォルト：設定なし
3. UDP エコータイプを指定し、その view に移行する	**type udp-echo**	ー
4. UDP パケットの宛先アドレスを指定する	**destination ip** *ip-address*	デフォルト：設定なし 宛先アドレスは、NQAサーバでリスニングサービスが設定されたIPアドレスと同一でなくてはいけません。
5. UDP パケットの宛先ポートを指定する	**destination port** *port-number*	デフォルト：設定なし 宛先ポート番号は、NQAサーバでリスニングサービスが設定されたポート番号と同一でなくてはいけません。
6. （オプション設定項目）各 UDP パケットのペイロードサイズを指定する	**data-size** *size*	デフォルト：100バイト

操作	コマンド	補足
7.　（オプション設定項目）各 UDP パケットのペイロードに入る文字列を指定する	**data-fill** *string*	デフォルト：0010203040506070809（16進数表示
8.　（オプション設定項目）UDP パケットの送信元ポートを指定する	**source port** *port-number*	デフォルト：設定なし
9.　（オプション設定項目）UDP パケットの送信元 IP アドレスを指定する	**source ip** *ip-address*	デフォルト: ICMPエコー要求パケットは送信元IPアドレスとして送信インタフェースのプライマリIPアドレスを使用します。 送信元IPアドレスは、ローカルインタフェースのIPアドレスで、アップ状態でなくてはいけません。 そうでなければUDPパケットが送信できません。

2.5.11 音声テストの設定

注意：
音声テストでポート 1～1023 を使用しないでください。1～1023 を使用した場合、このポートに関連したサービスが使えなくなります。

音声テストは VoIP ネットワーク性能を測定します。

音声テストは以下のように動作します。

1) NQA クライアントは指定した間隔で音声パケットを宛先装置（NQA サーバ）に送信します。

   音声パケットは以下のコーデックタイプがあります。

   - G.711 A-law
   - G.711 μ-law
   - G.729 A-law

2) 宛先装置は、受信した各音声パケットにタイムスタンプを追加し、NQA クライアントにパケットを送り返します。
3) 応答を受信すると、NQA クライアントは、タイムスタンプに従ってジッタと 1 方向遅延を計算します。

VoIP ネットワーク性能に反映される以下のパラメータは、音声テストによって収集されたメトリックを使用して計算することができます。

- **ICPIF（Calculated Planning Impairment Factor）** －パケットのロスや遅延による VoIP ネットワークの音声データの減衰を測定します。高い値は低いサービス品質を表します。
- **MOS（Mean Opinion Scores）**－ICPIF を使用して得られた 1～5 の MOS の値です。高い値は高いサービス品質を表します。

音声品質の評価は、ユーザの音声品質の許容度に依存します。音声品質に高い許容度を持つユーザの場合、アドバンテージファクタの設定を行う **advantage-factor** コマンドを使用します。システムが ICPIF 値を計算する場合、音声品質の評価用に ICPIF と MOS の値を修正するため、アドバンテージファクタが取りはずされます。

音声テストは、NQA サーバと NQA クライアントの両方が必要です。音声テストを実行する前に、NQA サーバで UDP リスニングサービスの設定を行う必要があります。UDP リスニングサービスの詳細は、コマンドマニュアルのセクション 11 *システム管理* "*NQA*"の "*NQA サーバの設定*"を参照してください。

1 回の音声テストで 1 回のテストが行われます。

以下に音声テストの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. NQA テストを作成し、NQA operation view に移行する	**nqa entry** *admin-name operation-tag*	デフォルト：設定なし
3. 音声タイプを指定し、その view に移行する	**type voice**	―
4. 音声パケットの宛先アドレスを指定する	**destination ip** *ip-address*	デフォルト：設定なし 宛先アドレスは、NQAサーバでリスニングサービスが設定されたIPアドレスと同一でなくてはいけません。
5. 音声パケットの宛先ポートを指定する	**destination port** *port-number*	デフォルト：設定なし 宛先ポートはNQAサーバでリスニングサービスを行っているポートです。
6. （オプション設定項目）コーデックタイプを指定する	**codec-type** { **g711a** | **g711u** | **g729a** }	デフォルト：G.711 A-law
7. （オプション設定項目）計算される MOS と ICPIF 値のアドバンテージファクタを設定する	**advantage-factor** *factor*	デフォルト：0
8. （オプション設定項目）音声パケットの送信元 IP アドレスを指定する	**source ip** *ip-address*	デフォルト：ICMPエコー要求パケットは送信元IPアドレスとして送信インタフェースのプライマリIPアドレスを使用します。 送信元IPアドレスはローカルインタフェースのIPアドレスにする必要があります。またローカルインタフェースはアップ状態にする必要があります。そうでない場合、音声パケットは送信できません。
9. （オプション設定項目）音声パケットの送信元ポート番号を指定する	**source port** *port-number*	デフォルト：設定なし

操作	コマンド	補足
10.（オプション設定項目）音声パケットのペイロードサイズを指定する	**data-size** *size*	デフォルト: コーデックタイプによって異なります。G.711A-law、G.711 μ-lawは172バイト、G.729 A-lawは32バイトです。
11.（オプション設定項目）各 UDP パケットのペイロードで使われる文字列を指定する	**data-fill** *string*	デフォルト：00010203040506070809（16進数表示）
12.（オプション設定項目）音声テストで送信する UDP パケット数を指定する	**probe packet-number** *packet-number*	デフォルト：1000
13.（オプション設定項目）音声パケットを送信する間隔を設定する	**probe packet-interval** *interval*	デフォルト：20ミリ秒
14.（オプション設定項目）NQA クライアントの音声パケットの受信待ち時間を指定する	**probe packet-timeout** *timeout*	デフォルト：5000ミリ秒

🕮 **メモ：**

display nqa result コマンドあるいは **display nqa statistics** コマンドを使用して音声テストを確認してください。**display nqa history** コマンドは、音声テストの結果や統計情報を表示しません。

2.5.12 DLSw テストの設定

DLSw テストは DLSw 装置の応答時間を測定します。

以下に DLSw テストの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. NQA テストを作成し、NQA operation view に移行する	**nqa entry** *admin-name operation-tag*	デフォルト：設定なし
3. DLSw タイプを指定し、その view に移行する	**type dlsw**	—
4. プローブパケットの宛先 IP アドレスを指定する	**destination ip** *ip-address*	デフォルト：設定なし

操作	コマンド	補足
5.　（オプション設定項目）プローブパケットの送信元 IP アドレスを指定する	**source ip** *ip-address*	デフォルト : ICMPエコー要求パケットは送信元IPアドレスとして送信インタフェースのプライマリIPアドレスを使用します。 送信元IPアドレスはローカルインタフェースのIPアドレスにする必要があります。またローカルインタフェースはアップ状態にする必要があります。そうでない場合、プローブパケットは送信できません。

2.5.13 NQA テストのオプションパラメータの設定

テストグループを指定しない場合、パラメータはすべてのテストタイプに適用されます。

NQA テストのオプションパラメータは 1 回のテストのみ有効です。

パス品質分析操作は、**description** コマンドと **tos** コマンドのみをサポートします。

以下に NQA テストのオプションパラメータの設定を示します。

操作	コマンド	補足
1.　system view に移行する	**system-view**	ー
2.　NQA テストを作成し、NQA operation view に移行する	**nqa entry** *admin-name operation-tag*	デフォルト：設定なし
3.　説明を設定する	**description** *text*	デフォルト：設定なし
4.　NQA テストを連続して行う間隔を指定する	**frequency** *interval*	デフォルト： 音声テストは60000ミリ秒、他のテストは0msです。 1回のテストで1回のテストが実行されます。 間隔が終了したとき、テストが完了していない場合、次のテストは開始しません。
5.　1 回の NQA テストの検査回数を指定する	**probe count** *times*	デフォルト：1回 音声テストでは無効です。1回のテストで1回のテストが実行されます。
6.　NQA テストのタイムアウト時間を指定する	**probe timeout** *timeout*	デフォルト：3000ms UDPジッタテストと音声テストでは無効です。
7.　テストパケットの TTL を指定する	**ttl** *value*	デフォルト：20 DHCPテストでは無効です。
8.　NQA テストパケットの IP パケットヘッダの ToS 値を設定する	**tos** *value*	デフォルト：0

操作	コマンド	補足
9. ルーティングテーブルバイパス機能を有効にする	**route-option bypass-route**	デフォルト：無効 DHCPテストでは無効です。
10. VPN インスタンスが実行される場所を指定する	**vpn-instance** *vpn-instance-name*	デフォルト：パブリックネットワークで実行されます。

2.5.14 しきい値監視機能の設定

I. しきい値タイプ

NQA テストは以下のしきい値タイプをサポートします。

- **平均** – モニタリングされた性能の平均値が、上限あるいは下限を超えた場合、しきい値違反が発生します。
- **合計** – テストのモニタデータがしきい値を違反した回数の合計を監視します。回数の合計数が特定の値に達するか超えた場合、しきい値違反が発生します。
- **連続** – テストグループを開始してからのモニタデータのしきい値違反の連続回数を監視します。モニタデータのしきい値違反の連続回数が特定の回数になった場合、しきい値違反が発生します。

平均、合計のしきい値タイプは NQA テストごとにカウントされますが、連続タイプはテストグループが開始されてからの時間となります。

II. トリガー動作

以下のアクションがトリガー動作となります。

- **none** – NQA は端末画面にのみ結果を表示します。NMS にトラップを送信しません。
- **trap-only** – NQA は端末画面に結果を表示します。NMS にトラップを送信します。
- **trigger-only** – NQA は端末画面に結果を表示します。コラボレーションに関連づけられたほかのモジュールにトラップを送信します。

QXシリーズはトリガー動作 **trigger-only** をサポートしていません。

III. リアクションエントリ

リアクションエントリでは、しきい値監視を行うため、監視対象、しきい値タイプ、トリガー動作を実装します。

リアクションエントリの状態には、無効、しきい値超過、しきい値未満があります。

- NQA のテストグループが開始する前は、リアクションエントリは無効の状態です。
- しきい値が違反している場合、エントリの状態はしきい値超過に設定されます。それ以外の場合、エントリの状態はしきい値未満に設定されています。

IV. 設定手順

しきい値監視の設定を行う前に、**snmp-agent target-host** コマンドを使用してトラップメッセージの宛先アドレスを設定してください。このコマンドの詳細は、コマンドマニュアルのセクション 11 *システム管理* "*SNMP*"を参照してください。

以下にしきい値監視機能の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. NQA テストを作成し、NQA operation view に移行する	**nqa entry** *admin-name operation-tag*	デフォルト：設定なし
3. NQA operation view に移行する	**type** { **dhcp** | **dlsw** | **dns** | **ftp** | **http** | **icmp-echo** | **snmp** | **tcp** | **udp-echo** | **udp-jitter** | **voice** }	―
4. 指定状況下になったときネットワーク管理サーバにトラップを送信する	**reaction trap** { **probe-failure** *consecutive-probe-failures* | **test-complete** | **test-failure** [*accumulate-probe-failures*] }	デフォルト：設定なし UDPジッタテストと音声テストは**test-complete**キーワードのみサポートしています。
5. しきい値監視機能を設定する	● 故障回数を監視する（UDPジッタテストと音声テストは未サポート）：**reaction** *item-number* **checked-element probe-fail threshold-type** { **accumulate** *accumulate-occurrences* | **consecutive** *consecutive-occurrences* } [**action-type none**]	―

2.5.15 NQA 統計情報収集機能の設定

NQA は統計情報グループとして同一の収集間隔で統計情報を収集します。統計情報グループについて情報を表示するには、**display nqa statistics** コマンドを使用します。

NQA は、1 回のみの NQA テストの統計情報グループを作成しません。**frequency** コマンドを使用し、テスト間隔を 0 に設定した場合、NQA は統計情報グループを作成しません。

以下に NQA 統計情報収集機能の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. NQA テストを作成し、NQA operation view に移行する	**nqa entry** *admin-name operation-tag*	デフォルト：設定なし
3. NQA テストタイプを指定し、その view に移行する	**type** { **dhcp** | **dlsw** | **dns** | **ftp** | **http** | **icmp-echo** | **snmp** | **tcp** | **udp-echo** | **udp-jitter** | **voice** }	―
4. （オプション設定項目）統計情報を収集する間隔を指定する	**statistics interval** *interval*	デフォルト：60分

操作	コマンド	補足
5.　（オプション設定項目）保持する統計情報グループ数の最大値を設定する	**statistics max-group** *number*	デフォルト：2グループ 最大値を0に設定すると統計情報を収集しません。 統計グループが最大数となったとき、新しい統計情報グループを保存するため、一番古い統計情報グループが削除されます。
6.　（オプション設定項目）統計情報グループの保持時間を指定する	**statistics hold-time** *hold-time*	デフォルト：120分 保持時間が終了したとき、統計グループは削除されます。

2.5.16 NQA 履歴記録保存の設定

操作	コマンド	補足
1.　system view に移行する	**system-view**	ー
2.　NQA テストを作成し、NQA operation view に移行する	**nqa entry** *admin-name operation-tag*	デフォルト：設定なし
3.　NQA operation type view に移行する	**type** { **dhcp** | **dlsw** | **dns** | **ftp** | **http** | **icmp-echo** | **snmp** | **tcp** | **udp-echo** }	UDPジッタテストと音声テストは無効です。
4.　NQA テストの履歴記録の保存を有効にする	**history-record enable**	デフォルト：無効
5.　（オプション設定項目）履歴記録の保存期間を設定する	**history-record keep-time** *keep-time*	デフォルト：120分 保存期間が満了したとき記録が削除されます。
6.　（オプション設定項目）履歴記録を保存できる最大数を指定する	**history-record number** *number*	デフォルト：50 もし最大数を超過した場合、一番古い履歴が削除されます。
7.　（オプション設定項目）履歴記録を表示する	**display nqa history**	ー

2.5.17 NQA クライアントにおける NQA テストのスケジューリング

指定した開始時間と終了時間（開始時間＋テスト間隔）を設定することにより、NQA テストグループをスケジューリングできます。指定した開始時間がシステム時間を過ぎていた場合、NQA テストは即座に開始します。開始時間と終了時間が共にシステム時間を過ぎていた場合、NQA テストは行われません。**display clock** コマンドにより現在のシステム時間を確認することができます。

以下に NQA テストのスケジューリングを設定するときの制限とガイドラインを示します。

- NQA operation view あるいはスケジュールされた NQA テストの view に移行することはできません。
- システム時間を調整しても、開始されたあるいは終了した NQA テストには影響しません。開始する前の NQA テストはシステム時間の調整のみが適用されます。

以下に NQA クライアントにおける NQA テストをスケジューリングする設定を示します。

操作	コマンド
1. system view に移行する	**system-view**
2. NQA テストのスケジューリングのパラメータを指定する	**nqa schedule** *admin-name operation-tag* **start-time** { *hh:mm:ss* [*yyyy/mm/dd* | *mm/dd/yyyy*] | **now** } **lifetime** { *lifetime* | **forever** } [**recurring**]

2.6 NQAの表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
NQAテストの履歴記録を表示する	**display nqa history** [*admin-name operation-tag*]
NQAテストの最新の結果を表示する	**display nqa result** [*admin-name operation-tag*]
NQAテストの統計情報を表示する	**display nqa statistics** [*admin-name operation-tag*]
NQAサーバ状態を表示する	**display nqa server**

2.7 NQA設定例

2.7.1 ICMP エコーテスト設定例

I. ネットワーク要件

図 2-2に示すように、Device A から Device C を通して Device B へのラウンドトリップ時間をテストするため、NQA クライアントから ICMP エコーテストを設定します。Device A のネクストホップは Device C です。

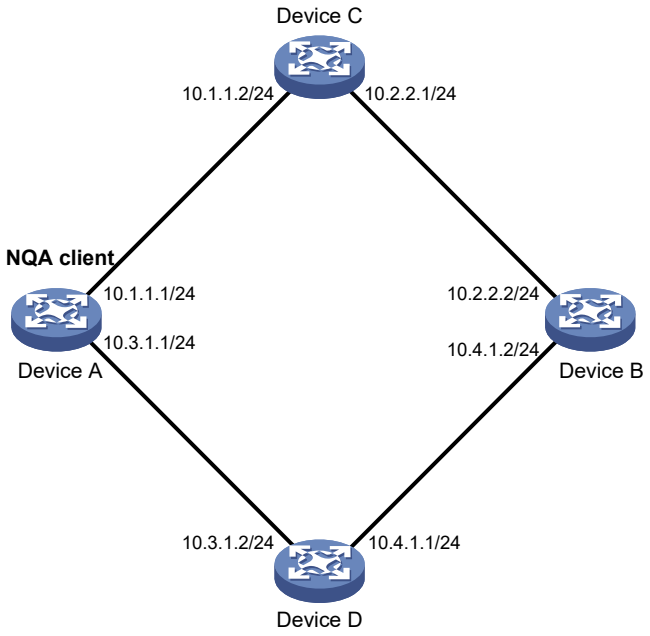


図 2-2 ネットワーク図

II. 設定手順

各インタフェースに IP アドレスを割り当てます。（詳細は省略します。）

Device が互いに通信できるようにスタティックルートあるいはルーティングプロトコルを設定します。（詳細は省略します。）

ICMP エコーテストを作成します。

```
<DeviceA> system-view
[DeviceA] nqa entry admin test1
[DeviceA-nqa-admin-test1] type icmp-echo
```

ICMP エコーリクエストの宛先 IP アドレスとして 10.2.2.2 を指定します。

```
[DeviceA-nqa-admin-test1-icmp-echo] destination ip 10.2.2.2
```

ネクストホップとして 10.1.1.2 を設定します。ICMP エコーリクエストは Device C から Device B に送信されます。

```
[DeviceA-nqa-admin-test1-icmp-echo] next-hop ip 10.1.1.2
```

ICMP エコーテストの検査回数を 10 回実行します。

```
[DeviceA-nqa-admin-test1-icmp-echo] probe count 10
```

ICMP エコーテストのタイムアウト時間を 500ms に指定します。

```
[DeviceA-nqa-admin-test1-icmp-echo] probe timeout 500
```

NQA テストを連続して行う間隔を 5000ms に設定します。

```
[DeviceA-nqa-admin-test1-icmp-echo] frequency 5000
```

NQA 履歴記録の保存を有効にします。

```
[DeviceA-nqa-admin-test1-icmp-echo] history-record enable
```

NQA 履歴記録の保存できる最大数を 10 に設定します。

```
[DeviceA-nqa-admin-test1-icmp-echo] history-record number 10
[DeviceA-nqa-admin-test1-icmp-echo] quit
```

ICMP エコーテストを開始します。

```
[DeviceA] nqa schedule admin test1 start-time now lifetime forever
```

ICMP エコーテスト開始から一定の時間が経過した後、テストを停止します。

```
[DeviceA] undo nqa schedule admin test1
```

ICMP エコーテストの最新の結果を表示します。

```
[DeviceA] display nqa result admin test1
NQA entry (admin admin, tag test1) test results:
    Send operation times: 10              Receive response times: 10
    Min/Max/Average round trip time: 2/5/3
    Square-Sum of round trip time: 96
    Last succeeded probe time: 2011-08-23 15:00:01.2
  Extended results:
    Packet loss ratio: 0%
    Failures due to timeout: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
```

ICMP エコーテストの履歴記録を表示します。

```
[DeviceA] display nqa history admin test1
NQA entry (admin admin, tag test) history records:
  Index      Response     Status           Time
  370        3            Succeeded        2007-08-23 15:00:01.2
  369        3            Succeeded        2007-08-23 15:00:01.2
  368        3            Succeeded        2007-08-23 15:00:01.2
  367        5            Succeeded        2007-08-23 15:00:01.2
  366        3            Succeeded        2007-08-23 15:00:01.2
  365        3            Succeeded        2007-08-23 15:00:01.2
  364        3            Succeeded        2007-08-23 15:00:01.1
  363        2            Succeeded        2007-08-23 15:00:01.1
  362        3            Succeeded        2007-08-23 15:00:01.1
  361        2            Succeeded        2007-08-23 15:00:01.1
```

出力では、Device A からのパケットが Device C を通して Device B に送信できることを示しています。NQA テスト中のパケットロスはありません。最小、最大、平均ラウンドトリップ時間はそれぞれ、2、5、3ms です。

2.7.2 DHCP テスト設定例

I. ネットワーク要件

図 2-3に示すように、Switch A が DHCP サーバ（Switch B）から IP アドレスを取得する時間をテストするため DHCP テストを設定します。

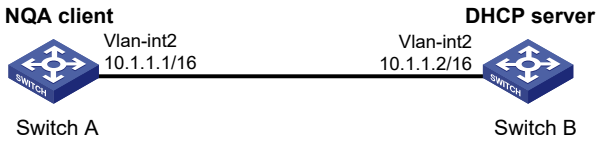


図 2-3 ネットワーク図

II. 設定手順

DHCP テストを作成します。

```
<SwitchA> system-view
[SwitchA] nqa entry admin test1
[SwitchA-nqa-admin-test1] type dhcp
```

宛先アドレスとして DHCP サーバの IP アドレス 10.1.1.2 を指定します。

```
[SwitchA-nqa-admin-test1-dhcp] destination ip 10.1.1.2
```

履歴記録を保存するように設定します。

```
[SwitchA-nqa-admin-test1-dhcp] history-record enable
[SwitchA-nqa-admin-test1-dhcp] quit
```

DHCP テストを開始します。

```
[SwitchA] nqa schedule admin test1 start-time now lifetime forever
```

DHCP テストを一定の期間実行したのち、テストを停止します。

```
[SwitchA] undo nqa schedule admin test1
```

DHCP テストの最新の結果を表示します。

```
[SwitchA] display nqa result admin test1
NQA entry (admin admin, tag test1) test results:
    Send operation times: 1              Receive response times: 1
    Min/Max/Average round trip time: 512/512/512
    Square-Sum of round trip time: 262144
    Last succeeded probe time: 2011-11-22 09:56:03.2
  Extended results:
    Packet loss ratio: 0%
    Failures due to timeout: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
```

DHCP テストの履歴記録を表示します。

```
[SwitchA] display nqa history admin test1
NQA entry (admin admin, tag test1) history records:
  Index      Response     Status           Time
  1          512          Succeeded        2011-11-22 09:56:03.2
```

出力では、Switch A が DHCP サーバから IP アドレスを取得するのに 512 ミリ秒かかることを示します。

2.7.3 DNS テスト設定例

I. ネットワーク要件

図 2-4に示すように、Device A が DHCP サーバから IP アドレスを取得するため DNS 解決時間の測定を行う DNS テストを設定します。



図 2-4 ネットワーク図

II. 設定手順

各インタフェースに IP アドレスを割り当てます。（詳細は省略します。）

Device が互いに通信できるようにスタティックルートあるいはルーティングプロトコルを設定します。（詳細は省略します。）

DNS テストを作成します。

```
<DeviceA> system-view
[DeviceA] nqa entry admin test1
[DeviceA-nqa-admin-test1] type dns
```

宛先アドレスとして DNS サーバの IP アドレス 10.2.2.2 を指定します。

```
[DeviceA-nqa-admin-test1-dns] destination ip 10.2.2.2
```

host.com のドメイン名に変換されるように指定します。

```
[DeviceA-nqa-admin-test1-dns] resolve-target host.com
```

履歴記録を保存するように設定します。

```
[DeviceA-nqa-admin-test1-dns] history-record enable
[DeviceA-nqa-admin-test1-dns] quit
```

DNS テストを開始します。

```
[DeviceA] nqa schedule admin test1 start-time now lifetime forever
```

DNS テストを一定の期間実行したのち、テストを停止します。

```
[DeviceA] undo nqa schedule admin test1
```

DNS テストの最新の結果を表示します。

```
[DeviceA] display nqa result admin test1
NQA entry (admin admin, tag test1) test results:
    Send operation times: 1              Receive response times: 1
    Min/Max/Average round trip time: 62/62/62
```

```
    Square-Sum of round trip time: 3844
    Last succeeded probe time: 2011-11-10 10:49:37.3
  Extended results:
    Packet loss ratio: 0%
    Failures due to timeout: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
```

DNS テストの履歴記録を表示します。

```
[DeviceA] display nqa history admin test1
NQA entry (admin admin, tag test) history records:
  Index      Response     Status           Time
  1          62           Succeeded        2011-11-10 10:49:37.3
```

出力では、Device A がドメイン名 host.com を IP アドレスに変換するのに 62 ミリ秒かかることを示します。

2.7.4 FTP テスト設定例

I. ネットワーク要件

図 2-5に示すように、Device A が FTP サーバにファイルをアップロードする時間を測定するために FTP テストを設定します。ログインユーザ名は admin、ログインパスワードは systemtest、FTP サーバに転送されるファイルは config.txt とします。



図 2-5 ネットワーク図

II. 設定手順

各インタフェースに IP アドレスを割り当てます。（詳細は省略します。）

Device が互いに通信できるようにスタティックルートあるいはルーティングプロトコルを設定します。（詳細は省略します。）

FTP テストを作成します。

```
<DeviceA> system-view
[DeviceA] nqa entry admin test1
[DeviceA-nqa-admin-test1] type ftp
```

FTP サーバの URL を指定します。

```
[DeviceA-nqa-admin-test-ftp] url ftp://10.2.2.2
```

送信元 IP アドレス 10.1.1.1 を指定します。

```
[DeviceA-nqa-admin-test1-ftp] source ip 10.1.1.1
```

Device が FTP サーバにファイル config.txt をアップロードするように設定します。

```
[DeviceA-nqa-admin-test1-ftp] operation put
[DeviceA-nqa-admin-test1-ftp] filename config.txt
```

FTP テストのユーザ名 admin を指定します。

```
[DeviceA-nqa-admin-test1-ftp] username admin
```

FTP テストのパスワード systemtest を指定します。

```
[DeviceA-nqa-admin-test1-ftp] password simple systemtest
```

履歴記録を保存するように設定します。

```
[DeviceA-nqa-admin-test1-ftp] history-record enable
[DeviceA-nqa-admin-test1-ftp] quit
```

FTP テストを開始します。

```
[DeviceA] nqa schedule admin test1 start-time now lifetime forever
```

FTP テストを一定期間実行したのち、テストを停止します。

```
[DeviceA] undo nqa schedule admin test1
```

FTP テストの最新の結果を表示します。

```
[DeviceA] display nqa result admin test1
NQA entry (admin admin, tag test1) test results:
    Send operation times: 1              Receive response times: 1
    Min/Max/Average round trip time: 173/173/173
    Square-Sum of round trip time: 29929
    Last succeeded probe time: 2011-11-22 10:07:28.6
  Extended results:
    Packet loss ratio: 0%
    Failures due to timeout: 0
    Failures due to disconnect: 0
    Failures due to no connection: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
```

FTP テストの履歴記録を表示します。

```
[DeviceA] display nqa history admin test1
NQA entry (admin admin, tag test1) history records:
  Index      Response     Status           Time
  1          173          Succeeded        2011-11-22 10:07:28.6
```

出力では、Device A が FTP サーバにファイルをアップロードするのに 173 ミリ秒かかることを示しています。

2.7.5 HTTP テスト設定例

I. ネットワーク要件

図 2-6に示すように HTTP サーバからデータを取得する時間をテストするため、NQA クライアントに HTTP テストを設定します。



図 2-6 ネットワーク図

II. 設定手順

各インタフェースに IP アドレスを割り当てます。（詳細は省略します。）

Device が互いに通信できるようにスタティックルートあるいはルーティングプロトコルを設定します。（詳細は省略します。）

HTTP テストを作成します。

```
<DeviceA> system-view
[DeviceA] nqa entry admin test1
[DeviceA-nqa-admin-test1] type http
```

HTTP サーバの URL を指定します。

```
[DeviceA-nqa-admin-test-http] url http://10.2.2.2/index.htm
```

HTTP サーバからデータを取得するように HTTP テストを設定します。

```
[DeviceA-nqa-admin-test1-http] operation get
```

HTTP version 1.0 を使用するように設定します。

```
[DeviceA-nqa-admin-test1-http] version v1.0
```

履歴記録を保存するように設定します。

```
[DeviceA-nqa-admin-test1-http] history-record enable
[DeviceA-nqa-admin-test1-http] quit
```

HTTP テストを開始します。

```
[DeviceA] nqa schedule admin test1 start-time now lifetime forever
```

HTTP テストを一定期間実行したのち、テストを停止します。

```
[DeviceA] undo nqa schedule admin test1
```

HTTP テストの最新の結果を表示します。

```
[DeviceA] display nqa result admin test1
NQA entry (admin admin, tag test1) test results:
    Send operation times: 1              Receive response times: 1
    Min/Max/Average round trip time: 64/64/64
    Square-Sum of round trip time: 4096
    Last succeeded probe time: 2011-11-22 10:12:47.9
  Extended results:
    Packet loss ratio: 0%
    Failures due to timeout: 0
    Failures due to disconnect: 0
```

```
    Failures due to no connection: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
```

HTTP テストの履歴記録を表示します。

```
[DeviceA] display nqa history admin test1
NQA entry (admin admin, tag test1) history records:
  Index      Response     Status           Time
  1          64           Succeeded        2011-11-22 10:12:47.9
```

出力では、Device A が HTTP サーバからデータを取得するのに 64 ミリ秒かかることを示します。

2.7.6 UDP ジッタテスト設定例

I. ネットワーク要件

図 2-7に示すように、Device A と Device B 間のジッタ、遅延、ラウンドトリップ時間を測定するため、UDP ジッタテストを設定します。



図 2-7 ネットワーク図

II. 設定手順

1) 各インタフェースに IP アドレスを割り当てます。（詳細は省略します。）
2) 各装置間で通信可能になるように、スタティックルートあるいはルーティングテーブルを設定します。（詳細は省略します。）
3) Device B を設定します。

NQA サーバを有効にします。

```
<DeviceB> system-view
[DeviceB] nqa server enable
```

IP アドレス 10.2.2.2、UDP ポート 9000 でリスニングサービスを設定します。

```
[DeviceB] nqa server udp-echo 10.2.2.2 9000
```

4) Device A を設定します。

UDP ジッタテストを作成します。

```
<DeviceA> system-view
[DeviceA] nqa entry admin test1
[DeviceA-nqa-admin-test1] type udp-jitter
```

UDP ジッタテストの宛先 IP アドレス 10.2.2.2 を設定します。

```
[DeviceA-nqa-admin-test1-udp-jitter] destination ip 10.2.2.2
```

宛先ポート 9000 を設定します。

```
[DeviceA-nqa-admin-test1-udp-jitter] destination port 9000
```

1000 ミリ秒の間隔で UDP ジッタテストを繰り返すように設定します。

```
[DeviceA-nqa-admin-test1-udp-jitter] frequency 1000
[DeviceA-nqa-admin-test1-udp-jitter] quit
```

UDP ジッタテストを開始します。

```
[DeviceA] nqa schedule admin test1 start-time now lifetime forever
```

UDP ジッタテストを一定期間実行したのち、テストを停止します。

```
[DeviceA] undo nqa schedule admin test1
```

UDP ジッタテストの最新の結果を表示します。

```
[DeviceA] display nqa result admin test1
NQA entry (admin admin, tag test1) test results:
    Send operation times: 10              Receive response times: 10
    Min/Max/Average round trip time: 15/32/17
    Square-Sum of round trip time: 3235
    Last packet received time: 2011-05-29 13:56:17.6
  Extended results:
    Packet loss ratio: 0%
    Failures due to timeout: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
    Packets out of sequence: 0
    Packets arrived late: 0
  UDP-jitter results:
   RTT number: 10
    Min positive SD: 4                    Min positive DS: 1
    Max positive SD: 21                   Max positive DS: 28
    Positive SD number: 5                 Positive DS number: 4
    Positive SD sum: 52                   Positive DS sum: 38
    Positive SD average: 10               Positive DS average: 10
    Positive SD square-sum: 754           Positive DS square-sum: 460
    Min negative SD: 1                    Min negative DS: 6
    Max negative SD: 13                   Max negative DS: 22
    Negative SD number: 4                 Negative DS number: 5
    Negative SD sum: 38                   Negative DS sum: 52
    Negative SD average: 10               Negative DS average: 10
    Negative SD square-sum: 460           Negative DS square-sum: 754
  One way results:
    Max SD delay: 15                      Max DS delay: 16
    Min SD delay: 7                       Min DS delay: 7
    Number of SD delay: 10                Number of DS delay: 10
    Sum of SD delay: 78                   Sum of DS delay: 85
    Square-Sum of SD delay: 666           Square-Sum of DS delay: 787
    SD lost packets: 0                   DS lost packets: 0
    Lost packets for unknown reason: 0
```

UDP ジッタテストの履歴記録を表示します。

```
[DeviceA] display nqa statistics admin test1
NQA entry (admin admin, tag test1) test statistics:
  NO. : 1
    Start time: 2011-05-29 13:56:14.0
    Life time: 47 seconds
    Send operation times: 410             Receive response times: 410
    Min/Max/Average round trip time: 1/93/19
```

```
    Square-Sum of round trip time: 206176
  Extended results:
    Packet loss ratio: 0%
    Failures due to timeout: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
    Packets out of sequence: 0
    Packets arrived late: 0
  UDP-jitter results:
   RTT number: 410
    Min positive SD: 3                    Min positive DS: 1
    Max positive SD: 30                   Max positive DS: 79
    Positive SD number: 186               Positive DS number: 158
    Positive SD sum: 2602                 Positive DS sum: 1928
    Positive SD average: 13               Positive DS average: 12
    Positive SD square-sum: 45304         Positive DS square-sum: 31682
    Min negative SD: 1                    Min negative DS: 1
    Max negative SD: 30                   Max negative DS: 78
    Negative SD number: 181               Negative DS number: 209
    Negative SD sum: 181                  Negative DS sum: 209
    Negative SD average: 13               Negative DS average: 14
    Negative SD square-sum: 46994         Negative DS square-sum: 3030
  One way results:
    Max SD delay: 46                      Max DS delay: 46
    Min SD delay: 7                       Min DS delay: 7
    Number of SD delay: 410               Number of DS delay: 410
    Sum of SD delay: 3705                 Sum of DS delay: 3891
    Square-Sum of SD delay: 45987         Square-Sum of DS delay: 49393
    SD lost packets: 0                  DS lost packets: 0
    Lost packets for unknown reason: 0
```

2.7.7 SNMP テスト設定例

I. ネットワーク要件

図 2-8に示すように、NQA クライアントが SNMP エージェントから応答を取得する時間を測定するため、SNMP テストを設定します。



図 2-8 ネットワーク図

II. 設定手順

1) 各インタフェースに IP アドレスを割り当てます。（詳細は省略します。）
2) 各装置間で通信可能になるように、スタティックルートあるいはルーティングテーブルを設定します。（詳細は省略します。）
3) SNMP エージェント（Device B）を設定します。

SNMP のバージョンを all に設定します。

```
<DeviceB> system-view
[DeviceB] snmp-agent sys-info version all
```

read コミュニティを public に設定します。

```
[DeviceB] snmp-agent community read public
```

write コミュニティを private に設定します。

```
[DeviceB] snmp-agent community write private
```

4)　Device A を設定します。

SNMP テストを作成します。

```
<DeviceA> system-view
[DeviceA] nqa entry admin test1
[DeviceA-nqa-admin-test1] type snmp
```

SNMP テストの宛先 IP アドレスを 10.2.2.2 に設定します。

```
[DeviceA-nqa-admin-test1-snmp] destination ip 10.2.2.2
```

履歴記録を保存するように設定します。

```
[DeviceA-nqa-admin-test1-snmp] history-record enable
[DeviceA-nqa-admin-test1-snmp] quit
```

SNMP テストを開始します。

```
[DeviceA] nqa schedule admin test1 start-time now lifetime forever
```

SNMP テストを一定期間実行したのち、テストを停止します。

```
[DeviceA] undo nqa schedule admin test1
```

SNMP テストの最新の結果を表示します。

```
[DeviceA] display nqa result admin test1
NQA entry (admin admin, tag test1) test results:
    Send operation times: 1              Receive response times: 1
    Min/Max/Average round trip time: 50/50/50
    Square-Sum of round trip time: 2500
    Last succeeded probe time: 2011-11-22 10:24:41.1
  Extended results:
    Packet loss ratio: 0%
    Failures due to timeout: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
```

SNMP テストの履歴記録を表示します。

```
[DeviceA] display nqa history admin test1
NQA entry (admin admin, tag test1) history records:
  Index      Response     Status           Time
  1          50           Succeeded        2011-11-22 10:24:41.1
```

出力では、Device A が SNMP エージェントから応答を受信するのに 50 ミリ秒かかることを示します。

2.7.8 TCP テスト設定例

I. ネットワーク要件

図 2-9に示すように、NQA クライアントが Device B の NQA サーバに TCP 接続を確立するまでの時間を測定するために TCP テストを設定します。



図 2-9 ネットワーク図

II. 設定手順

1) 各インタフェースに IP アドレスを割り当てます。（詳細は省略します。）
2) 各装置間で通信可能になるように、スタティックルートあるいはルーティングテーブルを設定します。（詳細は省略します。）
3) Device B を設定します。

NQA サーバを有効にします。

```
<DeviceB> system-view
[DeviceB] nqa server enable
```

IP アドレス 10.2.2.2、TCP ポート 9000 でリスニングサービスを設定します。

```
[DeviceB] nqa server tcp-connect 10.2.2.2 9000
```

4) Device A を設定します。

TCP テストを作成します。

```
<DeviceA> system-view
[DeviceA] nqa entry admin test1
[DeviceA-nqa-admin-test1] type tcp
```

宛先 IP アドレスを 10.2.2.2 に設定します。

```
[DeviceA-nqa-admin-test1-tcp] destination ip 10.2.2.2
```

宛先ポート番号を 9000 に設定します。

```
[DeviceA-nqa-admin-test1-tcp] destination port 9000
```

履歴記録を保存するように設定します。

```
[DeviceA-nqa-admin-test1-tcp] history-record enable
[DeviceA-nqa-admin-test1-tcp] quit
```

TCP テストを開始します。

```
[DeviceA] nqa schedule admin test1 start-time now lifetime forever
```

TCP テストを一定期間実行したのち、テストを停止します。

```
[DeviceA] undo nqa schedule admin test1
```

TCP テストの最新の結果を表示します。

```
[DeviceA] display nqa result admin test1
NQA entry (admin admin, tag test1) test results:
    Send operation times: 1              Receive response times: 1
    Min/Max/Average round trip time: 13/13/13
    Square-Sum of round trip time: 169
    Last succeeded probe time: 2011-11-22 10:27:25.1
  Extended results:
    Packet loss ratio: 0%
    Failures due to timeout: 0
    Failures due to disconnect: 0
    Failures due to no connection: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
```

TCP テストの履歴記録を表示します。

```
[DeviceA] display nqa history admin test1
NQA entry (admin admin, tag test1) history records:
  Index      Response     Status           Time
  1          13           Succeeded        2011-11-22 10:27:25.1
```

出力では、Device A が NQA サーバのポート 9000 と TCP 接続を確立するのに 13 ミリ秒かかることを示します。

2.7.9 UDP エコーテスト設定例

I. ネットワーク要件

図 2-10に示すように、Device A と Device B 間のラウンドトリップ時間をテストするように、UDP エコーテストを設定します。宛先ポート番号は 8000 番です。



図 2-10 ネットワーク図

II. 設定手順

1) 各インタフェースに IP アドレスを割り当てます。（詳細は省略します。）
2) Device が互いに通信できるようにスタティックルートあるいはルーティングプロトコルを設定します。（詳細は省略します。）
3) Device B を設定します。

NQA サーバを有効にします。

```
<DeviceB> system-view
[DeviceB] nqa server enable
```

IP アドレス 10.2.2.2、UDP ポート 8000 をリスニングするように設定します。

```
[DeviceB] nqa server udp-echo 10.2.2.2 8000
```

4)　Device A を設定します。

UDP エコーテストを作成します。

```
<DeviceA> system-view
[DeviceA] nqa entry admin test1
[DeviceA-nqa-admin-test1] type udp-echo
```

宛先 IP アドレスを 10.2.2.2 に設定します。

```
[DeviceA-nqa-admin-test1-udp-echo] destination ip 10.2.2.2
```

宛先ポート番号を 8000 に設定します。

```
[DeviceA-nqa-admin-test1-udp-echo] destination port 8000
```

履歴記録を保存するように設定します。

```
[DeviceA-nqa-admin-test1-udp-echo] history-record enable
[DeviceA-nqa-admin-test1-udp-echo] quit
```

UDP エコーテストを開始します。

```
[DeviceA] nqa schedule admin test1 start-time now lifetime forever
```

UDP エコーテストを一定期間実行したのち、テストを停止します。

```
[DeviceA] undo nqa schedule admin test1
```

UDP エコーテストの最新の結果を表示します。

```
[DeviceA] display nqa result admin test1
NQA entry (admin admin, tag test1) test results:
    Send operation times: 1              Receive response times: 1
    Min/Max/Average round trip time: 25/25/25
    Square-Sum of round trip time: 625
    Last succeeded probe time: 2011-11-22 10:36:17.9
  Extended results:
    Packet loss ratio: 0%
    Failures due to timeout: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
```

UDP エコーテストの履歴記録を表示します。

```
[DeviceA] display nqa history admin test1
NQA entry (admin admin, tag test1) history records:
  Index      Response     Status           Time
  1          25           Succeeded        2011-11-22 10:36:17.9
```

出力は、Device A と Device B のポート 8000 番の間のラウンドトリップ時間が 25ms であることを示します。

2.7.10 音声テスト設定例

I. ネットワーク要件

図 2-11に示すように、Device A と Device B 間のジッタ、遅延、MOS、ICPIF をテストするため音声テストを設定します。



図 2-11 ネットワーク図

II. 設定手順

1) 各インタフェースに IP アドレスを割り当てます。（詳細は省略します。）
2) 各装置間で通信可能になるように、スタティックルートあるいはルーティングテーブルを設定します。（詳細は省略します。）
3) Device B を設定します。

NQA サーバを有効にします。

```
<DeviceB> system-view
[DeviceB] nqa server enable
```

IP アドレス 10.2.2.2、UDP ポート 9000 でリスニングサービスを設定します。

```
[DeviceB] nqa server udp-echo 10.2.2.2 9000
```

4) Device A を設定します。

音声テストを作成します。

```
<DeviceA> system-view
[DeviceA] nqa entry admin test1
[DeviceA-nqa-admin-test1] type voice
```

宛先 IP アドレスを 10.2.2.2 に設定します。

```
[DeviceA-nqa-admin-test1-voice] destination ip 10.2.2.2
```

宛先ポート番号を 9000 に設定します。

```
[DeviceA-nqa-admin-test1-voice] destination port 9000
[DeviceA-nqa-admin-test1-voice] quit
```

音声テストを開始します。

```
[DeviceA] nqa schedule admin test1 start-time now lifetime forever
```

音声テストを一定期間実行したのち、テストを停止します。

```
[DeviceA] undo nqa schedule admin test1
```

音声テストの最新の結果を表示します。

```
[DeviceA] display nqa result admin test1
NQA entry (admin admin, tag test1) test results:
    Send operation times: 1000           Receive response times: 1000
    Min/Max/Average round trip time: 31/1328/33
    Square-Sum of round trip time: 2844813
    Last packet received time: 2011-06-13 09:49:31.1
  Extended results:
    Packet loss ratio: 0%
    Failures due to timeout: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
Packets out of sequence: 0
    Packets arrived late: 0
  Voice results:
   RTT number: 1000
    Min positive SD: 1                    Min positive DS: 1
    Max positive SD: 204                  Max positive DS: 1297
    Positive SD number: 257               Positive DS number: 259
    Positive SD sum: 759                  Positive DS sum: 1797
    Positive SD average: 2                Positive DS average: 6
    Positive SD square-sum: 54127         Positive DS square-sum: 1691967
    Min negative SD: 1                    Min negative DS: 1
    Max negative SD: 203                  Max negative DS: 1297
    Negative SD number: 255               Negative DS number: 259
    Negative SD sum: 759                  Negative DS sum: 1796
    Negative SD average: 2                Negative DS average: 6
    Negative SD square-sum: 53655         Negative DS square-sum: 1691776
  One way results:
    Max SD delay: 343                     Max DS delay: 985
    Min SD delay: 343                     Min DS delay: 985
    Number of SD delay: 1                 Number of DS delay: 1
    Sum of SD delay: 343                  Sum of DS delay: 985
    Square-Sum of SD delay: 117649        Square-Sum of DS delay: 970225
    SD lost packets: 0                   DS lost packets: 0
    Lost packets for unknown reason: 0
  Voice scores:
    MOS value: 4.38                       ICPIF value: 0
```

音声テストの統計情報を表示します。

```
[DeviceA] display nqa statistics admin test1
NQA entry (admin admin, tag test1) test statistics:
  NO. : 1

    Start time: 2011-06-13 09:45:37.8
    Life time: 331 seconds
    Send operation times: 4000           Receive response times: 4000
    Min/Max/Average round trip time: 15/1328/32
    Square-Sum of round trip time: 7160528
  Extended results:
    Packet loss ratio: 0%
    Failures due to timeout: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
Packets out of sequence: 0
    Packets arrived late: 0
  Voice results:
   RTT number: 4000
    Min positive SD: 1                    Min positive DS: 1
    Max positive SD: 360                  Max positive DS: 1297
    Positive SD number: 1030              Positive DS number: 1024
    Positive SD sum: 4363                 Positive DS sum: 5423
    Positive SD average: 4                Positive DS average: 5
    Positive SD square-sum: 497725        Positive DS square-sum: 2254957
    Min negative SD: 1                    Min negative DS: 1
    Max negative SD: 360                  Max negative DS: 1297
    Negative SD number: 1028              Negative DS number: 1022
```

```
    Negative SD sum: 1028                  Negative DS sum: 1022
    Negative SD average: 4                 Negative DS average: 5
    Negative SD square-sum: 495901         Negative DS square-sum: 5419
  One way results:
    Max SD delay: 359                      Max DS delay: 985
    Min SD delay: 0                        Min DS delay: 0
    Number of SD delay: 4                  Number of DS delay: 4
    Sum of SD delay: 1390                  Sum of DS delay: 1079
    Square-Sum of SD delay: 483202         Square-Sum of DS delay: 973651
    SD lost packets: 0                   DS lost packets: 0
    Lost packets for unknown reason: 0
  Voice scores:
    Max MOS value: 4.38                    Min MOS value: 4.38
    Max ICPIF value: 0                     Min ICPIF value: 0
```

2.7.11 DLSw テスト設定例

I. ネットワーク要件

図 2-12に示すように、DLSw 装置の応答時間を測定するため、DLSw テストを設定します。



図 2-12 ネットワーク図

II. 設定手順

各インタフェースに IP アドレスを割り当てます。（詳細は省略します。）

Device が互いに通信できるようにスタティックルートあるいはルーティングプロトコルを設定します。（詳細は省略します。）

DLSw テストを作成します。

```
<DeviceA> system-view
[DeviceA] nqa entry admin test1
[DeviceA-nqa-admin-test1] type dlsw
```

宛先 IP アドレスを 10.2.2.2 に設定します。

```
[DeviceA-nqa-admin-test1-dlsw] destination ip 10.2.2.2
```

履歴記録を保存するように設定します。

```
[DeviceA-nqa-admin-test1-dlsw] history-record enable
[DeviceA-nqa-admin-test1-dlsw] quit
```

DLSw テストを開始します。

```
[DeviceA] nqa schedule admin test1 start-time now lifetime forever
```

DLSw テストを一定期間実行したのち、テストを停止します。

```
[DeviceA] undo nqa schedule admin test1
```

DLSw テストの最新の結果を表示します。

```
[DeviceA] display nqa result admin test1
NQA entry (admin admin, tag test1) test results:
    Send operation times: 1              Receive response times: 1
    Min/Max/Average round trip time: 19/19/19
    Square-Sum of round trip time: 361
    Last succeeded probe time: 2011-11-22 10:40:27.7
  Extended results:
    Packet loss ratio: 0%
    Failures due to timeout: 0
    Failures due to disconnect: 0
    Failures due to no connection: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
```

DLSw テストの履歴記録を表示します。

```
[DeviceA] display nqa history admin test1
NQA entry (admin admin, tag test1) history records:
  Index      Response     Status           Time
  1          19           Succeeded        2011-11-22 10:40:27.7
```

出力では、DLSw 装置の応答時間が 19 ミリ秒であることを示します。

目次

このセクションのページは **11-x-x** です。

3 章 NTP 3-1
3.1 概要 3-1
3.1.1 NTP の動作 3-1
3.1.2 NTP アーキテクチャ 3-2
3.1.3 運用モード 3-3
3.1.4 NTP セキュリティ 3-5
3.1.5 プロトコルと標準 3-7
3.2 設定の制限とガイドライン 3-7
3.3 設定作業リスト 3-7
3.4 NTP サービスの有効化 3-7
3.5 NTP 運用モードの設定 3-7
3.5.1 NTP クライアント/サーバモードの設定 3-7
3.5.2 NTP シンメトリックアクティブ/パッシブモードの設定 3-8
3.5.3 NTP ブロードキャストモードの設定 3-8
3.5.4 NTP マルチキャストモードの設定 3-9
3.6 参照ソース用ローカルクロックの設定 3-10
3.7 NTP サービスアクセス制御権の設定 3-11
3.8 NTP 認証の設定 3-11
3.8.1 クライアント/サーバモードの NTP 認証の設定 3-11
3.8.2 シンメトリックアクティブ/パッシブモードの NTP 認証の設定 3-13
3.8.3 ブロードキャストモードの NTP 認証の設定 3-14
3.8.4 マルチキャストモードの NTP 認証の設定 3-16
3.9 NTP オプションパラメータの設定 3-18
3.9.1 NTP メッセージの送信元インタフェースの設定 3-18
3.9.2 インタフェースでの NTP メッセージ受信の無効化 3-19
3.9.3 ダイナミックアソシエーションの最大数の設定 3-19
3.9.4 NTP パケットの DSCP 値の設定 3-20
3.10 NTP の表示と維持 3-20
3.11 NTP 設定例 3-20
3.11.1 NTP クライアント/サーバモードの設定例 3-20
3.11.2 NTP シンメトリックアクティブ/パッシブモードの設定例 3-22
3.11.3 NTP ブロードキャストモードの設定例 3-23
3.11.4 NTP マルチキャストモードの設定例 3-25
3.11.5 NTP 認証を使用したクライアント/サーバモードの設定例 3-28
3.11.6 NTP 認証を使用したブロードキャストモードの設定例 3-30

3章 NTP

NTP（Network Time Protocol）を使用して、あるいはシステムクロックを変更することで、ネットワークで動作させる前に、信頼されたシステムクロックと同期を取ります。システムメッセージのタイムスタンプとログは、システム時刻を使用しているため、ネットワーク管理、チャージシステム、監査、分散コンピューティングなどを含む、さまざまなアプリケーションは正確なシステムクロックが必要となります。

3.1 概要

NTP はネットワーク装置間のシステムクロックを動的に同期させるため、一般的に大規模ネットワークで使用されます。手動でシステムクロックを設定するよりも、高いクロック精度が保証されます。NTP を有効に利用することで、装置間のシステムクロックを同期させ続けることができます。

NTP は UDP プロトコルで、UDP ポート 123 を使用します。

🕮 **メモ：**

NTP は、レイヤ 3 イーサネットインタフェースでサポートします。

3.1.1 NTP の動作

図 3-1に示すように、Device A と Device B の 2 つの Device 間でシステム時間を同期させる NTP の基本的なワークフローを示します。以下のように仮定します。

- システムクロックの同期を行う前に、Device A の時刻は 10:00:00 am で Device B の時刻は 11:00:00 am と設定されています。
- Device B は NTP サーバとして使用されます。Device A は Device B に同期化されます。
- NTP メッセージが Device A から Device B あるいは Device B から Device A に送信されるまで 1 秒かかります。

Device B で NTP メッセージを処理するのに 1 秒かかります。

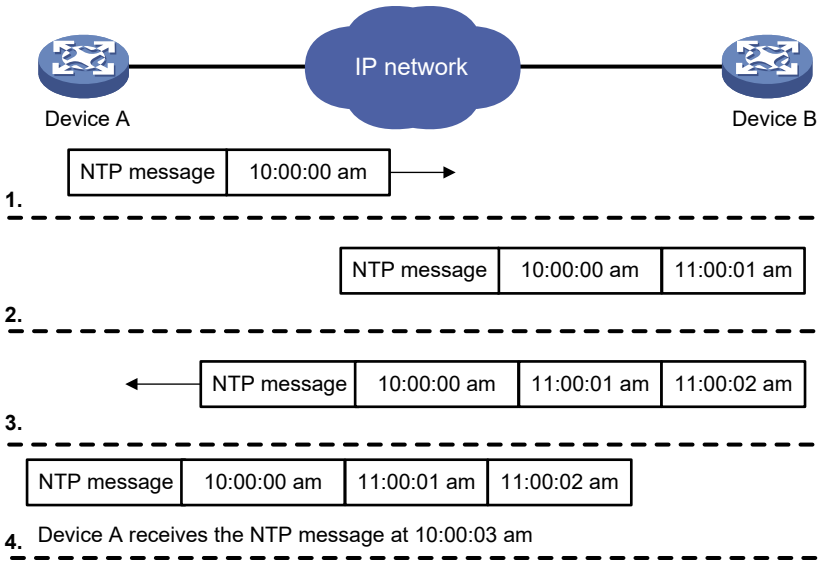


図 3-1 基本ワークフロー

以下に同期プロセスを示します。

1) Device A から Device B に NTP メッセージを送信します。メッセージは、Device A から発信されるときにタイムスタンプが与えられます。タイムスタンプは 10:00:00 am （T1） です。
2) NTP メッセージが Device B に届くと、Device B によってタイムスタンプが与えられます。タイムスタンプは 11:00:01 am （T2） です。
3) NTP メッセージが Device B から発信されるときに、Device B はメッセージにタイムスタンプを与えます。タイムスタンプは 11:00:02 am （T3） です。
4) Device A が NTP メッセージを受信したとき、Device A の現地時刻は 10:00:03 am （T4） です。

Device A には以下の 2 つの重要なパラメータを計算するための情報があります。

- **NTP メッセージのラウンドトリップ遅延**：遅延＝（T4 － T1） －（T3 － T2） ＝2 秒
- **Device A と Device B の間の時差**：オフセット＝（（T2 － T1） ＋（T3 － T4） ）/2 ＝1 時間

これらのパラメータにもとづき、Device A の時計を Device B の時計に同期することができます。

上記は、NTP の動作メカニズムについての概要です。詳細については、関連するプロトコルと標準を参照してください。

3.1.2 NTP アーキテクチャ

NTP はクロックの正確さを定義するため、図 3-2に示すように 1 から 16 の stratum（層）を使用します。stratum の値が小さいほど高い精度を持ちます。stratum 1 から 16 レベルのクロックは同期された時間で、stratum のレベル 16 のクロックは同期化されていないことを示します。

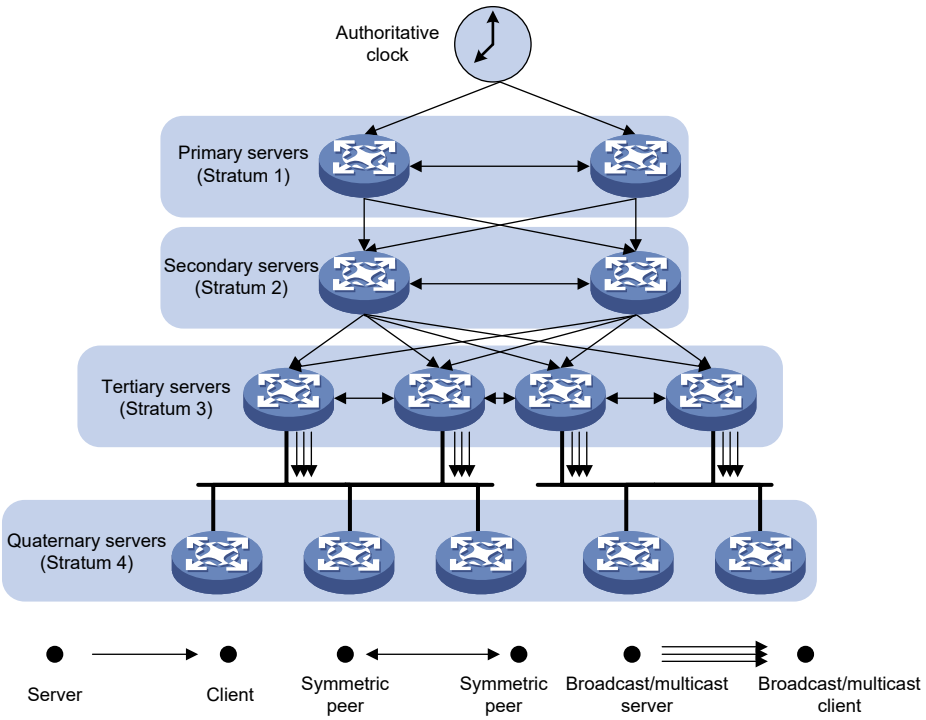


図 3-2 NTP アーキテクチャ

stratum レベル 1 の NTP サーバは、原子時計のような基準となるソースから時間を取得し、NTP サーバとして他の装置に時間を提供します。stratum レベル 2 のサーバは stratum レベル 1 のサーバなどから時間を取得します。

時間の正確性と有効性を保証するため、装置は複数の NTP サーバを指定することができます。装置は stratum のようなパラメータをもとにしてクロック ソースとして最適な NTP サーバを選択します。装置が選択するクロックは参照ソースと呼ばれます。時計の選択の詳細は関連するプロトコルと標準を参照してください。

もしネットワークの装置がもっとも権威のあるサーバに同期することができない場合、以下の処理を行うことができます。

- ネットワークから相対的に精度のあるクロックを持つ装置を選択します。
- ネットワークのほかの装置と同期させるため、参照クロックとして相対的に精度のある装置のローカルクロックを使用します。

3.1.3 運用モード

NTP は以下の運用モードをサポートします。

- クライアント/サーバモード
- シンメトリックアクティブ/パッシブモード
- ブロードキャストモード
- マルチキャストモード

表 3-1 NTP 運用モード

モード	作業処理	原則	アプリケーションシナリオ
クライアント/サーバ	クライアントではNTPサーバのIPアドレスを指定します。 クライアントはクロック同期メッセージをNTPサーバに送信します。 メッセージを受信したサーバは自動的にサーバのモードで動作し、応答を返します。 クライアントはサーバに複数同期した場合、サーバからの応答を受信した後、最適なクロックを選択し、ローカルクロックを最適な参照ソースと同期させます。	クライアントはサーバと同期することができますが、サーバはクライアントと同期することができません。	図 3-2に示すように、このモードは高いstratumの装置が低いstratumの装置に同期します。
シンメトリックアクティブ/パッシブ	シンメトリックアクティブピア上で、シンメトリックパッシブピアのIPアドレスを指定します。 シンメトリックアクティブピアは周期的にシンメトリックパッシブピアにクロック同期メッセージを送信します。 シンメトリックパッシブピアは自動的にシンメトリックパッシブモードで動作し、応答を送信します。 シンメトリックアクティブピアがサーバに複数同期した場合、サーバからの応答を受信した後、最適なクロックを選択し、ローカルクロックを最適な参照ソースと同期させます。	シンメトリックアクティブピアとシンメトリックパッシブピアは互いに同期することができます。もし両方が同期された場合、低いstratumのピアが高いstratumのピアに同期します。	図 3-2に示すように、このモードはバックアップとして動作させるため、同じstratumの2つ以上のサーバ間で使われます。 高いstratumのすべてのサーバと通信できない場合、サーバは同じstratumのサーバと同期します。
ブロードキャスト	サーバは周期的にブロードキャストアドレス255.255.255.255にクロック同期メッセージを送信します。 クライアントはサーバと同期するため、ブロードキャストメッセージに応答したサーバからブロードキャストメッセージを待ちます。 最初にブロードキャストメッセージを受信したとき、クライアントとサーバはネットワーク遅延を計算するため、メッセージの交換を開始します。ブロードキャストサーバのみがクロック同期メッセージを送信します。	ブロードキャストクライアントはブロードキャストサーバに同期することができますが、ブロードキャストサーバはブロードキャストクライアントに同期することができません。	ブロードキャストサーバはクロック同期メッセージを同じサブネットのクライアントに送信します。 図 3-2に示すように、このモードは潜在的に1つあるいは少ないサーバで、多くのクライアントがある環境で使われます。 ブロードキャストモードは、ブロードキャストサーバのみがクロック同期メッセージを送信するため、クライアント/サーバモードやシンメトリックアクティブ/パッシブよりも精度が低くなります。

モード	作業処理	原則	アプリケーションシナリオ
マルチキャスト	マルチキャストサーバは周期的にユーザが設定したマルチキャストアドレスにクロック同期メッセージを送信します。クライアントはマルチキャストメッセージに応答したサーバからマルチキャストメッセージを待ちます。	マルチキャストクライアントはマルチキャストサーバに同期することができますが、マルチキャストサーバはマルチキャストクライアントに同期することができません。	マルチキャストサーバはクロック同期メッセージを同じあるいは異なるサブネットのクライアントに送信します マルチキャストモードは、クライアント/サーバモードやシンメトリックアクティブ/パッシブよりも精度が低くなります。

この章では、NTP サーバあるいはサーバとは、クライアント/サーバモードの NTP サーバとして動作する装置を示します。タイムサーバとは、NTP サーバ、NTP シンメトリックピア、ブロードキャストサーバ、マルチキャストサーバを含んだ、クロック同期を行うことができるすべての装置を示します。

3.1.4 NTP セキュリティ

クロック同期のセキュリティを向上させるため、装置は NTP サービスアクセス制御権と認証機能をサポートします。

I. NTP サービスアクセス制御権の設定

ACL を用いて NTP サービスアクセス制御権を設定することができます。アクセス制御権は以下となります。

- **Peer**ー時刻要求と NTP コントロールクエリ（アラーム、認証ステータス、時間サーバなどの情報）を受信し、ローカル装置が隣接装置に自身を同期させることを可能とします。
- **Server**ー時刻要求と NTP コントロールクエリを受信するが、ローカル装置が隣接装置に自身を同期させることを可能としません。
- **Synchronization**ーアドレスリストを通過したアドレスを持つシステムからの時刻要求のみ受信します。
- **Query**ー隣接装置からローカル装置への NTP コントロールクエリのみ受信します。

装置が NTP 要求を受信した場合、もっとも制限の少ないアクセス制御権からもっとも制御されているアクセス制御権の順番（peer、server、synchronization、query）でアクセス制御権に対する要求にマッチします。

- アクセス制御権が設定されていない場合、**peer** はローカル装置と隣接装置に与えられます。
- 隣接装置の IP アドレスが複数のアクセス制御権のための ACL にマッチし、**Permit** となる場合、もっとも制限の少ないアクセス制御権が隣接装置に与えられます。ACL にマッチしない、または **deny** となった場合、アクセス制御権は与えられません。
- アクセス制御権のために指定された ACL が作成されない場合、関連したアクセス制御権は与えられません。
- アクセス制御権のために指定された ACL が 1 つも作成されない場合、**peer** が与えられます。

- アクセス制御権で指定された ACL にルールが含まれていない場合、アクセス制御権は与えられません。

この機能は、NTP を運用するシステムに最低限のセキュリティを提供します。より安全な方法としては NTP 認証があります。

II. NTP 認証

NTP 認証は、セキュリティのため、NTP メッセージを認証します。NTP メッセージが認証をパスしたとき、装置は、メッセージを受信し、クロック同期情報を取得します。もしパスしないとき、メッセージを廃棄します。この機能は、許可されていないサーバに同期をしないようにするために使われます。

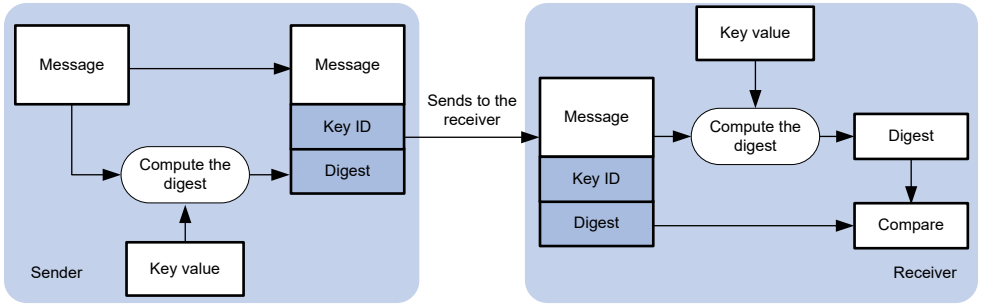


図 3-3 NTP 認証

図 3-3に示すように NTP 認証は以下のように動作します。

1) Sender は、キーID によって識別されたキーに従って NTP メッセージを計算するため認証アルゴリズムを使用します。NTP メッセージを計算したダイジェストとキーID を Receiver に送信します。
2) メッセージを受信すると Receiver は以下の処理を行います。

a) メッセージのキーIDに応じてキーを確認します。

b) ダイジェストを計算するため、キー、キーと同一の認証アルゴリズムを使用します。

c) NTPメッセージの計算したダイジェストとNTPメッセージに含まれているダイジェストと比較します。

- 計算したダイジェストと NTP メッセージに含まれているダイジェストが異なる場合、Receiver はメッセージを廃棄します。
- 計算したダイジェストと NTP メッセージに含まれているダイジェストが同一ですが作成の要求がない場合、Receiver はメッセージに応答します。NTP メッセージの詳細は、オペレーションマニュアルのセッション 11 *システム管理*“*NTP*”の“*ダイナミックアソシエーションの最大数の設定*”を参照してください。
- 計算したダイジェストと NTP メッセージに含まれているダイジェストが同一で、NTP セッションが作成されている場合、ローカル装置は Sender が認証 ID の使用を許可するか決定します。Sender が認証 ID の使用を許可されている場合、Receiver はメッセージを受信します。Sender が認証 ID の使用を許可されていない場合、Receiver はメッセージを廃棄します。

3.1.5 プロトコルと標準

- RFC 1305, *Network Time Protocol (Version 3) Specification, Implementation and Analysis*
- RFC 5905, *Network Time Protocol Version 4: Protocol and Algorithms Specification*

3.2 設定の制限とガイドライン

以下の設定の制限とガイドラインに従って NTP を設定してください。

- アグリゲートメンバーポートで NTP を設定することはできません。
- 頻繁にクロックが変更する、あるいは同期の失敗が発生することを防ぐため、ネットワークの参照クロックを複数指定しないでください。
- NTP としてシステムクロックソースを指定するため、**clock protocol** コマンドを使用してください。コマンドの詳細はコマンドマニュアルのセクション 1 *はじめに*“*装置管理*”を参照してください。

3.3 設定作業リスト

作業リスト
（必須設定項目） NTPサービスの有効化
（必須設定項目）NTP運用モードの設定
（オプション設定項目）参照ソース用ローカルクロックの設定
（オプション設定項目）NTPサービスアクセス制御権の設定
（オプション設定項目） NTP認証の設定
（オプション設定項目） NTPオプションパラメータの設定

3.4 NTPサービスの有効化

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. NTP サービスを有効にする	**ntp-service enable**	デフォルト：無効

3.5 NTP運用モードの設定

この章は NTP 運用モードの設定方法について記載します。

3.5.1 NTP クライアント/サーバモードの設定

NTP クライアントを設定するとき、以下のガイドラインに従います。

- サーバは他の装置によって同期させる必要があります。あるいは NTP クライアントを同期する前に参照ソースとしてローカルクロックを使用する必要があります。そうでなければクライアントは NTP サーバに同期することができません。
- サーバの stratum レベルがクライアントと等しいあるいは高いレベルである場合クライアントはサーバに同期しません。
- **ntp-service unicast-server** コマンドを繰り返して設定することで複数のサーバを設定することができます。
- 装置がクライアント/サーバモードで動作するとき、クライアントの IP アドレスを指定します。

以下に NTP クライアントの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. 装置の NTP サーバを指定する	**ntp-service unicast-server** { *server-name* | *ip-address* } [**authentication-keyid** *keyid* | **maxpoll** *maxpoll-interval* | **minpoll** *minpoll-interval* | **priority** | **source** *interface-type interface-number* | **version** *number*]*	デフォルト：指定なし

3.5.2 NTP シンメトリックアクティブ/パッシブモードの設定

NTP シンメトリックアクティブピアを設定するとき、以下のガイドラインに従います。

- NTP を有効にするため、シンメトリックパッシブピアで **ntp-service enable** コマンドを実行してください。そうでなければシンメトリックパッシブピアはシンメトリックアクティブピアから NTP メッセージを処理しません。
- シンメトリックアクティブピアあるいはシンメトリックパッシブピアのどちらかあるいは、その両方は同期化された状態にする必要があります。そうでなければ同期化することができません。
- **ntp-service unicast-peer** コマンドを繰り返して設定することで複数のシンメトリックパッシブピアを設定することができます。
- シンメトリックアクティブ/パッシブモードで装置が動作するとき、シンメトリックパッシブピア用にシンメトリックアクティブピアの IP アドレスを指定します。

以下に NTP シンメトリックアクティブピアの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. シンメトリックパッシブピアを指定する	**ntp-service unicast-peer** { *peer-name* | *ip-address* } [**authentication-keyid** *keyid* | **maxpoll** *maxpoll-interval* | **minpoll** *minpoll-interval* | **priority** | **source** *interface-type interface-number* | **version** *number*]*	デフォルト：指定なし

3.5.3 NTP ブロードキャストモードの設定

ブロードキャストサーバは、ブロードキャストクライアントを同期する前に、他の装置によって同期させる必要があります。あるいは参照ソースとしてローカルクロックを使用す

る必要があります。そうでなければブロードキャストクライアントはブロードキャストサーバに同期させることができません。

ブロードキャストサーバとクライアントの両方でブロードキャストモードの NTP を設定します。

I. ブロードキャストクライアントの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. interface view に移行する	**interface** *interface-type interface-number*	NTPブロードキャストメッセージを受信するインタフェースに移行します。
3. NTP ブロードキャストクライアントモードで動作するように装置を設定する	**ntp-service broadcast-client**	デフォルト：設定なし コマンドを実行した後、装置は指定したインタフェースからNTPブロードキャストメッセージを受信します。

II. ブロードキャストサーバの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. interface view に移行する	**interface** *interface-type interface-number*	NTPブロードキャストメッセージを送信するインタフェースに移行します。
3. NTP ブロードキャストサーバモードで動作するように装置を設定する	**ntp-service broadcast-server** [**authentication-keyid** *keyid* | **version** *number*]*	デフォルト：設定なし コマンドを実行した後、装置は指定したインタフェースからNTPブロードキャストメッセージを受信します。

3.5.4 NTP マルチキャストモードの設定

マルチキャストサーバは、マルチキャストクライアントを同期する前に、他の装置によって同期させる必要があります。あるいは参照ソースとしてローカルクロックを使用する必要があります。そうでなければマルチキャストクライアントはマルチキャストサーバに同期させることができません。

マルチキャストサーバとクライアントの両方でマルチキャストモードの NTP を設定します。

I. マルチキャストクライアントの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. interface view に移行する	**interface** *interface-type interface-number*	NTPマルチキャストメッセージを受信するインタフェースに移行します。

操作	コマンド	補足
3. NTP マルチキャストクライアントモードで動作するように装置を設定する	**ntp-service multicast-client** [*ip-address*]	デフォルト：設定なし コマンドを実行した後、装置は指定したインタフェースからNTPマルチキャストメッセージを受信します。

II. マルチキャストサーバの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. interface view に移行する	**interface** *interface-type interface-number*	NTPマルチキャストメッセージを送信するインタフェースに移行します。
3. NTP マルチキャストサーバモードで動作するように装置を設定する	**ntp-service multicast-server** [*ip-address*] [**authentication-keyid** *keyid* | **ttl** *ttl-number* | **version** *number*] *	デフォルト：設定なし コマンドを実行した後、装置は指定したインタフェースからNTPマルチキャストメッセージを送信します。

3.6 参照ソース用ローカルクロックの設定

I. 参照ソース用ローカルクロック設定

参照ソースとしてローカルクロックを設定することを可能にします。

II. 制限とガイドライン

参照ソースとしてローカルクロックを設定した後、ローカルクロックは同期化され、ネットワークのほかの装置に同期化するため、タイムサーバとして動作することができます。ローカルクロックが正確でない場合、タイムエラーが発生します。

🕮 **メモ：**

ntp-service refclock-master コマンドを有効にすることで QX を NTP マスタとして稼働させることが可能になります。しかし QX を NTP マスタとして運用した場合、うるう秒の挿入等が行われた際の情報を得ることができず、時刻のずれが発生します。また、装置内部の時計精度についても、一般的な PC 等と同様であるため、時計精度による時刻ずれも発生します。

信頼できる NTP サーバから時刻の取得を行い、同期して運用することを推奨します。

III. 設定要件

この機能を設定する前に、ローカルシステム時間を正しい値に設定してください。

IV. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. 参照ソース用ローカルクロックを設定する	**ntp-service refclock-master** [*ip-address*] [*stratum*]	デフォルト：設定なし

3.7 NTPサービスアクセス制御権の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. 隣接装置がローカル装置にアクセスするための NTP サービスアクセス制御権を設定する	**ntp-service** { **peer** | **query** | **server** | **synchronization** } **acl** *ipv4-acl-number*	デフォルト：peer

NTP サービスアクセス制御権をローカル装置に設定する前にアクセス制御権に関連した ACL を作成、設定してください。詳細はコマンドマニュアルのセクション 8 *ACL and QoS*” *ACL*”を参照してください。

3.8 NTP認証の設定

この章は NTP 認証の設定手順について記載します。

3.8.1 クライアント/サーバモードの NTP 認証の設定

サーバとクライアントで設定されたキーID とキーの値は同じにする必要があります。そうでなければ NTP 認証は失敗します。ピアの装置がローカル装置でキーID を使用することができることを確認してください。

以下にクライアントの NTP 認証の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. NTP 認証を有効にする	**ntp-service authentication enable**	デフォルト：無効
3. NTP 認証キーを設定する	**ntp-service authentication-keyid** *keyid* **authentication-mode md5** { **cipher** | **simple** } *string* *	デフォルト：設定なし
4. 認証キーをトラステッドキーとして設定する	**ntp-service reliable authentication-keyid** *keyid*	デフォルト：設定なし
5. NTP サーバとキーを関連づける	**ntp-service unicast-server** { *server-name* | *ip-address* } **authentication-keyid** *keyid*	ー

以下にサーバの NTP 認証の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. NTP 認証を有効にする	**ntp-service authentication enable**	デフォルト：無効
3. NTP 認証キーを設定する	**ntp-service authentication-keyid** *keyid* **authentication-mode md5** { **cipher** | **simple** } *string* *	デフォルト：設定なし
4. 認証キーをトラステッドキーとして設定する	**ntp-service reliable authentication-keyid** *keyid*	デフォルト：設定なし

クライアントとサーバで異なる設定が実行されると、NTP 認証の結果は異なります。詳細を表 3-2に示します。（ーは相違がないことを示します。）

以下に NTP 認証の結果を示します。

表 3-2 NTP 認証の結果

クライアント			サーバ		認証結果
NTP 認証を有効にする	キーをトラステッドキーとして設定する	NTP サーバにキーを関連づける	NTP 認証を有効にする	キーをトラステッドキーとして設定する	
Yes	Yes	Yes	Yes	Yes	認証は成功します。NTPメッセージは正常に送受信することができます。
Yes	Yes	Yes	Yes	No	認証は失敗します。NTPメッセージは正常に送受信することができません。
Yes	Yes	Yes	No	ー	認証は失敗します。NTPメッセージは正常に送受信することができません。
Yes	No	Yes	ー	ー	認証は失敗します。NTPメッセージは正常に送受信することができません。
Yes	ー	No	ー	ー	認証はありません。NTPメッセージは正常に送受信することができます。
No	ー	ー	ー	ー	認証はありません。NTPメッセージは正常に送受信することができます。

3.8.2 シンメトリックアクティブ/パッシブモードの NTP 認証の設定

アクティブピアとパッシブピアで設定されたキーID とキーの値は同じにする必要があります。そうでなければ NTP 認証は失敗します。ピアの装置がローカル装置でキーID を使用することができることを確認してください。

以下にアクティブピアの NTP 認証の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. NTP 認証を有効にする	**ntp-service authentication enable**	デフォルト：無効
3. NTP 認証キーを設定する	**ntp-service authentication-keyid** *keyid* **authentication-mode md5** { **cipher** | **simple** } *string* *	デフォルト：設定なし
4. 認証キーをトラステッドキーとして設定する	**ntp-service reliable authentication-keyid** *keyid*	デフォルト：設定なし
5. パッシブピアとキーを関連づける	**ntp-service unicast-peer** { *ip-address* | *peer-name* } **authentication-keyid** *keyid*	―

以下にパッシブピアの NTP 認証の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. NTP 認証を有効にする	**ntp-service authentication enable**	デフォルト：無効
3. NTP 認証キーを設定する	**ntp-service authentication-keyid** *keyid* **authentication-mode md5** { **cipher** | **simple** } *string* *	デフォルト：設定なし
4. 認証キーをトラステッドキーとして設定する	**ntp-service reliable authentication-keyid** *keyid*	デフォルト：設定なし

アクティブピアとパッシブピアで異なる設定が実行されると、NTP 認証の結果は異なります。詳細を表 3-3に示します。（―は相違がないことを示します。）

以下に NTP 認証の結果を示します。

表 3-3 NTP 認証の結果

アクティブピア			パッシブピア		認証結果
NTP 認証を有効にする	キーをトラステッドキーとして設定する	パッシブピアにキーを関連づける	NTP 認証を有効にする	キーをトラステッドキーとして設定する	
アクティブピアとパッシブピアのstratumレベルは考慮しません。					
Yes	Yes	Yes	Yes	Yes	認証は成功します。NTPメッセージは正常に送受信することができます。
Yes	Yes	Yes	Yes	No	認証は失敗します。NTPメッセージは正常に送受信することができません。

アクティブピア			パッシブピア		認証結果
NTP 認証を有効にする	キーをトラステッドキーとして設定する	パッシブピアにキーを関連づける	NTP 認証を有効にする	キーをトラステッドキーとして設定する	
Yes	Yes	Yes	No	ー	認証は失敗します。NTPメッセージは正常に送受信することができません。
Yes	ー	No	Yes	ー	認証は失敗します。NTPメッセージは正常に送受信することができません。
Yes	ー	No	No	ー	認証はありません。NTPメッセージは正常に送受信することができます。
No	ー	ー	Yes	ー	認証は失敗します。NTPメッセージは正常に送受信することができません。
No	ー	ー	No	ー	認証はありません。NTPメッセージは正常に送受信することができます。
アクティブピアはパッシブピアよりも高いstratumを持ちます。					
Yes	No	Yes	ー	ー	認証は失敗します。NTPメッセージは正常に送受信することができません。
パッシブピアはアクティブピアよりも高いstratumを持ちます。					
Yes	No	Yes	Yes	ー	認証は失敗します。NTPメッセージは正常に送受信することができません。
Yes	No	Yes	No	ー	認証はありません。NTPメッセージは正常に送受信することができます。

3.8.3 ブロードキャストモードの NTP 認証の設定

ブロードキャストクライアントとブロードキャストサーバで設定されたキーID とキーの値は同じにする必要があります。そうでなければ NTP 認証は失敗します。ピアの装置がローカル装置でキーID を使用することができることを確認してください。

以下にブロードキャストクライアントの NTP 認証の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. NTP 認証を有効にする	**ntp-service authentication enable**	デフォルト：無効

操作	コマンド	補足
3. NTP 認証キーを設定する	**ntp-service authentication-keyid** *keyid* **authentication-mode md5** { **cipher** | **simple** } *string* *	デフォルト：設定なし
4. 認証キーをトラステッドキーとして設定する	**ntp-service reliable authentication-keyid** *keyid*	デフォルト：設定なし

以下にブロードキャストサーバの NTP 認証の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. NTP 認証を有効にする	**ntp-service authentication enable**	デフォルト：無効
3. NTP 認証キーを設定する	**ntp-service authentication-keyid** *keyid* **authentication-mode md5** { **cipher** | **simple** } *string* *	デフォルト：設定なし
4. 認証キーをトラステッドキーとして設定する	**ntp-service reliable authentication-keyid** *keyid*	デフォルト：設定なし
5. interface view に移行する	**interface** *interface-type interface-number*	ー
6. ブロードキャストサーバとキーを関連づける	**ntp-service broadcast-server authentication-keyid** *keyid*	デフォルト：設定なし

ブロードキャストクライアントとブロードキャストサーバで異なる設定が実行されると、NTP 認証の結果は異なります。詳細を表 3-4に示します。（ーは相違がないことを示します。）

以下に NTP 認証の結果を示します。

表 3-4 NTP 認証の結果

ブロードキャストサーバ			ブロードキャストクライアント		認証の結果
NTP 認証を有効にする	キーをトラステッドキーとして設定する	ブロードキャストサーバとキーを関連づける	NTP 認証を有効にする	キーをトラステッドキーとして設定する	
Yes	Yes	Yes	Yes	Yes	認証は成功します。NTPメッセージは正常に送受信することができます。
Yes	Yes	Yes	Yes	No	認証は失敗します。NTPメッセージは正常に送受信することができません。
Yes	Yes	Yes	No	ー	認証は失敗します。NTPメッセージは正常に送受信することができません。
Yes	No	Yes	Yes	ー	認証は失敗します。NTPメッセージは正常に送受信することができません。

ブロードキャストサーバ			ブロードキャストクライアント		認証の結果
NTP 認証を有効にする	キーをトラステッドキーとして設定する	ブロードキャストサーバとキーを関連づける	NTP 認証を有効にする	キーをトラステッドキーとして設定する	
Yes	No	Yes	No	―	認証はありません。NTPメッセージは正常に送受信することができます。
Yes	―	No	Yes	―	認証は失敗します。NTPメッセージは正常に送受信することができません。
Yes	―	No	No	―	認証はありません。NTPメッセージは正常に送受信することができます。
No	―	―	Yes	―	認証は失敗します。NTPメッセージは正常に送受信することができません。
No	―	―	No	―	認証はありません。NTPメッセージは正常に送受信することができます。

3.8.4 マルチキャストモードの NTP 認証の設定

マルチキャストクライアントとマルチキャストサーバで設定されたキーID とキーの値は同じにする必要があります。そうでなければ NTP 認証は失敗します。ピアの装置がローカル装置でキーID を使用することができることを確認してください。

以下にマルチキャストクライアントの NTP 認証の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. NTP 認証を有効にする	**ntp-service authentication enable**	デフォルト：無効
3. NTP 認証キーを設定する	**ntp-service authentication-keyid** *keyid* **authentication-mode md5** { **cipher** | **simple** } *string* *	デフォルト：設定なし
4. 認証キーをトラステッドキーとして設定する	**ntp-service reliable authentication-keyid** *keyid*	デフォルト：設定なし

以下にマルチキャストサーバの NTP 認証の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. NTP 認証を有効にする	**ntp-service authentication enable**	デフォルト：無効

操作	コマンド	補足
3. NTP 認証を有効にする	**ntp-service authentication-keyid** *keyid* **authentication-mode md5** { **cipher** | **simple** } *string* *	デフォルト：設定なし
4. 認証キーをトラステッドキーとして設定する	**ntp-service reliable authentication-keyid** *keyid*	デフォルト：設定なし
5. interface view に移行する	**interface** *interface-type interface-number*	―
6. マルチキャストサーバとキーを関連づける	**ntp-service multicast-server** [*ip-address*] **authentication-keyid** *keyid*	デフォルト：設定なし

マルチキャストクライアントとマルチキャストサーバで異なる設定が実行されると、NTP 認証の結果は異なります。詳細を表 3-5に示します。（ーは相違がないことを示します。）

以下に NTP 認証の結果を示します。

表 3-5 NTP 認証の結果

マルチキャストサーバ			マルチキャストクライアント		認証の結果
NTP 認証を有効にする	キーをトラステッドキーとして設定する	マルチキャストサーバにキーを関連づける	NTP 認証を有効にする	キーをトラステッドキーとして設定する	
Yes	Yes	Yes	Yes	Yes	認証は成功します。NTPメッセージは正常に送受信することができます。
Yes	Yes	Yes	Yes	No	認証は失敗します。NTPメッセージは正常に送受信することができません。
Yes	Yes	Yes	No	―	認証は失敗します。NTPメッセージは正常に送受信することができません。
Yes	No	Yes	Yes	―	認証は失敗します。NTPメッセージは正常に送受信することができません。
Yes	No	Yes	No	―	認証はありません。NTPメッセージは正常に送受信することができます。
Yes	―	No	Yes	―	認証は失敗します。NTPメッセージは正常に送受信することができません。
Yes	―	No	No	―	認証はありません。NTPメッセージは正常に送受信することができます。

マルチキャストサーバ			マルチキャストクライアント		認証の結果
NTP 認証を有効にする	キーをトラステッドキーとして設定する	マルチキャストサーバにキーを関連づける	NTP 認証を有効にする	キーをトラステッドキーとして設定する	
No	―	―	Yes	―	認証は失敗します。NTPメッセージは正常に送受信することができません。
No	―	―	No	―	認証はありません。NTPメッセージは正常に送受信することができます。

3.9 NTPオプションパラメータの設定

この章はオプション作業設定項目について記載します。NTP セキュリティ、性能、信頼性を改善するために設定します。

3.9.1 NTP メッセージの送信元インタフェースの設定

インタフェースの状態の変更によって、NTP 通信の失敗を引き起こすことを防ぐため、常にアップ状態であるインタフェースの IP アドレスを使用するように設定します。たとえば常にアップ状態であるインタフェースはループバックインタフェースです。装置のインタフェースの状態の変更によって、NTP メッセージを受信できるようにするため、送信元インタフェースとしてループバックインタフェースを設定します。

装置が NTP リクエストに応答する場合、NTP 応答の送信元 IP アドレスは、NTP リクエストを受信したインタフェースの IP アドレスです。

以下に NTP メッセージの送信元インタフェースを指定するときのガイドラインを示します。

- **ntp-service unicast-server** コマンドあるいは **ntp-service unicast-peer** コマンドで、NTP メッセージの送信元インタフェースを指定した場合、**ntp-service unicast-server** コマンドあるいは **ntp-service unicast-peer** コマンドで指定したインタフェースは NTP メッセージの送信元インタフェースとして動作します。
- **ntp-service broadcast-server** コマンドあるいは **ntp-service multicast-server** コマンドが設定された場合、ブロードキャスト NTP メッセージあるいはマルチキャスト NTP メッセージの送信元インタフェースは、それぞれのコマンドで設定したインタフェースです。

以下に NTP メッセージの送信元インタフェースの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. NTP メッセージの送信元インタフェースを指定する	**ntp-service source** *interface-type interface-number*	デフォルト：設定なし

3.9.2 インタフェースでの NTP メッセージ受信の無効化

NTP が有効なとき、デフォルトですべてのインタフェースは NTP メッセージを受信することができます。セキュリティのため、インタフェースで NTP メッセージを受信しないようにすることができます。

以下に NTP メッセージの受信をインタフェースで無効にする設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. interface view に移行する	**interface** *interface-type interface-number*	―
3. インタフェースで NTP メッセージの受信を無効にする	**undo ntp-service inbound enable**	デフォルト：有効

3.9.3 ダイナミックアソシエーションの最大数の設定

NTP は以下のアソシエーションタイプがあります。

- **スタティックアソシエーション** ― 手動で作成したアソシエーション
- **ダイナミックアソシエーション** ― NTP を動作する間、システムによって作成された一時的なアソシエーションです。12 分以内にメッセージの交換が行われない場合、ダイナミックアソシエーションは削除されます。

以下に設定される異なるアソシエーションモードを示します。

- **クライアント/サーバモード** ― NTP サーバを指定した後、システムはクライアントでスタティックアソシエーションを作成します。サーバはアソシエーション（スタティックあるいはダイナミック）を作成するのではなく、単に受信したメッセージに対して、受動的に応答します。
- **シンメトリックアクティブ/パッシブモード** ― シンメトリックアクティブピアでシンメトリックパッシブピアを指定した後、シンメトリックアクティブピア上でスタティックアソシエーションが作成され、シンメトリックパッシブピアでダイナミックアソシエーションが作成されます。
- **ブロードキャスト/マルチキャストモード** ― サーバでスタティックアソシエーションが作成され、クライアントでダイナミックアソシエーションが作成されます。

1 つの装置で、スタティックアソシエーション、ダイナミックアソシエーションを含み、共通で最大 128 のアソシエーションを作成することができます。

ダイナミックアソシエーションが多くのシステムリソースを占有しないように、制限させるため、ダイナミックアソシエーションの最大数を制限します。

以下にダイナミックアソシエーションの最大数の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. ダイナミックアソシエーションの最大数を設定する	**ntp-service max-dynamic-sessions** *number*	デフォルト：100

3.9.4 NTP パケットの DSCP 値の設定

パケットの DSCP 値は、パケットの優先度レベルを指定し、パケットの優先度に影響します。

以下に NTP パケットの DSCP 値の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. NTP パケットの DSCP 値を設定する	**ntp-service dscp** *dscp-value*	デフォルト：48

3.10 NTPの表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
IPv4 NTPアソシエーションを表示する	**display ntp-service sessions** [**verbose**]
NTPサービスステータスの情報を表示する	**display ntp-service status**
ローカル装置からプライマリ参照ソースに戻ったNTPサーバの概要情報を表示する	**display ntp-service trace**

3.11 NTP設定例

3.11.1 NTP クライアント/サーバモードの設定例

I. ネットワーク要件

図 3-4に示すように設定します。

- Device A の stratum レベル 2 のローカルクロックを参照ソースとして設定します。
- Device B をクライアントモードで動作し、Device A を Device B の NTP サーバとして設定します。

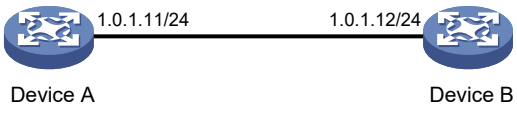


図 3-4 ネットワーク図

II. 設定手順

1) 図 3-4に示すように各インタフェースの IP アドレスを設定します。（詳細は省略します。）
2) Device A を設定します。

NTP サービスを有効にします。

```
<DeviceA> system-view
[DeviceA] ntp-service enable
```

参照ソースとして stratum レベル 2 のローカルクロックを指定します。

```
[DeviceA] ntp-service refclock-master 2
```

3) Device B を設定します。

NTP サービスを有効にします。

```
<DeviceB> system-view
[DeviceB] ntp-service enable
```

Device B が Device A に同期されるように、Device B の NTP サーバとして Device A を指定します。

```
[DeviceB] ntp-service unicast-server 1.0.1.11
```

III. 設定の確認

Device B が Device A に同期化され、Device B の stratum レベルが 3で Device A の stratum レベルが 2 であることを確認します。

```
[DeviceB] display ntp-service status
 Clock status: synchronized
 Clock stratum: 3
 System peer: 1.0.1.11
 Local mode: client
 Reference clock ID: 1.0.1.11
 Leap indicator: 00
 Clock jitter: 0.000977 s
 Stability: 0.000 pps
 Clock precision: 2^-19
 Root delay: 0.00383 ms
 Root dispersion: 16.26572 ms
 Reference time: d0c6033f.b9923965  Wed, Dec 29 2010 18:58:07.724
```

Device B と Device A 間で NTP アソシエーションが確立されていることを確認します。

```
[DeviceB] display ntp-service sessions
       source          reference       stra reach poll  now offset  delay disper
**************************************************************************
[12345]1.0.1.11        127.127.1.0        2     1   64   15   -4.0 0.0038 16.262
Notes: 1 source(master), 2 source(peer), 3 selected, 4 candidate, 5 configured.
 Total sessions: 1
```

3.11.2 NTP シンメトリックアクティブ/パッシブモードの設定例

I. ネットワーク要件

図 3-5に示すように、設定します。

- 参照ソースとして Device A のローカルクロックを stratum レベル 2 に設定します。
- シンメトリックアクティブモードで動作するように Device B を設定し、Device B のパッシブピアとして Device A を指定します。



図 3-5 ネットワーク図

II. 設定手順

1) 図 3-5に示すように各インタフェースの IP アドレスを設定します。(詳細は省略します。)
2) Device B を設定します。

NTP サービスを有効にします。

```
<DeviceB> system-view
[DeviceB] ntp-service enable
```

3) Device A を設定します。

NTP サービスを有効にします。

```
<DeviceA> system-view
[DeviceA] ntp-service enable
```

参照ソースとして stratum レベル 2 のローカルクロックを設定します。

```
[DeviceA] ntp-service refclock-master 2
```

シンメトリックパッシブピアとして Device B を設定します。

```
[DeviceA] ntp-service unicast-peer 3.0.1.32
```

III. 設定の確認

Device B が Device A に同期していることを確認します。

```
[DeviceB] display ntp-service status
 Clock status: synchronized
 Clock stratum: 3
 System peer: 3.0.1.31
 Local mode: sym_passive
 Reference clock ID: 3.0.1.31
```

```
 Leap indicator: 00
 Clock jitter: 0.000916 s
 Stability: 0.000 pps
 Clock precision: 2^-19
 Root delay: 0.00609 ms
 Root dispersion: 1.95859 ms
 Reference time: 83aec681.deb6d3e5  Wed, Jan  8 2014 14:33:11.081
```

Device B と Device A 間の IPv4 NTP アソシエーションが確立されていることを確認します。

```
[DeviceB] display ntp-service sessions
      source          reference       stra reach poll  now offset  delay disper
**************************************************************************
   [12]3.0.1.31       127.127.1.0        2    62   64   34 0.4251 6.0882 1392.1
Notes: 1 source(master), 2 source(peer), 3 selected, 4 candidate, 5 configured.
 Total sessions: 1
```

3.11.3 NTP ブロードキャストモードの設定例

I. ネットワーク要件

図 3-6に示すように、同一ネットワークセグメントで複数の装置用の NTP サーバとして Switch C が動作し、複数の装置間でクロックの同期を行います。

- Switch C のローカルクロックは参照ソースとして使用され、stratum レベル 2 です。
- Switch C はブロードキャストサーバモードで動作し、VLAN インタフェース 2 からブロードキャストメッセージを送信します。
- Switch A と Switch B はブロードキャストクライアントモードで動作し、VLAN インタフェース 2 を通してブロードキャストメッセージを受信します。

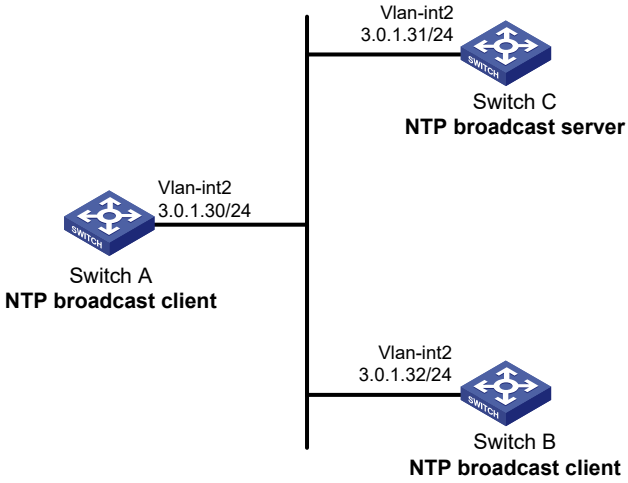


図 3-6 ネットワーク図

II. 設定手順

1) 図 3-6に示すように各インタフェースの IP アドレスを設定します。（詳細は省略します。）
2) Switch C を設定します。

NTP サービスを有効にします。

```
<SwitchC> system-view
[SwitchC] ntp-service enable
```

参照ソースとして stratum レベル 2 のローカルクロックを設定します。

```
[SwitchC] ntp-service refclock-master 2
```

ブロードキャストサーバモードで動作するように Switch C を設定し、VLAN インタフェース 2 からブロードキャストメッセージを送信します。

```
[SwitchC] interface vlan-interface 2
[SwitchC-Vlan-interface2] ntp-service broadcast-server
```

3)　Switch A を設定します。

NTP サービスを有効にします。

```
<SwitchA> system-view
[SwitchA] ntp-service enable
```

ブロードキャストクライアントモードで動作するように Switch A を設定し、VLAN インタフェース 2 からブロードキャストメッセージを受信します。

```
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ntp-service broadcast-client
```

4)　Switch B を設定します。

NTP サービスを有効にします。

```
<SwitchB> system-view
[SwitchB] ntp-service enable
```

ブロードキャストクライアントモードで動作するように Switch B を設定し、VLAN インタフェース 2 からブロードキャストメッセージを受信します。

```
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] ntp-service broadcast-client
```

III. 設定の確認

Switch A が Switch C に同期化され、Switch A の stratum レベルが 3 で、Switch C の stratum レベルが 2 であることを確認します。

```
[SwitchA-Vlan-interface2] display ntp-service status
 Clock status: synchronized
 Clock stratum: 3
 System peer: 3.0.1.31
 Local mode: bclient
 Reference clock ID: 3.0.1.31
 Leap indicator: 00
 Clock jitter: 0.044281 s
 Stability: 0.000 pps
 Clock precision: 2^-19
 Root delay: 0.00229 ms
 Root dispersion: 4.12572 ms
```

```
  Reference time: d0d289fe.ec43c720  Sat, Jan  8 2011  7:00:14.922
```

Switch A と Switch C 間で NTP アソシエーションが確立されていることを確認します。

```
[SwitchA-Vlan-interface2] display ntp-service sessions
      source          reference       stra reach poll  now offset  delay disper
**************************************************************************
 [1245]3.0.1.31       127.127.1.0        2     1   64  519   -0.0 0.0022 4.1257
Notes: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured.
 Total sessions: 1
```

3.11.4 NTP マルチキャストモードの設定例

I. ネットワーク要件

図 3-7に示すように、異なるネットワークセグメントで複数の装置用の NTP サーバとして Switch C が動作し、複数の装置間でクロックの同期を行います。

- Switch C のローカルクロックは参照ソースとして使用され、stratum レベル 2 です。
- Switch C はマルチキャストサーバモードで動作し、VLAN インタフェース 2 からマルチキャストメッセージを送信します。
- Switch A と Switch D はマルチキャストクライアントモードで動作し、それぞれ VLAN インタフェース 2 と VLAN インタフェース 3 を通してマルチキャストメッセージを受信します。

🕮 **メモ：**

この例では、Switch B は IPv4 マルチキャストルーティングをサポートする必要があります。

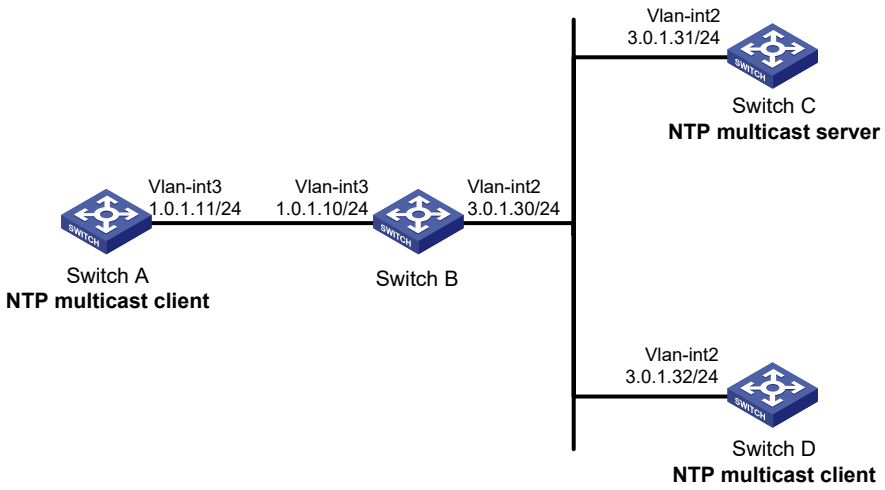


図 3-7 ネットワーク図

II. 設定手順

1) 図 3-7に示すように各インタフェースの IP アドレスを設定します。(詳細は省略します。)
2) Switch C を設定します。

NTP サービスを有効にします。

```
<SwitchC> system-view
[SwitchC] ntp-service enable
```

参照ソースとして stratum レベル 2 のローカルクロックを設定します。

```
[SwitchC] ntp-service refclock-master 2
```

マルチキャストサーバモードで動作するように Switch C を設定し、VLAN インタフェース 2 からマルチキャストメッセージを送信します。

```
[SwitchC] interface vlan-interface 2
[SwitchC-Vlan-interface2] ntp-service multicast-server
```

3) Switch D を設定します。

NTP サービスを有効にします。

```
<SwitchD> system-view
[SwitchD] ntp-service enable
```

マルチキャストクライアントモードで動作するように Switch D を設定し、VLAN インタフェース 2 からマルチキャストメッセージを送信します。

```
[SwitchD] interface vlan-interface 2
[SwitchD-Vlan-interface2] ntp-service multicast-client
```

4) 設定を確認します。

Switch D と Switch C は同一サブネットにあるため、Switch D は以下のことができます。

- Switch C からマルチキャスト機能を有効にしない状態で Switch C からマルチキャストメッセージを受信することができます。
- Switch C と同期することができます。

Switch D が Switch C に同期化され、Switch D の stratum レベルが 3 で、Switch C の stratum レベルが 2 であることを確認します。

```
[SwitchD-Vlan-interface2] display ntp-service status
Clock status: synchronized
Clock stratum: 3
System peer: 3.0.1.31
Local mode: bclient
Reference clock ID: 3.0.1.31
Leap indicator: 00
Clock jitter: 0.044281 s
Stability: 0.000 pps
Clock precision: 2^-19
Root delay: 0.00229 ms
Root dispersion: 4.12572 ms
Reference time: d0d289fe.ec43c720  Sat, Jan  8 2011  7:00:14.922
```

Switch D と Switch C 間で NTP アソシエーションが確立されていることを確認します。

```
[SwitchD-Vlan-interface2] display ntp-service sessions
      source          reference       stra reach poll  now offset  delay disper
```

```
**************************************************************************
 [1245]3.0.1.31       127.127.1.0       2     1   64  519   -0.0 0.0022 4.1257
Notes: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured.
 Total sessions: 1
```

5) Switch B を設定します。

Switch A と Switch C は異なるサブネットにあるため、Switch A が Switch C からマルチキャストメッセージを受信する前に、Switch B でマルチキャスト機能を有効にする必要があります。

IP マルチキャストルーティングと IGMP を有効にします。

```
<SwitchB> system-view
[SwitchB] multicast routing
[SwitchB-mrib] quit
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] pim sm
[SwitchB-Vlan-interface2] quit
[SwitchB] vlan 3
[SwitchB-vlan3] port gigabitethernet 1/0/1
[SwitchB-vlan3] quit
[SwitchB] interface vlan-interface 3
[SwitchB-Vlan-interface3] igmp enable
[SwitchB-Vlan-interface3] igmp static-group 224.0.1.1
[SwitchB-Vlan-interface3] quit
[SwitchB] igmp-snooping
[SwitchB-igmp-snooping] quit
[SwitchB] interface gigabitethernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] igmp-snooping static-group 224.0.1.1 vlan 3
```

6) Switch A を設定します。

NTP サービスを有効にします。

```
<SwitchA> system-view
[SwitchA] ntp-service enable
```

マルチキャストクライアントモードで動作するように Switch A を設定し、VLAN インタフェース 3 からマルチキャストメッセージを受信します。

```
[SwitchA] interface vlan-interface 3
[SwitchA-Vlan-interface3] ntp-service multicast-client
```

III. 設定の確認

Switch A が Switch C に同期化され、Switch A の stratum レベルが 3 で、Switch C の stratum レベルが 2 であることを確認します。

```
[SwitchA-Vlan-interface3] display ntp-service status
 Clock status: synchronized
 Clock stratum: 3
 System peer: 3.0.1.31
 Local mode: bclient
 Reference clock ID: 3.0.1.31
 Leap indicator: 00
 Clock jitter: 0.165741 s
 Stability: 0.000 pps
 Clock precision: 2^-19
 Root delay: 0.00534 ms
 Root dispersion: 4.51282 ms
 Reference time: d0c61289.10b1193f  Wed, Dec 29 2010 20:03:21.065
```

Switch A と Switch C 間で NTP アソシエーションが確立されていることを確認します。

```
[SwitchA-Vlan-interface3] display ntp-service sessions
       source          reference       stra reach poll  now offset  delay disper
**************************************************************************
 [1234]3.0.1.31       127.127.1.0        2   247   64  381   -0.0 0.0053 4.5128
Notes: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured.
 Total sessions: 1
```

3.11.5 NTP 認証を使用したクライアント/サーバモードの設定例

I. ネットワーク要件

- 図 3-8に示すように、Device A の stratum レベル 2 のローカルクロックは参照ソースとして使われます。
- Device B はクライアントモードで動作し、Device A は Device B の NTP サーバとして使用されます。
- Device A と Device B の両方で NTP 認証を設定します。

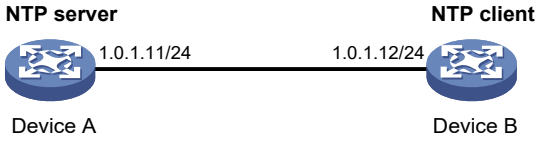


図 3-8 ネットワーク図

II. 設定手順

1) 図 3-8に示すように各インタフェースの IP アドレスを設定します。（詳細は省略します。）
2) Device A を設定します。

NTP サービスを有効にします。

```
<DeviceA> system-view
```

```
[DeviceA] ntp-service enable
```

参照ソースとして stratum レベル 2 のローカルクロックを指定します。

```
[DeviceA] ntp-service refclock-master 2
```

3) Device B を設定します。

NTP サービスを有効にします。

```
<DeviceB> system-view
[DeviceB] ntp-service enable
```

Device B で NTP 認証を有効にします。

```
[DeviceB] ntp-service authentication enable
```

認証キーを設定し、プレーンテキストでキーを入力します。

```
[DeviceB] ntp-service authentication-keyid 42 authentication-mode md5 simple aNiceKey
```

キーをトラステッドキーとして指定します。

```
[DeviceB] ntp-service reliable authentication-keyid 42
```

Device B の NTP サーバとして Device A を指定し、キーID を 42 としてサーバと関連づけます。

```
[DeviceB] ntp-service unicast-server 1.0.1.11 authentication-keyid 42
```

Device B が Device A のクロックの同期を行う前に、Device A の NTP 認証を有効にします。

4) Device A で NTP 認証を設定します。

NTP 認証を有効にします。

```
[DeviceA] ntp-service authentication enable
```

認証キーを設定し、プレーンテキストでキーを入力します。

```
[DeviceA] ntp-service authentication-keyid 42 authentication-mode md5 simple aNiceKey
```

キーをトラステッドキーとして指定します。

```
[DeviceA] ntp-service reliable authentication-keyid 42
```

III. 設定の確認

Device B が Device A に同期化され、Device B の stratum レベルが 3 で、Device A の stratum レベルが 2 であることを確認します。

```
[DeviceB] display ntp-service status
 Clock status: synchronized
 Clock stratum: 3
 System peer: 1.0.1.11
 Local mode: client
 Reference clock ID: 1.0.1.11
 Leap indicator: 00
 Clock jitter: 0.005096 s
 Stability: 0.000 pps
 Clock precision: 2^-19
```

```
 Root delay: 0.00655 ms
 Root dispersion: 1.15869 ms
 Reference time: d0c62687.ab1bba7d  Wed, Dec 29 2010 21:28:39.668
```

Device B と Device A 間で NTP アソシエーションが確立されていることを確認します。

```
[DeviceB] display ntp-service sessions
      source          reference       stra reach poll  now offset  delay disper
**************************************************************************
 [1245]1.0.1.11        127.127.1.0        2     1   64  519   -0.0 0.0065    0.0
Notes: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured.
 Total sessions: 1
```

3.11.6 NTP 認証を使用したブロードキャストモードの設定例

I. ネットワーク要件

図 3-9に示すように、同一ネットワークセグメントで複数の装置用の NTP サーバとして Switch C が動作し、複数の装置間でクロックの同期を行います。Switch A と Switch B は参照ソースを認証します。

- Switch C のローカルクロックは参照ソースとして使用され、stratum レベル 3 です。
- Switch C はブロードキャストサーバモードで動作し、VLAN インタフェース 2 からブロードキャストメッセージを送信します。
- Switch A と Switch B はブロードキャストクライアントモードで動作し、VLAN インタフェース 2 を通してブロードキャストメッセージを受信します。
- Switch A、Switch B、Switch C で NTP 認証を設定します。

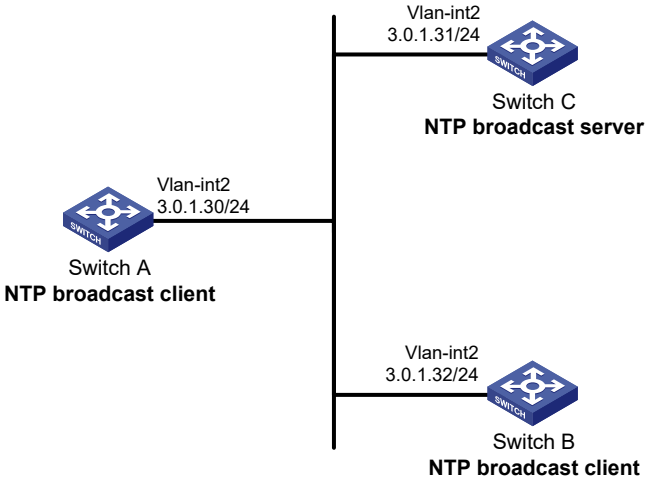


図 3-9 ネットワーク図

II. 設定手順

1) 図 3-9に示すように各インタフェースの IP アドレスを設定します。（詳細は省略します。）
2) Switch A を設定します。

NTP サービスを有効にします。

```
<SwitchA> system-view
[SwitchA] ntp-service enable
```

Switch A で NTP 認証を有効にします。認証キーID を 88 とし、キーの値を 123456 として、NTP 認証キーを設定します。プレーンテキストで入力し、キーをトラステッドキーとして指定します。

```
[SwitchA] ntp-service authentication enable
[SwitchA] ntp-service authentication-keyid 88 authentication-mode md5 simple 123456
[SwitchA] ntp-service reliable authentication-keyid 88
```

NTP ブロードキャストクライアントモードで動作するように Switch A を設定し、VLAN インタフェース 2 からブロードキャストメッセージを受信します。

```
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ntp-service broadcast-client
```

3)　Switch B を設定します。

NTP サービスを有効にします。

```
<SwitchB> system-view
[SwitchB] ntp-service enable
```

Switch B で NTP 認証を有効にします。認証キーID を 88 とし、キーの値を 123456 として、NTP 認証キーを設定します。プレーンテキストで入力し、キーをトラステッドキーとして指定します。

```
[SwitchB] ntp-service authentication enable
[SwitchB] ntp-service authentication-keyid 88 authentication-mode md5 simple 123456
[SwitchB] ntp-service reliable authentication-keyid 88
```

NTP ブロードキャストクライアントモードで動作するように Switch B を設定し、VLAN インタフェース 2 からブロードキャストメッセージを受信します。

```
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] ntp-service broadcast-client
```

4)　Switch C を設定します。

NTP サービスを有効にします。

```
<SwitchC> system-view
[SwitchC] ntp-service enable
```

参照ソースとして stratum レベル 3 のローカルクロックを指定します。

```
[SwitchC] ntp-service refclock-master 3
```

NTP ブロードキャストサーバモードで動作するように Switch C を設定し、VLAN インタフェース 2 からブロードキャストメッセージを送信します。

```
[SwitchC] interface vlan-interface 2
[SwitchC-Vlan-interface2] ntp-service broadcast-server
```

```
[SwitchC-Vlan-interface2] quit
```

5)　設定を確認します。

NTP 認証は Switch A と Switch B で有効となっていますが、Switch C では有効でないため、Switch A と Switch B は Switch C とローカルクロックを同期化することができません。

Switch B が Switch C に同期化されていないことを確認します。

```
[SwitchB-Vlan-interface2] display ntp-service status
 Clock status: unsynchronized
 Clock stratum: 16
 Reference clock ID: none
```

6)　Switch C で NTP 認証を設定します。

Switch C で NTP 認証を有効にします。認証キーID を 88 とし、キーの値を 123456 として、NTP 認証キーを設定します。プレーンテキストで入力し、キーをトラステッドキーとして指定します。

```
[SwitchC] ntp-service authentication enable
[SwitchC] ntp-service authentication-keyid 88 authentication-mode md5 simple 123456
[SwitchC] ntp-service reliable authentication-keyid 88
```

NTP ブロードキャストサーバとして Switch C を指定し、Switch C を認証キー88 に関連づけます。

```
[SwitchC] interface vlan-interface 2
[SwitchC-Vlan-interface2] ntp-service broadcast-server authentication-keyid 88
```

III. 設定の確認

Switch C で NTP 認証を有効にした後、Switch A と Switch B は Switch C にローカルクロックを同期化することができます。

```
[SwitchB-Vlan-interface2] display ntp-service status
 Clock status: synchronized
 Clock stratum: 4
 System peer: 3.0.1.31
 Local mode: bclient
 Reference clock ID: 3.0.1.31
 Leap indicator: 00
 Clock jitter: 0.006683 s
 Stability: 0.000 pps
 Clock precision: 2^-19
 Root delay: 0.00127 ms
 Root dispersion: 2.89877 ms
 Reference time: d0d287a7.3119666f  Sat, Jan  8 2011  6:50:15.191
```

Switch B と Switch C 間で NTP アソシエーションが確立されていることを確認します。

```
[SwitchB-Vlan-interface2] display ntp-service sessions
      source          reference       stra reach poll  now offset  delay disper
**************************************************************************
 [1245]3.0.1.31        127.127.1.0        3     3   64   68   -0.0 0.0000    0.0
Notes: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured.
 Total sessions: 1
```

目次

このセクションのページは **11-x-x** です。

4章 PoE 4-1
4.1 概要 4-1
4.2 PoE設定作業リスト 4-2
4.3 PIのPoEの有効化 4-2
4.4 PDによる突入電流の許容 4-3
4.5 PIの最大電力の設定 4-4
4.6 PI電力管理の設定 4-4
4.7 PoEモニタリングの設定 4-5
4.8 PoEプロファイルを使用したPIの設定 4-6
4.8.1 PoEプロファイルの設定 4-6
4.8.2 PoEプロファイルの適用 4-7
4.9 動作中でのPSEファームウェアのアップグレード 4-7
4.10 無停止給電 4-8
4.11 PoEの表示と維持 4-8
4.12 PoE設定例 4-8
4.13 PoEのトラブルシューティング 4-10
4.13.1 PIの優先度をcriticalに設定できない 4-10
4.13.2 PIにPoEプロファイルを適用できない 4-10

4章 PoE

🕮 **メモ:**

- PoE 機能は 10/100/1000 BASE-T イーサネットでサポートしています。PI view は PoE 機能をサポートしているポートの Ethernet interface view を意味します。
- PoE 機能は Version 7.4.61 以降のバージョンでサポートしています。
- poe standard コマンドと poe high-inrush enable コマンドの両機能を設定する場合は、先に poe high-inrush enable コマンドを設定してください。詳細はコマンドマニュアル -システム管理- 4 章 PoE の poe high-inrush enable を参照ください。

4.1 概要

IEEE 802.3at 準拠の PoE＋（Power Over Ethernet）は、ツイストペアケーブルを介して端末に電力を供給するネットワーク装置を有効にします。

図 4-1に示すように、PoE システムは以下の要素があります。

- **PoE 電源**－PoE 電源はすべての PoE システムの電力を供給します。
- **PSE**－PSE（電力供給装置）は PD（電力受電装置）を検出し、分類します。そして PD に電力を供給し、PD 電力と接続状態をモニタします。PSE は endpoint PSE と midspan PSE があります。

QX-S5100G シリーズの PSE は endpoint PSE です。複数の PSE が存在する装置は異なる PSE を識別するために PSE ID を使用します。PSE ID と PSE のスロットあるいはサブスロット番号間のマッピングを表示する場合、**display poe device** コマンドを使用します。

- **PI（電力インタフェース）**－ 電力インタフェースは PSE の PoE が有効な Ethernet インタフェースです。
- **PD（電力受電装置）**－ PD は PSE から電力を受電します。

PD は IP 電話、AP、ポータブルチャージャ、POS 端末、Web カメラなどがあります。

信頼性を向上させるため、冗長電力ソースに PD を接続することができます。

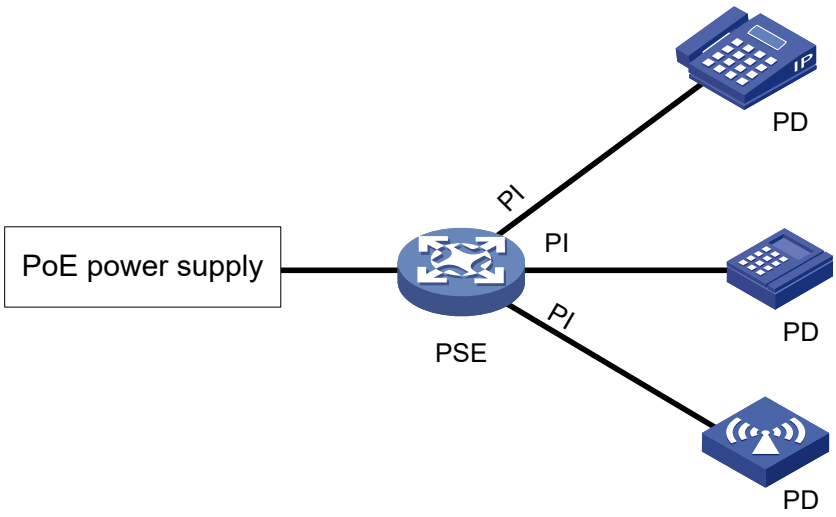


図 4-1 PoE システム図

4.2 PoE設定作業リスト

ポートで直接 PI を設定することができます。あるいは PoE プロファイルを設定し、PI に PoE プロファイルを適用することができます。1 つの PI を設定する場合、ポートに直接設定します。複数の PI を一括して設定する場合、PoE プロファイルを使用します。

PoE を設定する前に、PoE 電源と PSE が正常に動作することを確認してください。そうでない場合、PoE を設定できない、あるいは PoE の設定を適用することができません。

作業リスト
（必須設定項目）PIのPoEの有効化
（オプション設定項目）PIの最大電力の設定
（オプション設定項目）PI電力管理の設定
（オプション設定項目）PoE電力モニタリングの設定
（オプション設定項目）PoEプロファイルを使用したPIの設定 • PoEプロファイルの設定 • PoEプロファイルの適用
（オプション設定項目）動作中でのPSEファームウェアのアップグレード

4.3 PIのPoEの有効化

システムは PoE が有効な PI に接続された PD に電力を供給し、電力の予約のみを行います。

PI が PSE 電力の過負荷状態にならない場合、PoE を有効にすることができます。PoE 電力の過負荷は、すべての PI の消費電力の合計が PSE の最大電力を超過したときに発生します。PSE の最大電力は設定可能です。

PI が PSE 電力の過負荷になる場合、PI 電力管理が有効であるとき、PI で PoE を有効にすることができます。PI 電力管理の詳細は、オペレーションマニュアルのセクション 11 *システム管理*”*PoE*”の”*PI 電力管理の設定*”を参照してください。

PSE は、PI に接続されたカテゴリ 3 あるいはカテゴリ 5 ツイストペアを経由して、以下のモードで電力を供給します。

- **signal モード**－PSE はデータ信号線のペア（ピン 1、2、3、6）を経由して PD に DC 電力を供給します。
- **spare モード**－PSE はスペア信号線のペア（ピン 4、5、7、8）を経由して PD に DC 電力を供給します。

🕮 **メモ：**

- QX-S5100G シリーズは signal モードでのみ電力を供給します。
- PSE と PD が同一の電力供給モードを使用しているときのみ、直接 PD に電力を供給することができます。PSE と PD が異なる電力供給モードで使用している場合、PD に電力を供給するため、ツイストペアケーブルの信号線の順番を変更する必要があります。

以下に PI で PoE を有効にする設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． PI view に移行する	**interface** *interface-type interface-number*	―
3． PI で PoE を有効にする	**poe enable**	デフォルト：有効
4． （オプション設定項目）PI に接続された PD の説明を設定する	**poe pd-description** *text*	デフォルト：無効

4.4 PDによる突入電流の許容

🕮 **メモ:**

poe standard コマンドと poe high-inrush enable コマンドの両機能を設定する場合は、先に poe high-inrush enable コマンドを設定してください。詳細はコマンドマニュアル -システム管理- 4 章 PoE の poe high-inrush enable を参照ください。

PD の起動時に突入電流が発生し、PSE の自己保護を引き起こすことがあります。その結果、PSE は PD への電力供給を停止します。PD への電源供給を継続するには、PD が消費する突入電流を許可するようにこの機能を設定します。設定を変更する場合は注意してください。

IEEE 802.3 af および IEEE 802.3 at は、突入電流の仕様を定義します。この装置は、IEEE 802.3 af および IEEE 802.3 at で定義された突入電流の仕様をサポートします。

I. 設定手順

操作	コマンド	補足
5． system view に移行する	**system-view**	ー
6． PD による突入電流を許容する	**poe high-inrush enable pse** *pse-id*	デフォルト：無効

4.5 PIの最大電力の設定

PI の最大電力は接続された PD に供給できる最大電力です。PD が PI の最大電力より電力を必要とする場合、PI は PD に電力を供給しません。

以下に PI の最大電力の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． PI view に移行する	**interface** *interface-type interface-number*	ー
3． （オプション設定項目）PI の最大電力を設定する	**poe max-power** *max-power*	デフォルト：30000ミリW

4.6 PI電力管理の設定

PSE 電力が過負荷の状況下において、PI 電力管理機能を有効にすると、PSE は優先度をもとにして PI 電力の管理を行います。PI の電力供給の優先度レベルは critical、high、low の順番で低くなります。PD の優先度は、PD が接続している PI の優先度によって決められます。すべての PSE は同じ PI 電力管理メカニズムを使用します。

PI 電力管理を無効にした場合、PSE が過負荷となる可能性があります。PSE の電力が過負荷になると、最大 PSE 電力の状態にもとづいて動作を実行します。

最大 PSE 電力の状態	過負荷での PSE の動作
設定あり	PSEは新しいPDへの電力を停止します。
設定なし	PoE自己保護メカニズムが開始されたとき、PSEはすべてのPDへの電力を停止します。

PI 電力管理を有効にした場合、PSE が過負荷になると、PSE は既存の PD に電力を停止する、あるいは優先度をもとにして新しい PD の動作を実行します。

新しい PD の優先度	PD の動作
low	PSEは新しいPDに電力を供給しません。
high	● lowの優先度のPDが存在する場合、PSEは既存のlowの優先度のPDへの電力の供給を停止します。そして新しいPDに電力を供給します。 ● lowの優先度のPDが存在しない場合、PSEは新しいPDに電力を供給しません。

新しい PD の優先度	PD の動作
critical	• lowあるいはhighの優先度のPDが存在する場合、PSEは既存のlowあるいはhighの優先度のPDへの電力の供給を停止します。そして新しいPDに電力を供給します。 • lowあるいはhighの優先度のPDが存在しない場合、PSEは新しいPDに電力を供給しません。

🕮 **メモ：**

- 電力があらかじめ予約されている PI への設定は変更ありません。
- QX-S5100G シリーズの保証余力電力は 30W です。

複数の新しい PD が電力供給を必要とする場合、PSE は優先度が高い順で PD に電力を供給します。優先度が同じ場合、もっとも小さい PD の ID を持つ PD が優先されます。

複数の既存の PD が電力供給を停止する必要がある場合、PSE は優先度が低い順で PD への電力を停止します。優先度が同じ場合、もっとも大きい PD の ID を持つ PD から電力を停止します。

PSE は保証された PSE 電力を予約することで、critical の優先度を持つ PI への電力供給を停止しないことを保証します。PI に電力供給を停止しないように割り当てる場合、PI に critical の優先度を設定します。そうでない場合、ほかの PI に電力を供給できるようにするため、PI に high あるいは low の優先度を設定します。

critical の優先度を持つ PI を設定する前に、保証余力電力が、PI の最大電力以上であることを確認してください。

保証余力電力は、PSE で供給可能な電力から、PoE が有効および無効な critical の優先度を持つ PI の最大電力の合計を引いた値です。

以下に PI 電力管理の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． PI 電力管理を有効にする	**poe pd-policy priority**	デフォルト：無効
3． PI view に移行する	**interface** *interface-type interface-number*	―
4． （オプション設定項目）PI の電力供給の優先度を設定する	**poe priority** { **critical** | **high** | **low** }	デフォルト：low

4.7 PoEモニタリングの設定

システムは PSE 電力の使用率をモニタし、PSE 電力供給がしきい値を超過あるいは下回ったとき、SNMP notification メッセージを送信します。

PSE 電力の使用率がしきい値を越えたあるいは下回った場合、システムは超過あるいは下回った都度、SNMP notification メッセージを送信します。SNMP notification の詳細はオペレーションマニュアルのセクション 11 *システム管理*" *SNMP*" を参照してください。

以下に PSE 電力アラームのしきい値の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． PSE の電力アラームのしきい値を設定する	**poe utilization-threshold** *value* **pse** *pse-id*	デフォルト：80%

4.8 PoEプロファイルを使用したPIの設定

PoE プロファイルは複数の PoE の設定を集めたものです。

ポートで PI を設定する、あるいは PoE プロファイルを使用して PI を設定することができます。PI のパラメータを設定するとき以下のガイドラインに従ってください。

- **poe max-power** *max-power* コマンドと **poe priority** { **critical** | **high** | **low** }コマンドは同一の方式になるようにしてください。
- 異なる方式でパラメータを設定した場合、最初の設定が有効となります。設定を変更する場合、最初の設定を削除してから、再度設定を行ってください。

PI の一括設定と PD 固有の PI の設定を行う場合、PoE プロファイルを活用することができます。

- PoE プロファイルを用いて、複数の PI に同じ設定を行うことができます。同じ PoE プロファイルで設定された PI は同じ PoE 機能となります。
- PoE プロファイルで PD の PoE 設定を定義することができます。PD が接続している PI に PoE プロファイルを適用することができます。PD が別の PI に移動したとき、PoE プロファイルを新しい PI に適用することで、再度設定する必要がありません。それによって PoE の設定を簡略化することができます。

4.8.1 PoE プロファイルの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． PoE プロファイルを作成し、PoE profile view に移行する	**poe-profile** *profile-name* [*index*]	デフォルト：設定なし
3． PoE を有効にする	**poe enable**	デフォルト：有効
4． （オプション設定項目）PI の最大電力を設定する	**poe max-power** *max-power*	デフォルト：30000ミリW
5． （オプション設定項目）PI の電力供給の優先度を設定する	**poe priority** { **critical** | **high** | **low** }	デフォルト：low

4.8.2 PoE プロファイルの適用

PoE プロファイルは system view あるいは PI view で適用することができます。system view あるいは PI view の両方の view で設定した場合、後から設定した view の設定が適用されます。PoE プロファイルは、複数の PI に適用できますが、PI は 1 つの PoE プロファイルのみ適用されます。

PoE プロファイルが適用されている場合、PoE プロファイルを変更する前に **undo apply poe-profile** コマンドあるいは **undo apply poe-profile interface** コマンドを使用してください。

I. 複数の PI への PoE プロファイルの適用（system view）

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. 1つ以上の PI に PoE プロファイルを適用する	**apply poe-profile** { **index** *index* | **name** *profile-name* } **interface** *interface-range*	デフォルト：設定なし

II. 1 つの PI への PoE プロファイルの適用（PI view）

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. PI に PoE プロファイルを適用する	**apply poe-profile** { **index** *index* | **name** *profile-name* }	デフォルト：設定なし

4.9 動作中でのPSEファームウェアのアップグレード

装置の動作中に以下のモードで PSE ファームウェアをアップグレードすることができます。

- **refresh モード**– PSE ファームウェアを削除しないで PSE ファームウェアをアップグレードします。通常、refresh モードで PSE ファームウェアをアップグレードします。
- **full モード**– 現在の PSE ファームウェアを削除し、新しい PSE ファームウェアで再起動します。PSE ファームウェアが故障し、PoE コマンドを実行できない場合、full モードを使用します。

装置の再起動による中断によって、PSE ファームウェアのアップグレードに失敗した場合、装置を再起動し、再度 full モードで PSE ファームウェアのアップグレードを行います。アップグレードを行った後、新しい PSE ファームウェアを適用するため、手動で装置を再起動します。

以下に装置の動作中に PSE ファームウェアのアップグレードの方法を示します。

操作	コマンド
1. system view に移行する	**system-view**
2. 装置の動作中に PSE ファームウェアのアップグレードを行う	**poe update** { **full** | **refresh** } *filename* [**pse** *pse-id*]

4.10 無停止給電

QX-S5100G シリーズはデフォルトで WarmReboot 時の無停止給電に対応しています。無停止給電は、PD への給電を停止せず装置を再起動する機能です。

I. 制限事項とガイドライン

- 本機能は reboot コマンドによる再起動の際に動作します。AC ケーブルの抜き差しや電源の瞬断による再起動の際には動作しません。
- ソフトウェア更新による reboot を行う場合、更新するソフトウェアに PoE に関連する修正がない場合のみ、本機能が動作します。
- BootMenu でソフトウェアを更新する場合は、本機能は動作しません。
- PoE のファームウェアを更新する場合は、本機能は動作しません。
- 無停止給電による装置起動中は、PD との接続ポートはリンクダウンします。

4.11 PoEの表示と維持

すべての view で display コマンドを実行することができます。

操作	コマンド
PSE情報を表示する	**display poe device** [**slot** *slot-number*]
PIの電力供給の情報を表示する	**display poe interface** [*interface-type interface-number*]
PIの電力情報を表示する	**display poe interface power** [*interface-type interface-number*]
PSEの情報を表示する	**display poe pse** [*pse-id*]
PSEのすべてのPIの電力供給の状態を表示する	**display poe pse** *pse-id* **interface**
PSEのすべてのPIの電力情報を表示する	**display poe pse** *pse-id* **interface power**
PoEプロファイルのすべての情報を表示する	**display poe-profile** [**index** *index* | **name** *profile-name*]
PIに適用されたPoEプロファイルの情報を表示する	**display poe-profile interface** *interface-type interface-number*

4.12 PoE設定例

I. ネットワーク要件

図 4-2に示すように、以下の要件に従って PoE を設定します。

- IP phone と AP に電力の供給を行います。
- 電力過負荷の状態になったとき、IP phone への電力の供給を優先させます。
- AP B の最大電力を 9000 ミリ W に割り当てます。

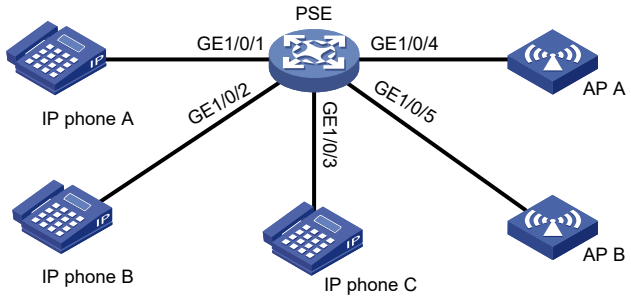


図 4-2 ネットワーク図

II. 設定手順

装置で、電力管理を有効に設定します。GigabitEthernet 1/0/1、GigabitEthernet 1/0/2、GigabitEthernet 1/0/3 で電力供給の優先度を critical に設定します。

```
<PSE> system-view
[PSE] interface gigabitethernet 1/0/1
[PSE-GigabitEthernet1/0/1] poe enable
[PSE-GigabitEthernet1/0/1] poe priority critical
[PSE-GigabitEthernet1/0/1] quit
[PSE] interface gigabitethernet 1/0/2
[PSE-GigabitEthernet1/0/2] poe enable
[PSE-GigabitEthernet1/0/2] poe priority critical
[PSE-GigabitEthernet1/0/2] quit
[PSE] interface gigabitethernet 1/0/3
[PSE-GigabitEthernet1/0/3] poe enable
[PSE-GigabitEthernet1/0/3] poe priority critical
[PSE-GigabitEthernet1/0/3] quit
```

GigabitEthernet 1/0/4、GigabitEthernet 1/0/5 で電力管理を有効に設定します。GigabitEthernet 1/0/5 の最大電力を 9000 ミリ W に設定します。

```
[PSE] interface gigabitethernet 1/0/4
[PSE-GigabitEthernet1/0/4] poe enable
[PSE-GigabitEthernet1/0/4] quit
[PSE] interface gigabitethernet 1/0/5
[PSE-GigabitEthernet1/0/5] poe enable
[PSE-GigabitEthernet1/0/5] poe max-power 9000
```

III. 設定の確認

IP phone と AP で正常に電力が取得できることを確認するため、IP phone と AP を PSE に接続します。（詳細は省略します。）

4.13 PoEのトラブルシューティング

4.13.1 PI の優先度を critical に設定できない

I. 症状

PI の電力供給の優先度の設定が失敗します。

II. 分析

可能性のある理由を以下に示します。

1) PI の保証余力電力が PI で要求された最大電力よりも小さいです。
2) PI の優先度がすでに設定されています。

III. 解決策

以下を確認してください。

1) 1 番目のケースの場合、PSE の最大電力を増加するか、PSE の残りの電力を変更できないとき、PI の最大電力を削減します。
2) 2 番目のケースの場合、すでに設定されている優先度を削除します。
3) 問題が解決しない場合、NEC に問い合わせてください。

4.13.2 PI に PoE プロファイルを適用できない

I. 症状

PI に PoE プロファイルを適用できません。

II. 分析

可能性のある理由を以下に示します。

1) PoE プロファイルのいくつかの設定がすでに設定されています。
2) PoE プロファイルのいくつかの設定が PI の設定要件を満たしていません。
3) すでに別の PoE プロファイルが PI に適用されています。

III. 解決策

以下を確認してください。

1) 1 番目のケースの場合、もとの設定を削除します。
2) 2 番目のケースの場合、PoE プロファイルの設定を修正します。
3) 3 番目のケースの場合、PI から予定していない PoE プロファイルの適用を削除します。
4) 問題が解決しない場合、NEC に問い合わせてください。

目次

このセクションのページは **11-x-x** です。

5 章 SNMP 5-1
5.1 概要 5-1
5.1.1 SNMP の構造 5-1
5.1.2 MIB と view ベースの MIB アクセス管理 5-1
5.1.3 SNMP の動作 5-2
5.1.4 プロトコルバージョン 5-2
5.1.5 アクセスコントロールモード 5-3
5.2 SNMP 基本パラメータの設定 5-3
5.2.1 SNMPv1 あるいは SNMPv2c 基本パラメータの設定 5-3
5.2.2 SNMPv3 基本パラメータの設定 5-5
5.3 SNMP ロギングの設定 5-7
5.4 SNMP 通知の設定 5-7
5.4.1 SNMP notification の有効化 5-8
5.4.2 ホストへ notification を送信する SNMP エージェントの設定 5-8
5.5 SNMP の表示と維持 5-10
5.6 設定例 5-10
5.6.1 SNMPv1/SNMPv2c の設定例 5-10
5.6.2 SNMPv3 の設定例 5-12

5章 SNMP

5.1 概要

SNMP（Simple Network Management Protocol）はネットワークで装置にアクセスし、操作させるための管理システムとして、ベンダ、物理的な特徴、相互接続技術に関係なく、広く使われているインタネット標準プロトコルです。

SNMP を使用することで、装置の状態のモニタリング、トラブルシューティング、コリジョンの統計情報やほかの情報の管理を行うため、ネットワーク管理者が装置の情報を確認し、設定することができます。

5.1.1 SNMP の構造

SNMP は以下の機能で構成されています。

- **SNMP マネジャー** – NMS（network management system）上で動作し、ネットワーク内の SNMP-capable デバイスをモニタし管理します。
- **SNMP エージェント** – 管理対象デバイス上で動作し、NMS からのリクエストを受信し操作します。インタフェースの状態の変化などのイベント発生時に NMS に Trap を送信します。
- **MIB（Management Information Base）** – SNMP **マネジャー**が読み取り、設定するために、SNMP エージェントによって保持されているインタフェース状態や CPU 使用率などの変数を指定します。

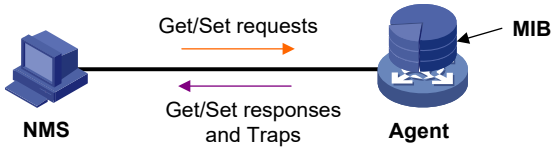


図 5-1 NMS、エージェント、MIB の関係

5.1.2 MIB と view ベースの MIB アクセス管理

MIB はツリー構造の「ノード」「オブジェクト」と呼ばれる変数を保存し、各ノードを固有の OID で区別します。OID はルートノードからリーフノードへのパスを示す番号列です。図 5-2では、オブジェクト B は OID {1.2.1.1}で区別されます。

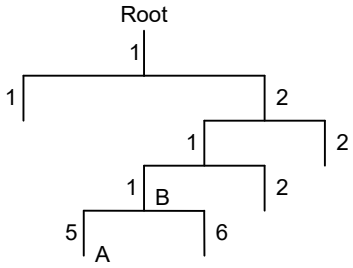


図 5-2 MIB ツリー

MIB view は、アクセス制限のある MIB オブジェクトの集合（あるいは MIB オブジェクト階層）を表し、view 名によって識別されます。MIB view に含まれる MIB オブジェクトはアクセス可能ですが、MIB view から除外されている MIB オブジェクトはアクセスできません。

MIB view は複数の view を持つことができます。複数の view は、*view-name oid-tree* の組み合わせで識別されます。

SNMP グループあるいはコミュニティに MIB view を割り当てることによって、MIB のアクセスを管理することができます。

5.1.3 SNMP の動作

SNMP は以下の基本的な動作を提供します。

- **Get** – エージェント MIB の SNMP オブジェクトノードを取得します。
- **Set** – エージェント MIB のオブジェクトノードの値を変更します。
- **Notification** – SNMP エージェントが NMS にイベントを通知するため、trap あるいは inform があります。Notification の 2 つのタイプの違いは、inform では ack（確認応答）が必要ですが、trap では必要ありません。trap は SNMPv1、SNMPv2c、SNMPv3 で有効ですが、inform は SNMPv2c、SNMPv3 でのみ有効です。

5.1.4 プロトコルバージョン

QX シリーズは、SNMPv1、SNMPv2c、SNMPv3 をサポートします。NMS と SNMP エージェントは相互に通信するため、同じ SNMP バージョンを使用する必要があります。

- **SNMPv1** – 認コミュニティ名で認証を行います。SNMP エージェントにアクセスするために、NMS は SNMP エージェントでセットしたものと同じコミュニティ名を使わなければなりません。NMS が使用するコミュニティ名がエージェントでセットしたものと違う場合、NMS はエージェントにアクセスするための SNMP セッションを構築することができない、もしくはエージェントからの Trap と Notification を受信することができません。
- **SNMPv2c** – コミュニティ名で認証を行います。SNMPv1 と互換を取り、より多くの動作モード、データ タイプ、エラーコードをサポートします。

- **SNMPv3** – USM （User-Based Security Model） を使ってセキュアな SNMP 通信を実現します。整合性、信頼性、および機密保持のために SNMP パケットを認証し暗号化する、認証とプライバシーのメカニズムを設定できます。

5.1.5 アクセスコントロールモード

SNMP は MIB オブジェクトにアクセスするため、以下のモードを使用します。

- VACM（View-based Access Control Model）モデル－VACM モードは MIB view を SNMP コミュニティやユーザに割り当てることで、MIB オブジェクトへのアクセスを制御します。

もし同じ SNMP コミュニティやユーザに複数回割り当てた場合、最後に作成した設定が適用されます。

VACM モードは NMS から MIB オブジェクトにアクセスする権限のみ必要です。

5.2 SNMP基本パラメータの設定

SNMPv3 は SNMPv1、SNMPv2c と多くの点で異なります。章を分けて設定方法について説明します。

5.2.1 SNMPv1 あるいは SNMPv2c 基本パラメータの設定

ユーザロールが network-admin あるいは level-15 のユーザのみ SNMPv1 あるいは SNMPv2c コミュニティ、ユーザ、グループを作成することができます。ほかのユーザロールのユーザは関連コマンド、SNMPv1 あるいは SNMPv2c 機能のコマンドへのアクセスが許可されていたとしても、SNMPv1 あるいは SNMPv2c コミュニティ、ユーザ、グループを作成することができません。

以下に SNMPv1 あるいは SNMPv2c 基本パラメータの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	–
2. （オプション設定項目） SNMP エージェントを有効にする	**snmp-agent**	デフォルト：無効 **snmp-agent calculate-password** コマンドを除いた**snmp-agent** で始まるいずれかのコマンドで SNMP エージェントを有効にできます。 IPアドレスを設定するまで SNMPポートは開きません。
3. （オプション設定項目） システム連絡先を設定する	**snmp-agent sys-info contact** *sys-contact*	デフォルト：設定なし
4. （オプション設定項目） システム所在地を設定する	**snmp-agent sys-info location** *sys-location*	デフォルト：設定なし

操作	コマンド	補足
5. SNMPv1 あるいは SNMPv2c を有効にする	**snmp-agent sys-info version** { **all** | { **v1** | **v2c** | **v3** } * }	デフォルト：SNMPv3が有効
6. （オプション設定項目） ローカルエンジン ID を変更する	**snmp-agent local-engineid** *engineid*	デフォルト: ローカルエンジン ID はCompany ID＋ device ID
7. （オプション設定項目） MIB view を作成または更新する	**snmp-agent mib-view** { **excluded** | **included** } *view-name oid-tree* [**mask** *mask-value*]	デフォルト：**ViewDefault** このview は**iso**サブツリーのすべてのオブジェクトが対象ですが、**snmpUsmMIB**と**snmpVacmMIB**と**snmpModules.18**はアクセス可能です。 *view-name*、*old-tree*のペアはそれぞれviewのレコードを表します。別のMIBサブツリーマスクに同じレコード名を複数回指定した場合、最後の設定が有効です。
8. SNMP アクセス権を設定する	• （アプローチ1） SNMPコミュニティを作成する： **snmp-agent community** { **read** | **write** } [**simple** | **cipher**] *community-name* [**mib-view** *view-name*] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } | **acl ipv6** { *ipv6-acl-number* | **name** *ipv6-acl-name* }]* • （アプローチ2） SNMPv1/SNMPv2cグループを作成し、グループにユーザを追加する： • **snmp-agent group** { **v1** | **v2c** } *group-name* [**read-view** *view-name*] [**write-view** *view-name*] [**notify-view** *view-name*] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } | **acl ipv6** { *ipv6-acl-number* | **name** *ipv6-acl-name* }]* • **snmp-agent usm-user** { **v1** | **v2c** } *user-name group-name* [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } | **acl ipv6** { *ipv6-acl-number* | **name** *ipv6-acl-name* }]*	どちらか一方のアプローチを使用します。 デフォルト：SNMPグループあるいはSNMPコミュニティは設定なし アプローチ2の*user-name*はアプローチ1のコミュニティ名と同じで、NMBで設定されるコミュニティ名と同じでなければなりません。
9. （オプション設定項目） SNMP エージェントが送受信できる SNMP パケットの最大バイトサイズ（バイト）を設定する	**snmp-agent packet max-size** *byte-count*	デフォルト：1500バイト

操作	コマンド	補足
10.（オプション設定項目） SNMP レスポンスパケットの DSCP 値を設定する	**snmp-agent packet response dscp** *dscp-value*	デフォルト：0 Version 7.2.30を含む以降のソフトウェアからサポートしています。

5.2.2 SNMPv3 基本パラメータの設定

ユーザロールが network-admin あるいは level-15 のユーザのみ SNMPv3 コミュニティ、ユーザ、グループを作成することができます。ほかのユーザロールのユーザは関連コマンド、SNMPv3 機能のコマンドへのアクセスが許可されていたとしても、SNMPv3 コミュニティ、ユーザ、グループを作成することができません。

SNMPv3 ユーザはグループで管理されます。グループのすべての SNMPv3 ユーザは同じセキュリティモデルを共有しますが、異なる認証、プライバシーキーの設定を使用することができます。ユーザのセキュリティモデルを設定し、SNMP 間の通信が失敗しないようにするため、グループのセキュリティモデルの設定とセキュリティキーは、表 5-1に従い、NMS の設定に合わせる必要があります。

表 5-1 異なるセキュリティモデルの基本セキュリティの設定要件

セキュリティモデル	グループのセキュリティモデルキーワード	ユーザのセキュリティキー設定	補足
プライバシーあり、認証あり	privacy	認証キー、 プライバシーキー	認証キーあるいはプライバシーキーが設定されていない場合、SNMP 間の通信は失敗します。
プライバシーなし、認証あり	authentication	認証キー	認証キーが設定されていない場合、SNMP間の通信は失敗します。 ユーザのプライバシーキー（ある場合）は影響しません。
認証なし、プライバシーなし	authentication あるいはprivacyのいずれもありません。	なし	認証キー、プライバシーキーが設定されても適用されません。

以下に SNMPv3 基本パラメータの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2.（オプション設定項目） SNMP エージェントを有効にする	**snmp-agent**	デフォルト：無効 **snmp-agent calculate-password** コマンドを除いた**snmp-agent** で始まるいずれかのコマンドで SNMP エージェントを有効にできます。

操作	コマンド	補足
3.　（オプション設定項目） システム連絡先を設定する	**snmp-agent sys-info contact** *sys-contact*	デフォルト：設定なし
4.　（オプション設定項目） システム所在地を設定する	**snmp-agent sys-info location** *sys-location*	デフォルト：設定なし
5.　SNMPv3 を有効にする	**snmp-agent sys-info version** { **all** | { **v1** | **v2c** | **v3** } * }	デフォルト：SNMPv3が有効です。
6.　（オプション設定項目） ローカルエンジン ID を設定する	**snmp-agent local-engineid** *engineid*	デフォルト：ローカルエンジン ID はCompany ID＋ device ID です。 ⚠ **重要：** ローカルエンジンIDの変更後、既存のSNMPv3ユーザと暗号キーは無効になります。SNMPv3ユーザと暗号キーを再設定してください。
7.　（オプション設定項目） MIB view を作成または更新する	**snmp-agent mib-view** { **excluded** | **included** } *view-name oid-tree* [**mask** *mask-value*]	デフォルト：**ViewDefault** このviewは**iso**サブツリーのすべてのオブジェクトが対象ですが、**snmpUsmMIB**と**snmpVacmMIB**と**snmpModules.18**はアクセス可能です。 *view-name*、*old-tree*のペアはそれぞれviewのレコードを表します。別のMIBサブツリーマスクに同じレコード名を複数回指定した場合、最後の設定が有効です。
8.　（オプション設定項目）SNMPv3 グループを作成する	**snmp-agent group v3** *group-name* [**authentication** | **privacy**] [**read-view** *read-view*] [**write-view** *view-name*] [**notify-view** *view-name*] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } | **acl ipv6** { *ipv6-acl-number* | **name** *ipv6-acl-name* }]*	デフォルト：設定なし
9.　（オプション設定項目） 平文テキストキーを暗号キーに変換する	**snmp-agent calculate-password** *plain-password* **mode** { **3desmd5** | **3dessha** | **md5** | **sha** } { **local-engineid** | **specified-engineid** *engineid* }	–
10. SNMPv3ユーザを作成する	**snmp-agent usm-user v3** *user-name group-name* [{ **cipher** | **simple** } **authentication-mode** { **md5** | **sha** } *auth-password* [**privacy-mode** { **3des** | **aes128** | **des56** } *priv-password*]] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } | **acl ipv6** { *ipv6-acl-number* | **name** *ipv6-acl-name* }]*	**cipher**キーワードが指定されると、*auth-password*と*priv-password*は暗号キーとして使用されます。

操作	コマンド	補足
11.（オプション設定項目）SNMP エージェントが送受信できる SNMP パケットの最大バイトサイズ（バイト）を設定する	**snmp-agent packet max-size** *byte-count*	デフォルト：1500バイト

5.3 SNMPロギングの設定

必要なときのみ SNMP ロギングを設定してください。SNMP ロギングを設定するとメモリに負担をかけ、装置の性能に影響を与える可能性があります。

SNMP エージェントは、GET リクエスト、SET リクエスト、SET 応答、SNMP 通知、SNMP 認証失敗をロギングしますが、GET 応答はロギングしません。

- **GET オペレーション** – エージェントは NMS の IP アドレス、アクセスノード名、ノード OID をロギングします。
- **SET オペレーション** – エージェントは NMS の IP アドレス、アクセスノード名、ノード OID、変数値、エラーコード、エラーインデックスをロギングします
- **通知トラッキング** – NMS に SNMP 通知を送信したのち、エージェントをロギングします。
- **SNMP 認証失敗** – エージェントは SNMP 認証の失敗をロギングします。

SNMP モジュールは Information Center にログを送信します。

コンソールやログバッファなどの特定の宛先にメッセージを出力するため、Information Center を設定することができます。各ログエントリのノードフィールド（MIB ノード名）と値フィールド（MIB ノードの値）の合計最大サイズは 1024 バイトです。最大サイズを超過した場合、Information Center はフィールドのデータを切り捨てます。Information Center の詳細は、オペレーションマニュアルのセクション 11 *システム管理*“*Information Center*”を参照してください。

以下に SNMP ロギングの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	–
2.（オプション設定項目）SNMP ロギングを有効にする	**snmp-agent log** { **all** | **authfail** | **get-operation** | **set-operation** }	デフォルト：無効
3.（オプション設定項目）SNMP 通知ロギングを有効にする	**snmp-agent trap log**	デフォルト：無効

5.4 SNMP通知の設定

SNMP エージェントはリンク状態の変更やユーザログイン、ログアウトなどの重要なイベントの notification （trap、inform）を NMS に通知します。特に説明がない限り、コマンドラインの **trap** キーワードは trap と inform を含みます。

5.4.1 SNMP notification の有効化

必要なときのみ SNMP notification を有効にしてください。SNMP notification はメモリに負担をかけ、装置の性能に影響を与える可能性があります。

インタフェースのリンク状態が変更したとき、以下を行ってください。

- **snmp-agent trap enable standard** [**linkdown** | **linkup**] *コマンドを設定し、グローバルで linkUp あるいは linkDown notification を有効にしてください。
- インタフェースで **enable snmp trap updown** コマンドを設定し、インタフェースで linkUp あるいは linkDown notification を有効にしてください。

モジュールで notification を有効にした後、notification がモジュールの設定に依存して作成されます。詳細は、各モジュールの設定ガイドを参照してください。

以下に SNMP notification を有効にする設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． notification を有効にする	**snmp-agent trap enable** [**configuration** | *protocol* | **standard** [**authentication** | **coldstart** | **linkdown** | **linkup** | **warmstart**] * | **system**]	デフォルト：**configuration**、**standard**、**system**が有効です。ほかのSNMP notificationはモジュールによって変わります。
3． interface view に移行する	**interface** *interface-type interface-number*	―
4． リンク状態の notification を有効にする	**enable snmp trap updown**	デフォルト：有効

5.4.2 ホストへ notification を送信する SNMP エージェントの設定

ホストに trap あるいは inform する notification を送信する SNMP エージェントを設定することができます。一般的にホストは NMS で、解析や管理に使われます。trap を受信したとき、NMS は trap を受信するとき確認応答を送信しないため、trap は inform よりも少ないリソースで使用することができます。

I. 設定ガイドライン

ネットワークの輻輳が発生する、あるいは宛先に到達できないとき、SNMP エージェントはキューに notification をバッファします。キューのサイズと notification の保持時間（キューに保持できる最大時間）を設定することができます。notification は保持時間が満了したとき削除されます。notification のキューが一杯になったとき、もっとも古い notification が自動的に削除されます。

インタフェースの説明やインタフェースタイプを追加させるため、標準 linkUp/linkDown notification を拡張することができますが、NMS が拡張 SNMP メッセージをサポートしていることを確認する必要があります。

inform を送信するために、以下を確認してください。

- SNMP エージェントと NMS は SNMPv2c あるいは SNMPv3 を使用します。

- SNMPv3 が使用される場合、SNMPv3 基本設定を行う際に NMS の SNMP エンジン ID を設定してください。また SNMPv3 ユーザを作成するとき、SNMP エンジンの IP アドレスを指定してください。

II. 設定要件

- NMS として基本 SNMP の設定と同じように SNMP エージェントを設定してください。SNMPv1 あるいは SNMPv2c を使用する場合、コミュニティ名を設定してください。SNMPv3 を使用する場合、notification の SNMPv3 ユーザ、MIB view を設定してください。
- SNMP エージェントと NMS が互いに到達可能であるようにしてください。

III. 設定手順

以下にホストに notification を送信する SNMP エージェントの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	–
2. 宛先ホストを設定する	• （アプローチ1）宛先ホストに trapを送信する： **snmp-agent target-host trap address udp-domain** { *ipv4-address* | **ipv6** *ipv6-address* } [**udp-port** *port-number*] **params securityname** *security-string* [**v1** | **v2c** | **v3** [**authentication** | **privacy**]] • （アプローチ2）宛先ホストに informを送信する： **snmp-agent target-host inform address udp-domain** { *ipv4-address* | **ipv6** *ipv6-address* } [**udp-port** *port-number*] **params securityname** *security-string* { **v2c** | **v3** [**authentication** | **privacy**] }	どちらか一方を使用します。 デフォルト：設定なし
3. （オプション設定項目）notificationの送信元アドレスを設定する	**snmp-agent** { **inform** | **trap** } **source** *interface-type interface-number*	デフォルト：SNMPは送信元IPアドレスとして出力インタフェースのIPアドレスを使用します。
4. （オプション設定項目） 拡張 linkUp/linkDown notification を有効にする	**snmp-agent trap if-mib link extended**	デフォルト：標準 linkUp/linkDown notificationを使用します
5. （オプション設定項目）notificationキューサイズを設定する	**snmp-agent trap queue-size** *size*	デフォルト：100
6. （オプション設定項目）notificationライフタイムを設定する	**snmp-agent trap life** *seconds*	デフォルト：120秒

5.5 SNMPの表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
連絡先、所在地、SNMP のバージョンを含むSNMPエージェントのシステム情報を表示する	**display snmp-agent sys-info** [**contact** | **location** | **version**]*
SNMPエージェント統計情報を表示する	**display snmp-agent statistics**
ローカルエンジンIDを表示する	**display snmp-agent local-engineid**
SNMPグループ情報を表示する	**display snmp-agent group** [*group-name*]
notificationキューの基本情報を表示する	**display snmp-agent trap queue**
notificationを送信できるモジュールおよびnotificationの状態（有効あるいは無効）を表示する	**display snmp-agent trap-list**
SNMPv3ユーザ情報を表示する	**display snmp-agent usm-user** [**engineid** *engineid* | **group** *group-name* | **username** *user-name*]*
SNMP v1または SNMP v2c のコミュニティ情報を表示する	**display snmp-agent community** [**read** | **write**]
MIB view情報を表示する	**display snmp-agent mib-view** [**exclude** | **include** | **viewname** *view-name*]

5.6 設定例

5.6.1 SNMPv1/SNMPv2c の設定例

SNMPv1 の設定手順は SNMPv2c 設定手順と同一です。この設定例は SNMPv1 を使用します。

I. ネットワーク要件

図 5-3に示すように、NMS（1.1.1.2/24）は SNMPv1 で SNMP エージェント（1.1.1.1/24）を管理します。エージェントはイベントを報告する notification を NMS に自動的に送信します。

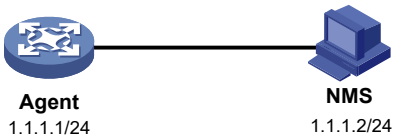


図 5-3 ネットワーク図

II. 設定手順

1)　SNMP エージェントを設定します。

エージェントの IP アドレスを設定し、NMS と通信可能であることを確認します。（詳細は省略します。）

SNMPv1 を指定し、読み込みのみのコミュニティ **public** と読み書き可能なコミュニティ **private** を生成します。

```
<Agent> system-view
[Agent] snmp-agent sys-info version v1
[Agent] snmp-agent community read public
[Agent] snmp-agent community write private
```

エージェントの連絡先と所在地情報を設定します。

```
[Agent] snmp-agent sys-info contact NEC
[Agent] snmp-agent sys-info location Tokyo
```

SNMP notification を有効にし、SNMP trap の宛先として IP アドレスが 1.1.1.2 の NMS を設定し、コミュニティ名として **public** を使用します。（NMS が trap を受信できること確認するため、**snmp-agent target-host** コマンドで設定されている SNMP のバージョンを NMS と同一に指定します。）

```
[Agent] snmp-agent trap enable
[Agent] snmp-agent target-host trap address udp-domain 1.1.1.2 params securityname public v1
```

2)　SNMP NMS を設定します。

- □　SNMPv1 を指定します。
- □　読み込みのみのコミュニティ **public** と読み書き可能なコミュニティ **private** を作成します。
- □　必要に応じて、タイムアウト時間と再トライを行う最大数を設定します。

NMS の設定についての詳細は、NMS のマニュアルを参照してください。

🕮 **メモ：**

エージェントと NMS の SNMP 設定は同一にする必要があります。

III. 設定の確認

エージェントから Null0 インタフェースの MTU 値を取得します。取得に成功します。

```
Send request to 1.1.1.1/161 ...
Protocol version: SNMPv1
Operation: Get
Request binding:
1: 1.3.6.1.2.1.2.2.1.4.135471
Response binding:
1: Oid=ifMtu.135471 Syntax=INT Value=1500
Get finished
```

エージェントの MIB ノードの値を取得するため、wrong コミュニティ名を使用します。NMS で trap の認証に失敗していることがわかります。

```
1.1.1.1/2934 V1 Trap = authenticationFailure
SNMP Version = V1
Community = public
Command = Trap
Enterprise = 1.3.6.1.4.1.43.1.16.4.3.50
GenericID = 4
SpecificID = 0
Time Stamp = 8:35:25.68
```

5.6.2 SNMPv3 の設定例

I. ネットワーク要件

図 5-4に示すように、NMS（1.1.1.2/24）は SNMPv3 でエージェント（1.1.1.1/24）のインタフェース状態をモニタし管理します。エージェントはイベントを通知する notification を NMS に自動的に送信します。

NMS とエージェントは SNMP セッションを構成するときに認証を行います。認証アルゴリズムは SHA-1 で、認証キーは **123456TESTauth&!**です。NMS とエージェント間のパケットは、AES アルゴリズム、プライバシーキー**123456TESTencr&!**で暗号化されます。

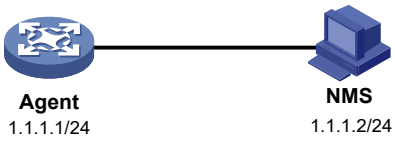


図 5-4 ネットワーク図

II. 設定手順

1)　SNMP エージェントを設定します。

エージェントの IP アドレス 1.1.1.1/24 を設定し、NMS と通信可能であることを確認します。（詳細は省略します。）

SNMPv3 グループ **managev3group** を作成します。test view の SNMPv3 グループ **managev3group** に、アクセス権限を設定します。snmpMIB ノード（OID：1.3.6.1.6.3.1）下のオブジェクト（linkUp オブジェ気宇と、linkDown オブジェクトを含みます。）を読み込みのみできるように設定し、ほかの MIB オブジェクトはアクセスできないようにします。

```
<Agent> system-view
[Agent] undo snmp-agent mib-view ViewDefault
[Agent] snmp-agent mib-view included test snmpMIB
[Agent] snmp-agent group v3 managev3group privacy read-view test
```

SNMPv3 グループ **managev3group** にアクセス権限を設定します。test view のシステムノード（OID：1.3.6.1.2.1.1）とインタフェースノード（OID：1.3.6.1.2.1.2）下のオブジェクトを読み書きできるように設定します。

```
[Agent] snmp-agent mib-view included test 1.3.6.1.2.1.1
[Agent] snmp-agent mib-view included test 1.3.6.1.2.1.2
[Agent] snmp-agent group v3 managev3group privacy read-view test write-view test
```

ユーザ **VACMtest** を、SNMPv3 グループ **managev3group** に追加し、認証アルゴリズム **sha**、認証キー**123456TESTauth&!**、暗号化アルゴリズム **aes128**、プライバシーキー**123456TESTencr&!**を設定します。

```
[Agent] snmp-agent usm-user v3 VACMtest managev3group simple authentication-mode sha 123456TESTauth&! privacy-mode aes128 123456TESTencr&!
```

エージェントの連絡先と所在地情報を設定します。

```
[Agent] snmp-agent sys-info contact NEC
[Agent] snmp-agent sys-info location Tokyo
```

エージェントで notifications を有効にします。Trap の宛先として 1.1.1.2 の NMS を指定し、Trap のユーザ名を **VACMtest** に設定します。

```
[Agent] snmp-agent trap enable
[Agent] snmp-agent target-host trap address udp-domain 1.1.1.2 params VACMtest v3 privacy
```

2) SNMP NMS を設定します。
   - □ SNMPv3 を指定します。
   - □ SNMPv3 ユーザ **VACMtest** を作成します。
   - □ 認証機能とプライバシー機能の両方を有効にしてください。
   - □ 認証に **SHA-1** を使用し、暗号化に **AES** を設定してください。
   - □ 認証キー**123456TESTauth&!**とプライバシーキー**123456TESTencr&!**を設定してください。
   - □ 必要に応じて、タイムアウト時間と再トライを行う最大数を設定します。

NMS の設定についての詳細は、NMS のマニュアルを参照してください。

🕮 **メモ：**

エージェントと NMS の SNMP 設定は同一にする必要があります。

III. 設定の確認

エージェントにアクセスするためユーザ名 VACMtest を使用します。

sysName ノードの値を回復します。値 Agent が戻ります。

Sysname に sysName ノードの値を設定します。取得に成功します。

エージェントでインタフェースをシャットダウンあるいはアップにします。NMS は linkUP （OID：1.3.6.1.6.3.1.1.5.4） あるいは linkDown （OID：1.3.6.1.6.3.1.1.5.3）の notification を受信します。

目次

このセクションのページは **11-x-x** です。

6 章 RMON 6-1
6.1 概要 6-1
6.1.1 RMON グループ 6-1
6.1.2 アラームグループとプライベートアラームグループのサンプルタイプ 6-3
6.1.3 プロトコルと標準 6-4
6.2 RMON 統計機能の設定 6-4
6.2.1 RMON イーサネット統計機能エントリの作成 6-4
6.2.2 RMON 履歴管理エントリの作成 6-4
6.2.3 RMON アラーム機能の設定 6-5
6.3 RMON の表示と維持 6-6
6.4 RMON 設定例 6-7
6.4.1 イーサネット統計情報グループの設定例 6-7
6.4.2 履歴グループの設定例 6-7
6.4.3 アラーム機能の設定例 6-8

6章 RMON

6.1 概要

RMON（Remote Monitoring）は、SNMP を拡張した機能です。リモートモニタリングとネットワーク装置とサブネットの管理を行います。RMON モニタ（ネットワーク装置に組み込まれた RMON エージェント）は定期的に、または継続的に、ポートに接続されたネットワークのトラフィック統計情報を収集します。統計情報がアラームのしきい値を超えたとき、管理対象装置は、自動的にトラップを送信することができます。NMS は、常に MIB 変数をポーリングし結果を比較する必要はありません。

RMON は、例外条件の NMS を通知するために SNMP トラップを使用しています。RMON SNMP トラップは、ブロードキャストトラフィックのしきい値を超過したトラフィックイベントなど、様々なイベントを報告します。対照的に、SNMP 標準トラップは、リンクアップ、リンクダウン、モジュールの障害などの装置の動作状態の変化を報告します。

SNMP の詳細は、オペレーションマニュアルのセクション 11 *システム管理* "*SNMP*"を参照してください。

NEC は、RMON モニタとして、組み込み RMON エージェントの機能を提供しています。NMS は RMON MIB にアクセスすることで基本的な SNMP の動作を行うことができます。

6.1.1 RMON グループ

標準 RMON グループのうち、NEC では、統計情報グループ、履歴グループ、イベントグループ、アラームグループ、プローブ設定グループ、およびユーザ履歴グループをサポートします。プローブ設定グループとユーザ履歴グループは CLI から設定できません。設定を行うために MIB にアクセスする必要があります。

I. 統計情報グループ

統計情報グループは、モニタされたイーサネットインタフェースのトラフィック情報の統計情報を取得し、イーサネット統計情報テーブル（ethernetStatsTable）の統計情報を記録します。統計情報は以下があります。

- ネットワークの衝突数
- CRC アライメントエラー
- アンダーサイズ/オーバーサイズパケット
- ブロードキャスト数
- マルチキャスト数
- 受信バイト数
- 受信パケット数

イーサネット統計情報テーブルの統計情報は統計情報の総数です。

II. 履歴グループ

履歴グループは、定期的にインタフェース上のトラフィック情報の統計情報を収集し、履歴レコードテーブル（ethernetHistoryTable）の統計情報を記録します。統計情報は以下があります。

- 帯域幅使用率
- エラーパケット数
- パケットの合計数

履歴レコードテーブルは各サンプリング間隔でインタフェースに受信されたトラフィックの統計情報を記録します。

III. イベントグループ

イベントグループは、アラームグループとプライベートアラームグループで定義されているアラームによって発生したイベントの作成と通知を制御します。RMON アラームイベントは以下の方法で処理されます。

- **Log**－イベントログテーブル内のイベント情報（発生したイベント時間、イベントの内容を含みます。）をロギングします。管理装置は、SNMP Get 操作によってログを収集することができます。
- **Trap**－イベントが発生したとき、NMS に SNMP 通知を送信します。
- **Log-Trap**－イベントログテーブルのイベント情報をロギングし、イベントが発生したときに、SNMP 通知を送信します。
- **None**－処理を行いません。

IV. アラームグループ

RMON アラームグループは、インタフェース上の受信パケット（etherStatsPkts）のカウントなどのアラーム変数をモニタします。アラームエントリを作成したのち、RMON エージェントは指定した間隔でモニタアラーム変数の値を取得します。モニタ対象の変数の値が増加方向のしきい値を超えると、増加方向のイベントが発生します。変数の値が減少方向のしきい値を下回ると、減少方向のイベントが発生します。その後イベントは、イベントグループで定義したように処理されます。

アラームエントリがしきい値を連続して複数回交差する場合、RMON エージェントは、最初のしきい値が交差したときにアラームイベントを発生します。サンプリングされた値が増加方向あるいは減少方向のしきい値を超えた時点で 1 つのイベントが発生します。反対方向のしきい値を超えるまで次のイベントは発生しません。たとえば、図 6-1に示すように、増加方向のしきい値を超えると 1 つのイベントが発生し、減少方向のしきい値を超えるまで次のイベントは発生しません。

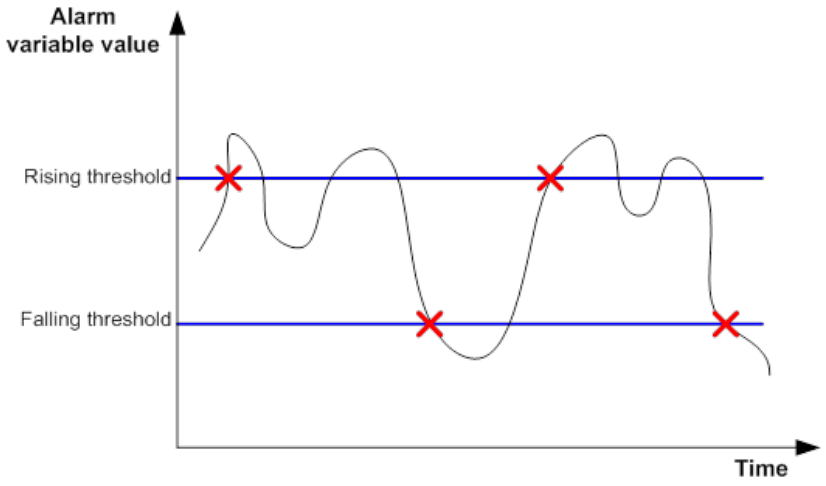


図 6-1 増加方向と減少方向のアラームイベント

V. プライベートアラームグループ

プライベートアラームグループは複数のアラーム変数の値を計算し、計算結果を定義済みの増加方向と減少方向のしきい値と比較します。

RMON エージェントは変数をサンプリングし、プライベートアラームにもとづいたアラームアクションを以下のように行います。

1) ユーザ定義した形式のプライベートアラーム変数をサンプリングします。
2) 定義した形式にもとづいてサンプリングした値を計算します。
3) 定義されたしきい値と計算した値を比較し、以下のいずれかのアクションを行います。
   - □ 比較結果が増加方向のしきい値以上である場合、増加方向のアラームイベントに関するイベントをトリガします。
   - □ 比較結果が減少方向のしきい値以下である場合、減少方向のアラームイベントに関するイベントをトリガします。

アラームエントリがしきい値を連続して複数回交差する場合、RMON エージェントは、最初のしきい値が交差したときにアラームイベントを発生します。サンプリングされた値が増加方向あるいは減少方向のしきい値を超えた時点で 1 つのイベントが発生します。反対方向のしきい値を超えるまで次のイベントは発生しません。たとえば、増加方向のしきい値を超えると 1 つのイベントが発生し、減少方向のしきい値を超えるまで次のイベントは発生しません。

6.1.2 アラームグループとプライベートアラームグループのサンプルタイプ

RMON エージェントは以下のサンプルタイプをサポートします。

- **absolute**– RMON は、サンプル値をしきい値と直接比較します。増加方向のしきい値と減少方向のしきい値の変数を、サンプリングした後に比較します。
- **delta**– RMON は現在のサンプル値を最後に取得したサンプル値から引き、その差を増加方向のしきい値と減少方向のしきい値と比較します。

6.1.3 プロトコルと標準

- RFC 4502, *Remote Network Monitoring Management Information Base Version 2*
- RFC 2819, *Remote Network Monitoring Management Information Base Status of this Memo*

6.2 RMON統計機能の設定

RMON 統計機能はイーサネット統計グループと履歴グループによって実装されます。

イーサネット統計グループはイーサネット統計情報テーブルで定義された変数であり、記録されたコンテンツは、統計エントリが現在時刻に作成された時点からの変数の合計です。設定の詳細は、オペレーションマニュアルのセクション 11 *システム管理* "*RMON*"の"*RMON イーサネット統計機能エントリの作成*"を参照してください。

ヒストリグループは、各サンプリング間隔の変数で収集された統計情報を提供します。ヒストリグループは収集を管理するため、履歴管理テーブルを使用し、履歴テーブルに収集された統計情報を記録します。設定の詳細は、オペレーションマニュアルのセクション 11 *システム管理* "*RMON*"の"*RMON 履歴管理エントリの作成*"を参照してください。

6.2.1 RMON イーサネット統計機能エントリの作成

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. interface view に移行する	**interface** *interface-type interface-number*	―
3. RMON 統計情報テーブルにインタフェースのエントリを作成する	**rmon statistics** *entry-number* [**owner** *text*]	デフォルト：設定なし 1つのイーサネットインタフェースに1つの統計エントリを作成できます。

6.2.2 RMON 履歴管理エントリの作成

1 つのインタフェースに複数の履歴管理エントリを設定することができますが、エントリ数とサンプリング間隔は同一にしてはいけません。

指定したバケットサイズが有効な履歴テーブルサイズを超過しても、履歴管理エントリを作成することができます。RMON はバケットサイズを可能な限り予期したサイズに設定します。

以下に RMON 履歴管理エントリの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. interface view に移行する	**interface** *interface-type interface-number*	―

操作	コマンド	補足
3. RMON 履歴管理テーブルにインタフェースのエントリを作成する	**rmon history** *entry-number* **buckets** *number* **interval** *sampling-interval* [**owner** *text*]	デフォルト：設定なし

6.2.3 RMON アラーム機能の設定

RMON アラーム機能を設定するときに、以下のガイドラインに従ってください。

- RMON アラーム機能の設定を行う前、アラームが発生したとき NMS に通知するため、SNMP エージェントを設定してください。SNMP エージェントについては、オペレーションマニュアルのセクション 11 *システム管理*"*SNMP*"を参照してください。
- 新しいイベント、アラーム、プライベートアラームを作成するために以下の条件が必要です。
  - □ 新しいエントリのパラメータは、すでに存在するエントリと同じにすることはできません。
  - □ エントリ数が最大になっていないこと。

表 6-1に比較されるパラメータとエントリの制限を示します。

表 6-1 RMON の設定制限

エントリ	比較パラメータ	エントリの最大数
イベント	● イベント記述（**description** *string*） ● イベントタイプ（**log**、**trap**、**logtrap**、**none**） ● コミュニティ名（*security-string*）	60
アラーム	● アラーム変数（*alarm-variable*） ● サンプリング間隔（*sampling-interval*） ● サンプルタイプ（**absolute**、**delta**） ● 増加方向のしきい値（*threshold-value1*） ● 減少方向のしきい値 （*threshold-value2*）	60
プライベートアラーム	● アラーム変数式（*prialarm-formula*） ● サンプリング間隔（*sampling-interval*） ● サンプルタイプ（**absolute**、**delta**） ● 増加方向のしきい値（*threshold-value1*） ● 減少方向のしきい値 （*threshold-value2*）	50

以下に RMON アラーム機能の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. （オプション設定項目）イベントテーブルにイベントエントリを作成する	**rmon event** *entry-number* [**description** *string*] { **log** | **log-trap** *security-string* | **none** | **trap** *security-string* } [**owner** *text*]	デフォルト：設定なし

操作	コマンド	補足
3. アラームテーブルあるいはプライベートアラームテーブルにエントリを作成する	• アラームテーブルにエントリを作成する： **rmon alarm** *entry-number alarm-variable sampling-interval* { **absolute** | **delta** } [**startup-alarm** { **falling** | **rising** | **rising-falling** }] **rising-threshold** *threshold-value1 event-entry1* **falling-threshold** *threshold-value2 event-entry2* [**owner** *text*] • プライベートアラームテーブルにエントリを作成する： **rmon prialarm** *entry-number prialarm-formula prialarm-des sampling-interval* { **absolute** | **delta** } [**startup-alarm** { **falling** | **rising** | **rising-falling** }] **rising-threshold** *threshold-value1 event-entry1* **falling-threshold** *threshold-value2 event-entry2* **entrytype** { **forever** | **cycle** *cycle-period* } [**owner** *text*]	デフォルト：設定なし アラームを作成されていないイベントと関連付けることができますが、イベントを設定したのち、アラームが動作します。

6.3 RMONの表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
RMON統計情報を表示する	**display rmon statistics** [*interface-type interface-number*]
RMON履歴管理エントリと履歴サンプルを表示する	**display rmon history** [*interface-type interface-number*]
RMONアラームエントリを表示する	**display rmon alarm** [*entry-number*]
RMONプライベートアラームエントリを表示する	**display rmon prialarm** [*entry-number*]
RMONイベントエントリを表示する	**display rmon event** [*entry-number*]
イベントエントリのログ情報を表示する	**display rmon eventlog** [*entry-number*]

6.4 RMON設定例

6.4.1 イーサネット統計情報グループの設定例

I. ネットワーク要件

図 6-2に示すように、GigabitEthernet 1/0/1 のトラフィックの統計情報の合計を収集するため、Device 上で RMON イーサネット統計情報グループエントリを作成します。

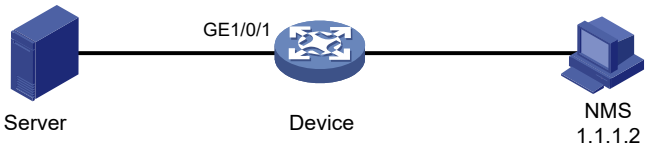


図 6-2 ネットワーク図

II. 設定手順

GigabitEthernet 1/0/1 の RMON イーサネット統計情報エントリを作成します。

```
<Device> system-view
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] rmon statistics 1 owner user1
```

GigabitEthernet 1/0/1 の RMON エージェントで収集された統計情報を表示します。

```
<Device> display rmon statistics gigabitethernet 1/0/1
EtherStatsEntry 1 owned by user1 is VALID.
  Interface : GigabitEthernet1/0/1<ifIndex.3>
  etherStatsOctets          : 21657     , etherStatsPkts           : 307
  etherStatsBroadcastPkts   : 56        , etherStatsMulticastPkts  : 34
  etherStatsUndersizePkts   : 0         , etherStatsOversizePkts   : 0
  etherStatsFragments       : 0         , etherStatsJabbers        : 0
  etherStatsCRCAlignErrors  : 0         , etherStatsCollisions     : 0
  etherStatsDropEvents (insufficient resources): 0
  Incoming packets by size:
  64      : 235       ,  65-127   : 67        ,  128-255   : 4
  256-511: 1          ,  512-1023: 0          ,  1024-1518: 0
```

#NMS から SNMP Get 操作を行いトラフィックの統計情報を取得します。(詳細は省略します。)

6.4.2 履歴グループの設定例

I. ネットワーク要件

図 6-3に示すように、1 分ごとの GigabitEthernet 1/0/1 のトラフィックの統計情報をサンプリングするため、Device 上で RMON 履歴管理エントリを作成します。

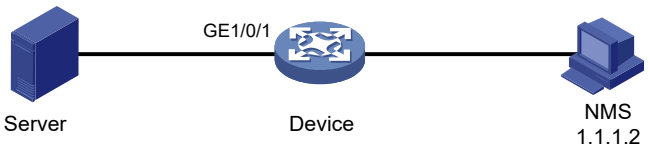


図 6-3 ネットワーク図

II. 設定手順

1 分ごとの GigabitEthernet 1/0/1 のトラフィックの統計情報をサンプリングするため、RMON 履歴管理エントリを作成します。履歴統計テーブルに最大 8 つのインタフェース用のサンプルを記録します。

```
<Device> system-view
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] rmon history 1 buckets 8 interval 60 owner user1
```

GigabitEthernet 1/0/1 で収集された履歴統計情報を表示します。

```
[Device-GigabitEthernet1/0/1] display rmon history
HistoryControlEntry 1 owned by user1 is VALID
  Sampled interface     : GigabitEthernet1/0/1<ifIndex.3>
  Sampling interval     : 60(sec) with 8 buckets max
  Sampling record 1 :
    dropevents        : 0         , octets               : 834
    packets           : 8         , broadcast packets    : 1
    multicast packets : 6         , CRC alignment errors : 0
    undersize packets : 0         , oversize packets     : 0
    fragments         : 0         , jabbers              : 0
    collisions        : 0         , utilization          : 0
  Sampling record 2 :
    dropevents        : 0         , octets               : 962
    packets           : 10        , broadcast packets    : 3
    multicast packets : 6         , CRC alignment errors : 0
    undersize packets : 0         , oversize packets     : 0
    fragments         : 0         , jabbers              : 0
    collisions        : 0         , utilization          : 0
```

NMS から SNMP Get 操作を行いトラフィックの統計情報を取得します。（詳細は省略します。）

6.4.3 アラーム機能の設定例

I. ネットワーク要件

図 6-4に示すように、GigabitEthernet 1/0/1 の入力トラフィックの入力トラフィックの統計情報をモニタし、以下のイベントが発生するとき、SNMP でアラームを送信します。

- サンプリング間隔の値が 5 秒で、増加方向のしきい値（100）を超えます。
- サンプリング間隔の値が 5 秒で、減少方向のしきい値（50）を下回ります。

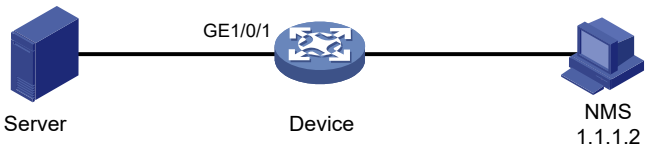


図 6-4 ネットワーク図

II. 設定手順

1.1.1.2 の NMS の SNMP 設定と同様に、SNMP エージェント（Device）の設定を行います。この例では SNMPv1、public コミュニティの読み込み、プライベートコミュニティの書き込みの設定を使用します。

```
<Device> system-view
[Device] snmp-agent
[Device] snmp-agent community read public
[Device] snmp-agent community write private
[Device] snmp-agent sys-info version v1
[Device] snmp-agent trap enable
[Device] snmp-agent trap log
[Device] snmp-agent target-host trap address udp-domain 1.1.1.2 params securityname public
```

GigabitEthernet 1/0/1 の RMON イーサネット統計情報エントリを作成します。

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] rmon statistics 1 owner user1
[Device-GigabitEthernet1/0/1] quit
```

#ノード 1.3.6.1.2.1.16.1.1.1.4.1 の delta サンプル値が 100 を超えた場合、あるいは 50 を下回った場合、SNMP 通知を送信するために RMON イベントエントリ、RMON アラームエントリを作成します。

```
[Device] rmon event 1 trap public owner user1
[Device] rmon alarm 1 1.3.6.1.2.1.16.1.1.1.4.1 5 delta rising-threshold 100 1 falling-threshold 50 1 owner user1
```

🕮 メモ：

1.3.6.1.2.1.16.1.1.1.4.1 は GigabitEthernet 1/0/1 のオブジェクトインスタンスです。ここで 1.3.6.1.2.1.16.1.1.1.4 は入力トラフィックの合計オブジェクトを示し、1 は GigabitEthernet 1/0/1 の RMON イーサネット統計情報エントリインデックスです。

RMON アラームエントリを表示します。

```
<Device> display rmon alarm 1
AlarmEntry 1 owned by user1 is VALID.
  Sample type                    : delta
  Sampled variable              : 1.3.6.1.2.1.16.1.1.1.4.1<etherStatsOctets.1>
  Sampling interval (in seconds) : 5
  Rising threshold               : 100(associated with event 1)
  Falling threshold              : 50(associated with event 1)
  Alarm sent upon entry startup  : risingOrFallingAlarm
  Latest value                   : 0
```

GigabitEthernet 1/0/1 の統計情報を表示します。

```
<Device> display rmon statistics gigabitethernet 1/0/1
EtherStatsEntry 1 owned by user1 is VALID.
  Interface : GigabitEthernet1/0/1<ifIndex.3>
  etherStatsOctets         : 57329     , etherStatsPkts          : 455
  etherStatsBroadcastPkts  : 53        , etherStatsMulticastPkts : 353
  etherStatsUndersizePkts  : 0         , etherStatsOversizePkts  : 0
  etherStatsFragments      : 0         , etherStatsJabbers       : 0
  etherStatsCRCAlignErrors : 0         , etherStatsCollisions    : 0
  etherStatsDropEvents (insufficient resources): 0
  Incoming packets by size :
  64     : 7         ,  65-127  : 413       ,  128-255  : 35
  256-511: 0         ,  512-1023: 0         ,  1024-1518: 0
```

アラームが開始したとき、NMS は notification を受信します。

目次

このセクションのページは **11-x-x** です。

7 章 NETCONF 7-1
7.1 概要 7-1
7.1.1 NETCONF の構成 7-1
7.1.2 NETCONF メッセージフォーマット 7-2
7.1.3 NETCONF の使用方法 7-3
7.1.4 プロトコルと標準 7-3
7.2 NETCONF 設定作業リスト 7-4
7.3 NETCONF セッションの確立 7-4
7.3.1 制限とガイドライン 7-4
7.3.2 NETCONF セッション属性の設定 7-5
7.3.3 NETCONF over SOAP セッションの確立 7-5
7.3.4 NETCONF over SSH セッションの確立 7-6
7.3.5 NETCONF over Telnet あるいは NETCONF over console セッションの確立 7-7
7.3.6 capability の交換 7-7
7.4 デバイス設定情報の取得 7-8
7.4.1 制限とガイドライン 7-8
7.4.2 デバイス設定と状態情報の取得 7-8
7.4.3 デフォルト以外の設定の取得 7-10
7.4.4 NETCONF 情報の取得 7-11
7.4.5 YANG ファイルコンテンツの取得 7-12
7.4.6 NETCONF セッション情報の取得 7-12
7.4.7 インタフェーステーブルのデータエントリの取得例 7-13
7.4.8 デフォルト以外の構成データの取得例 7-14
7.4.9 シスログ設定データの取得例 7-15
7.4.10 NETCONF セッション情報の取得例 7-16
7.5 データのフィルタリング 7-17
7.5.1 概要 7-17
7.5.2 制限とガイドライン 7-17
7.5.3 テーブルベースのフィルタリング 7-17
7.5.4 列ベースのフィルタリング 7-17
7.5.5 正規表現と一致するデータのフィルタリング 7-20
7.5.6 条件付き一致によるデータのフィルタリング 7-21
7.6 稼働中の設定のロック、ロック解除 7-22
7.6.1 設定のロック、ロック解除 7-22
7.6.2 制限とガイドライン 7-22
7.6.3 稼働中の設定のロック 7-22
7.6.4 稼働中の設定のロック解除 7-22
7.6.5 稼働中の設定のロック例 7-23
7.7 設定の変更 7-24
7.7.1 <edit-config>オペレーション 7-24
7.7.2 設定手順 7-24
7.7.3 設定の変更例 7-25
7.8 稼働中の設定の保存 7-26
7.8.1 <save>オペレーション 7-26

7.8.2 制限とガイドライン....7-26
7.8.3 設定手順....7-26
7.8.4 稼働中の設定の保存例....7-27
7.9 設定の読み込み....7-27
7.9.1 <load>オペレーション....7-27
7.9.2 設定とガイドライン....7-27
7.9.3 設定手順....7-28
7.10 設定のロールバック....7-28
7.10.1 制限とガイドライン....7-28
7.10.2 設定ファイルにもとづいた設定のロールバック....7-28
7.10.3 ロールバックポイントにもとづいた設定のロールバック....7-29
7.11 NETCONF による CLI オペレーションの実行....7-33
7.11.1 NETCONF による CLI オペレーション....7-33
7.11.2 制限とガイドライン....7-33
7.11.3 設定手順....7-33
7.11.4 CLI オペレーションの実行例....7-33
7.12 イベントの登録....7-34
7.12.1 イベントの登録....7-34
7.12.2 制限とガイドライン....7-34
7.12.3 シスログイベントの登録....7-34
7.12.4 NETCONF によってモニタされるイベントの登録....7-35
7.12.5 モジュールで報告されたイベントの登録....7-36
7.12.6 シスログイベントの登録例....7-37
7.13 NETCONF セッションの終了....7-38
7.13.1 NETCONF セッションの終了....7-38
7.13.2 設定手順....7-38
7.13.3 別の NETCONF セッションの終了例....7-39
7.14 CLI への復帰....7-39

7章 NETCONF

7.1 概要

NETCONF (Network Configuration Protocol)は、XML ベースの、フィルタリング機能を持ったネットワーク管理プロトコルです。NETCONF は、ネットワークデバイスを管理、運用するためにプログラマブルなメカニズムを提供します。NETCONF を使用して、デバイスのパラメータ設定、パラメータ値や統計情報を取得できます。

NETCONF メッセージでは、それぞれのデータは固定の要素として包含されています。これにより、同じベンダの異なるデバイスにおいて、同一のアクセス方法と結果出力を提供することが可能になります。異なるベンダのデバイスにおいても、NETCONF メッセージの XML マッピングにより、同一の効果を得ることも可能になります。異なるベンダの異なるデバイスにより構築されるネットワーク環境において、デバイスの設定と管理をシンプルで能率的に行うために、NETCONF をベースにした NMS システムを開発するし、デバイスを簡単に効率的な方法で設定、管理を行うことができます。

7.1.1 NETCONF の構成

NETCONF は 4 つのレイヤ(content レイヤ、operations レイヤ、RPC レイヤと transport protocol レイヤ)から構成されます。

表 7-1 NETCONF レイヤと XML レイヤ

NETCONF レイヤ	XML レイヤ	説明
Content	コンフィグレーションデータ、状態と統計情報	Contentレイヤは、コンフィグレーションデータ、状態と統計情報からなる管理オブジェクトを含んでいます。設定可能なデータの詳細はデバイスのNETCONF XML APIを参照してください。
Operations	<get>,<get-config>,<edit-config>…	Operationsレイヤは、XMLでエンコードされたパラメータにより記述されたRPC処理として実行される、基本的なオペレーションセットを定義します。NETCONFの基本動作には、データ取得、コンフィグレーション、ロックとセッション処理があります。
RPC	<rpc>,<rpc-reply>	RPCレイヤは、シンプルでトランスポート層に依存しない、RPCエンコードのフレーミングメカニズムを提供します。<rpc>要素と<rpc-rely>要素は、NETCONFの要求と応答のデータ(operationsレイヤとcontentレイヤ)を囲むために使用されます。

NETCONF レイヤ	XML レイヤ	説明
Transport protocol	Console/Telnet/SSH/HTTP/HTTPS/TLS	信頼性の高い接続指向のシリアルデータリンクを提供します。 次のトランスポートレイヤセッションを使用できます。 ● Telnetを介したNETCONF、SSHを介したNETCONF、およびコンソールを介したNETCONFを含むCLIセッション ● NETCONF over HTTPセッションおよびNETCONF over HTTPSセッション ● NETCONF over SOAP over HTTPおよびNETCONF over SOAP over HTTPSを含む、SOAPセッション上のNETCONF

7.1.2 NETCONF メッセージフォーマット

I. NETCONF

すべての NETCONF メッセージは XML ベースであり、RFC4741 に準拠しています。デバイスが受信するすべての NETCONF メッセージは、実際に処理される前に XML スキーマのチェックをパスしなければなりません。もし XML スキーマチェックに失敗すると、デバイスはクライアントにエラーメッセージを送信します。

デバイス、オペレーションデータによってサポートされる NETCONF オペレーションの詳細はデバイスの NETCONF XML API を参照してください。

以下の例は、デバイスの全インタフェースの全パラメータを取得する NETCONF メッセージです。

```
<?xml version="1.0" encoding="utf-8"?>
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <get-bulk>
    <filter type="subtree">
      <top xmlns="http://www.nec.com/netconf/data:1.0">
        <Ifmgr>
          <Interfaces>
                <Interface/>
          </Interfaces>
        </Ifmgr>
      </top>
    </filter>
  </get-bulk>
</rpc>
```

II. NETCONF over SOAP

すべての NETCONF-over-SOAP メッセージは XML ベースで、RFC4741 準拠です。NETCONF メッセージは SOAP（Simple Object Access Protocol）メッセージ中の<BODY>要素で包含されます。また、NETCONF over SOAP メッセージは、以下のルールに従います。

- SOAP メッセージは、SOAP エンベロープの名前空間を使用しなければなりません。
- SOAP メッセージは、SOAP エンコーディングの名前空間を使用しなければなりません。
- SOAP メッセージは、以下の情報を含むことができません。
  - □ DTD 参照
  - □ XML 処理命令

以下の例は、デバイスの全インタフェースのすべてのパラメータを取得する NETCONF-over-SOAP メッセージです。

```
<env:Envelope xmlns:env="http://www.w3.org/2003/05/soap-envelope">
  <env:Header>
    <auth:Authentication                                    env:mustUnderstand="1"
xmlns:auth="http://www.nec.com/netconf/base:1.0">
      <auth:AuthInfo>800207F0120020C</auth:AuthInfo>
    </auth:Authentication>
  </env:Header>
  <env:Body>
    <rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
      <get-bulk>
        <filter type="subtree">
          <top xmlns="http://www.nec.com/netconf/data:1.0">
            <Ifmgr>
              <Interfaces>
                <Interface/>
              </Interfaces>
            </Ifmgr>
          </top>
        </filter>
      </get-bulk>
    </rpc>
  </env:Body>
</env:Envelope>
```

7.1.3 NETCONF の使用方法

NETCONF の表 7-2に示した方法で、デバイスの運用と設定が可能です。

表 7-2 NETCONF のデバイス設定方法

設定ツール	ログイン方法	補足
CLI	• コンソールポート • SSH • Telnet	NETCONFを実行するには、適切なNETCONFメッセージをCLIのXML viewにコピーします。この方法は、開発とテスト目的です。
デバイスの標準Webインタフェース	• HTTP • HTTPS	システムは、Web 設定上のインタフェース操作をNETCONFメッセージに自動的に変換し、デバイスに送信してNETCONFオペレーションを実行します。
専用設定ツール	N/A	この方法を使用するには、NETCONF over SOAP を有効にする必要があります。転送を行うため、NETCONFメッセージはSOAPにカプセル化されます。

7.1.4 プロトコルと標準

- RFC 3339, *Date and Time on the Internet: Timestamps*
- RFC 4741, *NETCONF Configuration Protocol*
- RFC 4742, *Using the NETCONF Configuration Protocol over Secure SHell (SSH)*
- RFC 4743, *Using NETCONF over the Simple Object Access Protocol (SOAP)*
- RFC 5277, *NETCONF Event Notifications*
- RFC 5381, *Experience of Implementing NETCONF over SOAP*
- RFC 5539, *NETCONF over Transport Layer Security (TLS)*
- RFC 6241, *Network Configuration Protocol*

7.2 NETCONF設定作業リスト

作業リスト
(必須設定項目) NETCONFセッションの確立 1.　（オプション設定項目）NETCONF セッションの属性の設定 2.　NETCONF over SOAP セッションの確立 3.　NETCONF over SSH セッションの確立 4.　NETCONF over Telnet あるいは NETCONF over console セッションの確立 5.　capability の交換
（オプション設定項目）デバイス設定情報の取得 • デバイス設定と状態情報の取得 • デフォルト以外の設定の取得 • YANGファイルコンテンツの取得 • NETCONFセッション情報の取得
（オプション設定項目）データのフィルタリング • テーブルベースのフィルタリング • 列ベースのフィルタリング
（オプション設定項目）稼働中の設定のロック、ロック解除 • 稼働中の設定のロック • 稼働中の設定のロック解除
（オプション設定項目）設定の変更
（オプション設定項目）設定ファイルの管理 • 稼働中の設定の保存 • 設定の読み込み • 設定のロールバック
（オプション設定項目）NETCONFによるCLIオペレーションの実行
（オプション設定項目）イベントの登録 • シスログイベントの登録 • NETCONFによってモニタされるイベントの登録 • モジュールで報告されたイベントの登録
（オプション設定項目）NETCONFセッションの終了
（オプション設定項目）CLIへの復帰

7.3 NETCONFセッションの確立

7.3.1 制限とガイドライン

NETCONF セッションが確立した後、デバイスは自動でクライアントに capability を送信します。ほかの NETCONF オペレーションを実行する前に、デバイスにクライアントの capability を送信する必要があります。

NETCONF オペレーションを実行する前に、デバイスで設定あるいは管理しているユーザがいないことを確認してください。複数のユーザが同時にデバイスを設定あるいは管理した場合、予想外の結果が生じる可能性があります。

デバイスは **aaa session-limit** コマンドで NETCONF セッション数の最大値を設定することができます。もし上限に達すると、新しいユーザはデバイスにアクセスできません。

7.3.2 NETCONF セッション属性の設定

I. NETCONF のモジュール固有のネームスペース

NETCONF は以下のタイプのネームスペースをサポートします。

- **共通ネームスペース**– 共通ネームスペースはすべてのモジュールで共有されます。パケットのネームスペースは共通のネームスペースを使用します。ネームスペースは <top>エレメントで示します。モジュールは<top>エレメントの下にリストされます。

例:

```
<rpc message-id="100" xmlns="urn:ietf:Params:xml:ns:netconf:base:1.0">
   <get-bulk>
      <filter type="subtree">
         <top xmlns="http://www.nec.com/netconf/data:1.0">
            <Ifmgr>
               <Interfaces>
               </Interfaces>
            </Ifmgr>
         </top>
      </filter>
   </get-bulk>
</rpc>
```

II. 設定手順

手順	コマンド	補足
1. system view に移行する	**system-view**	ー
2. NETCONF ロギングを有効化する	**netconf log source** { { **agent** | **soap** | **web** } * } { **protocol-operation** { **all** | { **action** | **config** | **get** | **session** | **set** | **syntax** | **others** } * } | **verbose** }	デフォルトは、NETCONF ロギングが無効です。

7.3.3 NETCONF over SOAP セッションの確立

I. NETCONF over SOAP

カスタムユーザインタフェースを使用して、デバイスへの NETCONF over SOAP セッションを確立し、NETCONF オペレーションを実行できます。NETCONF over SOAP は、NETCONF メッセージを SOAP メッセージにカプセル化し、HTTP または HTTPS 経由で SOAP メッセージを送信します。

II. 制限とガイドライン

認証ドメインを SOAP 要求の< UserName >パラメータに追加できます。認証ドメインは、現在の要求でのみ有効です。

III. 設定手順

手順	コマンド	補足
1. system view に移行する	**system-view**	ー

手順	コマンド	補足
2. NETCONF over SOAP を有効化する	**netconf soap { http | https } enable**	デフォルトでは、NETCONF over SOAPが無効です。
3. カスタムユーザインタフェースを使用して、デバイスで NETCONF over SOAP セッションを確立する		カスタムユーザインタフェースの詳細は、インタフェースのユーザガイドを参照してください。

7.3.4 NETCONF over SSH セッションの確立

I. 制限とガイドライン

NETCONF メッセージのフォーマットが正しいことを確認する場合、メッセージをコピーして貼り付けます。手動でメッセージを入力しないでください。

NETCONF オペレーションを実行している間は、NETCONF メッセージの貼り付けや **Enter** キーの押下など、ほかのオペレーションを実行しないでください。

デバイスが NETCONF メッセージを識別するためには、各 NETCONF メッセージの最後に終端文字列“**]]>]]>**”を追加する必要があります。この文書の例は、必ずしもこの終端文字列を持っているわけではありません。 実際のオペレーションには終端文字列を追加してください。

II. 設定要件

NETCONF over SSH セッションを確立する場合、最初に SSH を通してデバイスにログインしてください。

III. 設定手順

操作	コマンド	補足

SSHセッション上で NETCONFを確立する	必要に応じて以下のどちらかのオプションを実行してください。
	• 次のコマンドを順番に実行して、SSHセッション上で NETCONFを確立する
	  • **quit**
	  • **xml**
	• カスタムユーザインタフェースを使用して、デバイスで NETCONF over SSHセッションを確立する
		XML viewプロンプトが表示されるとNETCONF over SSHセッションが正常に確立されます。
		カスタムユーザインタフェースの詳細は、インタフェースのユーザガイドを参照してください。

7.3.5 NETCONF over Telnet あるいは NETCONF over console セッションの確立

I. 制限とガイドライン

NETCONF メッセージのフォーマットが正しいことを確認する場合、メッセージをコピーして貼り付けます。手動でメッセージを入力しないでください。

NETCONF オペレーションを実行している間は、NETCONF メッセージの貼り付けや **Enter** キーの押下など、ほかのオペレーションを実行しないでください。

デバイスが NETCONF メッセージを識別するためには、各 NETCONF メッセージの最後に終端文字列“**]]>]]>**”を追加する必要があります。 この文書の例は、必ずしもこの終端文字列を持っているわけではありません。 実際のオペレーションには終端文字列を追加してください。

II. 設定要件

NETCONF over SSH セッションを確立する場合、最初に Telnet またはコンソールポートを通してデバイスにログインしてください。

III. 設定手順

操作	コマンド	補足
XML viewに移行する	**xml**	user viewで使用可能です。 XML viewプロンプトが表示されると、NETCONF over Telnet あるいはNETCONF over consoleセッションが正常に確立されます。

7.3.6 capability の交換

I. capabilityの交換

NETCONF セッションが確立されると、デバイスはその機能をクライアントに送信します。ほかの NETCONF オペレーションを実行する前に、クライアントの機能をデバイスに送信するために hello メッセージを使用する必要があります。

II. デバイスからクライアントへの Hello メッセージ

```
<?xml version="1.0" encoding="UTF-8"?><hello
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"><capabilities><capability>urn
:ietf:params:netconf:base:1.1</capability><capability>urn:ietf:params:Netconf
:writable-running</capability><capability>urn:ietf:params:netconf:capability:
notification:1.0</capability><capability>urn:ietf:params:netconf:capability:v
alidate:1.1</capability><capability>urn:ietf:params:netconf:capability:interl
eave:1.0</capability><capability>urn:nec:params:netconf:capability:nec-netcon
f-ext:1.0</capability></capabilities><session-id>1</session-id></hello>]]>]]>
```

<capabilities> エレメントはデバイスでサポートします。

<session-id> エレメントは NETCONF セッションに割り当てられて固有の ID を保持します。

III. クライアントからデバイスへの Hello メッセージ

デバイスから hello メッセージを受信した後、次の hello メッセージをコピーして、クライアントがサポートする機能をデバイスに通知します。

```
<hello xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <capabilities>
    <capability>
     capability-set
   </capability>
 </capabilities>
</hello>
```

項目	説明
capability-set	クライアントがサポートする一連の機能を指定します。 各ユーザ定義capabilityセットを囲むには、<capability> タグと </capability>タグを使用します。

7.4 デバイス設定情報の取得

7.4.1 制限とガイドライン

<get>、<get-bulk>、<get-config>、<get-bulk-config> オペレーションを行う間、NETCONF はクライアントにデータを送信する前に取得したデータにある認識できない文字列を(?)に置き換えます。

<get><netconf-state/></get>オペレーションは、データのフィルタリングをサポートしていません。NETCONF オペレーションの詳細はデバイスの NETCONF XML API を参照してください。

7.4.2 デバイス設定と状態情報の取得

次の NETCONF オペレーションを使用して、デバイス設定と状態情報を取得できます。

- **<get> オペレーション**– 指定した条件に一致するすべてのデバイス設定と状態情報を取得します。
- **<get-bulk> オペレーション**– 指定したインデックスのあるデータエントリの隣にあるデータエントリからデータエントリを取得します。1つのデータ入力には、デバイス設定エントリと状態情報エントリが含まれます。 返される出力にはインデックス情報は含まれません。

<get>メッセージと<get-bulk>メッセージは、次のフォーマットを共有します。

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <getoperation>
    <filter>
      <top xmlns="http://www.nec.com/netconf/data:1.0">
          Specify the module, submodule, table name, and column name
      </top>
    </filter>
  </getoperation>
</rpc>
```

項目	説明
getoperation	オペレーション名です。 **get**、**get-bulk**があります。
filter	モジュール名、サブモジュール名、テーブル名、列名などのフィルタ条件を指定します。 ● モジュール名を指定すると、指定したモジュールのデータが取得されます。 モジュール名を指定しない場合、操作はすべてのモジュールのデータを取得します。 ● サブモジュール名を指定すると、指定したサブモジュールのデータが取得されます。 サブモジュール名を指定しない場合、操作はすべてのサブモジュールのデータを取得します。 ● テーブル名を指定すると、指定したテーブルのデータが取得されます。 テーブル名を指定しない場合、操作はすべてのテーブルのデータを取得します。 ● インデックス列のみを指定した場合、操作はすべての列のデータを取得します。 索引列およびその他の列を指定すると、その索引列と指定した列のデータが取得されます。

<get-bulk>メッセージは、**count** 属性と **index** 属性を保持できます。

項目	説明
index	インデックスを指定します。 この項目を指定しない場合、インデックス値はデフォルト1で始まります。
count	データエントリの数を指定します。 **count**属性は、次のルールに準拠しています。 ● **count**属性はモジュールノードおよびテーブルノードに配置できます。 ほかのノードでは、解決できません。 ● **count**属性がモジュールノードに配置されると、子孫ノードに**count**属性が含まれていない場合、子孫ノードはこの**count**属性を継承します。 ● <get-bulk>操作は、次のいずれかの条件が発生した場合に、指定したインデックスのあるデータエントリから始まる残りのデータエントリをすべて取得します。 　• **count**属性は指定しません。 　• 一致するデータエントリの数が**count**属性の値よりも小さいです。

次の<get-bulk>メッセージの例では、**count** 属性と **index** 属性を指定します。

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc      message-id="100"      xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"
xmlns:xc="http://www.nec.com/netconf/base:1.0">
  <get-bulk>
    <filter type="subtree">
      <top                          xmlns="http://www.nec.com/netconf/data:1.0"
xmlns:base="http://www.nec.com/netconf/base:1.0">
        <Syslog>
          <Logs xc:count="5">
            <Log>
              <Index>10</Index>
           </Log>
            </Logs>
```

```
        </Syslog>
      </top>
    </filter>
  </get-bulk>
</rpc>
```

インタフェース情報を取得する場合、デバイスは、<lfIndex>要素の整数値がインタフェース名またはインデックスを表すかどうかを識別できません。 VPN インスタンス情報を取得する場合、デバイスは<vrfindex>要素の整数値が VPN 名またはインデックスを示すかどうかを識別できません。問題を解決するには、**valuetype** 属性を使用して値タイプを指定できます。

valuetype 属性には、次の値があります。

値	説明
name	<lfIndex>または<vrfindex>要素が名前を持っています。
index	<lfIndex>または<vrfindex>要素がインデックスを持っています。
auto	デバイスのデフォルト値は、インタフェースまたはVPNインスタンスマッチングの名前として<lfIndex>または<vrfindex>要素の値を使用します。 一致しない場合、デバイスは、インタフェースまたはVPNインスタンスマッチングのインデックスとして使用します。

次の例では、<lfIndex>エレメントの index-type 値を指定します。

```
<rpc xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <getoperation>
    <filter>
      <top                          xmlns="http://www.nec.com/netconf/config:1.0"
xmlns:base="http://www.nec.com/netconf/base:1.0">
       <VLAN>
        <TrunkInterfaces>
          <Interface>
            <IfIndex base:valuetype="index">1</IfIndex>
          </Interface>
        </TrunkInterfaces>
       </VLAN>
      </top>
    </filter >
  </getoperation>
</rpc>
```

<get> あるいは < get-bulk> オペレーションが成功した場合、デバイスは取得したデータを次のフォーマットで返します。

```
<?xml version="1.0"?>
<rpc-reply message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <data>
     Device state and configuration data
  </data>
</rpc-reply>
```

7.4.3 デフォルト以外の設定の取得

<get-config> および <get-bulk-config> オペレーションは、デフォルト以外のすべての設定を取得するために使用されます。<get-config>、<get-bulk-config>メッセージには、データをフィルタするための<filter>エレメントを含めることができます。

<get-config>および<get-bulk-config>メッセージは類似しています。<get-config>メッセージの例を次に示します。

```
<?xml version="1.0"?>
```

```
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <get-config>
    <source>
      <running/>
    </source>
    <filter>
      <top xmlns="http://www.nec.com/netconf/config:1.0">
          Specify the module name, submodule name, table name, and column name
      </top>
    </filter>
  </get-config>
</rpc>
```

<get-config>または<get-bulk-config>オペレーションが成功すると、デバイスは取得したデータを次のフォーマットで返します。

```
<?xml version="1.0"?>
<rpc-reply message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <data>
    Data matching the specified filter
  </data>
</rpc-reply>
```

7.4.4 NETCONF 情報の取得

NETCONF 情報を取得するには<get><netconf-state/></get>メッセージを使用します。

#次のテキストをクライアントにコピーし、NETCONF 情報を取得します。

```
<?xml version="1.0" encoding="UTF-8"?>
  <rpc message-id="m-641" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
    <get>
      <filter type='subtree'>
        <netconf-state
xmlns='urn:ietf:params:xml:ns:yang:ietf-netconf-monitoring'>
            <getType/>
        </netconf-state>
      </filter>
    </get>
  </rpc>
```

getType の値を指定しない場合、取得オペレーションはすべての NETCONF 情報を取得します。

getType の値は、次のいずれかのオペレーション指定できます。

操作	説明
capabilities	デバイス機能を取得します。
datastores	デバイスからデータベースを取得します。
schemas	デバイスからYANGファイル名のリストを取得します。
sessions	デバイスからセッション情報を取得します。
statistics	NETCONF統計情報を取得します。

<get><netconf-state/></get>オペレーションが成功すると、デバイスは次のフォーマットで応答を返します。

```
<?xml version="1.0"?>
<rpc-reply message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <data>
     Retrieved NETCONF information
  </data>
</rpc-reply>
```

7.4.5 YANG ファイルコンテンツの取得

YANG ファイルは、デバイスがサポートする NETCONF オペレーションを保存します。ユーザは、YANG ファイルのコンテンツを取得および分析することによって、サポートされるオペレーションを知ることができます。

YANG ファイルはデバイスソフトウェアに統合され、*yang_identifier@yang_version.yang* のフォーマットで名前が付けられます。**dir** コマンドを実行して YANG ファイル名を表示することはできません。 YANG ファイル名の取得方法については、オペレーションマニュアルのセクション 11 *システム管理*“*NETCONF*”の“*NETCONF 情報の取得*”を参照してください。

#次のテキストをクライアントにコピーして、**syslog-data@2017-01-01.yang** という名前の YANG ファイルを取得します。

```
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <get-schema xmlns='urn:ietf:params:xml:ns:yang:ietf-netconf-monitoring'>
    <identifier>syslog-data</identifier>
    <version>2017-01-01</version>
    <format>yang</format>
  </get-schema>
</rpc>
```

<get-schema>オペレーションが成功すると、デバイスは次のオペレーションで応答を返します。

```
<?xml version="1.0"?>
<rpc-reply message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <data>
     Content of the specified YANG file
  </data>
</rpc-reply>
```

7.4.6 NETCONF セッション情報の取得

<get-sessions>オペレーションを使用して、デバイスの NETCONF セッション情報を取得します。

#次のメッセージをクライアントにコピーして、デバイスから NETCONF セッション情報を取得します。

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <get-sessions/>
</rpc>
```

<get-sessions> オペレーションが成功すると、デバイスは次のフォーマットで応答を返します。

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <get-sessions>
    <Session>
      <SessionID>Configuration session ID</SessionID>
      <Line>Line information</Line>
      <UserName>Name of the user creating the session</UserName>
      <Since>Time when the session was created</Since>
      <LockHeld>Whether the session holds a lock</LockHeld>
    </Session>
  </get-sessions>
</rpc-reply>
```

7.4.7 インタフェーステーブルのデータエントリの取得例

I. ネットワーク要件

インタフェーステーブルのデータエントリを取得します。

II. 設定手順

XML view に移行します。

```
<Switch> xml
```

#クライアントでサポートされている NETCONF 機能のデバイスに通知します。

```
<hello xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <capabilities>
    <capability>urn:ietf:params:netconf:base:1.0</capability>
  </capabilities>
</hello>
```

#インタフェーステーブルのデータエントリを取得します。

```
<rpc      message-id="100"      xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"
xmlns:web="urn:ietf:params:xml:ns:netconf:base:1.0">
  <get-bulk>
    <filter type="subtree">
      <top                          xmlns="http://www.nec.com/netconf/data:1.0"
xmlns:web="http://www.nec.com/netconf/base:1.0">
        <Ifmgr>
          <Interfaces web:count="1">
          </Interfaces>
        </Ifmgr>
      </top>
    </filter>
  </get-bulk>
</rpc>
```

III. 設定の確認

クライアントが次のテキストを受信すると、<get-bulk>オペレーションが成功します。

```
<rpc-reply                      xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"
xmlns:web="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="100">
  <data>
    <top xmlns="http://www.nec.com/netconf/data:1.0">
      <Ifmgr>
        <Interfaces>
          <Interface>
            <IfIndex>3</IfIndex>
            <Name>GigabitEthernet1/0/2</Name>
            <AbbreviatedName>GE1/0/2</AbbreviatedName>
            <PortIndex>3</PortIndex>
            <ifTypeExt>22</ifTypeExt>
            <ifType>6</ifType>
            <Description>GigabitEthernet1/0/2 Interface</Description>
            <AdminStatus>2</AdminStatus>
            <OperStatus>2</OperStatus>
            <ConfigSpeed>0</ConfigSpeed>
            <ActualSpeed>100000</ActualSpeed>
            <ConfigDuplex>3</ConfigDuplex>
            <ActualDuplex>1</ActualDuplex>
          </Interface>
        </Interfaces>
      </Ifmgr>
    </top>
  </data>
</rpc-reply>
```

7.4.8 デフォルト以外の構成データの取得例

I. ネットワーク要件

デフォルト以外の設定データをすべて取得します。

II. 設定手順

XML view に移行します。

```
<Switch> xml
```

#クライアントでサポートされている NETCONF 機能のデバイスに通知します。

```
<hello xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <capabilities>
    <capability>
            urn:ietf:params:netconf:base:1.0
    </capability>
  </capabilities>
</hello>
```

#デフォルト以外のすべての構成データを取得します。

```
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <get-config>
    <source>
      <running/>
    </source>
  </get-config>
</rpc>
```

III. 設定の確認

クライアントが次のテキストを受信すると、<get-config>オペレーションが成功します。

```
<rpc-reply                    xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"
xmlns:web="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="100">
    <data>
        <top xmlns="http://www.nec.com/netconf/config:1.0">
            <Ifmgr>
                <Interfaces>
                    <Interface>
                        <IfIndex>1307</IfIndex>
                        <Shutdown>1</Shutdown>
                    </Interface>
                    <Interface>
                        <IfIndex>1308</IfIndex>
                        <Shutdown>1</Shutdown>
                    </Interface>
                    <Interface>
                        <IfIndex>1309</IfIndex>
                        <Shutdown>1</Shutdown>
                    </Interface>
                    <Interface>
                        <IfIndex>1311</IfIndex>
                            <VlanType>2</VlanType>
                    </Interface>
                    <Interface>
                        <IfIndex>1313</IfIndex>
                            <VlanType>2</VlanType>
                    </Interface>
                </Interfaces>
            </Ifmgr>
            <Syslog>
                <LogBuffer>
                    <BufferSize>120</BufferSize>
```

```
                </LogBuffer>
            </Syslog>
            <System>
                <Device>
                    <SysName>Sysname</SysName>
                    <TimeZone>
                        <Zone>+11:44</Zone>
                        <ZoneName>beijing</ZoneName>
                    </TimeZone>
                </Device>
            </System>
        </top>
    </data>
</rpc-reply>
```

7.4.9 シスログ設定データの取得例

I. ネットワーク要件

シスログモジュールの構成データを取得します。

II. 設定手順

XML view に移行します。

```
<Switch> xml
```

#クライアントでサポートされている NETCONF 機能のデバイスに通知します。

```
<hello xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <capabilities>
    <capability>
            urn:ietf:params:netconf:base:1.0
    </capability>
  </capabilities>
</hello>
```

シスログモジュールの構成データを取得します。

```
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <get-config>
    <source>
      <running/>
    </source>
    <filter type="subtree">
      <top xmlns="http://www.nec.com/netconf/config:1.0">
        <Syslog/>
      </top>
    </filter>
  </get-config>
</rpc>
```

III. 設定の確認

クライアントが次のテキストを受信すると、<get-config>オペレーションが成功します。

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="100">
    <data>
        <top xmlns="http://www.nec.com/netconf/config:1.0">
            <Syslog>
                    <LogBuffer>
                        <BufferSize>120</BufferSize>
                    </LogBuffer>
            </Syslog>
        </top>
```

```
    </data>
</rpc-reply>
```

7.4.10 NETCONF セッション情報の取得例

I. ネットワーク要件

NETCONF セッション情報を取得します。

II. 設定手順

XML view に移行します。

```
<Switch> xml
```

#次のメッセージをクライアントにコピーして、デバイスとの機能を交換します。

```
<hello xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <capabilities>
    <capability>
            urn:ietf:params:netconf:base:1.0
    </capability>
  </capabilities>
</hello>
```

#次のメッセージをクライアントにコピーして、デバイス上の現在の NETCONF セッション情報を取得します。

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <get-sessions/>
</rpc>
```

III. 設定の確認

クライアントが次のメッセージを受信すると、オペレーションは正常に実行されます。

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="100">
    <get-sessions>
        <Session>
            <SessionID>1</SessionID>
            <Line>vty0</Line>
            <UserName></UserName>
            <Since>2017-01-07T00:24:57</Since>
            <LockHeld>false</LockHeld>
        </Session>
    </get-sessions>
</rpc-reply>
```

出力には、次の情報が表示されます。

- 既存の NETCONF セッションのセッション ID は 1 です。
- ログインユーザタイプは vty0 です。
- ログイン時間は 2017-01-07T00:24:57 です。
- ユーザは設定のロックを保持しません。

7.5 データのフィルタリング

7.5.1 概要

フィルタを定義して、<get>、<get-bulk>、<get-config>、または<get-bulk-config>オペレーションを実行するときにフィルタを設定できます。 データのフィルタリングには次のタイプがあります。

- **表ベースのフィルタリング**－テーブル情報をフィルタします。
- **列ベースのフィルタリング**－単一列の情報をフィルタします。

7.5.2 制限とガイドライン

テーブルベースのフィルタリングを有効にするには、列ベースのフィルタリングを行う前にテーブルベースのフィルタリングを設定する必要があります。

7.5.3 テーブルベースのフィルタリング

I. テーブルベースのフィルタリング

ネームスペースは **http://www.nec.com/netconf/base:1.0** です。 属性名は **filter** です。テーブルベースの一致のサポートについては、NETCONF XML API リファレンスを参照してください。

#次のテキストをクライアントにコピーして、IP アドレス 1.1.1.0 と、IPv4 ルーティングテーブルからのマスク長 24 を持つ最長データを取得します。

```
<rpc      message-id="100"      xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"
xmlns:nec="http://www.nec.com/netconf/base:1.0">
  <get>
    <filter type="subtree">
      <top xmlns="http://www.nec.com/netconf/data:1.0">
        <Route>
         <Ipv4Routes>
           <RouteEntry nec:filter="IP 1.1.1.0 MaskLen 24 longer"/>
         </Ipv4Routes>
        </Route>
      </top>
    </filter>
  </get>
</rpc>
```

II. 制限とガイドライン

テーブルベースのフィルタリングを使用するには、**filter** 行属性の一致条件を指定します。

7.5.4 列ベースのフィルタリング

I. 列ベースのフィルタリング

列ベースのフィルタリングには、完全一致フィルタリング、正規表現一致フィルタリング、条件付き一致フィルタが含まれます。 完全一致フィルタリングは優先順位がもっとも高

く、条件付き一致フィルタリングはもっとも優先順位が低くなります。 複数のフィルタ条件を指定すると、優先順位がもっとも高いものが有効になります。

II. 完全一致フィルタリング

完全一致フィルタを実装するために、XML メッセージでエレメント値を指定できます。複数のエレメント値を指定すると、指定したすべての値に一致するデータが戻されます。

#次のテキストをクライアントにコピーして、UP 状態のすべてのインタフェースの設定データを取得します。

```
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <get>
    <filter type="subtree">
      <top xmlns="http://www.nec.com/netconf/data:1.0">
        <Ifmgr>
          <Interfaces>
            <Interface>
              <AdminStatus>1</AdminStatus>
            </Interface>
          </Interfaces>
        </Ifmgr>
      </top>
    </filter>
  </get>
</rpc>
```

完全一致フィルタを実装する行の現在のテーブルの列名と同じ属性名を指定することもできます。 この属性名に一致する設定データのみが戻されます。 上記エレメント値ベースの完全一致フィルタリングと同等の XML メッセージを以下に示します。

```
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <get>
    <filter type="subtree">
      <top
xmlns="http://www.nec.com/netconf/data:1.0"xmlns:data="http://www.nec.com/netc
onf/data:1.0">
        <Ifmgr>
          <Interfaces>
            <Interface data:AdminStatus="1"/>
          </Interfaces>
        </Ifmgr>
      </top>
    </filter>
  </get>
</rpc>
```

上記の例では、エレメント値ベースの完全一致フィルタリングと属性名ベースの完全一致フィルタリングの両方が、すべてのインタフェースの同じインデックスおよび列情報をアップ状態で取得できることを示しています。

III. 正規表現マッチングフィルタリング

文字による複雑なデータフィルタリングを実装するには、特定の要素に対して **regExp** 属性を追加します。

サポートされるデータ型には、整数、日付と時刻、文字列、IPv4 アドレス、IPv4 マスク、IPv6 アドレス、MAC アドレス、OID、およびタイムゾーンがあります。

#次のテキストをクライアントにコピーし、インタフェースの説明を取得します。すべての文字が A～Z の大文字である必要があります。

```
<rpc      message-id="100"      xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"
xmlns:nec="http://www.nec.com/netconf/base:1.0">
  <get-config>
```

```
    <source>
      <running/>
    </source>
    <filter type="subtree">
      <top xmlns="http://www.nec.com/netconf/config:1.0">
        <Ifmgr>
          <Interfaces>
            <Interface>
              <Description nec:regExp="^[A-Z]*$"/>
            </Interface>
          </Interfaces>
        </Ifmgr>
      </top>
    </filter>
  </get-config>
</rpc>
```

IV. 条件付き一致フィルタリング

数字と文字列で複雑なデータ フィルタリングを実装するには、特定の要素に **match** 属性を追加できます。表 7-3に条件付き一致演算子を示します。

表 7-3 条件付き一致演算子

操作	演算子	備考
More than	match="more:*value*"	指定した値より大きい値です。 サポートされるデータ型には、日付、数字、文字列があります。
Less than	match="less:*value*"	指定した値未満の値です。 サポートされるデータ型には、日付、数字、文字列があります。
Not less than	match="notLess:*value*"	指定した値以上の値です。 サポートされるデータ型には、日付、数字、文字列があります。
Not more than	match="notMore:*value*"	指定された値以下の値です。 サポートされるデータ型には、日付、数字、文字列があります。
Equal	match="equal:*value*"	指定した値に等しい値です。 サポートされるデータ型には、日付、数字、文字列、OID、およびBOOLがあります。
Not equal	match="notEqual:*value*"	指定した値と等しくない値です。 サポートされるデータ型には、日付、数字、文字列、OID、およびBOOLがあります。
Include	match="include:*string*"	指定された文字列を含みます。 サポートされるデータ型には文字列のみが含まれます。
Not include	match="exclude:*string*"	指定された文字列を除外します。 サポートされるデータ型には文字列のみが含まれます。
Start with	match="startWith:*string*"	指定した文字列で開始します。 サポートされるデータ型には、文字列とOIDが含まれます。
End with	match="endWith:*string*"	指定した文字列で終了します。 サポートされるデータ型には文字列のみが含まれます。

次のテキストをクライアントにコピーして、CPU 使用率が 50%以上のエンティティに関する拡張情報を取得します。

```
<rpc      message-id="100"      xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"
xmlns:nec="http://www.nec.com/netconf/base:1.0">
  <get>
    <filter type="subtree">
      <top xmlns="http://www.nec.com/netconf/data:1.0">
        <Device>
          <ExtPhysicalEntities>
            <Entity>
              <CpuUsage nec:match="more:50"></CpuUsage>
            </Entity>
```

```
          </ExtPhysicalEntities>
        </Device>
      </top>
    </filter>
  </get>
</rpc>
```

7.5.5 正規表現と一致するデータのフィルタリング

I. ネットワーク要件

Ifmgr モジュールの下の Interfaces テーブルの **Description** 列の **Gigabit** を含むすべてのデータを取得します。

II. 設定手順

XML view に移行します。

```
<Switch> xml
```

クライアントでサポートされている NETCONF 機能のデバイスに通知します。

```
<hello xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <capabilities>
    <capability>
           urn:ietf:params:netconf:base:1.0
    </capability>
  </capabilities>
</hello>
```

Ifmgr モジュールの下の Interfaces テーブルの **Description** 列の **Gigabit** を含むすべてのデータを取得します。

```
<?xml version="1.0"?>
<rpc     message-id="100"     xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"
xmlns:nec="http://www.nec.com/netconf/base:1.0">
  <get>
    <filter type="subtree">
      <top xmlns="http://www.nec.com/netconf/data:1.0">
        <Ifmgr>
          <Interfaces>
            <Interface>
              <Description nec:regExp="(Gigabit)+"/>
            </Interface>
          </Interfaces>
        </Ifmgr>
      </top>
    </filter>
  </get>
</rpc>
```

III. 設定の確認

クライアントが次のテキストを受信すると、オペレーションは成功します。

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply                    xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"
xmlns:nec="http://www.nec.com/netconf/base:1.0" message-id="100">
    <data>
        <top xmlns="http://www.nec.com/netconf/data:1.0">
            <Ifmgr>
                <Interfaces>
                    <Interface>
                        <IfIndex>2681</IfIndex>
                        <Description>GigabitEthernet1/0/1
Interface</Description>
```

```
                    </Interface>
                    <Interface>
                        <IfIndex>2685</IfIndex>
                        <Description>GigabitEthernet1/0/2
Interface</Description>
                    </Interface>
                    <Interface>
                        <IfIndex>2689</IfIndex>
                        <Description>GigabitEthernet1/0/3
Interface</Description>
                    </Interface>
                </Interface>
            </Ifmgr>
        </top>
    </data>
</rpc-reply>
```

7.5.6 条件付き一致によるデータのフィルタリング

I. ネットワーク要件

Ifmgr モジュールの下の Interfaces テーブルで、ifindx 値が 5000 以上の **Name** 列のデータを取得します。

II. 設定手順

XML view に移行します。

```
<Switch> xml
```

クライアントでサポートされている NETCONF 機能のデバイスに通知します。

```
<hello xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <capabilities>
    <capability>
            urn:ietf:params:netconf:base:1.0
    </capability>
  </capabilities>
</hello>
```

Ifmgr モジュールの下の Interfaces テーブルで ifindx 値が 5000 以上の **Name** 列のデータを取得します。

```
<rpc      message-id="100"      xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"
xmlns:nec="http://www.nec.com/netconf/base:1.0">
  <get>
    <filter type="subtree">
      <top xmlns="http://www.nec.com/netconf/data:1.0">
        <Ifmgr>
          <Interfaces>
            <Interface>
              <IfIndex nec:match="notLess:5000"/>
              <Name/>
            </Interface>
          </Interfaces>
        </Ifmgr>
      </top>
    </filter>
  </get>
</rpc>
```

III. 設定の確認

クライアントが次のテキストを受信すると、オペレーションは成功します。

```
<?xml version="1.0" encoding="UTF-8"?>
```

```
<rpc-reply                    xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"
xmlns:nec="http://www.nec.com/netconf/base:1.0" message-id="100">
    <data>
        <top xmlns="http://www.nec.com/netconf/data:1.0">
            <Ifmgr>
                <Interfaces>
                    <Interface>
                        <IfIndex>7241</IfIndex>
                        <Name>NULL0</Name>
                    </Interface>
                </Interfaces>
            </Ifmgr>
        </top>
    </data>
</rpc-reply>
```

7.6 稼働中の設定のロック、ロック解除

7.6.1 設定のロック、ロック解除

CLI、NETCONF、SNMP などのデバイスを設定するには、複数の方法があります。 デバイスの設定、管理、またはトラブルシューティングを行う前に、ほかのユーザがデバイス設定を変更できないように設定をロックできます。 構成をロックすると、設定を変更したり、設定をロック解除するために<edit-config>オペレーションを実行できます。ほかのユーザは設定のみを読み込むことができます。

NETCONF セッションを閉じると、システムは設定をロック解除します。 設定を手動でロック解除することもできます。

7.6.2 制限とガイドライン

<lock>オペレーションは、デバイスの稼働中の設定をロックします。 特定のモジュールの設定をロックするために使用することはできません。

7.6.3 稼働中の設定のロック

稼働中の設定をロックするには、次のテキストをクライアントにコピーします。

```
<?xml version="1.0" encoding="UTF-8"?>
  <rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
    <lock>
      <target>
        <running/>
      </target>
    </lock>
  </rpc>
```

<lock>オペレーションが成功すると、デバイスは次のフォーマットで応答を返します。

```
<?xml version="1.0" encoding="UTF-8"?>
  <rpc-reply message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
     <ok/>
</rpc-reply>
```

7.6.4 稼働中の設定のロック解除

次のテキストをクライアントにコピーして、稼働中の設定をロック解除します。

```
<?xml version="1.0" encoding="UTF-8"?>
  <rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
    <unlock>
      <target>
        <running/>
      </target>
    </unlock>
  </rpc>
```

<unlock> オペレーションが成功すると、デバイスは次のフォーマットで応答を返します。:

```
<?xml version="1.0" encoding="UTF-8"?>
    <rpc-reply                                                    message-id="100"
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
      <ok/>
</rpc-reply>
```

7.6.5 稼働中の設定のロック例

I. ネットワーク要件

デバイス構成をロックして、ほかのユーザがデバイス設定を変更できないようにします。

II. 設定手順

XML view に移行します。

```
<Switch> xml
```

#クライアントでサポートされている NETCONF 機能のデバイスに通知します。

```
<hello xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
    <capabilities>
        <capability>
            urn:ietf:params:netconf:base:1.0
        </capability>
    </capabilities>
</hello>
```

設定をロックします。

```
<?xml version="1.0" encoding="UTF-8"?>
  <rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
    <lock>
      <target>
        <running/>
      </target>
    </lock>
  </rpc>
```

III. 設定の確認

クライアントが次の応答を受信すると、<lock>オペレーションが成功します。

```
<?xml version="1.0" encoding="UTF-8"?>
    <rpc-reply                                                    message-id="100"
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
      <ok/>
</rpc-reply>
```

別のクライアントがロック要求を送信すると、デバイスは次の応答を返します。

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
<rpc-error>
  <error-type>protocol</error-type>
  <error-tag>lock-denied</error-tag>
  <error-severity>error</error-severity>
```

```
  <error-message xml:lang="en"> Lock failed because the NETCONF lock is held by
another session.</error-message>
  <error-info>
    <session-id>1</session-id>
  </error-info>
  </rpc-error>
</rpc-reply>
```

出力は、<lock>オペレーションが失敗したことを示します。 セッション ID 1 のクライアントはロックを保持しています。

7.7 設定の変更

7.7.1 <edit-config>オペレーション

<edit-config>オペレーションは、merge、create、replace、remove、delete、default-operation、error-option、test-option、incremental 属性をサポートします。

7.7.2 設定手順

#次のテキストをクライアントにコピーして、<edit-config>オペレーションを実行します。

```
<?xml version="1.0"?>
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <edit-config>
    <target><running></running></target>
<error-option>
   error-option
</error-option>
    <config>
      <top xmlns="http://www.nec.com/netconf/config:1.0">
        Specify the module name, submodule name, table name, and column name
      </top>
    </config>
  </edit-config>
</rpc>
```

<error-option>エレメントはオペレーション中に発生するエラーに応じて実行されるアクションを示します。以下に値を示します。

値	説明
stop-on-error	<edit-config>オペレーションを停止します。
continue-on-error	<edit-config>オペレーションを継続します。
rollback-on-error	<edit-config>オペレーションが実行される前に設定をロールバックします。 デフォルトでデバイスが設定をロールバックする間、<edit-config>オペレーションは実行することができません。 ロールバック時間がクライアントの待ち時間を超過した場合、クライアントは<edit-config>オペレーションが失敗したと認識し、オペレーションを再度実行します。前回のロールバックが完了していないため、オペレーションは別のロールバックを開始します。このプロセスが繰り返される場合、CPUとメモリリソースが使い果たされ、デバイスが再起動します。 設定のロールバックを行う間、<edit-config>オペレーションを実行できるようにするためには**DisableEditConfigWhenRollback**属性の値を**false**に変更します。

<edit-config> オペレーションが成功すると、デバイスは次のフォーマットで応答を返します。

```
<?xml version="1.0">
<rpc-reply message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <ok/>
</rpc-reply>
```

<get>>オペレーションを実行し、現在のエレメントの値が<edit-config>オペレーションを通して実行された値と同一であることを確認します。

7.7.3 設定の変更例

I. ネットワーク要件

シスログモジュールのログバッファを 512 に変更します。

II. 設定手順

XML view に移行します。

```
<Switch> xml
```

クライアントでサポートされている NETCONF 機能のデバイスに通知します。

```
<hello xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <capabilities>
    <capability>urn:ietf:params:netconf:base:1.0</capability>
  </capabilities>
</hello>
```

シスログモジュールのログバッファを 512 に変更します。

```
<rpc      message-id="100"      xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"
xmlns:web="urn:ietf:params:xml:ns:netconf:base:1.0">
  <edit-config>
    <target>
      <running/>
    </target>
    <config>
      <top                        xmlns="http://www.nec.com/netconf/config:1.0"
web:operation="merge">
        <Syslog>
          <LogBuffer>
            <BufferSize>512</BufferSize>
          </LogBuffer>
        </Syslog>
      </top>
    </config>
  </edit-config>
</rpc>
```

III. 設定の確認

クライアントが以下のテキストを受信した場合、<edit-config> オペレーションが成功します。

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
    <ok/>
</rpc-reply>
```

7.8 稼働中の設定の保存

7.8.1 <save>オペレーション

<save>オペレーションは稼働中の設定を設定ファイルに保存し、次回に起動するメインのスタートアップコンフィグレーションファイルとしてファイルを指定します。

7.8.2 制限とガイドライン

<save>オペレーションはリソースを集中的に使用します。システムリソースが大量に占有されている場合、このオペレーションを実行しないでください。

7.8.3 設定手順

次のテキストをクライアントにコピーします。

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <save OverWrite="false">
    <file>Configuration file name</file>
  </save>
</rpc>
```

項目	説明
file	名前で設定ファイル.cfgを指定します。名前は記憶媒体の名前から始まる必要があります。 ファイル列を指定する場合、ファイル名が必要です。 デバイスはテキストとバイナリ形式の設定ファイルの両方に保存することができます。 ● 指定された.cfgファイルが存在しない場合、稼働中の設定ファイルを保存するため、デバイスはバイナリ形式の設定ファイルを作成します。 ● ファイル列を指定しない場合、デバイスは稼働中の設定ファイルをテキスト形式とバイナリ形式の次回に起動するスタートアップコンフィグレーションファイルに保存します。
OverWrite	ファイルが既に存在する場合、指定したファイルに上書きするかどうかを指定します。以下の値を使用できます。 ● **true**– ファイルを上書きします。 ● **false**– ファイルを上書きしません。稼働中のコンフィグレーションは保存することができません。システムはエラーメッセージを表示します。 デフォルトは**true**です。

<save> オペレーションが成功すると、デバイスは次のフォーマットで応答を返します。

```
<?xml version="1.0" encoding="UTF-8"?>
    <rpc-reply                                                    message-id="100"
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
      <ok/>
</rpc-reply>
```

7.8.4 稼働中の設定の保存例

I. ネットワーク要件

稼働中の設定を **config.cfg** に保存します。

II. 設定手順

XML view に移行します。

```
<Switch> xml
```

クライアントでサポートされている NETCONF 機能のデバイスに通知します。

```
<hello xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <capabilities>
    <capability>
           urn:ietf:params:netconf:base:1.0
    </capability>
  </capabilities>
</hello>
```

デバイスの稼働中の設定を **config.cfg** に保存します。

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <save>
    <file>config.cfg</file>
  </save>
</rpc>
```

III. 設定の確認

クライアントが次の応答を受信すると、<save>オペレーションは成功します。

```
<?xml version="1.0" encoding="UTF-8"?>
    <rpc-reply                                                    message-id="100"
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
      <ok/>
</rpc-reply>
```

7.9 設定の読み込み

7.9.1 <load>オペレーション

<load>オペレーションは、設定ファイルから稼働中の設定に次のように設定をマージします。

- 稼働中の設定に存在しない設定を読み込みます。
- 稼働中の設定に存在する設定を上書きします。

7.9.2 設定とガイドライン

<load>オペレーションを実行するとき、以下の制限とガイドラインに従ってください。

- <load>オペレーションはリソースを集中的に使用します。システムリソースが大量に占有されている場合、このオペレーションを実行しないでください。

- コンフィグレーション成ファイル内の設定によっては､既存の設定と競合する場合があります。 ファイルの設定を適用するには、既存の競合する設定を削除し、設定ファイルを読み込みます。

7.9.3 設定手順

次のテキストをクライアントにコピーして、デバイスの設定ファイルを読み込みます。

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <load>
   <file>Configuration file name</file>
  </load>
</rpc>
```

設定ファイル名は、記憶媒体名で開始する必要があります。**.cfg** 拡張子を指定します。

<load>オペレーションが成功すると、デバイスは次のフォーマットで応答を返します。

```
<?xml version="1.0" encoding="UTF-8"?>
    <rpc-reply                                                    message-id="100"
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
      <ok/>
</rpc-reply>
```

7.10 設定のロールバック

7.10.1 制限とガイドライン

<rollback>オペレーションはリソースを集中的に使用します。システムリソースが大量に占有されている場合、このオペレーションを実行しないでください。

デフォルトでは、デバイスが設定をロールバック中に<edit-config>オペレーションを実行できません。設定のロールバック中に<edit-config>オペレーションを実行できるようにするには、**DisableEditConfigWhenRollback** 属性の値を **false** に変更する<action>オペレーションを実行します。

7.10.2 設定ファイルにもとづいた設定のロールバック

次のテキストをクライアントにコピーして、稼働中の設定を設定ファイルの設定にロールバックします。

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <rollback>
    <file>Specify the configuration file name</file>
  </rollback>
</rpc>
```

<rollback> オペレーションが成功すると、デバイスは次のフォーマットで応答を返します。

```
<?xml version="1.0" encoding="UTF-8"?>
    <rpc-reply                                                    message-id="100"
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
      <ok/>
</rpc-reply>
```

7.10.3 ロールバックポイントにもとづいた設定のロールバック

I. ロールバックポイントにもとづいた設定のロールバック

ロールバックポイントにもとづいて稼働中の設定をロールバックするには、次のいずれかの状況が発生します。

- NETCONF クライアントがロールバック要求を送信します。
- NETCONF セッションアイドル時間がロールバックアイドルタイムアウト時間より長いです。
- NETCONF クライアントがデバイスから予期せず切断されました。

II. 制限とガイドライン

複数のユーザが同時にデバイスを設定する場合があります。 ほかのユーザが稼働中の設定を変更することを防ぐため、設定をロールバックする前に、システムをロックしてからシステムをロックしてください。

III. 設定手順

1) 稼働中の設定をロックします。詳細はオペレーションマニュアルのセクション 11 *システム管理 “NETCONF”の “稼働中の設定のロック、ロック解除”*を参照してください。
2) ロールバックポイントにもとづいて設定のロールバックを有効にします。

次のテキストをクライアントにコピーして<save-point>/<begin>オペレーションを実行します。

```
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
       <save-point>
         <begin>
           <confirm-timeout>100</confirm-timeout>
        </begin>
       </save-point>
 </rpc>
```

項目	説明
confirm-timeout	ロールバックアイドルタイムアウト時間を指定します。設定範囲は1～65535秒です。デフォルトは600秒です。このアイテムはオプションです。

<save-point/begin>オペレーションが成功すると、デバイスは次のフォーマットで応答を返します。

```
<rpc-reply message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <data>
    <save-point>
       <commit>
          <commit-id>1</commit-id>
       </commit>
    </save-point>
  </data>
</rpc-reply>
```

3) 稼働中の設定を変更します。詳細はオペレーションマニュアルのセクション 11 *システム管理 “NETCONF”の “設定の変更”*を参照してください。
4) ロールバックポイントをマークします。

システムは最大 50 のロールバックポイントをサポートしています。制限に達した場合は、<save-point>/<commit>オペレーションの **force** 属性を指定して、もっとも初期のロールバックポイントを上書きします。

次のテキストをクライアントにコピーして<save-point>/<commit>オペレーションを実行します。

```
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <save-point>
    <commit>
      <label>SUPPORT VLAN<label>
      <comment>vlan 1 to 100 and interfaces. Each vlan used for different custom
as follows: ……</comment>
     </commit>
  </save-point>
</rpc>
```

<label> および<comment>エレメントはオプションです。

<save-point>/<commit> オペレーションが成功すると、デバイスは次のフォーマットで応答を返します。:

```
<rpc-reply message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <data>
    <save-point>
       <commit>
          <commit-id>2</commit-id>
       </commit>
    </save-point>
  </data>
</rpc-reply>
```

5) ロールバックポイントの設定の記録を取得します。

次のテキストは、<save point/get-commits>要求のメッセージフォーマットを示します。

```
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <save-point>
    <get-commits>
      <commit-id/>
      <commit-index/>
      <commit-label/>
    </get-commits>
  </save-point>
</rpc>
```

指定したロールバックポイントの設定の記録を取得する場合、<commit-id/>、<commit-index/>、 <commit-label/>エレメントを指定します。エレメントが指定されていない場合、オペレーションはすべてのロールバックポイント設定の記録を取得します。

#次のテキストをクライアントにコピーして<save-point>/<get-commits>オペレーションを実行します。

```
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <save-point>
    <get-commits>
      <commit-label>SUPPORT VLAN</commit-label>
    </get-commits>
  </save-point>
</rpc>
```

<save-point/get-commits> オペレーションが成功すると、デバイスは次のフォーマットで応答を返します。

```
<rpc-reply message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
   <data>
      <save-point>
         <commit-information>
           <CommitID>2</CommitID>
           <TimeStamp>Sun Jan 1 11:30:28 2017</TimeStamp>
           <UserName>test</UserName>
           <Label>SUPPORT VLAN</Label>
         </commit-information>
    </save-point>
```

```
  </data>
</rpc-reply>
```

6) ロールバックポイントに対応する設定データを取得します。

次のテキストは、<save-point>/<get-commit-information>要求のメッセージフォーマットを示します。

```
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <save-point>
    <get-commit-information>
       <commit-information>
         <commit-id/>
         <commit-index/>
         <commit-label/>
      </commit-information>
      <compare-information>
         <commit-id/>
         <commit-index/>
         <commit-label/>
      </compare-information
    </get-commit-information>
  </save-point>
</rpc>
```

<commit-id/>、<commit-index/>、<commit-label/>のいずれかのエレメントを指定します。<compare-information>エレメントはオプションです。

項目	説明
commit-id	ロールバックポイントを固有に識別します。
commit-index	最近設定された50のロールバックポイントを指定します。 値が0の場合、もっとも最後に設定されたロールポイントです。49がもっとも古く設定されたロールポイントを示します。
commit-label	ロールバックポイントの固有のラベルを指定します。
get-commit-information	もっとも最後に設定されたロールバックポイントに対応する設定データを取得します。

次のテキストをクライアントにコピーして<save-point>/<get-commit-information>オペレーションを実行します。

```
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <save-point>
    <get-commit-information>
               <commit-information>
                  <commit-label>SUPPORT VLAN</commit-label>
               </commit-information>
    </get-commit-information>
  </save-point>
</rpc>
```

<save-point/get-commit-information> オペレーションが成功すると、デバイスは次のフォーマットで応答を返します。

```
<rpc-reply message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
   <data>
     <save-point>
        <commit-information>
           <content>
              …
              interface vlan 1
              …
           </content>
        </commit-information>
     </save-point>
   </data>
```

```
</rpc-reply>
```

7)　ロールバックポイントにもとづいて設定をロールバックします。

構成は、NETCONF セッションアイドルタイマが満了したときに、最後に設定されたロールバックポイントにもとづいて自動的にロールバックすることもできます。

次のテキストをクライアントにコピーして<save-point>/<rollback>オペレーションを実行します。

```
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <save-point>
    <rollback>
      <commit-id/>
      <commit-index/>
      <commit-label/>
    </rollback>
  </save-point>
</rpc>
```

<commit-id/>、<commit-index/>、<commit-label/>のいずれかのエレメントを指定します。エレメントが指定されていない場合、オペレーションは最後に構成されたロールバックポイントにもとづいて設定をロールバックします。

項目	説明
commit-id	ロールバックポイントを固有に識別します。
commit-index	最近設定された50のロールバックポイントを指定します。 値が0の場合、もっとも最後に設定されたロールポイントです。49がもっとも古く設定されたロールポイントを示します。
commit-label	ロールバックポイントの固有のラベルを指定します。

<save-point/rollback> オペレーションが成功すると、デバイスは次のフォーマットで応答を返します。

```
<rpc-reply message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <ok></ok>
</rpc-reply>
```

8)　ロールバックの設定を終了します。

次のテキストをクライアントにコピーして<save-point>/<end>オペレーションを実行します。

```
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <save-point>
    <end/>
  </save-point>
</rpc>
```

<save-point/end> オペレーションが成功すると、デバイスは次のフォーマットで応答を返します。:

```
<rpc-reply message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
   <ok/>
</rpc-reply>
```

9)　設定をロック解除します。詳細はオペレーションマニュアルのセクション 11 *システム管理　“NETCONF”の“稼働中の設定のロック、ロック解除”*を参照してください。

7.11 NETCONFによるCLIオペレーションの実行

7.11.1 NETCONF による CLI オペレーション

デバイスを設定するために、XML メッセージにコマンドラインを含めることができます。

7.11.2 制限とガイドライン

NETCONF を介した CLI オペレーションはリソースを集中的に使用します。次のタスクを実行しないことを推奨します。

- 複数のコマンド行を 1 つの XML メッセージに含めます。
- ほかのユーザが NETCONF の CLI オペレーションを実行している場合、NETCONF を使用して CLI オペレーションを実行します。

7.11.3 設定手順

次のテキストをクライアントにコピーしてコマンドを実行します。

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <CLI>
    <Execution>
      Commands
    </Execution>
  </CLI>
</rpc>
```

<Execution>エレメントには、1 行に 1 つのコマンドを持つ複数のコマンドを含めることができます。

CLI オペレーションが成功すると、デバイスは次のフォーマットで応答を返します。:

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <CLI>
    <Execution>
      <![CDATA[Responses to the commands]]>
    </Execution>
  </CLI>
</rpc-reply>
```

7.11.4 CLI オペレーションの実行例

I. ネットワーク要件

デバイスに **display vlan** コマンドを送信します。

II. 設定手順

XML view に移行します。

```
<Switch> xml
```

#クライアントでサポートされている NETCONF 機能のデバイスに通知します。

```
<hello xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <capabilities>
```

```
    <capability>
            urn:ietf:params:netconf:base:1.0
    </capability>
  </capabilities>
</hello>
```

次のテキストをクライアントにコピーして、**display vlan** コマンドを実行します。

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <CLI>
    <Execution>
          display vlan
    </Execution>
  </CLI>
</rpc>
```

III. 設定の確認

クライアントが次のテキストを受信すると、オペレーションは成功します。

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <CLI>
    <Execution><![CDATA[
<Switch>display vlan
 Total VLANs: 1
 The VLANs include:
 1(default)
   ]]>
   </Execution>
  </CLI>
</rpc-reply>
```

7.12 イベントの登録

7.12.1 イベントの登録

デバイスでイベントが発生すると、デバイスはイベントに関する情報をイベントに登録している NETCONF クライアントに送信します。

7.12.2 制限とガイドライン

登録は、現在のセッションでのみ有効です。 セッションが終了するとキャンセルされます。

登録するイベントストリームを指定しない場合、デバイスはシスログイベント通知を NETCONF クライアントに送信します。

7.12.3 シスログイベントの登録

次のメッセージをクライアントにコピーして、登録を完了します。

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <create-subscription
xmlns="urn:ietf:params:xml:ns:netconf:notification:1.0">
    <stream>NETCONF</stream>
      <filter>
        <event xmlns="http://www.nec.com/netconf/event:1.0">
          <Code>code</Code>
```

```
            <Group>group</Group>
              <Severity>severity</Severity>
          </event>
        </filter>
        <startTime>start-time</startTime>
        <stopTime>stop-time</stopTime>
    </create-subscription>
</rpc>
```

項目	説明
stream	イベントストリームを指定します。シスログイベントストリームの名前は**NETCONF**です。
event	イベントを指定します。登録できるイベントについては、デバイスのシステムログメッセージを参照してください。
code	ログメッセージの記号シンボルを指定します。
group	ログメッセージのモジュール名を指定します。
severity	ログメッセージのseverityレベルを指定します。
start-time	登録の開始時間を指定します。
stop-time	登録の終了時間を指定します。

登録が成功すると、デバイスは次のフォーマットで応答を返します。

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply                                                    message-id="100"
xmlns:netconf="urn:ietf:params:xml:ns:netconf:base:1.0">
    <ok/>
</rpc-reply>
```

登録が失敗した場合、デバイスは次のフォーマットでエラーメッセージを返します。

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
<rpc-error>
   <error-type>error-type</error-type>
   <error-tag>error-tag</error-tag>
   <error-severity>error-severity</error-severity>
   <error-message xml:lang="en">error-message</error-message>
</rpc-error>
</rpc-reply>
```

エラーメッセージの詳細については、RFC4741 を参照してください。

7.12.4 NETCONF によってモニタされるイベントの登録

この節の説明に従ってイベントを登録すると、NETCONF は定期的に登録されたイベントをポーリングし、登録条件に一致するイベントを NETCONF クライアントに送信します。

次のメッセージをクライアントにコピーして、登録を完了します。

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
<create-subscription xmlns='urn:ietf:params:xml:ns:netconf:notification:1.0'>
  <stream>NETCONF_MONITOR_EXTENSION</stream>
  <filter>
    <NetconfMonitor xmlns='http://www.nec.com/netconf/monitor:1.0'>
      <XPath>XPath</XPath>
      <Interval>interval</Interval>
      <ColumnConditions>
        <ColumnCondition>
          <ColumnName>ColumnName</ColumnName>
          <ColumnValue>ColumnValue</ColumnValue>
          <ColumnCondition>ColumnCondition</ColumnCondition>
        </ColumnCondition>
      </ColumnConditions>
```

```
      <MustIncludeResultColumns>
        <ColumnName>columnName</ColumnName>
      </MustIncludeResultColumns>
    </NetconfMonitor>
  </filter>
<startTime>start-time</startTime>
<stopTime>stop-time</stopTime>
</create-subscription>
</rpc>
```

項目	説明
stream	イベントストリームを指定します。イベントストリームの名前は **NETCONF_MONITOR_EXTENSION**です。
NetconfMonitor	イベントのフィルタ情報を指定します。
XPath	*ModuleName*[/*SubmoduleName*]/*TableName* のフォーマットでイベントのパスを指定します。
interval	登録条件に一致するイベントを取得するためのNETCONFの間隔を指定します。設定範囲は1~4294967秒です。 デフォルトは300秒です。
ColumnName	列名を[*GroupName*.]*ColumnName*のフォーマットで指定します。
ColumnValue	基準値を指定します。
ColumnCondition	オペレータを指定します。 • **more** • **less** • **notLess** • **notMore** • **equal** • **notEqual** • **include** • **exclude** • **startWith** • **endWith** 基準値のタイプに従ってオペレータを選択します。
start-time	登録の開始時間を指定します。
stop-time	登録の終了時間を指定します。

サブスクリプションが成功すると、デバイスは次のフォーマットで応答を返します。

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply                                                    message-id="100"
xmlns:netconf="urn:ietf:params:xml:ns:netconf:base:1.0">
    <ok/>
</rpc-reply>
```

7.12.5 モジュールで報告されたイベントの登録

この節の説明に従ってイベントを登録すると、指定されたモジュールは登録されたイベントを NETCONF に報告します。 NETCONF は、イベントを NETCONF クライアントに送信します。

次のメッセージをクライアントにコピーして、登録を完了します。

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc     message-id="100"     xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"
xmlns:xs="http://www.nec.com/netconf/base:1.0">
```

```
<create-subscription xmlns="urn:ietf:params:xml:ns:netconf:notification:1.0">
<stream>XXX_STREAM</stream>
   <filter type="subtree">
<event
xmlns="http://www.nec.com/netconf/event:1.0/xxx-features-list-name:1.0">
       <ColumnName xs:condition="Condition">value</ColumnName>
</event>
</filter>
<startTime>start-time</startTime>
<stopTime>stop-time</stopTime>
</create-subscription>
</rpc>
```

属性	説明
stream	イベントストリームを指定します。
event	イベント名を指定します。 イベントストリームには、複数のイベントが含まれます。 イベントはイベントストリームと同じネームスペースを使用します。
ColumnName	列の名前を指定します。
ColumnCondition	オペレータを指定します。 • **more** • **less** • **notLess** • **notMore** • **equal** • **notEqual** • **include** • **exclude** • **startWith** • **endWith** 基準値のタイプに従ってオペレータを選択します。
value	列の基準値を指定します。
start-time	登録の開始時間を指定します。
stop-time	登録の終了時間を指定します。

サブスクリプションが成功すると、デバイスは次のフォーマットで応答を返します。

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply                                                    message-id="100"
xmlns:netconf="urn:ietf:params:xml:ns:netconf:base:1.0">
    <ok/>
</rpc-reply>
```

7.12.6 シスログイベントの登録例

I. ネットワーク要件

時間制限なしでシスログイベントを登録するようにクライアントを設定します。登録が正常に終了すると、デバイスとクライアント間のセッションが終了する前に、デバイス上のすべてのイベントがクライアントに送信されます。

II. 設定手順

XML view に移行します。

```
<Switch> xml
```

#クライアントでサポートされている NETCONF 機能のデバイスに通知します。

```
<hello xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <capabilities>
    <capability>
            urn:ietf:params:netconf:base:1.0
    </capability>
  </capabilities>
</hello>
```

時間制限なしのシスログイベントを登録します。

```
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <create-subscription
xmlns="urn:ietf:params:xml:ns:netconf:notification:1.0">
    <stream>NETCONF</stream>
  </create-subscription>
</rpc>
```

III. 設定の確認

#クライアントが次の応答を受信した場合、登録は正常に終了します。

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="100">
    <ok/>
</rpc-reply>
```

#別のクライアント(192.168.100.130)がデバイスにログインすると、デバイスは、すべてのイベントを登録しているクライアントに通知を送信します。

```
<?xml version="1.0" encoding="UTF-8"?>
<notification xmlns="urn:ietf:params:xml:ns:netconf:notification:1.0">
    <eventTime>2011-01-04T12:30:52</eventTime>
    <event xmlns="http://www.nec.com/netconf/event:1.0">
        <Group>SHELL</Group>
        <Code>SHELL_LOGIN</Code>
        <Slot>1</Slot>
        <Severity>Notification</Severity>
        <context>VTY logged in from 192.168.100.130.</context>
    </event>
</notification>
```

7.13 NETCONFセッションの終了

7.13.1 NETCONF セッションの終了

NETCONF を使用すると、1つのクライアントがほかのクライアントの NETCONF セッションを終了できます。セッションが終了したクライアントは、user view に戻ります。

7.13.2 設定手順

#次のメッセージをクライアントにコピーし、NETCONF セッションを終了します。

```
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <kill-session>
    <session-id>
      Specified session-ID
    </session-id>
  </kill-session>
</rpc>
```

<kill-session> オペレーションが成功すると、デバイスは次のフォーマットで応答を返します。:

```
<?xml version="1.0" encoding="UTF-8"?>
    <rpc-reply                                                    message-id="100"
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
      <ok/>
</rpc-reply>
```

7.13.3 別の NETCONF セッションの終了例

I. ネットワーク要件

セッション ID 1 のユーザはセッション ID 2 のセッションを終了します。

II. 設定手順

XML view に移行します。

```
<Switch> xml
```

クライアントでサポートされている NETCONF 機能のデバイスに通知します。

```
<hello xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <capabilities>
    <capability>
            urn:ietf:params:netconf:base:1.0
    </capability>
  </capabilities>
</hello>
```

セッション ID 2 でセッションを終了します。

```
<rpc message-id="100"xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <kill-session>
    <session-id>2</session-id>
  </kill-session>
</rpc>
```

III. 設定の確認

クライアントが次のテキストを受信すると、セッション ID 2 の NETCONF セッションが終了し、セッション ID 2 のクライアントが XML view から user view に戻ります。

```
<?xml version="1.0" encoding="UTF-8"?>
  <rpc-reply message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
    <ok/>
</rpc-reply>
```

7.14 CLIへの復帰

I. 制限とガイドライン

XML view から CLI に戻る前に、デバイスとクライアント間の capability の交換を最初に完了する必要があります。

II. 設定手順

次のテキストをクライアントにコピーして、XML view から CLI に戻ります。

```
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
```

```
   <close-session/>
</rpc>
```

デバイスが close-session 要求を受信すると、次の応答を送信し、CLI の user view に戻ります。

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
   <ok/>
</rpc-reply>
```

目次

このセクションのページは **11-x-x** です。

8 章 プロセスモニタリングとメンテナンス 8-1
8.1 ユーザプロセスの表示と維持 8-1

8章 プロセスモニタリングとメンテナンス

システムソフトウェアは、フル機能でモジュラー型の Linux カーネルをベースにした拡張可能なネットワークオペレーティングシステムです。システムソフトウェアは、独立した以下のプロセスがあります。

- **ユーザプロセス**－ユーザスペースで動作します。ユーザプロセスでたいていのソフトウェア機能が動作します。各プロセスは、独立して動作します。あるプロセスが故障しても、その他のプロセスに影響しません。システムは自動的にユーザプロセスをモニタリングします。システムは preemptive マルチスレッティングをサポートしています。プロセスは複数のアクティビティをサポートするために、複数のスレッドを動作することができます。マルチスレッティングの実装は、ソフトウェアのバージョンに依存します。

8.1 ユーザプロセスの表示と維持

すべての view で **display** コマンドを実行でき、user view でその他のコマンドを実行できます。

操作	コマンド
プロセス例外に関する情報を表示する	**display exception context** [**count** *value*] [**slot** *slot-number*]
コアファイルディレクトリを表示する	**display exception filepath** [**slot** *slot-number*]
カーネルスレッドのデッドループ情報を表示する	**display kernel deadloop** *show-number* [*offset*] [**verbose**] [**slot** *slot-number* [**cpu** *cpu-number*]]
カーネルスレッドの例外情報を表示する	**display kernel exception** *show-number* [*offset*] [**verbose**] [**slot** *slot-number* [**cpu** *cpu-number*]]
カーネルスレッドの再起動情報を表示する	**display kernel reboot** *show-number* [*offset*] [**verbose**] [**slot** *slot-number* [**cpu** *cpu-number*]]
例外でコアファイルを作成するためのプロセスを有効あるいは無効にし、コアファイルの最大数(デフォルトは 1）を設定する	**process core** { **maxcore** *value* | **off** } { **job** *job-id* | **name** *process-name* } [**slot** *slot-number*]
コアファイルを保存するディレクトリ（デフォルトはマスタ装置の flash:/）を指定する	**exception filepath** *directory*
プロセス例外に関する情報を削除する	**reset exception context** [**slot** *slot-number*]
カーネルスレッドのデッドループ情報を削除する	**reset kernel deadloop** [**slot** *slot-number* [**cpu** *cpu-number*]]
カーネルスレッドの例外情報を削除する	**reset kernel exception** [**slot** *slot-number* [**cpu** *cpu-number*]]
カーネルスレッドの再起動情報を削除する	**reset kernel reboot** [**slot** *slot-number* [**cpu** *cpu-number*]]

目次

このセクションのページは **11-x-x** です。

9 章 ポートミラーリング 9-1
9.1 概要 9-1
9.1.1 用語 9-1
9.1.2 ポートミラーリングの分類と実行 9-2
9.2 ローカルポートミラーリングの設定 9-5
9.2.1 ローカルポートミラーリング設定作業リスト 9-5
9.2.2 ローカルミラーリンググループの作成 9-6
9.2.3 ローカルミラーリンググループのソースポートの作成 9-6
9.2.4 ローカルミラーリンググループのモニタポートの作成 9-7
9.3 レイヤ 2 リモートポートミラーリングの設定 9-7
9.3.1 リフレクタポートを使用したレイヤ 2 リモートポートミラーリングの設定作業リスト 9-8
9.3.2 出力ポートを使用したレイヤ 2 リモートポートミラーリングの設定作業リスト .. 9-8
9.3.3 ディスティネーションデバイスのリモートディスティネーショングループの設定 9-9
9.3.4 ソースデバイスのリモートソースグループの設定 9-10
9.4 複数モニタポートのローカルミラーリングの設定 9-13
9.4.1 設定の制限とガイドライン 9-14
9.4.2 設定手順 9-14
9.5 ポートミラーリングの表示と維持 9-15
9.6 ポートミラーリングの設定例 9-16
9.6.1 ローカルポートミラーリングの設定例 9-16
9.6.2 レイヤ 2 リモートポートミラーリングの設定例（リフレクタポート） 9-17
9.6.3 レイヤ 2 リモートポートミラーリングの設定例（出力ポート） 9-20
9.6.4 複数のモニタポートのローカルポートミラーリングの設定例 9-23

9章 ポートミラーリング

9.1 概要

ポートミラーリングはポートを通過したパケットを分析するために、データ監視端末が接続されているモニタポートへパケットをコピーします。

9.1.1 用語

以下にポートミラーリングの設定で使用する用語を示します。

I. ミラーリングソース

1 つのモニタ対象ポートをミラーリングソースにすることができます。モニタ対象ポートはソースポートと呼ばれます。ミラーリングソースを通過するパケットはパケットを解析するデータをモニタリングするデバイスに接続するポートにコピーされます。コピーはミラーパケットと呼ばれます。

II. ソースデバイス

ミラーリングソースが存在するデバイスは”送信元デバイス”あるいは”ソースデバイス”と呼ばれます。

III. ミラーリング宛先

ミラーリング宛先は、ミラーリングされたパケットの宛先ポート（別名モニタポートとも呼ばれます）であり、データ監視装置に接続します。モニタポートが存在するデバイスは"宛先デバイス"あるいは”ディスティネーションデバイス”と呼ばれます。モニタポートは、接続されている監視装置にミラーリングされたパケットを転送します。

モニタポートは複数のポートをモニタすることができ、場合によっては複数の重複したパケットを受信する可能性があります。たとえば、以下の状況が存在するとき、2つのパケットのコピーはポート 1 で受信されます。

- ポート 1 は同一デバイス上のポート 2 とポート 3 の送受信トラフィックをモニタします。
- パケットがポート 2 からポート 3 へ転送されます。

IV. ミラーリング方向

ミラーリング方向は、受信トラフィック、送信トラフィック、送受信トラフィックがあり、モニタリングソースでコピーされます。

- **受信** –　ミラーリングソースで受信したパケットをコピーします。
- **送信** –　ミラーリングソースに送信したパケットをコピーします。
- **送受信** –　ミラーリングソースで送受信したパケットをコピーします。

🕮 **メモ：**

- 受信トラフィックミラーリングでは、もとのパケットの VLAN タグもミラーリングされるパケットにコピーされます。
- 送信トラフィックミラーリングでは、ミラーリングされるパケットは送信インタフェースの VLAN タグを送信します。

V. ミラーリンググループ

ポートミラーリングはポートミラーリンググループによって実行されます。ミラーリンググループには 3 つのタイプ（ローカル、リモートソース、リモート宛先ミラーリング）があります。ミラーリンググループの詳細は、オペレーションマニュアルのセクション 11 *システム管理*”*ポートミラーリング*”の”*ポートミラーリングの分類と実行*”を参照してください。

VI. リフレクタポート、出力ポート、リモートプローブ VLAN

リフレクタポート、リモートプローブ VLAN、および出力ポートは、レイヤ 2 リモートポートミラーリングに使用されます。リモートプローブ VLAN は、ミラーリングされたパケットを宛先デバイスに送信するための専用の VLAN です。リフレクタポートと出力ポートのどちらも、送信元デバイス上に存在し、ミラーリングされたパケットをリモートプローブ VLAN に送信します。出力ポートは、リモートプローブ VLAN に属している必要がありますが、リフレクタポートはそうでなくても構いません。リフレクタポート、出力ポート、リモートプローブ VLAN、レイヤ 2 リモートポートミラーリングの詳細については、オペレーションマニュアルのセクション 11 *システム管理*”*ポートミラーリング*”の”*ポートミラーリングの分類と実行*”を参照してください。

🕮 **メモ：**

ポートミラーリングの装置でソースポート、宛先ポート、リフレクタポート、出力ポートを除くすべてのポートは共通ポートと呼ばれます。

9.1.2 ポートミラーリングの分類と実行

ポートミラーリングは、ローカルポートミラーリングとリモートポートミラーリングがあります。

- **ローカルポートミラーリング**－ミラーリングソースとミラーリング宛先が同一装置にあります。
- **リモートポートミラーリング**－ミラーリングソースとミラーリング宛先が異なる装置にあります。

I. ローカルポートミラーリング

ローカルポートミラーリングでは、以下の状況となります。

- ソースデバイスは、データをモニタリングするデバイスに直接接続されています。
- ソースデバイスは、データをモニタリングするデバイスにミラーリングしたパケットを転送する宛先デバイスとして動作できます。

ローカルミラーリンググループは、同一装置上のミラーリングソースとミラーリング宛先を含むミラーリンググループです。

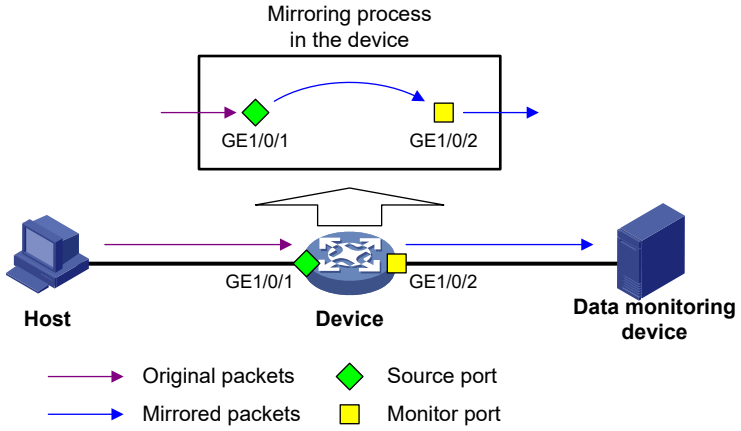


図 9-1 ローカルポートミラーリングの実行

図 9-1に示すように、ソースポート GigabitEthernet 1/0/1 とモニタポート GigabitEthernet 1/0/2 は同じデバイス上にあります。GigabitEthernet 1/0/1 のパケットは GigabitEthernet 1/0/2 にコピーされ、解析を行うためデータ監視装置に転送されます。

II. リモートポートミラーリング

リモートポートミラーリングでは、以下の状況となります。

- ミラーリングソースとミラーリング宛先は別のデバイス上に配置され、別のミラーリンググループに属します。
- ソースデバイスはモニタリングデバイスに直接接続されていません。
- ソースデバイスは宛先デバイスにミラーしたパケットをコピーします。宛先デバイスではデータをモニタリングするデバイスに転送します。

リモートソースグループはミラーリングソースを含むミラーリンググループです。リモート宛先グループはそれぞれミラーリングディスティネーションを含むミラーリンググループです。送信元デバイスと宛先デバイスの間のデバイスは、中間デバイスです。

ミラーリングソースとミラーリング宛先は同一レイヤ 2 ネットワークの異なる装置に存在するため、リモートポートミラーリングは、レイヤ 2 リモートポートミラーリングとも呼ばれます。

ソースデバイス上でリフレクタポートあるいは出力ポートが有効である場合、レイヤ 2 リモートポートミラーリングを動作させることができます。リフレクタポートを使用する方

式はリフレクタポート方式と呼ばれます。出力ポートを使用する方式は出力ポート方式と呼ばれます。

- **リフレクタポート方式**－パケットは以下のようにミラーリングされます。
  - ソースデバイスはミラーリングソースで受信されたパケットをリフレクタポートにコピーします。
  - リフレクタポートはリモートプローブ VLAN のミラーリングされたパケットをブロードキャストします。
  - 中間デバイスはリモートプローブ VLAN を通して宛先デバイスにミラーリングされたパケットを転送します。
  - ミラーリングされたパケットを受信すると、宛先デバイスはミラーリングされたパケットの ID がリモートプローブ VLAN ID と同一かどうか確認します。2 つの VLAN ID が一致する場合、宛先デバイスはモニタポートを通してデータをモニタするデバイスにミラーリングされたパケットを転送します。

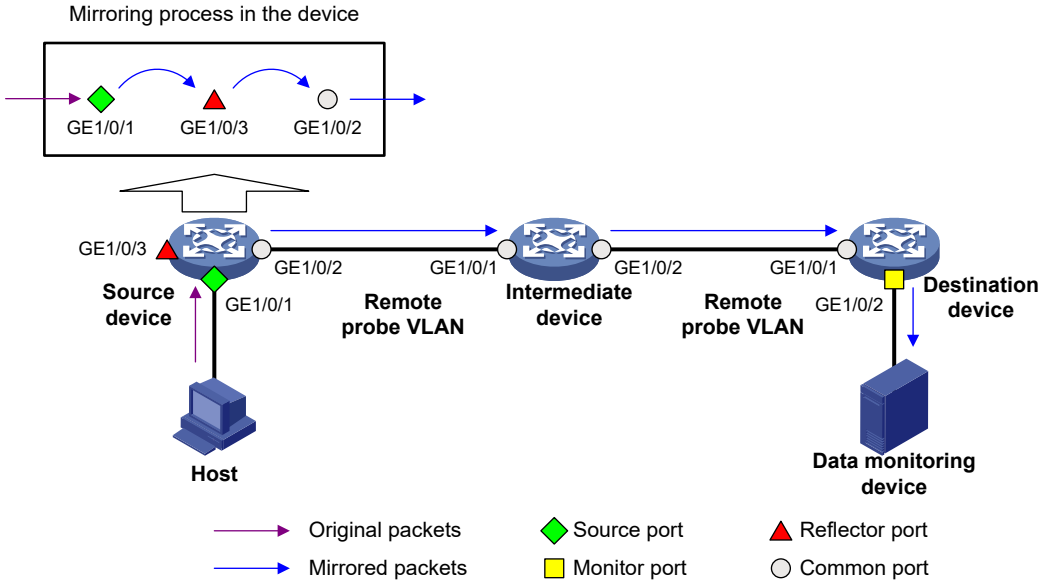


図 9-2 リフレクタポート方式によるレイヤ 2 リモートポートミラーリングの実行

- **出力ポート方式**－パケットは以下のようにミラーリングされます。
  - ソースデバイスはミラーリングソースで受信されたパケットを出力ポートにコピーします。
  - 出力ポートは中間デバイスにミラーリングされたパケットを転送します。
  - 中間デバイスはリモートプローブ VLAN のミラーリングされたパケットをブロードキャストし、宛先デバイスにミラーリングされたパケットを転送します。
  - ミラーリングされたパケットを受信すると、宛先デバイスはミラーリングされたパケットの ID がリモートプローブ VLAN ID と同一かどうか確認します。2 つの VLAN ID が一致する場合、宛先デバイスはモニタポートを通してデータをモニタするデバイスにミラーリングされたパケットを転送します。

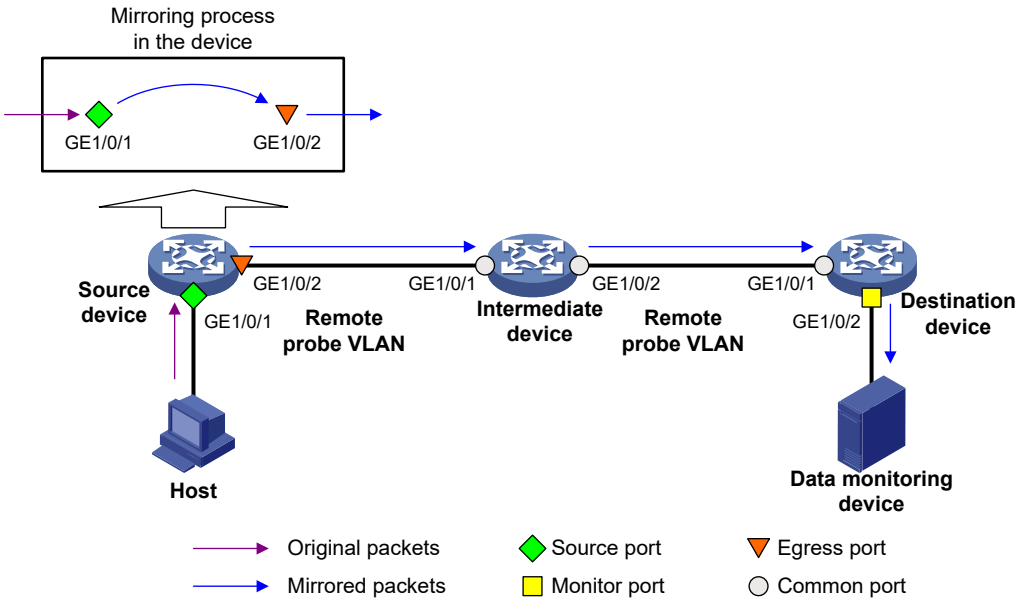


図 9-3 出力ポート方式によるレイヤ 2 リモートポートミラーリングの実行

リフレクタポート方式では、リフレクタポートはリモートプローブ VLAN のミラーリングされたパケットをブロードキャストします。ソースデバイスのソースポート以外のポートをリモートプローブ VLAN に割り当てることで、ローカルポートミラーリングが動作するリフレクタポート方式を使用することができます。出力ポート方式はこのような方法でローカルポートミラーリングを動作させることはできません。

ミラーされたパケットをレイヤ 2 転送するため、ソースデバイスと宛先デバイスに向いている中間デバイスのポートにリモートプローブ VLAN を割り当てます。

ミラーリンググループのポートの双方向のトラフィックをモニタするため、ソースデバイス、中間デバイス、宛先デバイスのリモートプローブ VLAN の MAC アドレスの学習を無効にする必要があります。MAC アドレスの学習の詳細は、オペレーションマニュアルのセクション 3 *アクセス "MAC アドレステーブル"*を参照してください。

9.2 ローカルポートミラーリングの設定

ローカルポートミラーリングはソースポートとミラーリングポートが設定されているときのみ適用されます。

9.2.1 ローカルポートミラーリング設定作業リスト

作業リスト
1.　（必須設定項目）ローカルミラーリンググループの作成
2.　（必須設定項目）ローカルミラーリンググループのソースポートの作成
3.　（必須設定項目）ローカルミラーリンググループのモニタポートの作成

9.2.2 ローカルミラーリンググループの作成

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. ローカルミラーリンググループを作成する	**mirroring-group** *group-id* **local**	デフォルト：設定なし

9.2.3 ローカルミラーリンググループのソースポートの作成

ローカルミラーリンググループのソースポートは、以下のいずれかの方法で設定することができます。

- system view でミラーリンググループにソースポートを割り当てます。
- interface view でソースポートとしてミラーリンググループにポートを割り当てます。

  interface view でミラーリンググループに複数のポートを割り当てる場合、上記の方法を繰り返してください。

I. 設定の制限とガイドライン

ローカルミラーリンググループにソースポートを設定するとき、以下の設定の制限とガイドラインに従ってください。

- レイヤ 2 アグリゲートインタフェースはソースポートとして設定することができません。
- ミラーリンググループは複数のソースポートを持つことができます。
- ソースポートはリフレクタポート、出力ポート、モニタポートとして同時に設定できません。

II. system view でのソースポートの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. 指定したローカルミラーリンググループにモニタポートを設定する	**mirroring-group** *group-id* **mirroring-port** *interface-list* { **both** | **inbound** | **outbound** }	デフォルト：設定なし

III. interface view でのソースポートの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. interface view に移行する	**interface** *interface-type interface-number*	―
3. 指定したミラーリンググループにモニタポートを設定する	**mirroring-group** *group-id* **mirroring-port** { **both** | **inbound** | **outbound** }	デフォルト：設定なし

9.2.4 ローカルミラーリンググループのモニタポートの作成

ミラーリンググループのモニタポートを設定する場合、以下のいずれかの方法で設定することができます。

- system view でミラーリンググループのモニタポートを設定します。
- interface view でポートをモニタポートとしてミラーリンググループに割り当てることができます。

I. 設定の制限とガイドライン

ローカルミラーリンググループにモニタポートを設定するとき、以下の設定の制限とガイドラインに従ってください。

- モニタポートでスパニングツリー機能を有効にしないでください。
- レイヤ 2 アグリゲートインタフェースはモニタポートとして設定することができません。
- モニタポートは、ポートミラーリングのために使用してください。データをモニタリングするデバイスがミラーされたトラフィックのみを受信するように、ポートミラーリングのモニタポートを使用してください。

II. system view でのモニタポートの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. 指定したローカルミラーリンググループにモニタポートを設定する	**mirroring-group** *group-id* **monitor-port** *interface-type interface-number*	デフォルト：設定なし

III. interface view でのモニタポートの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. interface view に移行する	**interface** *interface-type interface-number*	―
3. 指定したミラーリンググループにモニタポートを設定する	**mirroring-group** *group-id* **monitor-port**	デフォルト：設定なし

9.3 レイヤ2リモートポートミラーリングの設定

レイヤ 2 リモートポートミラーリングを設定するため、以下の作業を実行してください。

- ソースデバイスでリモートソースグループを設定してください。
- ディスティネーションデバイスで連携するリモートディスティネーショングループを設定してください。
- 中間デバイスがある場合、以下のデバイスとポートでリモートプローブ VLAN を許可するように設定してください。
  - □　中間デバイス

□　ソースデバイスと中間デバイスとディスティネーションデバイスで中間デバイスに接続されているポート

レイヤ 2 リモートポートミラーリングを設定するとき、以下の設定の制限とガイドラインに従ってください。

- 出力ポートをリモートプローブ VLAN に割り当ててください。リフレクタポートはリモートプローブ VLAN に割り当てる必要がありません。
- リモートディスティネーションデバイスにミラーパケットが到達するように、VLAN ID が削除あるいは変更されていないことを確認してください。
- MVRP とレイヤ 2 リモートポートミラーリングを同時に設定しないでください。設定した場合、MVRP は間違ったポートしてリモートプローブ VLAN を登録する可能性があります。それによりモニタポートは予期しないトラフィックのコピーを受信する可能性があります。
- ディスティネーションデバイス、中間デバイス、ソースデバイスの順番で設定することを推奨します。

9.3.1 リフレクタポートを使用したレイヤ 2 リモートポートミラーリングの設定作業リスト

作業リスト
（必須設定項目） ディスティネーションデバイスのリモートディスティネーショングループの設定
1． リモートディスティネーショングループの作成
2． リモートディスティネーショングループのモニタポートの設定
3． リモートディスティネーショングループのリモートプローブ VLAN の設定
4． リモートプローブ VLAN へのモニタポートの割り当て
（必須設定項目） ソースデバイスのリモートソースグループの設定
1． リモートソースグループの作成
2． リモートソースグループのソースポートの設定
3． リモートソースグループのリフレクタポートの設定
4． リモートソースグループのリモートプローブ VLAN の設定

9.3.2 出力ポートを使用したレイヤ 2 リモートポートミラーリングの設定作業リスト

作業リスト
（必須設定項目） ディスティネーションデバイスのリモートディスティネーショングループの設定
1． リモートディスティネーショングループの作成
2． リモートディスティネーショングループのモニタポートの設定
3． リモートディスティネーショングループのリモートプローブ VLAN の設定
4． リモートプローブ VLAN へのモニタポートの割り当て
（必須設定項目） ソースデバイスのリモートソースグループの設定
1． リモートソースグループの作成
2． リモートソースグループのソースポートの設定
3． リモートソースグループの出力ポートの設定
4． リモートソースグループのリモートプローブ VLAN の設定

9.3.3 ディスティネーションデバイスのリモートディスティネーショングループの設定

I. リモートディスティネーショングループの作成

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. リモートディスティネーショングループを作成する	**mirroring-group** *group-id* **remote-destination**	デフォルト：設定なし

II. リモートディスティネーショングループのモニタポートの設定

ミラーリンググループのモニタポートを設定する場合、以下のいずれかの方法で設定することができます。

- system view でミラーリンググループのモニタポートを設定します。
- interface view でモニタポートとしてポートをミラーリンググループに割り当てることができます。

リモートディスティネーショングループのモニタポートを設定するとき、以下の設定の制限とガイドラインに従ってください。

- モニタポートでスパニングツリー機能を無効にしてください。
- アグリゲートインタフェースはモニタポートとして設定することができません。
- モニタリングデバイスが、ミラーリングしたトラフィックのみを受信し、解析できるように、ミラーリングしたトラフィックと通常の転送トラフィックを混在しないで、ポートミラーリングのみモニタポートを使用してください。
- モニタポートは 1 つのミラーリンググループにのみ属することができます。

以下に system view でのリモートディスティネーショングループのモニタポートの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. リモートディスティネーショングループのモニタポートを設定する	**mirroring-group** *group-id* **monitor-port** *interface-type interface-number*	デフォルト：設定なし

以下に interface view でのリモートディスティネーショングループのモニタポートの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. interface view に移行する	**interface** *interface-type interface-number*	―
3. ポートをリモートディスティネーショングループのモニタポートに設定する	**mirroring-group** *group-id* **monitor-port**	デフォルト：設定なし

III. リモートディスティネーショングループのリモートプローブ VLAN の設定

リモートディスティネーショングループのリモートプローブ VLAN を設定するとき、以下の制限とガイドラインに従ってください。

- リモートプローブ VLAN を設定する前に、最初にスタティック VLAN を作成してください。
- VLAN がリモートプローブ VLAN として設定されている場合、ポートミラーリング専用としてリモートプローブ VLAN を使用してください。VLAN インタフェースを作成、あるいは VLAN のためにほかの機能を設定しないでください。
- ソースデバイスとディスティネーションデバイスの、リモートディスティネーショングループのリモートプローブ VLAN を同一に設定してください。

以下にリモートディスティネーショングループのリモートプローブ VLAN の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. リモートディスティネーショングループのリモートプローブ VLAN を設定する	**mirroring-group** *group-id* **remote-probe vlan** *vlan-id*	デフォルト：設定なし

IV. リモートプローブ VLAN へのモニタポートの割り当て

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. モニタポートの interface view に移行する	**interface** *interface-type interface-number*	―
3. プローブ VLAN にポートを割り当てる	● アクセスポート：**port access vlan** *vlan-id* ● トランクポート：**port trunk permit vlan** *vlan-id* ● ハイブリッドポート：**port hybrid vlan** *vlan-id* { **tagged** | **untagged** }	**port access vlan**コマンド、**port trunk permit vlan**コマンド、**port hybrid vlan**コマンドについての詳細は、コマンドマニュアルのセクション3 *アクセス VLAN*”を参照してください。

9.3.4 ソースデバイスのリモートソースグループの設定

I. リモートソースグループの作成

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. リモートソースグループを作成する	**mirroring-group** *group-id* **remote-source**	デフォルト：設定なし

II. リモートソースグループのソースポートの設定

リモートソースグループのソースポートを設定するとき、以下のいずれかの設定を行うことができます。

- system view でリモートソースグループにソースポートを割り当てます。
- interface view でリモートソースグループにソースポートを割り当てます。

  interface view でリモートソースグループに複数のポートを割り当てる場合、上記の方法を繰り返してください。

リモートソースグループのソースポートを設定するとき、以下の制限とガイドラインに従ってください。

- ミラーリンググループのソースポートをミラーリンググループのリモートプローブ VLAN に割り当てないでください。
- ミラーリンググループは複数のソースポートを持つことができます。
- ソースポートはリフレクタポート、モニタポート、出力ポートと同時に設定できません。
- ミラーリンググループは 1 つの入力トラフィックのミラーリング、1 つの出力トラフィックのミラーリングの最大 2 つの双方向のミラーリンググループを設定することができます。双方向のソースポートは、1 つのミラーリンググループにのみ割り当てることができます。
- 出力トラフィックのミラーリングあるいは双方向トラフィックのミラーリングを行う場合、装置は 1 つのミラーリンググループのみサポートします。
- レイヤ 2 アグリゲーションインタフェースはソースポートとして設定することができません。

以下に system view でのリモートソースグループのソースポートの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. リモートソースグループのソースポートを設定する	**mirroring-group** *group-id* **mirroring-port** *interface-list* { **both** | **inbound** | **outbound** }	デフォルト：設定なし

以下に interface view でのリモートソースグループのソースポートの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. interface view に移行する	**interface** *interface-type interface-number*	—
3. ポートをリモートソースグループのソースポートに設定する	**mirroring-group** *group-id* **mirroring-port** { **both** | **inbound** | **outbound** }	デフォルト：設定なし

III. リモートソースグループのリフレクタポートの設定

リモートソースグループのリフレクタポートを設定するとき、以下のいずれかの設定を行うことができます。

- system view でリモートソースのリフレクタポートを設定します。
- interface view でポートをリフレクタポートとしてリモートソースグループグループに割り当てることができます。

リモートソースグループのリフレクタポートを設定するとき、以下の制限とガイドラインに従ってください。

- リフレクタポートとして設定するポートは未使用のポートを設定してください。リフレクタポートにネットワークケーブルを接続しないでください。
- リフレクタポートとして設定された場合、ポートの既存の設定が削除されます。リフレクタポートのほかの機能を設定しないでください。
- IRF スタックポートが 1 つの物理インタフェースにのみ接続されている場合、リフレクタポートとして物理インタフェースを設定しないでください。設定した場合、IRF スタックが分割します。
- ミラーリンググループは 1 つのリフレクタポートのみ含めることができます。
- リフレクタポートの通信モード、MDI、通信速度の設定は変更することができません。

以下に system view でのリモートソースグループのリフレクタポートの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. リモートソースグループのリフレクタポートを設定する	**mirroring-group** *group-id* **reflector-port** *interface-type interface-number*	デフォルト：設定なし

以下に interface view でのリモートソースグループのリフレクタポートの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. interface view に移行する	**interface** *interface-type interface-number*	―
3. ポートをリモートソースグループのリフレクタポートに設定する	**mirroring-group** *group-id* **reflector-port**	デフォルト：設定なし

IV. リモートソースグループの出力ポートの設定

リモートソースグループの出力ポートを設定するとき、以下のいずれかの設定を行うことができます。

- system view でリモートソースグループの出力ポートを設定します。
- interface view でポートを出力ポートとしてリモートソースグループに割り当てることができます。

リモートソースグループの出力ポートを設定するとき、以下のガイドラインに従ってください。

- 出力ポートで以下の機能を無効にしてください。
  - □ スパニングツリー
  - □ 802.1X
  - □ IGMP snooping
  - □ スタティック ARP
  - □ MAC アドレス学習
- ミラーリンググループは 1 つの出力ポートのみ含めることができます。
- 既存のミラーリンググループのソースポートを出力ポートにすることはできません。

以下に system view でのリモートソースグループの出力ポートの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. リモートソースグループの出力ポートを設定する	**mirroring-group** *group-id* **monitor-egress** *interface-type interface-number*	デフォルト：設定なし

以下に interface view でのリモートソースグループの出力ポートの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. interface view に移行する	**interface** *interface-type interface-number*	ー
3. ポートをリモートソースグループの出力ポートに設定する	**mirroring-group** *group-id* **monitor-egress**	デフォルト：設定なし

V. リモートソースグループのリモートプローブ VLAN の設定

リモートソースグループのリモートプローブ VLAN を設定するとき、以下の制限とガイドラインに従ってください。

- リモートプローブ VLAN を設定する前に、スタティック VLAN が設定されていることを確認してください。
- リモートプローブ VLAN として VLAN を設定したとき、ポートミラーリング専用としてリモートプローブ VLAN を使用することを推奨します。VLAN インタフェースを作成、あるいは VLAN のためにほかの機能を設定しないでください。
- ソースデバイスと宛先デバイス上のリモートミラーリンググループは、同じリモートプローブ VLAN を使用する必要があります。

以下にリモートソースグループのリモートプローブ VLAN の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. リモートソースグループのリモートプローブ VLAN を設定する	**mirroring-group** *group-id* **remote-probe vlan** *vlan-id*	デフォルト：設定なし

9.4 複数モニタポートのローカルミラーリングの設定

通常、ローカルミラーリンググループのモニタポートは 1 つのみ設定できます。複数のデータモニタリング装置のローカルデバイスのトラフィックをモニタすることができません。複数のモニタポートをサポートするようにローカルポートミラーリングを設定するためレイヤ 2 リモートポートミラーリングのリモートプローブ VLAN を使用します。

レイヤ 2 リモートポートミラーリングで、ミラーパケットリモートプローブ VLAN が設定され、ミラーリングされたパケットがリモートプローブ VLAN にブロードキャストされます。複数のデータのモニタリングデバイスをリモートプローブ VLAN のメンバポートに接続することで、複数のデータモニタリング装置のローカルデバイスのトラフィックをモニタすることができます。

設定のフローは以下となります。

1) デバイスのリモートソースグループを作成します。
2) ミラーリンググループのソースポートを指定します。
3) リモートソースグループのリモートプローブ VLAN を設定します。
4) データモニタリングデバイスに接続しているポートをリモートプローブ VLAN に割り当てます。

これによってソースポートのミラーリングされたパケットはリモートプローブ VLAN にブロードキャストされます。そしてデータモニタリングデバイスに接続しているポートに送信されます。データモニタリングデバイスはミラーリングされたパケットを受信することができます。

9.4.1 設定の制限とガイドライン

複数のモニタポートでローカルポートミラーリングを設定するとき、以下の制限とガイドラインに従ってください。

- デバイスで使用されていないポートをリフレクタポートとして設定してください。リフレクタポートにネットワークケーブルを接続しないでください。
- ポートをリフレクタポートとして設定したとき、工場出荷状態の設定に戻ります。リフレクタポートでほかの機能を設定しないでください。
- ミラーリンググループのソースポートをミラーリンググループのリモートプローブ VLAN に割り当てないでください。
- VLAN は、1 つのリモートソースグループ用のリモートプローブ VLAN として動作することができます。ポートミラーリングのリモートプローブ VLAN と同時に使用しないでください。VLAN の VLAN インタフェースを作成あるいはほかの設定を実行しないでください。
- リモートプローブ VLAN はスタティック VLAN にする必要があります。
- リモートミラーリンググループのリモートプローブ VLAN として設定されている VLAN を削除する場合、最初にミラーリンググループからリモートプローブ VLAN を削除してください。

9.4.2 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. リモートソースグループを作成する	**mirroring-group** *group-id* **remote-source**	デフォルト：設定なし

操作	コマンド	補足
3. リモートソースグループのソースポートを設定する	● system view で設定する： **mirroring-group** *group-id* **mirroring-port** *interface-list* { **both** | **inbound** | **outbound** } ● interface view で設定する： 1. interface view に移行する： **interface** *interface-type interface-number* 2. ソースポートとしてミラーリングポートを割り当てる： **mirroring-group** *group-id* **mirroring-port** { **both** | **inbound** | **outbound** } 3. system view に戻る： **quit**	デフォルト：設定なし
4. リモートソースグループのリフレクタポートを設定する	**mirroring-group** *group-id* **reflector-port** *interface-type interface-number*	デフォルト：設定なし
5. リモートプローブ VLAN として設定される VLAN を作成する	**vlan** *vlan-id*	―
6. VLAN にモニタポートを割り当てる	**port** *interface-list*	デフォルト：VLAN1
7. system view に戻る	**quit**	―
8. リモートソースグループのリモートプローブ VLAN として VLAN を設定する	**mirroring-group** *group-id* **remote-probe vlan** *vlan-id*	デフォルト：設定なし

9.5 ポートミラーリングの表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
ミラーリンググループの情報を表示する	**display mirroring-group** { *group-id* | **all** | **local** | **remote-destination** | **remote-source** }

9.6 ポートミラーリングの設定例

9.6.1 ローカルポートミラーリングの設定例

I. ネットワーク要件

図 9-4に示すように、Marketing Department、Technical Department の 2 つの Department で双方向のパケットをモニタリングできるように、ソースポートでのローカルポートミラーリングを設定します。

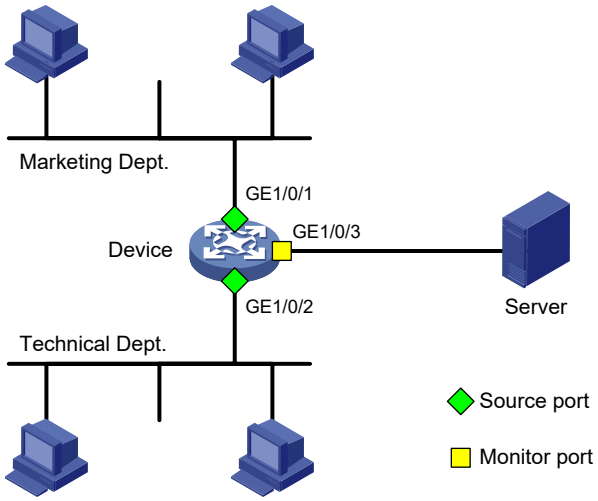


図 9-4 ネットワーク図

II. 設定手順

ローカルミラーリンググループ 1 を作成します。

```
<Device> system-view
[Device] mirroring-group 1 local
```

ローカルミラーリンググループ 1 のソースポートとして GigabitEthernet 1/0/1、GigabitEthernet 1/0/2 を設定します。

```
[Device] mirroring-group 1 mirroring-port gigabitethernet 1/0/1 gigabitethernet 1/0/2 both
```

ローカルミラーリンググループ 1 のモニタポートとして GigabitEthernet 1/0/3 を設定します。

```
[Device] mirroring-group 1 monitor-port gigabitethernet 1/0/3
```

モニタポート GigabitEthernet 1/0/3 のスパニングツリー機能を無効にします。

```
[Device] interface gigabitethernet 1/0/3
[Device-GigabitEthernet1/0/3] undo stp enable
[Device-GigabitEthernet1/0/3] quit
```

III. 設定の確認

すべてのミラーリンググループの設定を表示します。

```
[Device] display mirroring-group all
Mirroring group 1:
    Type: Local
    Status: Active
    Mirroring port:
        GigabitEthernet1/0/1  Both
        GigabitEthernet1/0/2  Both
    Monitor port: GigabitEthernet1/0/3
```

9.6.2 レイヤ 2 リモートポートミラーリングの設定例（リフレクタポート）

I. ネットワーク要件

図 9-5に示すように、Marketing Department の双方向トラフィックをモニタリングするため、レイヤ 2 リモートポートミラーリングを設定します。

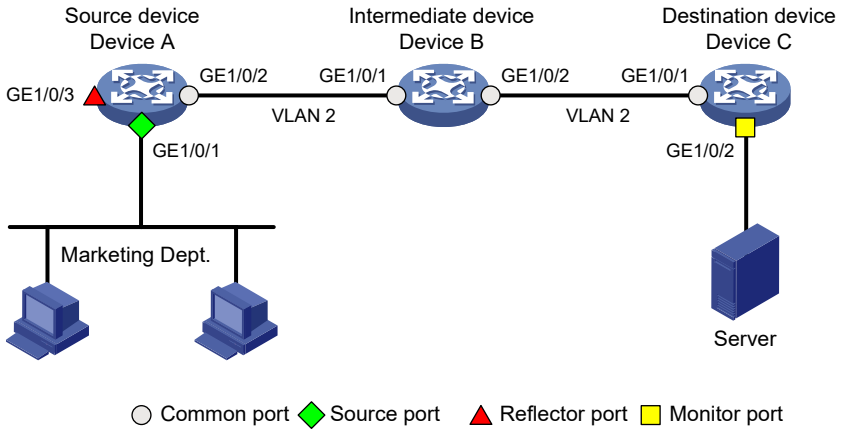


図 9-5 ネットワーク図

II. 設定手順

1)　Device C（ディスティネーションデバイス）を設定します。

トランクポートして GigabitEthernet 1/0/1 を設定し、VLAN 2 のパケットを許可するように設定します。

```
<DeviceC> system-view
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] port link-type trunk
[DeviceC-GigabitEthernet1/0/1] port trunk permit vlan 2
[DeviceC-GigabitEthernet1/0/1] quit
```

リモートディスティネーショングループを作成します。

```
[DeviceC] mirroring-group 2 remote-destination
```

VLAN 2 を作成します。

```
[DeviceC] vlan 2
```

VLAN 2 で MAC アドレス学習を無効にします。

```
[DeviceC-vlan2] undo mac-address mac-learning enable
[DeviceC-vlan2] quit
```

ミラーリンググループのリモートプローブ VLAN として設定される VLAN 2 を作成します。

```
[DeviceC] mirroring-group 2 remote-probe vlan 2
```

ミラーリンググループのモニタポートとして GigabitEthernet 1/0/2 を設定します。

```
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] mirroring-group 2 monitor-port
```

GigabitEthernet 1/0/2 のスパニングツリーを無効にします。

```
[DeviceC-GigabitEthernet1/0/2] undo stp enable
```

VLAN 2 に GigabitEthernet 1/0/2 を割り当てます。

```
[DeviceC-GigabitEthernet1/0/2] port access vlan 2
[DeviceC-GigabitEthernet1/0/2] quit
```

2)　Device B （中間デバイス）を設定します。

VLAN 2 を作成します。

```
<DeviceB> system-view
[DeviceB] vlan 2
```

VLAN 2 で MAC アドレス学習を無効にします。

```
[DeviceB-vlan2] undo mac-address mac-learning enable
[DeviceB-vlan2] quit
```

トランクポートして GigabitEthernet 1/0/1 を設定し、VLAN 2 のパケットを許可するように設定します。

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port link-type trunk
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 2
[DeviceB-GigabitEthernet1/0/1] quit
```

トランクポートして GigabitEthernet 1/0/2 を設定し、VLAN 2 のパケットを許可するように設定します。

```
[DeviceB] interface gigabitethernet 1/0/2
```

```
[DeviceB-GigabitEthernet1/0/2] port link-type trunk
[DeviceB-GigabitEthernet1/0/2] port trunk permit vlan 2
[DeviceB-GigabitEthernet1/0/2] quit
```

3)　Device A （ソースデバイス）を設定します。

リモートソースグループを作成します。

```
<DeviceA> system-view
[DeviceA] mirroring-group 1 remote-source
```

VLAN 2 を作成します。

```
[DeviceA] vlan 2
```

VLAN 2 で MAC アドレス学習を無効にします。

```
[DeviceA-vlan2] undo mac-address mac-learning enable
[DeviceA-vlan2] quit
```

ミラーリンググループのリモートプローブ VLAN として設定される VLAN 2 を作成します。

```
[DeviceA] mirroring-group 1 remote-probe vlan 2
```

ミラーリンググループのソースポートとして GigabitEthernet 1/0/1 を設定します。

```
[DeviceA] mirroring-group 1 mirroring-port gigabitethernet 1/0/1 both
```

ミラーリンググループのリフレクタポートとして GigabitEthernet 1/0/3 を設定します。

```
[DeviceA] mirroring-group 1 reflector-port gigabitethernet 1/0/3
This operation may delete all settings made on the interface. Continue? [Y/N]:
y
```

トランクポートして GigabitEthernet 1/0/2 を設定し、VLAN 2 のパケットを許可するように設定します。

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port link-type trunk
[DeviceA-GigabitEthernet1/0/2] port trunk permit vlan 2
[DeviceA-GigabitEthernet1/0/2] quit
```

III. 設定の確認

Device C のミラーリンググループの設定を確認します。

```
[DeviceC] display mirroring-group all
Mirroring group 2:
    Type: Remote destination
    Status: Active
    Monitor port: GigabitEthernet1/0/2
    Remote probe VLAN: 2
```

Device A のミラーリンググループの設定を確認します。

```
[DeviceA] display mirroring-group all
Mirroring group 1:
    Type: Remote source
    Status: Active
    Mirroring port:
        GigabitEthernet1/0/1  Both
    Reflector port: GigabitEthernet1/0/3
    Remote probe VLAN: 2
```

9.6.3 レイヤ 2 リモートポートミラーリングの設定例（出力ポート）

I. ネットワーク要件

図 9-6に示すように、Marketing Department の双方向トラフィックをモニタリングするため、レイヤ 2 リモートポートミラーリングを設定します。

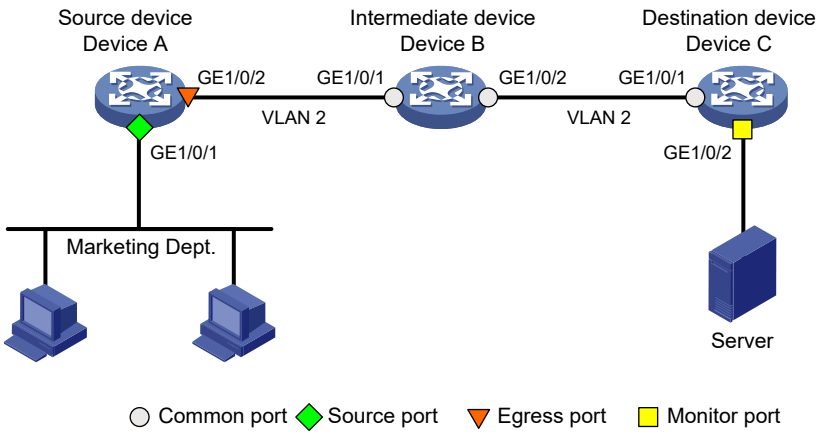


図 9-6 ネットワーク図

II. 設定手順

1)　Device C（ディスティネーションデバイス）を設定します。

トランクポートして GigabitEthernet 1/0/1 を設定し、VLAN 2 のパケットを許可するように設定します。

```
<DeviceC> system-view
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] port link-type trunk
[DeviceC-GigabitEthernet1/0/1] port trunk permit vlan 2
[DeviceC-GigabitEthernet1/0/1] quit
```

リモートディスティネーショングループを作成します。

```
[DeviceC] mirroring-group 2 remote-destination
```

VLAN 2 を作成します。

```
[DeviceC] vlan 2
```

VLAN 2 で MAC アドレス学習を無効にします。

```
[DeviceC-vlan2] undo mac-address mac-learning enable
[DeviceC-vlan2] quit
```

ミラーリンググループのリモートプローブ VLAN として設定される VLAN 2 を作成します。

```
[DeviceC] mirroring-group 2 remote-probe vlan 2
```

ミラーリンググループのモニタポートとして GigabitEthernet 1/0/2 を設定します。

```
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] mirroring-group 2 monitor-port
```

GigabitEthernet 1/0/2 のスパニングツリーを無効にします。

```
[DeviceC-GigabitEthernet1/0/2] undo stp enable
```

アクセスポートとして VLAN2 に GigabitEthernet 1/0/2 を割り当てます。

```
[DeviceC-GigabitEthernet1/0/2] port access vlan 2
[DeviceC-GigabitEthernet1/0/2] quit
```

2) Device B （中間デバイス）を設定します。

VLAN 2 を作成します。

```
<DeviceB> system-view
[DeviceB] vlan 2
```

VLAN 2 で MAC アドレスの学習を無効にします。

```
[DeviceB-vlan2] undo mac-address mac-learning enable
[DeviceB-vlan2] quit
```

トランクポートして GigabitEthernet 1/0/1 を設定し、VLAN 2 のパケットを許可するように設定します。

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port link-type trunk
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 2
[DeviceB-GigabitEthernet1/0/1] quit
```

トランクポートして GigabitEthernet 1/0/2 を設定し、VLAN 2 のパケットを許可するように設定します。

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] port link-type trunk
[DeviceB-GigabitEthernet1/0/2] port trunk permit vlan 2
[DeviceB-GigabitEthernet1/0/2] quit
```

3) Device A （ソースデバイス）を設定します。

リモートソースグループを作成します。

```
<DeviceA> system-view
[DeviceA] mirroring-group 1 remote-source
```

VLAN 2 を作成します。

```
[DeviceA] vlan 2
```

VLAN 2 で MAC アドレスの学習を無効にします。

```
[DeviceA-vlan2] undo mac-address mac-learning enable
[DeviceA-vlan2] quit
```

#ミラーリンググループのリモートプローブ VLAN として VLAN 2 を設定します。

```
[DeviceA] mirroring-group 1 remote-probe vlan 2
```

ミラーリンググループのソースポートとして GigabitEthernet 1/0/1 を設定します。

```
[DeviceA] mirroring-group 1 mirroring-port gigabitethernet 1/0/1 both
```

ミラーリンググループの出力ポートとして GigabitEthernet 1/0/2 を設定します。

```
[DeviceA] mirroring-group 1 monitor-egress gigabitethernet 1/0/2
```

トランクポートして GigabitEthernet 1/0/2 を設定し、VLAN 2 のパケットを許可するように設定します。

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port link-type trunk
[DeviceA-GigabitEthernet1/0/2] port trunk permit vlan 2
```

ポートのスパニングツリーを無効にします。

```
[DeviceA-GigabitEthernet1/0/2] undo stp enable
[DeviceA-GigabitEthernet1/0/2] quit
```

III. 設定の確認

Device C のミラーリンググループの設定を確認します。

```
[DeviceC] display mirroring-group all
Mirroring group 2:
    Type: Remote destination
    Status: Active
    Monitor port: GigabitEthernet1/0/2
    Remote probe VLAN: 2
```

Device A のミラーリンググループの設定を確認します。

```
[DeviceA] display mirroring-group all
Mirroring group 1:
    Type: Remote source
    Status: Active
    Mirroring port:
        GigabitEthernet1/0/1  Both
    Monitor egress port: GigabitEthernet1/0/2
```

```
    Remote probe VLAN: 2
```

9.6.4 複数のモニタポートのローカルポートミラーリングの設定例

I. ネットワーク要件

図 9-7に示すように、Department A、Department B、Department C は、GigabitEthernet1/0/1、GigabitEthernet1/0/2、GigabitEthernet1/0/3 を通して、それぞれ Device A と接続されています。3 つの部門の双方向トラフィックを監視できるように、3 つのデータモニタリングデバイス（Server A、Server B、Server C）を有効にし、ポートミラーリングを設定します。

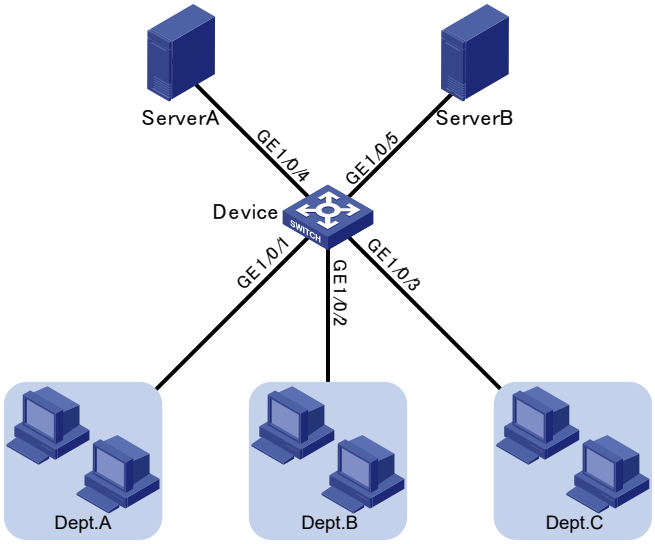


図 9-7 ネットワーク図

II. 設定手順

リモートソースミラーリンググループ 1 を作成します。

```
<Device> system-view
[Device] mirroring-group 1 remote-source
```

リモートソースグループ 1 のソースポートとして GigabitEthernet 1/0/1～GigabitEthernet 1/0/3 を設定します。

```
[Device] mirroring-group 1 mirroring-port gigabitethernet 1/0/1 to gigabitethernet 1/0/3 both
```

Device A の未使用ポート（例：GigabitEthernet 1/0/6）をリモートソースグループ 1 のリフレクタポートとして設定します。

```
[Device] mirroring-group 1 reflector-port gigabitethernet 1/0/6
This operation may delete all settings made on the interface. Continue? [Y/N]:y
```

#VLAN 10 を作成します。データモニタリングデバイスに接続されている GigabitEthernet 1/0/4、GigabitEthernet 1/0/5 を VLAN 10 に割り当てます。

```
[Device] vlan 10
[Device-vlan10] port gigabitethernet 1/0/4 to gigabitethernet 1/0/5
[Device-vlan10] quit
```

リモートソースグループ 1 のリモートプローブ VLAN として VLAN 10 を設定します。

```
[Device] mirroring-group 1 remote-probe vlan 10
```

目次

このセクションのページは **11-x-x** です。

10 章 トラフィックミラーリング 10-1
10.1 トラフィックミラーリングの設定作業リスト 10-1
10.2 一致条件の設定 10-1
10.3 トラフィック動作の設定 10-2
10.4 QoS ポリシーの設定 10-2
10.5 QoS ポリシーの適用 10-2
10.5.1 インタフェースへの QoS ポリシーの適用 10-2
10.5.2 VLAN への QoS ポリシーの適用 10-3
10.5.3 グローバルへの QoS ポリシーの適用 10-3
10.6 トラフィックミラーリングの設定例 10-3
10.6.1 ネットワーク要件 10-3
10.6.2 設定手順 10-4
10.6.3 設定の確認 10-5

10章 トラフィックミラーリング

トラフィックミラーリングは、パケットの監視と解析を行うために、指定したパケットを指定した宛先にコピーします。これは QoS ポリシーにもとづいて実行されます。

トラフィックミラーリングを設定するため、以下の作業を実行します。

- トラフィッククラスを定義し、ミラーリングされるパケットを分類するために一致条件を設定します。一致基準を定義し、解析されたパケットを柔軟に分類します。
- 指定された宛先に対する一致基準に適合するパケットをミラーリングするようにトラフィックの動作を設定します。

以下のインタフェースにミラーリングされるよう、トラフィックを設定することができます。

- **インタフェース**－データをモニタする装置に接続するインタフェースに一致するパケットをコピーします。データをモニタリングするデバイスはインタフェースで受信されたパケットを解析します。

QoS ポリシー、トラフィッククラス、トラフィック動作の詳細は、コマンドマニュアルのセクション 8 *ACL and QoS*"*QoS ポリシー*"を参照してください。

10.1 トラフィックミラーリングの設定作業リスト

作業リスト
（必須設定項目） 一致条件の設定
（必須設定項目）トラフィック動作の設定
（必須設定項目） QoSポリシーの設定
（必須設定項目） QoSポリシーの適用 ● インタフェースへのQoSポリシーの適用 ● VLANへのQoSポリシーの適用 ● グローバルへのQoSポリシーの適用

mirror-to コマンドを除いたコマンドの詳細は、コマンドマニュアルのセクション 8 *ACL and QoS*"*QoS ポリシー*"を参照してください。

10.2 一致条件の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	－
2. クラスを作成し class view に移行する	**traffic classifier** *classifier-name* [**operator** { **and** | **or** }]	デフォルト：設定なし
3. 一致条件の設定をする	**if-match** *match-criteria*	デフォルト：設定なし

10.3 トラフィック動作の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. トラフィック動作を設定し traffic behavior view に移行する	**traffic behavior** *behavior-name*	デフォルト：設定なし ミラーリングアクションを含むトラフィック動作に最大4つの設定を行うことができます。5つ以上のトラフィック動作を設定した場合、最初の4つのトラフィック動作が適用されます。
3. トラフィック動作のミラーリング宛先を指定する	**mirror-to interface** *interface-type interface-number*	デフォルト：設定なし トラフィック動作において、1つのインタフェースのみトラフィックを監視することができます。複数回コマンドを実行した場合、最後に行った設定が適用されます。
4. （オプション設定項目）トラフィック動作の設定を表示する	**display traffic behavior**	すべてのviewで実行可能です。

10.4 QoSポリシーの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. QoS ポリシーを作成し qos policy view に移行する	**qos policy** *policy-name*	デフォルト：設定なし
3. QoS ポリシーのトラフィック動作とクラスを関連づける	**classifier** *classifier-name* **behavior** *behavior-name*	デフォルト：設定なし
4. （オプション設定項目）QoS ポリシーの設定を表示する	**display qos policy**	すべてのviewで実行可能です。

10.5 QoSポリシーの適用

10.5.1 インタフェースへの QoS ポリシーの適用

インタフェースに QoS ポリシーを適用することで、インタフェース上の指定された方向にトラフィックをミラーリングすることができます。ポリシーは複数のインタフェースに適用することができますが、インタフェースの一つの方向（入力または出力）で、1 つのポリシーだけを適用することができます。

出力方向のトラフィックミラーリングはサポートしていません。

インタフェースに QoS ポリシーを適用するには、以下の手順に従ってください。

操作	コマンド
1. system view に移行する	**system-view**
2. interface view に移行する	**interface** *interface-type interface-number*
3. インタフェースに QoS ポリシーを適用する	**qos apply policy** *policy-name* **inbound**

10.5.2 VLAN への QoS ポリシーの適用

VLAN に QoS ポリシーを適用することで、VLAN 内のすべてのポート上の指定された方向にトラフィックをミラーリングすることができます。

出力方向のトラフィックミラーリングはサポートしていません。

VLAN に QoS ポリシーを適用するには、以下の手順に従ってください。

操作	コマンド
1. system view に移行する	**system-view**
2. VLAN に QoS ポリシーを適用する	**qos vlan-policy** *policy-name* **vlan** *vlan-id-list* **inbound**

10.5.3 グローバルへの QoS ポリシーの適用

グローバルに QoS ポリシーを適用することで、すべてのポートで指定された方向にトラフィックをミラーリングすることができます。

出力方向のトラフィックミラーリングはサポートしていません。

すべてのポートに QoS ポリシーを適用するには、以下の手順に従ってください。

操作	コマンド
1. system view に移行する	**system-view**
2. グローバルに QoS ポリシーを適用する	**qos apply policy** *policy-name* **global inbound**

10.6 トラフィックミラーリングの設定例

10.6.1 ネットワーク要件

図 10-1に示すように、サーバが以下のトラフィックをミラーリングできるようにトラフィックミラーリングを設定します。

- Technical Department がインターネットにアクセスする送信トラフィックを監視します。
- Technical Department が平日の 8:00 から 18:00 までの間に Marketing Department に送信する IP トラフィックを監視します。

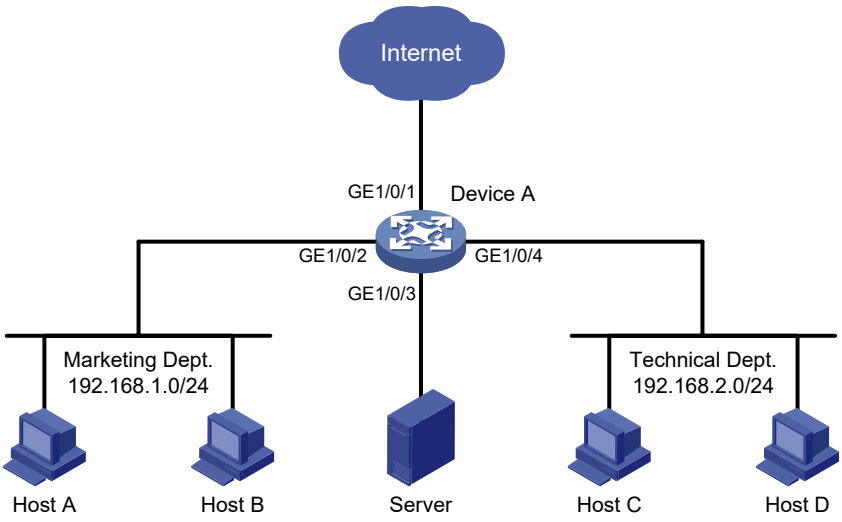


図 10-1 ネットワーク図

10.6.2 設定手順

時間範囲 work を作成します。work の就業時間は平日の 8:00 から 18:00 までです。

```
<DeviceA> system-view
[DeviceA] time-range work 8:00 to 18:00 working-day
```

就業時間内に Technical Department からのパケットがインターネットにアクセスできるよう拡張 IPv4 ACL 3000 を作成します。

```
[DeviceA] acl advanced 3000
[DeviceA-acl-ipv4-adv-3000] rule permit tcp source 192.168.2.0 0.0.0.255 destination-port eq www
[DeviceA-acl-ipv4-adv-3000] rule permit ip source 192.168.2.0 0.0.0.255 destination 192.168.1.0 0.0.0.255 time-range work
[DeviceA-acl-ipv4-adv-3000] quit
```

トラフィッククラス **tech_c** を作成し、ACL 3000 の一致条件を設定します。

```
[DeviceA] traffic classifier tech_c
[DeviceA-classifier-tech_c] if-match acl 3000
[DeviceA-classifier-tech_c] quit
```

トラフィック動作 **tech_b** を作成し、GigabitEthernet 1/0/3 ポートのトラフィックミラーリングの動作を設定します。

```
[DeviceA] traffic behavior tech_b
[DeviceA-behavior-tech_b] mirror-to interface gigabitethernet 1/0/3
[DeviceA-behavior-tech_b] quit
```

QoS ポリシー**tech_p** を作成し、QoS ポリシーのトラフィック動作 **tech_b** とトラフィッククラス **tech_c** を関連づけます。

```
[DeviceA] qos policy tech_p
[DeviceA-qospolicy-tech_p] classifier tech_c behavior tech_b
[DeviceA-qospolicy-tech_p] quit
```

QoS ポリシー**tech_p** を GigabitEthernet 1/0/4 の入力パケットに適用します。

```
[DeviceA] interface gigabitethernet 1/0/4
[DeviceA-GigabitEthernet1/0/4] qos apply policy tech_p inbound
[DeviceA-GigabitEthernet1/0/4] quit
```

10.6.3 設定の確認

設定の完了後、サーバは以下のことができます。

- Technical Department がインターネットにアクセスする送信トラフィックを監視することができます。
- 就業時間内に Technical Department が Marketing Department に送信する IP トラフィックのすべてを監視することができます。

目次

このセクションのページは **11-x-x** です。

11 章 sFlow.....11-1
11.1 プロトコルと標準.....11-1
11.2 sFlow 設定作業リスト.....11-1
11.3 sFlow エージェントと sFlow コレクタ情報の設定.....11-2
11.4 フローサンプリングの設定.....11-2
11.5 カウンタサンプリングの設定.....11-3
11.6 sFlow の表示と維持.....11-3
11.7 sFlow 設定例.....11-4
11.7.1 ネットワーク要件.....11-4
11.7.2 設定手順.....11-4
11.7.3 設定の確認.....11-5
11.8 sFlow 設定のトラブルシューティング.....11-5
11.8.1 リモート sFlow コレクタが sFlow パケットを受信できない.....11-5

11章 sFlow

sFlow （Sampled Flow） は、トラフィック監視技術です。

図 11-1に示すように、sFlow システムは、装置に組み込まれた sFlow エージェントとリモートの sFlow コレクタから構成されます。sFlow エージェントはトラフィック統計情報と sFlow が有効なインタフェースからのパケットを収集し、sFlow パケットにカプセル化します。sFlow パケットバッファが一杯になった時、または sFlow パケットのエージタイム（1 秒で固定）が終了した時、sFlow エージェントは以下の作業を行います。

- UDP データグラムに sFlow パケットをカプセル化します。
- 指定された sFlow コレクタに UDP データグラムを送信します。

sFlow コレクタは sFlow パケットを分析し、結果を表示します。1 つの sFlow コレクタは複数の sFlow エージェントをモニタすることができます。

sFlow には、以下の 2 つのサンプリングメカニズムがあります。

- **フローサンプリング** － パケットの内容情報を取得します。
- **カウンタサンプリング** － インタフェーストラフィック統計情報を取得します。

sFlow はフローサンプリングとカウンタサンプリングを同時に使用することが可能です。

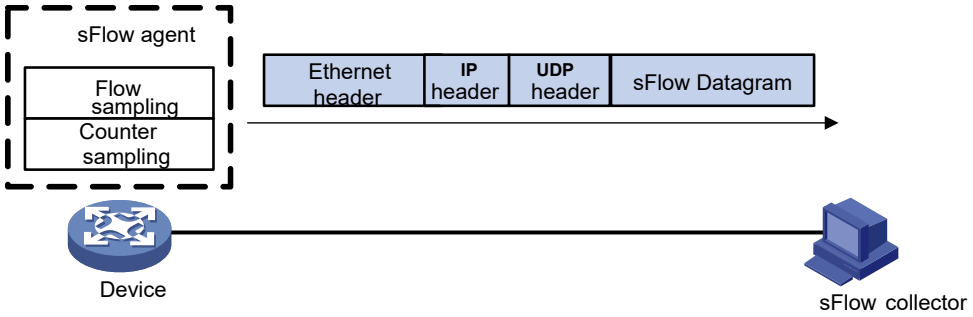


図 11-1 sFlow システム

11.1 プロトコルと標準

- RFC 3176, *InMon Corporation's sFlow: A Method for Monitoring Traffic in Switched and Routed Networks*
- sFlow.org, *sFlow Version 5*

11.2 sFlow設定作業リスト

作業リスト
（必須設定項目） sFlowエージェントとsFlowコレクタ情報の設定

作業リスト
以下の設定のすくなくとも1つを実行します。 ● フローサンプリングの設定 ● カウンタサンプリングの設定

11.3 sFlowエージェントとsFlowコレクタ情報の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. （オプション設定項目）sFlow エージェントの IP アドレスを設定する	**sflow agent** { **ip** *ipv4-address* | **ipv6** *ipv6-address* }	デフォルト : sFlow エージェントの IP アドレスは設定されていません。装置は定期的に sFlow エージェントの IP アドレスがあるかどうかを確認します。ない場合、装置は自動で sFlow エージェントの IPv4 アドレスを選択します。選択された IPv4 アドレスは設定ファイルに保存されません。 🕮 メモ : ● sFlow エージェントの IP アドレスを手動で設定することを推奨します。 ● 装置で sFlow エージェントの IP アドレスを1つのみ設定することができます。新しく設定した IP アドレスは、古い IP アドレスを上書きします。
3. sFlow コレクタ情報を設定する	**sflow collector** *collector-id* { **ip** *ipv4-address* | **ipv6** *ipv6-address* } [**port** *port-number*] [**datagram-size** *size*] [**time-out** *seconds*] [**description** *string*]	デフォルト : 設定なし
4. （オプション設定項目）sFlow パケットの送信元 IP アドレスを指定する	**sflow source** { **ip** *ipv4-address* | **ipv6** *ipv6-address* }*	デフォルト : ルーティングによって送信元 IP アドレスが決まります。

11.4 フローサンプリングの設定

Ethernet インタフェースでフローサンプリングの設定をします。インタフェースの sFlow エージェントは、以下の作業を行います。

1) 設定されたパラメータによってインタフェースのパケットをサンプリングします。
2) sFlow パケットにカプセル化します。
3) UDP パケットに sFlow パケットをカプセル化し、指定された sFlow コレクタに UDP パケットを送信します。

以下にフローサンプリングの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Ethernet interface view に移行する	**interface** *interface-type interface-number*	―
3. （オプション設定項目）フローサンプリングモードを設定する	**sflow sampling-mode random**	―
4. フローサンプリングを有効にし、パケットのサンプリング間隔を指定する	**sflow sampling-rate** *rate*	デフォルト：設定なし サンプリングするパケット数は8192以上の2^nに設定することを推奨します。たとえば32768です。
5. （オプション設定項目）パケットごとにコピーできるサンプルパケットの最大コピー長を設定する（パケットヘッダから数えます）	**sflow flow max-header** *length*	デフォルト：128バイト デフォルトにすることを推奨します。
6. sFlow コレクタを指定する	**sflow flow collector** *collector-id*	デフォルト：設定なし

11.5 カウンタサンプリングの設定

Ethernet インタフェースでカウンタサンプリングの設定をします。sFlow エージェントは以下の作業を行います。

1) sFlow エージェントは周期的にインタフェースのカウンタ情報を収集します。
2) sFlow パケットにカウンタ情報をカプセル化します。
3) UDP パケットに sFlow パケットをカプセル化し、指定された sFlow コレクタに UDP パケットを送信します。

以下にカウンタサンプリングの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Ethernet interface view に移行する	**interface** *interface-type interface-number*	―
3. カウンタサンプリングを有効にし、パケットのサンプリング間隔を指定する	**sflow counter interval** *interval*	デフォルト：無効
4. sFlow コレクタを指定する	**sflow counter collector** *collector-id*	デフォルト：設定なし

11.6 sFlowの表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
sFlow設定を表示する	**display sflow**

11.7 sFlow設定例

11.7.1 ネットワーク要件

図 11-2に示すように以下の設定を行います。

- Device は、GigabitEthernet 1/0/1 で、sFlow（フローサンプリングとカウンタサンプリングを含む）を有効にし、ポートのトラフィックを監視します。
- Device は、GigabitEthernet 1/0/3 を通して sFlow コレクタに sFlow パケットを送信します。

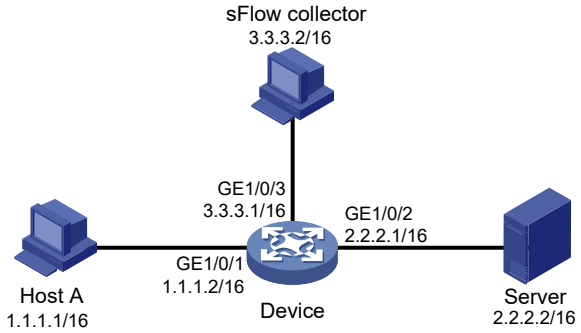


図 11-2 ネットワーク図

11.7.2 設定手順

1) 図 11-2に示すように、インタフェースの IP アドレス、サブネットマスクを設定します。（詳細は省略します。）
2) sFlow エージェントを設定し、sFlow コレクタの情報を設定します。

sFlow エージェントの IP アドレスを設定します。

```
<Device> system-view
[Device] sflow agent ip 3.3.3.1
```

sFlow コレクタの情報を設定します。sFlow コレクタの ID を 1、IP アドレスを 3.3.3.2、ポート番号を 6343（デフォルトです。）、説明を **netserver** に設定します。

```
[Device] sflow collector 1 ip 3.3.3.2 description netserver
```

3) カウンタサンプリングを設定します。

カウンタサンプリングを有効にし、GigabitEthernet 1/0/1 のサンプリング間隔を 120 秒に設定します。

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] sflow counter interval 120
```

カウンタサンプリングの sFlow コレクタ 1 を指定します。

```
[Device-GigabitEthernet1/0/1] sflow counter collector 1
```

4) フローサンプリングを設定します。

フローサンプリングを有効にし、モードを random、サンプリング間隔を 32768 に設定します。

```
[Device-GigabitEthernet1/0/1] sflow sampling-mode random
[Device-GigabitEthernet1/0/1] sflow sampling-rate 32768
```

フローサンプリングの sFlow コレクタ 1 を指定します。

```
[Device-GigabitEthernet1/0/1]  sflow flow collector 1
```

11.7.3 設定の確認

以下の項目を確認します。

- sFlow が有効な GigabitEthernet 1/0/1 がアクティブです。
- カウンタサンプリング間隔を 120 秒です。
- フローサンプリングのサンプリング間隔を 32768 に設定します。（32768 パケットごとに 1 パケットをサンプリングします。）

```
[Device-GigabitEthernet1/0/1]  display sflow
sFlow datagram version: 5
Global information:
Agent IP: 3.3.3.1(CLI)
Source address:
Collector information:
ID    IP              Port  Aging      Size VPN-instance Description
1     3.3.3.2         6343  N/A        1400              netserver
Port information:
Interface      CID   Interval(s) FID   MaxHLen Rate     Mode      Status
GE1/0/1        1     120         1     128     32768    Random    Active
```

11.8 sFlow設定のトラブルシューティング

11.8.1 リモート sFlow コレクタが sFlow パケットを受信できない

I. 症状

リモート sFlow コレクタが sFlow パケットを受信できません。

II. 分析

- sFlow コレクタが指定されていません。
- sFlow がインタフェースで設定されていません。
- sFlow エージェントで指定された sFlow コレクタの IP アドレスが、リモート sFlow コレクタの IP アドレスと異なります。
- 装置と sFlow コレクタ間の物理的なリンクが故障しています。

- sFlow パケット長が以下の 2 つの値の合計よりも小さいです。
  - □ sFlow パケットヘッダ長
  - □ パケットごとにフローサンプリングがコピーできるバイト数

III. 解決策

問題を解決するため以下のことを確認してください。

1) **display sflow** コマンドを使用し、sFlow が正しく設定されていることを確認してください。
2) sFlow コレクタと通信する装置に正しい IP アドレスが設定されていることを確認してください。
3) 装置と sFlow コレクタ間の物理的なリンクがアップしていることを確認してください。
4) sFlow パケット長が以下の 2 つの値の合計よりも大きいことを確認してください。
   - □ sFlow パケットヘッダ長
   - □ パケットごとにフローサンプリングがコピーできるバイト数（デフォルトの値を推奨します。）

目次

このセクションのページは **11-x-x** です。

12 章 Information Center 12-1
12.1 概要 12-1
12.1.1 ログタイプ 12-1
12.1.2 ログレベル 12-1
12.1.3 ログの出力先 12-2
12.1.4 デフォルト出力ルール 12-2
12.1.5 Diagnostic ログのデフォルト出力ルール 12-2
12.1.6 hidden ログのデフォルト出力ルール 12-3
12.1.7 ログフォーマット 12-3
12.2 Information Center 設定作業リスト 12-5
12.3 コンソールへのログの出力 12-6
12.4 モニタ端末へのログの出力 12-6
12.5 ログホストへのログの出力 12-7
12.6 ログバッファへのログの出力 12-7
12.7 ログファイルへのログの保存 12-8
12.8 ログの最小記録期間の設定 12-9
12.9 情報の同期出力の設定 12-9
12.10 モジュールのログ抑制の設定 12-10
12.11 インタフェースでのリンクアップ/ダウンのログ情報生成の無効化 12-10
12.12 ログメッセージの SNMP notification の送信の有効化 12-10
12.13 Diagnostic ログファイルへの Diagnostic ログの保存 12-11
12.14 Information Center の表示と維持 12-12
12.15 設定例 12-12
12.15.1 コンソールへのログ出力の設定例 12-12
12.15.2 UNIX ログホストへのログ出力の設定例 12-13
12.15.3 Linux ログホストへのログ出力の設定例 12-15

12章 Information Center

12.1 概要

Information Center は、送信元モジュールによって作成されたログを受信し、ユーザが定義した出力ルールに従って、異なる宛先にログを出力します。送信元モジュールにもとづいて、分類、フィルタリング、出力することができます。サポートされる送信元を表示するには、**info-center source ?**コマンドを使用します。

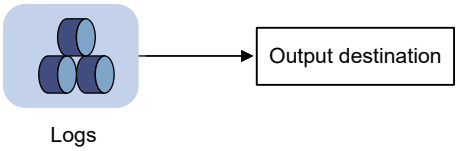


図 12-1 Information center の図

デフォルトで Information Center は有効です。Information Center が有効な場合、情報の分類や出力のため、システム性能にある程度影響を与えます。システムリソースが不十分である場合、リソースの消費を防ぐため Information Center を無効にしてください。

12.1.1 ログタイプ

ログは以下のタイプに分類されます。

- **Common ログ** － 共通なシステム情報の記録です。本章では、特に指定がない場合、ログは Common ログを示します。
- **Diagnostic ログ** － デバッグメッセージ記録です。
- **Hidden ログ** － 入力コマンドのような端末で表示されないログ情報です。

12.1.2 ログレベル

ログは重要度により 0～7 の 8 つのレベルに分類されます。装置は指定されたレベル以上の重要度レベルを出力します。たとえば出力ルールを 6（informational）と設定した場合、0～6 までの重要度のログが出力されます。

表 12-1 ログレベル

重要度	レベル	説明
0	Emergency	システムが使用できません。たとえば、システムの許可が終了しました。
1	Alert	即急に対応が必要です。たとえば、インタフェースのトラフィックが上限を超えました。

重要度	レベル	説明
2	Critical	深刻な状態です。たとえば、装置の温度が上限を超えました、電源モジュールが故障しました、FAN トレイが故障しました。
3	Error	エラー状態です。たとえば、リンク状態が変更しました。
4	Warning	警告状態です。たとえば、インタフェースが切断されました、あるいはメモリリソースが上限まで使われました。
5	Notification	通常通りですが、注意状態です。たとえば、装置にログインしました、あるいは装置が再起動しました。
6	Informational	情報メッセージです。たとえば、コマンドあるいはpingが実行されました。
7	Debug	デバッグメッセージです。

12.1.3 ログの出力先

システムは、コンソール、モニタ端末、ログバッファ、ログホスト、ログファイルの宛先にログを出力します。ログの出力先は独立しており、Information Center を有効にした後、設定することができます。

12.1.4 デフォルト出力ルール

デフォルト出力ルールはログの送信元モジュールと出力先の重要度レベルを定義しています。出力ルールにマッチしたログが、出力先に出力されます。表 12-2にデフォルト出力ルールを示します。

表 12-2 デフォルト出力ルール

出力先	ログ送信元モジュール	出力装置	重要度
コンソール	サポートされるすべてのモジュール	有効	Debug
モニタ端末	サポートされるすべてのモジュール	無効	Debug
ログホスト	サポートされるすべてのモジュール	有効	Informational
ログバッファ	サポートされるすべてのモジュール	有効	Informational
ログファイル	サポートされるすべてのモジュール	有効	Informational

12.1.5 Diagnostic ログのデフォルト出力ルール

Diagnostic ログは Diagnostic ログファイルにのみ出力することができます。送信元モジュールと重要度でフィルタすることはできません。表 12-3に Diagnostic ログのデフォルト出力ルールを示します。

表 12-3 Diagnostic ログのデフォルト出力ルール

出力先	ログ送信元モジュール	出力装置	重要度
Diagnosticログファイル	サポートされるすべてのモジュール	有効	Debug

12.1.6 hidden ログのデフォルト出力ルール

Hidden ログはログホスト、ログバッファ、ログファイルに出力することができます。表 12-4に hidden ログのデフォルト出力ルールを示します。

表 12-4 hidden ログのデフォルト出力ルール

出力先	ログ送信元モジュール	出力装置	重要度
ログホスト	サポートされるすべてのモジュール	有効	Informational
ログバッファ	サポートされるすべてのモジュール	有効	Informational
ログファイル	サポートされるすべてのモジュール	有効	Informational

12.1.7 ログフォーマット

ログのフォーマットは出力先で異なります。表 12-5にログ情報の標準のログフォーマットを示します。このフォーマットは使用するツールによって異なります。

表 12-5 ログフォーマット

出力先	フォーマット	例
コンソール、モニタ端末、ログバッファ、ログファイル	Prefix Timestamp Sysname Module/Level/Mnemonic: Content	%Nov 24 14:21:43:502 2010 Sysname SHELL/5/SHELL_LOGIN: VTY logged in from 192.168.1.26
ログホスト	<PRI>Timestamp Sysname %%vvModule/Level/Mnemonic: Source; Content	<190>Nov 24 16:22:21 2010 Sysname %%10 SHELL/5/SHELL_LOGIN: -DevIP=1.1.1.1; VTY logged in from 192.168.1.26

表 12-6にログメッセージのフィールドの説明を示します。

表 12-6 ログフィールドの説明

フィールド	説明
Prefix (information type)	ログホスト以外の宛先へのログはタイムスタンプの前識別子があります。 ● パーセントの識別子（%）はinformational以上のレベルのログを示しています。 ● アスタリスク（*）の識別子はデバッグログを示します。 ● アスタリスク（^）の識別子はdiagnosticログを示します。
PRI (priority)	ログホストへのログはタイムスタンプの前にプライオリティの識別子があります。プライオリティは、facility*8+levelという式で計算されます。 ● **facility**はロギングファシリティ名です。16～23の値に対応したファシリティ名はlocal0～local7です。**info-center loghost**コマンドで設定されます。ログホストでログのソースを識別するのに使われます。対応するログソースのログをクエリやフィルタするのに使用します。 ● **level**は重要度（Severity）の範囲で0～7です。表 12-1に詳細を示します。
Timestamp	ログが作成されたときの時間を記録します。 ログホストとほかの宛先に送信したログは、異なる精度のタイムスタンプを持ちます。タイムスタンプのフォーマットは異なるコマンドで設定されます。詳細を表 12-7と表 12-8に示します。
Sysname （ホスト名あるいはホストのIPアドレス）	Sysnameはログが作成された装置のホスト名あるいはIPアドレスです。装置の名前を修正する場合は**sysname**コマンドを使用します。
% % (vendor ID)	このフィールドは、ベンダを識別するために使用します。出力先がログホストである場合のみ表示されます。
vv (version information)	このフィールドは、ログのバージョン識別子で、値は10です。出力先がログホストである場合のみ表示されます。
Module	このフィールドは、システム情報を作成するモジュールの名前を示します。system viewで**info-center source ?**コマンドを入力すると、モジュールの一覧を参照できます。
Level	ログのレベルを識別します。表 12-1に重要度のレベルの詳細を示します。
Mnemonic	ログの概要が記載されます。最大32文字の文字列です。
Source	ログの送信元を識別します。値はIRFスタックメンバ装置のIDとログの送信者のIPアドレスが含まれます。
Content	ログの内容が記載されます。

表 12-7 タイムスタンプの精度と設定コマンド

アイテム	ログホスト	コンソール、モニタ端末、ログバッファ、ログファイル
精度	秒	ミリ秒
設定コマンド	**info-center timestamp loghost**	**info-center timestamp**

表 12-8 タイムスタンプパラメータの内容

パラメータ	内容	例
boot	時間はシステムが開始してからのミリ秒で記載された経過時間です。フォーマットはxxx.yyyです。xxxは上位32ビットでyyyは下位32ビットです。 ログホストを除いたすべての宛先に送信される出力先のログでサポートされます。	% 0.109391473 Sysname FTPD/5/FTPD_LOGIN: User ftp (192.168.1.23) has logged in successfully. 0.109391473は**boot**フォーマットのタイムスタンプです。
date	ログホストに出力されるログの現在日時と時間です。フォーマットはmmm dd hh:mm:ss yyyです。あるいはほかの宛先に出力されるログの現在日時と時間です。フォーマットはMMM DD hh:mm:ss:xxx YYYYです。すべてのログでサポートされます。	% May 30 05:36:29:579 2003 Sysname FTPD/5/FTPD_LOGIN: User ftp (192.168.1.23) has logged in successfully. May 30 05:36:29:579 2003は**date**フォーマットのタイムスタンプです。
iso	ISO 8601で規定されたタイムスタンプです。ログホストへ送付するログのみサポートします。	<189>2003-05-30T06:42:44 Sysname %%10FTPD/5/FTPD_LOGIN(l): User ftp (192.168.1.23) has logged in successfully. 2003-05-30T06:42:44は**iso**フォーマットのタイムスタンプです。
none	タイムスタンプが含まれていません。 すべてのログでサポートされます。	% Sysname FTPD/5/FTPD_LOGIN: User ftp (192.168.1.23) has logged in successfully. タイムスタンプが含まれません
no-year-date	年を除いた現在時間と時間です。フォーマットはMMM DD hh:mm:ss:xxxです。 ログホストに送信されるログのみでサポートされます。	<189>May 30 06:44:22 Sysname %%10FTPD/5/FTPD_LOGIN(l): User ftp (192.168.1.23) has logged in successfully. May 30 06:44:22は**no-year-date**フォーマットのタイムスタンプです。

12.2 Information Center設定作業リスト

作業リスト
以下の少なくとも1つの作業を実行します。 ● コンソールへのログの出力 ● モニタ端末へのログの出力 ● ログホストへのログの出力 ● ログバッファへのログの出力 ● ログファイルへのログの保存
（オプション設定項目） ログの最小記録期間の設定
（オプション設定項目） 情報の同期出力の設定
（オプション設定項目） モジュールのログ抑制の設定
（オプション設定項目） インタフェースでのリンクアップ/ダウンのログ情報生成の無効化
（オプション設定項目） ログメッセージのSNMP notificationの送信の有効化
Diagnosticログファイルへの Diagnosticログの保存

12.3 コンソールへのログの出力

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. Information Center を有効にする	**info-center enable**	デフォルト：有効
3. コンソールへのログの出力ルールを設定する	**info-center source** { *module-name* | **default** } { **console** | **logbuffer** | **logfile** | **loghost** | **monitor** } { **deny** | **level** *severity* }	デフォルト出力ルールについての詳細は、オペレーションマニュアルのセクション 11 *システム管理*”*Information Center*”の”*概要*”の”*デフォルト出力ルール*”を参照してください。
4. （オプション設定項目）タイムスタンプのフォーマットを設定する	**info-center timestamp** { **boot** | **date** | **none** }	デフォルト：**date**
5. user view に戻る	**quit**	ー
6. （オプション設定項目）コンソールへのログの出力を有効にする	**terminal monitor**	デフォルト: コンソールでは有効、モニタ端末では無効です。
7. 現在の端末でデバッグ情報の表示を有効にする	**terminal debugging**	デフォルト：無効
8. （オプション設定項目）コンソールに出力されるログの重要度を設定する	**terminal logging level** *severity*	デフォルト：6（informational）

12.4 モニタ端末へのログの出力

AUX、VTY、VTY line を通して装置にログインしているモニタ端末です。

以下にモニタ端末へのログ出力の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. Information Center を有効にする	**info-center enable**	デフォルト：有効
3. モニタ端末へのログの出力ルールを設定する	**info-center source** { *module-name* | **default** } { **console** | **logbuffer** | **logfile** | **loghost** | **monitor** } { **deny** | **level** *severity* }	デフォルト出力ルールについての詳細は、オペレーションマニュアルのセクション 11 *システム管理*”*Information Center*”の”*概要*”の”*デフォルト出力ルール*”を参照してください。
4. （オプション設定項目）タイムスタンプのフォーマットを設定する	**info-center timestamp** { **boot** | **date** | **none** }	デフォルト：**date**
5. user view に戻る	**quit**	ー

操作	コマンド	補足
6. モニタ端末へのログの出力を有効にする	**terminal monitor**	デフォルト: コンソールでは有効、モニタ端末では無効です。
7. 現在の端末でデバッグ情報の表示を有効にする	**terminal debugging**	デフォルト：無効
8. （オプション設定項目）モニタ端末に出力されるログの重要度を設定する	**terminal logging level** *severity*	デフォルト：6（informational）

12.5 ログホストへのログの出力

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. Information Center を有効にする	**info-center enable**	デフォルト：有効
3. ログホストへのログの出力ルールを設定する	**info-center source** { *module-name* | **default** } { **console** | **logbuffer** | **logfile** | **loghost** | **monitor** } { **deny** | **level** *severity* }	デフォルト出力ルールについての詳細は、オペレーションマニュアルのセクション 11 *システム管理*”*Information Center*”の”*概要*”の”*デフォルト出力ルール*”を参照してください。
4. （オプション設定項目）出力ログの送信元 IP アドレスを指定する	**info-center loghost source** *interface-type interface-number*	デフォルト: ルータの出力インタフェースにマッチするプライマリIPアドレスです。
5. （オプション設定項目）タイムスタンプのフォーマットを設定する	**info-center timestamp loghost** { **date** | **iso** | **no-year-date** | **none** }	デフォルト：**date**
6. ログホストを指定し、関連するパラメータを設定する	**info-center loghost** { *hostname* | *ipv4-address* | **ipv6** *ipv6-address* } [**port** *port-number*] [**facility** *local-number*]	デフォルト：設定なし *port-number*引数はログホストで設定された値と同じにする必要があります。異なる場合ログを受信できません。装置は最大20のログホストをサポートします。

12.6 ログバッファへのログの出力

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. Information Center を有効にする	**info-center enable**	デフォルト：有効
3. ログバッファへの出力を有効にする	**info-center logbuffer**	デフォルト：有効

操作	コマンド	補足
4.　（オプション設定項目）ログバッファに保存できるバッファサイズの最大数を設定する	**info-center logbuffer size** *buffersize*	デフォルト：512
5.　ログバッファの出力ルールを設定する	**info-center source** { *module-name* | **default** } { **console** | **logbuffer** | **logfile** | **loghost** | **monitor** } { **deny** | **level** *severity* }	デフォルト出力ルールについての詳細は、オペレーションマニュアルのセクション 11 *システム管理*”*Information Center*”の”*概要*”の”*デフォルト出力ルール*”を参照してください。
6.　（オプション設定項目）タイムスタンプのフォーマットを設定する	**info-center timestamp** { **boot** | **date** | **none** }	デフォルト：**date**

12.7 ログファイルへのログの保存

システムは指定された間隔（デフォルトで 24 時間）でログバッファのログをログファイルに保存します。また手動で保存することができます。ログファイルバッファにログを保存した後、システムはログファイルバッファをクリアします。

ログファイルが容量に達すると、システムは最初のログに新しいログを上書きします。

以下にログファイルへのログの保存の設定を示します。

操作	コマンド	補足
1.　system view に移行する	**system-view**	ー
2.　Information Center を有効にする	**info-center enable**	デフォルト：有効
3.　ログファイル機能を有効にする	**info-center logfile enable**	デフォルト：有効
4.　（オプション設定項目）ログファイルの最大記憶容量を設定する	**info-center logfile size-quota** *size*	デフォルト：10MB ログファイルの動作を正常に行うため、1MB～10MBのサイズに設定してください。
5.　（オプション設定項目）ログファイルを保存するディレクトリを指定する	**info-center logfile directory** *dir-name*	デフォルト：flash:/logfile IRFスタックの再起動やマスタ/メンバの切り替えで設定は消去されます。
6.　ログファイルにログファイルバッファのログを保存する	● ログファイルを記録する間隔を設定する：**info-center logfile frequency** *freq-sec* ● 手動でログファイルを記録する：**logfile save**	デフォルト：ログファイルを記録する間隔は86400秒です。 すべてのviewで**logfile save**コマンドを実行できます。

🕮 **メモ：**

- **info-center logfile frequency** コマンドでログファイルをセーブする周期を著しく短くした場合、フラッシュメモリの書き込み可能回数の超過や、装置動作に影響を与える恐れがあります。したがって、通常はデフォルト値での使用を推奨します。
- ログファイルのサイズは、フラッシュメモリの空き容量を超えない範囲で設定する必要があります。通常はデフォルト値で使用することを推奨します。**info-center logfile size-quota** コマンドで設定を変更する場合、フラッシュメモリの空き容量を **dir** コマンドで確認してください。

12.8 ログの最小記録期間の設定

ログバッファにあるログの記録期間の最小値を設定することができます。この機能はログが指定した時間内に新しいログによって上書きしてしまうことを防ぎます。

ログバッファあるいはログファイルが一杯になったとき、新しいログはデフォルトでもっとも古いログに新しいログを上書きします。最小記録期間を設定した後、システムはログを削除するかどうか決定するため、ログの最小記録期間を確認します。システムクロックからログが作成された時間を引いた時間はログの記録期間となります。

- ログの記録期間が最小記録期間以下である場合、システムはログを削除しません。新しいログは保存されません。
- ログの記録期間が最小記録期間より長い場合、システムは新しいログを保存するため、ログを削除します。

以下にログの最小記録期間の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. ログの最小記録期間を設定する	**info-center syslog min-age** *min-age*	デフォルト：設定なし

12.9 情報の同期出力の設定

システムログの出力が行われると、設定の操作が中断されてしまいます。ログが出力される前に、以前に入力されたコマンドを見つける必要があります。

情報の同期出力とは、システムログの出力によりユーザの入力が中断された場合、中断されたところから操作を継続できるようにするため、ログの出力後、以前に入力されたコマンドおよび、コマンドプロンプト（編集モードのコマンドプロンプト、あるいは対話モードの[Y/N]の文字列）を表示させることができます。

以下に情報の同期出力の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. 情報の同期出力を設定する	**info-center synchronous**	デフォルト：無効

12.10 モジュールのログ抑制の設定

I. モジュールのログ抑制

ログの出力を抑止します。この機能を使用して、関係のないログを除外できます。

モジュールの特定の mnemonic を持つすべてのログまたはログの出力を抑制するログ抑制ルールを設定するには、次の作業を実行します。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. モジュールのログ抑制ルールを設定する	**info-center logging suppress module** *module-name* **mnemonic** { **all** | *mnemonic-value* }	デフォルト : 装置はモジュールからのログの出力を抑制しません。

12.11 インタフェースでのリンクアップ/ダウンのログ情報生成の無効化

デフォルトでは、インタフェースのリンク状態が変わるときに、装置のすべてのインタフェースはリンクアップ/ダウンのログ情報を生成します。そのため、以下のような場合、指定したインタフェースの情報生成を無効にすることができます。

インタフェースの情報を監視するため、通常はデフォルトの有効にすることを推奨します。

- あるインタフェースの状態にのみ関係している場合です。この場合、ほかのインタフェースのリンクアップ/ダウンのログ情報を生成できないようにします。
- インタフェースのリンク状態が安定せず、不必要なログ情報が連続して生成される場合です。この場合、ほかのインタフェースのリンクアップ/ダウンのログ情報を生成できないようにします。

以下にインタフェースのリンクアップ/ダウンのログ情報の生成を無効の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. interface view に移行する	**interface** *interface-type interface-number*	ー
3. インタフェースのリンクアップ/ダウンのログ情報の生成を無効にする	**undo enable log updown**	デフォルト : すべてのインタフェースは、インタフェースの状態が変化したとき、リンクアップ/ダウンのログ情報を生成します。

12.12 ログメッセージのSNMP notificationの送信の有効化

snmp-agent trap enable syslog コマンドを有効にすると、装置はシスログメッセージによる SNMP notification の送信を有効にします。

装置は SNMP notification をカプセル化し、SNMP モジュールとログバッファに送信します。

SNMP モジュールが受信した SNMP notification を正常に送信するため、装置で SNMP の設定を行ってください。SNMP の設定については、オペレーションマニュアルのセクション 11 *システム管理*“*SNMP*”を参照してください。

以下にシスログメッセージによる SNMP notification の送信を有効化の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. ログメッセージの SNMP notification の送信を有効にする	**snmp-agent trap enable syslog**	デフォルト：無効

12.13 Diagnosticログファイルへの Diagnosticログの保存

I. Diagnostic ログの保存

デフォルトでは、Diagnostic ログファイル機能は、24 時間ごとに Diagnostic ログファイルバッファから Diagnostic ログファイルに Diagnostic ログを保存します。保存間隔を調整するか、Diagnostic ログを Diagnostic ログファイルに手動で保存できます。Diagnostic ログを Diagnostic ログファイルに保存すると、システムは Diagnostic ログファイルバッファを削除します。

装置がサポートする Diagnostic ログファイルは 1 つだけです。Diagnostic ログファイルの容量が最大です。容量に達すると、システムは最も古い Diagnostic ログを新しいログに置き換えます。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. Diagnostic ログファイル機能を有効にする	**info-center diagnostic-logfile enable**	デフォルト：有効
3. （オプション設定項目）Diagnostic ログファイルの最大サイズを設定する	**info-center diagnostic-logfile quota** *size*	デフォルト：10 MB 正常に動作させるには*size*を 1 MB~10 MBに設定します。
4. （オプション設定項目）Diagnostic ログファイルのディレクトリを指定する	**info-center diagnostic-logfile directory** *dir-name*	デフォルト：**flash:/diagfile** このコマンドは、IRFスタックリブートまたはマスタ/下位スイッチオーバーが発生した場合には実行できません。

操作	コマンド	補足
5. Diagnostic ログファイルバッファ内の Diagnostic ログを Diagnostic ログファイルに保存する	必要に応じて1つのオプションを選択する ● 自動Diagnosticログファイルの保存間隔を設定 **info-center diagnostic-logfile frequency** *freq-sec* ● DiagnosticログをDiagnostic ログファイルに手動で保存 **diagnostic-logfile save**	デフォルト：保存間隔は86400秒 **diagnostic-logfile save**コマンドはどのviewでも使用できます。

12.14 Information Centerの表示と維持

すべての view で **display** コマンドを実行でき、user view で **reset** コマンドを実行できます。

操作	コマンド
Diagnosticログファイルの設定を表示する	**display diagnostic-logfile summary**
各出力先の情報を表示する	**display info-center**
ログバッファの状態とログ情報を表示する	**display logbuffer** [**reverse**] [**level** *severity* | **size** *buffersize* | **slot** *slot-number*]*
ログバッファの概要を表示する	**display logbuffer summary** [**level** *severity* | **slot** *slot-number*]*
ログファイルの設定を表示する	**display logfile summary**
ログバッファを削除する	**reset logbuffer**

12.15 設定例

12.15.1 コンソールへのログ出力の設定例

I. ネットワーク要件

Device は warning 以上の重要度のレベルの FTP ログをコンソールに出力するように設定します。

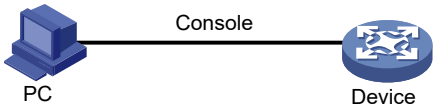


図 12-2 ネットワーク図

II. 設定手順

Information Center を有効にします。

```
<Device> system-view
[Device] info-center enable
```

コンソールへのログ出力を無効にします。

```
[Device] info-center source default console deny
```

それぞれのチャネルのデフォルトのシステム設定が異なるため、特定のチャネル（この例では **console**）では、必要に応じて、すべてのモジュールのログ情報の出力を無効にし、不要な情報が出力されないように出力ルールを設定します。

warning レベル以上の重要度の FTP ログをコンソールに出力するように設定します。

```
[Device] info-center source ftp console level warning
[Device] quit
```

コンソールでログの表示を有効にします。（この機能はデフォルトで有効です。）

```
<Device> terminal logging level 6
<Device> terminal monitor
The current terminal is enabled to display logs.
```

設定を行った後、FTP モジュールがログを生成した場合、Information Center は自動的にコンソールにログを送信し、ログを表示します。

12.15.2 UNIX ログホストへのログ出力の設定例

I. ネットワーク要件

Device が informational 以上の重要度のレベルの FTP ログを UNIX ログホストに出力するように設定します。



図 12-3 ネットワーク図

II. 設定手順

設定を行う前に、Device とログホストが互いに通信可能であることを確認してください。（詳細は省略します。）

1)　Device を設定します。

Information Center を有効にします。

```
<Device> system-view
[Device] info-center enable
```

ログホスト 1.2.0.1/16 を指定し、ロギングファシリティを **local4** に指定します。

```
[Device] info-center loghost 1.2.0.1 facility local4
```

ログホストにログの出力を無効にします。

```
[Device] info-center source default loghost deny
```

不要な情報が出力されないようにするため、出力ルールを設定する前に、ログを出力するすべてのモジュールが、指定した宛先（この例では **loghost**）に出力しないようにします。

informational レベル以上の重要度の FTP ログをログホストに出力するように設定します。

```
[Device] info-center source ftp loghost level informational
```

2)　ログホストを設定します。

以下の設定は Solaris で行ったものです。ほかの UNIXシステムの設定は同様に行います。

a)　rootユーザとしてログホストにログインします。

b)　ディレクトリ/**var/log**/にサブディレクトリ**Device**を作成します。ディレクトリ**Device**にファイル**info.log**を作成し、**Device**からログを保存します。

```
# mkdir /var/log/Device
# touch /var/log/Device/info.log
```

c)　ディレクトリ/**etc**/のファイル**syslog.conf**を編集し、以下の内容を追加します。

```
# Device configuration messages
local4.info /var/log/Device/info.log
```

この設定で、ホストがログを受信するために使用する **local4** はロギングファシリティの名前です。**info** は重要度のレベルです。UNIX システムは、**informational** の重要度のログ情報をファイル/**var/log/Device/info.log** に記録します。

🕮 **メモ：**

ファイル/**etc/syslog.conf** を編集するときのガイドラインを以下に示します。

- コメントは個別の行に記入し、#記号で始めてください。
- ファイル名に不要なスペース等をいれないでください。
- ロギングファシリティ名とファイル/**etc/syslog.conf** が指定するログ情報の重要度は、**info-center loghost** コマンドと **info-center source** コマンドで Device に設定したものと一致しなければなりません。一致しないと、ログ情報は正しくログホストに出力されないことがあります。

---

d)　**syslogd**のプロセスIDを表示します。**syslogd**プロセスを削除し、**syslogd**の使用を再開するコマンド（**-r**オプション変更された構成を実施させる）を実行してください。

```
# ps -ae | grep syslogd
147
```

```
# kill -HUP  147
# syslogd -r &
```

上記設定後は、Device は関連するファイルに FTP ログ情報を保存できるようになります。

12.15.3 Linux ログホストへのログ出力の設定例

I. ネットワーク要件

Device が informational の重要度のレベルの FTP ログを Linux ログホスト 1.2.0.1/16 に出力するように設定します。



図 12-4 ネットワーク図

II. 設定手順

設定を行う前に、Device とログホストが互いに通信可能であることを確認してください。（詳細は省略します。）

1)　Device を設定します。

Information Center を有効にします。

```
<Device> system-view
[Device] info-center enable
```

ログホスト 1.2.0.1/16 を指定し、ロギングファシリティを **local5** に指定します。

```
[Device] info-center loghost 1.2.0.1 facility local5
```

ログホストにログの出力を無効にします。

```
[Device] info-center source default loghost deny
```

不要な情報が出力されないようにするため、出力ルールを設定する前に、ログを出力するすべてのモジュールが、指定した宛先（この例では **loghost**）に出力しないようにします。

informational レベル以上の重要度の FTP ログをログホストに出力するように設定します。

```
[Device] info-center source ftp loghost level informational
```

2)　ログホストを設定します。

以下の設定は Solaris で行ったものです。ほかの UNIXシステムの設定は同様に行います。

a)　rootユーザとしてログホストにログインします。

b)　ディレクトリ/**var/log**/にサブディレクトリ**Device**を作成します。ディレクトリ

Deviceにファイル**info.log**を作成し、**Device**からログを保存します。

```
# mkdir /var/log/Device

# touch /var/log/Device/info.log
```

c)　ディレクトリ/**etc**/のファイル**syslog.conf**を編集し、以下の内容を追加します。

```
# Device configuration messages
local5.info /var/log/Device/info.log
```

この設定で、ホストがログを受信するために使用する **local5** はロギングファシリティの名前です。**info** は重要度のレベルです。Linux システムは、**informational** の重要度のログ情報をファイル/**var**/**log**/**Device**/**info.log** に記録します。

🕮 **メモ：**

ファイル/**etc/syslog.conf** を編集するときのガイドラインを以下に示します。

- コメントは個別の行に記入し、#記号で始めてください。
- ファイル名に不要なスペース等をいれないでください。
- ロギングファシリティ名とファイル/**etc/syslog.conf** が指定するログ情報の重要度は、**info-center loghost** コマンドと **info-center source** コマンドで Device に設定したものと一致しなければなりません。一致しないと、ログ情報は正しくログホストに出力されないことがあります。

---

d)　**syslogd**のプロセスIDを表示し、**syslogd**プロセスを削除、**syslogd**の使用を再開するコマンド（**-r**オプション変更された構成を実施させる）を実行してください。

Linux ログホストで **syslogd** プロセスに**-r** のオプションが付けられていることを確認してください。

```
# ps -ae | grep syslogd

147

# kill -9 147

# syslogd -r &
```

上記設定後は、Device は関連するファイルにログ情報を保存できるようになります。

目次

このセクションのページは **11-x-x** です。

13 章 NetMeister 13-1
13.1 概要 13-1
13.1.1 NetMeister の利用 13-1
13.1.2 設定手段について 13-3
13.2 設定作業リスト 13-4
13.2.1 手動設定による NetMeister の利用 13-5
13.2.2 ゼロタッチプロビジョニング機能による NetMeister の利用 13-7
13.3 NetMeister による管理 13-14
13.3.1 タブ一覧 13-15
13.4 NetMeister の設定例 13-15
13.5 NetMeister 利用のトラブルシューティング 13-17
13.5.1 NetMeister に QXが登録できない 13-17
13.5.2 NetMeister でグラフが正しく表示されない。 13-18
13.5.3 NetMeister のリモートログインが使えない 13-18
13.5.4 ファームウェア更新が成功しない 13-18
13.5.5 NetMeisterPrime 機能が使用できない 13-19

13章 NetMeister

🕮 メモ:

IRF スタックでの NetMeister 利用は、Version7.1.8 を含む以降のソフトウェアからサポートしています。IRF スタックで利用する場合、MAC アドレスが Master 選定によって変化しないように irf mac-address persistent always コマンドを設定してください。また、IRF 分裂によって同一 MAC の装置が複数登録されないように MAD 機能を利用して下さい。

Version 7.1.11 を含む以降のソフトウェアから親機モードでの NetMeister への接続をサポートしています。

13.1 概要

NetMeister(ネットマイスター)は、NEC プラットフォームズが提供するクラウド型統合管理サービスです。NetMeister 対応のネットワーク機器をクラウド上で一元的に管理することができます。この章では、本装置を NetMeister に登録するための設定について説明します。

NetMeister の操作/詳細に関しては、以下 NetMeister ポータルサイトをご確認ください。

https://www.necplatforms.co.jp/product/netmeister/

13.1.1 NetMeister の利用

NetMeister を利用する場合、あらかじめ NetMeister のサイトで「アカウント登録」と「グループ登録」が必要です。

QX シリーズは、NetMeister における親機モード、および、子機モードをサポートします。

親機モードでは、NetMeister と MQTT によって直接接続状態を確立し、NetMeister によって管理する事ができます。ただし、親機モードには、NetMeister Prime(有償サービス)の利用が必要です。NetMeister Prime については NetMeister が提供する操作ガイドをご確認ください。

子機モードでは、親機モードの装置と連携する事で NetMeister からの応答を受け、NetMeister によって管理する事ができます。図 13-1に示すように、子機モードだけでは NetMeister を利用できません。

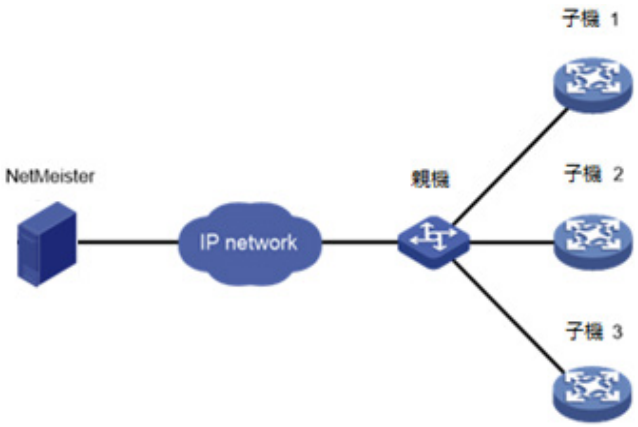


図 13-1 NetMeister との接続イメージ

子機モードを NetMeister によって管理する場合、親機モードの機器と同じのグループに属する必要があります。図 13-2に示すように、子機モードは、親機モードの機器との通信と NetMeister と直接通信の両方を利用して NetMeister 上で管理され、NetMeister に関する通信は https(ssl)でおこなわれます(デフォルトポート番号: 443)。親機モードの NetMeister に関する通信は mqtt(デフォルトポート番号:8883)と https(ssl)でおこなわれます。 (デフォルトポート番号:443)

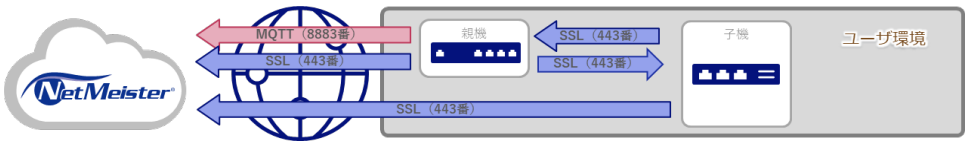


図 13-2 NetMeister への通信イメージ

図 13-3に示すように、プロキシサーバを用いて外部ネットワークに接続をしている環境でも NetMeister を利用可能です。プロキシサーバのアドレスを設定することで、NetMeister 宛の通信をプロキシサーバ経由でおこなうようことが可能です。

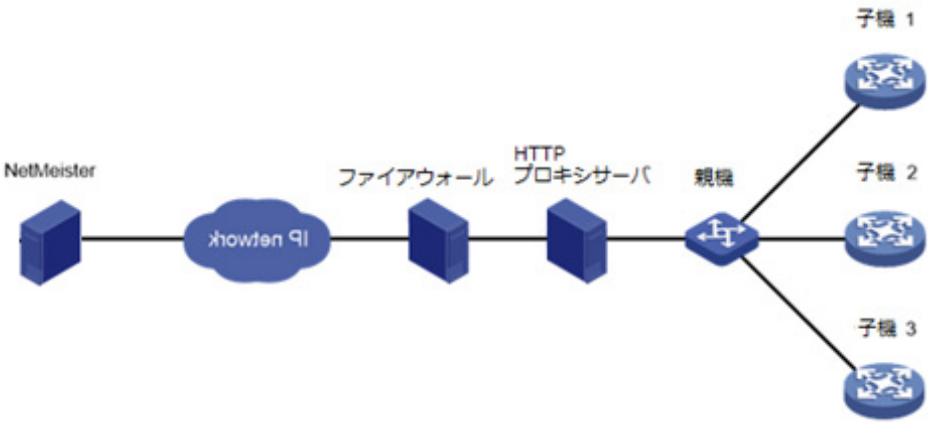


図 13-3 プロキシサーバを用いた NetMeister との接続イメージ

図 13-4に示すように、子機で NetMeister への接続に proxy サーバを利用する場合、NetMeister 宛の通信のみ proxy サーバを経由します。親機と子機の間にプロキシサーバ及びファイアウォールがある様な特殊な環境の場合、親機と子機の間の通信を透過させるた

めに、ファイアウォールで親機の LAN 側 IP 宛の通信を許可する必要があります。同様に、ファイアウォールを跨ぐ位置にある NTP サーバ/DNS サーバ/SSH クライアント等との通信をする場合は、それらの許可も必要です。

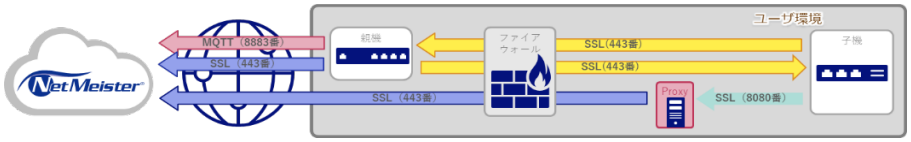


図 13-4 プロキシサーバを用いた NetMeister の通信イメージ

13.1.2 設定手段について

装置を NetMeister で管理をするためには、装置に手動でコンフィグを設定して環境に接続する手段と、ゼロタッチプロビジョニング機能(ZTP 機能)を利用して接続する手段があります。

ゼロタッチプロビジョニング機能は、スタートアップコンフィグレーションファイルを設定されていない状態で装置が起動する場合、NetMeister の親機から受けた DHCP パケットの情報を元に NetMeister から自動でコンフィグレーションファイルを取得し、適用することを可能にします。ゼロタッチプロビジョニング機能は装置に起動コンフィグが設定されていない状態で起動した際に自動で動作します。

図 13-5に示すように、ゼロタッチプロビジョニング機能を利用する場合、管理者が事前に NetMeister 上に装置情報と利用するコンフィグレーションファイルを登録しておくことで、現場で装置設置をする作業者が、装置の操作をすることなく NetMeister に接続することが可能です。

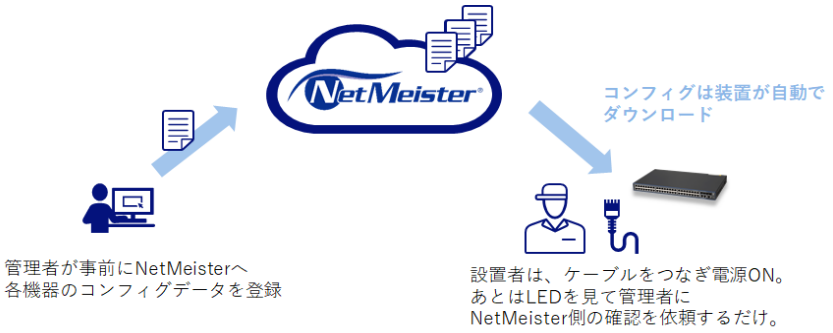


図 13-5 ゼロタッチプロビジョニングのイメージ

ゼロタッチプロビジョニング機能は、Auto Config 機能と交互に実行されます。Auto Config 機能についてはオペレーションマニュアルのセクション 1 *はじめに* “*Auto Config*” を参照してください。

13.2 設定作業リスト

設定作業リスト
手動設定による NetMeister の利用
外部ネットワークへの接続準備 ● (必須設定項目) 自装置の IP アドレスの設定 ● (必須設定項目) 使用する DNS サーバの設定 ● (必須設定項目) ルーティングの設定
NetMeister機能に関係する追加設定 ● (推奨設定項目) 時刻、及び、タイムゾーン(+9:00)の設定 ● (オプション設定項目) Web コンソールユーザの設定 ● (オプション設定項目) SSH ユーザの設定 ● (オプション設定項目) LLDP の設定
NetMeisterを利用するための設定 親機モードの場合 ● (オプション設定項目) NetMeister 上に表示するホスト名の設定 ● (必須設定項目) 親機モードの設定 ● (必須設定項目) グループ ID とグループパスワードの設定 ● (オプション設定項目) MQTT ポート番号の設定 ● (必須設定項目) 拠点 ID の指定 ● (オプション設定項目) プロキシサーバのアドレスの設定 ● (必須設定項目) NetMeister 機能の有効化 子機モードの場合 ● (オプション設定項目) NetMeister 上に表示するホスト名の設定 ● (必須設定項目) グループ ID とグループパスワードの設定 ● (必須設定項目) 親機の IP アドレスとポート番号の設定 ● (オプション設定項目) プロキシサーバのアドレスの設定 ● (必須設定項目) NetMeister 機能の有効化
ゼロタッチプロビジョニング機能による NetMeister の利用
事前準備作業 ● (必須設定項目)親機の設定 ● (必須設定項目)コンフィグレーションファイルの準備 ● (必須設定項目)装置情報の確認
NetMeisterへの情報登録 ● (必須設定項目)コンフィグレーションファイルの登録 ● (必須設定項目)装置情報の登録 ● (必須設定項目)プロビジョニングの設定
設置作業 ● (必須設定項目)プロビジョニングの有効化

13.2.1 手動設定による NetMeister の利用

I. 外部ネットワークへの接続準備

NetMeister と通信をするために、装置は親機を通して外部ネットワークに接続できる環境に接続されている必要があります。自装置の IP アドレス、使用する DNS サーバ、ルーティングの設定をしてください。DNS サーバは、親機から通知される NetMeister のアドレスを把握するために必要です。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. VLAN インタフェースを作成し、VLAN interface view に移行する	**interface vlan-interface** *vlan-interface-id*	ー
3. VLAN インタフェースに IP アドレスを割り当てる	・固定アドレスを割り当てる。 **ip address** *ip-address* { *mask* | *mask-length* } [**sub**] ・DHCPでアドレスを取得する **ip address dhcp-alloc**	デフォルト：設定なし
4. VLAN view から戻る	**quit**	ー
5. DNS サーバの IP アドレスを指定する	**dns server** *ip-address*	デフォルト：設定なし DHCPサーバから情報を取得する場合は設定の必要はありません。
6. ルーティングの設定をする	**ip route-static** *dest-address* { *mask-length* | *mask* } { *interface-type interface-number* [*next-hop-address*] | *next-hop-address* } [**permanent** | **track** *track-entry-number*] [**preference** *preference*] [**tag** *tag-value*] [**description** *text*]	デフォルト：設定なし DHCPサーバから情報を取得する場合は設定の必要はありません。

II. NetMeister 機能に関係する追加設定

NetMeister で利用する機能によっては従来の装置機能を設定しておく必要があります。

それぞれの機能の設定手順についてはそれぞれの機能の章を参照してください。

NetMeister 機能	必要設定	補足
CPU/メモリ/温度/ポートトラフィック情報表示	時刻 （手動/NTP）、及び、タイムゾーン（+9:00）	設定をしない場合、正しいグラフ情報になりません。
HTTPSでリモートログインする	Webコンソール利用設定	
SSHでリモートログインする	SSH接続利用設定	
デバイスマップを見る（L2モード）	LLDP有効化	親機でも設定が必要です。

III. NetMeister を利用するための設定

1)　親機モードの場合

NetMeister を利用するために、NetMeister のサイトで設定したグループ ID、グループパスワードを設定してください。MQTT のポート番号は 443 に変更が可能です。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. (オプション設定項目) NetMeister 上に表示するホスト名を設定する	**sysname** *sysname*	デフォルト：装置名
3. 親機モードを有効にする	**netmeister mode parent**	デフォルト：無効
4. グループ ID とグループパスワードを設定する	**netmeister account** *account* **password** { **cipher** *cipherPassword* | **simple** *plainPassword* }	デフォルト：設定なし
5. (オプション設定項目) MQTTポート番号の設定	**netmeister parent-mode mqtt port { 8883 | 443]**	デフォルト：8883
6. (必須設定項目) 拠点 ID の指定	**netmeister parent-mode sitename** *string*	デフォルト：設定なし
7. (オプション設定項目) プロキシサーバのアドレスを指定する。	**netmeister proxy url** *url* [**username** *username* **password** { **cipher** | **simple** } *string*]	デフォルト：設定なし
8. NetMeister 機能の有効化	**netmeister enable**	デフォルト：無効

2)　子機モードの場合

NetMeister を利用するために、NetMeister のサイトで設定したグループ ID、グループパスワードと、親機の IP アドレス、ポート番号の設定をしてください。プロキシサーバのアドレスを設定すると、NetMeister への https 通信のために任意のプロキシサーバを利用します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. (オプション設定項目) NetMeister 上に表示するホスト名を設定する	**sysname** *sysname*	デフォルト：装置名
3. グループ ID とグループパスワードを設定する	**netmeister account** *account* **password** { **cipher** *cipherPassword* | **simple** *plainPassword* }	デフォルト：設定なし
4. 親機の IP アドレスとポート番号を指定する	**netmeister parent ip** *ip-address* [**port** *port-number*]	デフォルト：設定なし 最大2つまで設定が可能です。 ポート番号を指定しない場合、デフォルトで443が使用されます。
5. (オプション設定項目) プロキシサーバのアドレスを指定する。	**netmeister proxy url** *url* [**username** *username* **password** { **cipher** | **simple** } *string*]	デフォルト：設定なし
6. NetMeister 機能の有効化	**netmeister enable**	デフォルト：無効

IV. NetMeister の表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
NetMeisterおよび親機との接続状態を表示する	**display netmeister**

13.2.2 ゼロタッチプロビジョニング機能による NetMeister の利用

🕮 **メモ:**
ゼロタッチプロビジョニング機能は Version 7.1.4 を含む以降のソフトウェアからサポートしています。

I. 事前準備作業

🕮 **メモ:**
ゼロタッチプロビジョニング機能の利用可能条件:
- 子機モードで接続する場合、親機モードで接続している装置が必要です。
- Option43 を付与できる DHCP サーバが必要です。事前に装置で利用する正しいコンフィグレーションファイルの準備が必要です。
- 準備するコンフィグレーションファイルは、 1装置につき 1 つ必要です。
- 事前に利用する装置の MACアドレス、シリアルナンバー、装置名の情報が必要です。
- コンフィグダウンロード時は、NetMeister 側でダウンロードの有効時間の指定が必要です。

1) DHCP サーバの設定

ゼロタッチプロビジョニング機能を利用する場合、DHCP サーバで Option43 の設定をするか、NetMeister 機能のゼロタッチプロビジョニング子機対応をサポートする親機を DHCP サーバとしてください。設定方法は親機のマニュアル、および NetMeister 操作ガイドを参照してください。

- DHCP サーバ設定 : 子機が外部ネットワークに通信ができるように IP アドレス/DNS サーバアドレス/デフォルトゲートウェイアドレスを設定してください。また、Option43 で以下の内容を通知してください。

  Option43 のフォーマット :

  NEC,zerotouch,<親機 IPv4 アドレス>,<親機待ち受けポート>

  例） NEC,zerotouch,192.0.2.1,443

- NetMeister 機能のゼロタッチプロビジョニング子機対応をサポートする親機を DHCP サーバとして利用する場合、ゼロタッチをおこなう装置にのみ Option43 を付与する設定が可能です。設定方法は使用する親機のマニュアルを参照してください。

🕮 **メモ:**
Option 43 によって通知された親機モードの装置が proxy サーバを利用して NetMeister に接続している場合、子機は NetMeister からのコンフィグレーションファイル取得にその装置と同様の proxy サーバを経由します。親機との通信は proxy サーバを経由しません。

Version 7.1.11 を含む以降のソフトウェアからは proxy サーバを経由したゼロタッチプロビジョニングを行う場合以外は Option 43 を必要としません。

2) コンフィグレーションファイルの準備

ゼロタッチプロビジョニング機能で設定を行う対象装置のために、コンフィグファイルをテキストで作成し、zip 圧縮してください。間違ったコンフィグファイルを使用しないよう、あらかじめ実機で確認をしたコンフィグを使用することを推奨します。

下記に用意するコンフィグレーションファイルのサンプル（子機モード）を示します。

```
#
 clock timezone JST add 09:00:00
#
 ssh server enable
#
 ip https enable
#
 lldp global enable
#
interface Vlan-interface1
 ip address dhcp-alloc
#
 ntp-service enable
 ntp-service unicast-server 1.1.1.2
#
line vty  0
 authentication-mode scheme
#
local-user nec class manage
 password simple qx12345678
 service-type ssh https
 authorization-attribute user-role network-admin
#
 netmeister enable
 netmeister account test password simple abcdefg
 netmeister parent ip 1.1.1.1 port 443
#
```

3) 装置情報の確認

ゼロタッチプロビジョニング機能を利用する装置の MAC アドレス、シリアルナンバー、装置名の情報を確認してください。 MAC アドレス、シリアルナンバー、装置名は、梱包箱または装置の本体ラベルに記載されています。

II. NetMeister への情報登録

NetMeister にログインしてください。(NetMeister を利用するためのアカウントおよびグループの作成についての説明は省略します。NetMeister 操作ガイドを確認してください。)

1) NetMeister でのゼロタッチプロビジョニングは、NetMeister 画面左側メニューの「設定」からおこないます。



図 13-6 設定メニューの表示

2) ゼロタッチプロビジョニングの設定のために編集モードにします。



図 13-7 編集モードへの変更

3) コンフィグレーションファイルを NetMeister 上に登録します。



図 13-8 コンフィグ登録画面

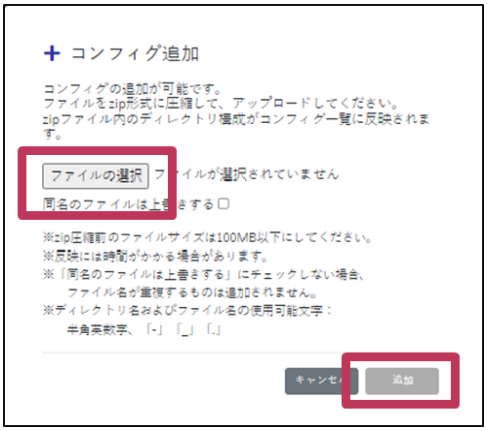


図 13-9 コンフィグの選択

メモ:

NetMeister へのコンフィグレーションファイルの登録は zip 形式でおこないます。複数のコンフィグレーションファイルをフォルダに格納して zip 圧縮しておくことで一度に登録も可能です。



図 13-10 コンフィグ登録後の表示

4)　ゼロタッチプロビジョニングを利用する装置情報を登録します。

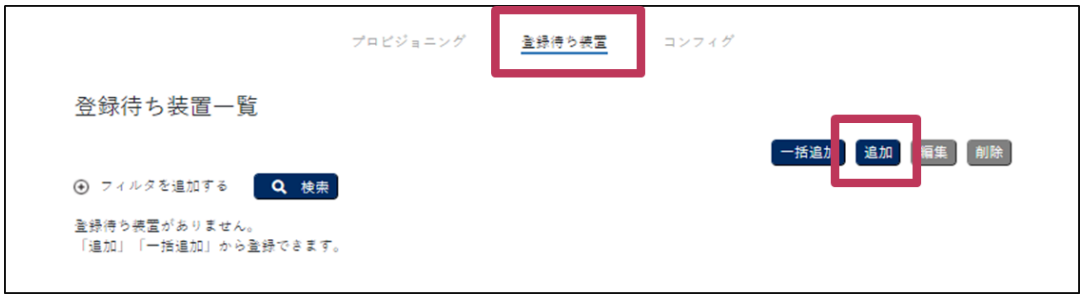


図 13-11 登録待ち装置設定画面



図 13-12 装置情報の登録例

メモ:

装置情報の登録では、シリアル番号の入力は大文字小文字を区別します。
MAC アドレスの入力は大文字小文字を区別しません。
「：」「-」などは含めないでください。
シリーズ名、機種名の選択を間違えないよう注意してください。



図 13-13 登録後の表示

5)　登録したコンフィグレーションファイルと装置情報を紐づけます。



図 13-14 プロビジョニングの設定画面

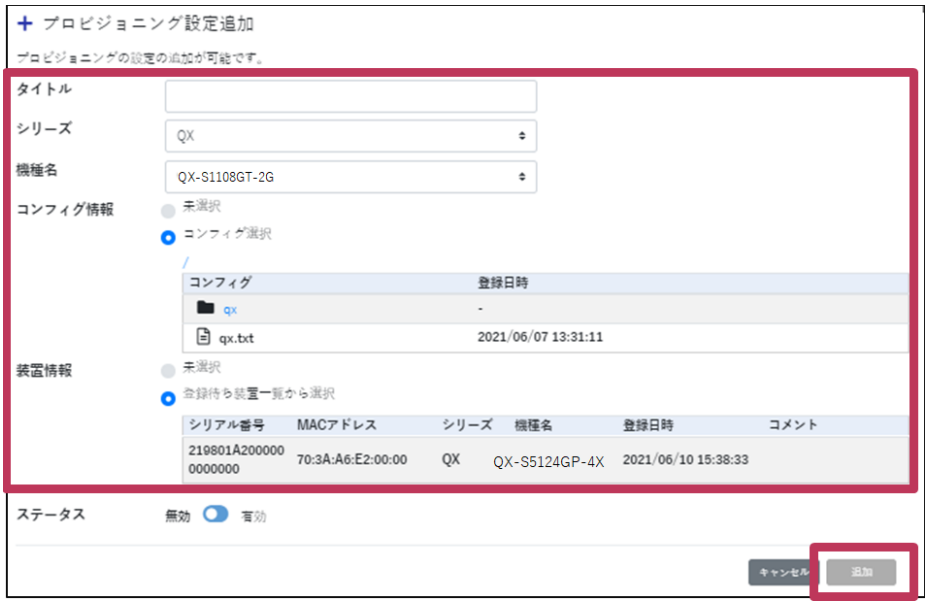


図 13-15 装置とコンフィグの選択

🕮 メモ:

タイトルは任意の文字列を入力してください。
シリーズ名と装置名を選択すると、他は選択可能なものだけが表示されますので任意の組み合わせを選択してください。
設置作業者がすぐに作業をしない場合はステータスを[無効]で登録しておきます。

III. 設置作業

1)　設置作業者が作業する時間を考慮し、コンフィグのダウンロード可能時間を設定します。一覧から対象の行を選択すると、現在の設定情報が下に表示されます。



図 13-16 プロビジョニング設定一覧

2)　選択した設定のステータスを[編集]から有効にし、コンフィグダウンロード可能時間を設定します。



図 13-17 ステータスの変更と DL 有効時間の設定

メモ:

有効時にダウンロード後の無効パターンを指定できますが、QXのゼロタッチプロビジョニングは、ダウンロード完了時はコンフィグを次回起動のコンフィグとして保存、再起動しますので、どちらを選んでも 1 度のみの取得動作です。(次回以降の起動時は保存済のコンフィグを使用して起動します。)

---

3)　設置場所で設置作業者が指定の装置を開梱します。
4)　準備後、管理者に装置設置開始の連絡をします。
5)　管理者は NetMeister 上で対象のゼロタッチプロビジョニングの有効化をします。
6)　設置作業者は指定の環境に装置を接続します。
7)　接続した装置は NetMeister から自動的にコンフィグを取得します。

QXのゼロタッチプロビジョニングでは、取得したコンフィグデータを自動で次回起動のコンフィグとしてセットし、再起動します。

DHCP サーバの設定ミスやインターネット環境に出られない環境など、何らかの理由で失敗している場合はリトライを繰り返し、再起動はしません。環境を見直してください。ゼロタッチプロビジョニングのプロセスを止めるためには、CLI で<Ctrl+C>または<Ctrl+D>を押下してください。

8)　再起動を LED 変化で確認し、管理者に連絡します。

起動時の LED 変化は下記の通りです。

表 13-1 QX-S5100G シリーズ

状態	Power LED
Boot 起動	オレンジ点灯
System 起動中	緑点滅→点灯(3 回)→(ポート LED 上下点灯)→緑点灯
ゼロタッチプロビジョニング中	緑点灯(及びポート LinkUP)
ゼロタッチプロビジョニング成功時	(自動再起動)オレンジ点灯
起動中	緑点滅→点灯(3 回)→(ポート LED 上下点灯)→緑点灯
起動完了	緑点灯(及びポート LinkUP)

9)　NetMeister 上で状態を確認します。



図 13-18 動作状態の確認

結果がダウンロード成功の場合、コンフィグ取得を終えています。装置詳細画面に装置が表示されたことをチェックしてください。装置情報の誤入力や、環境の問題で NetMeister にアクセスができていない場合はカウントがされません。



図 13-19 装置一覧の確認

装置が再起動し、起動したにもかかわらず装置一覧に表示されない場合、準備されたコンフィグに NetMeister に接続するための設定の不備がある可能性があります。

装置一覧に装置が表示されれば NetMeister で管理ができています。

IV. 参考

NetMeister であらかじめアカウント管理から通知設定でゼロタッチ通知にチェックをいれておくと、ゼロタッチプロビジョニングによるコンフィグ取得成功時にメールが通知されます。



図 13-20 アカウント管理



図 13-21 通知の設定

13.3 NetMeisterによる管理

Netmeister の操作、及び、対応機能に関しては、NetMeister が提供する操作ガイドをご確認ください。

13.3.1 タブ一覧

NetMeister 上の装置詳細の画面に表示されるタブは、機器ごとに表示される内容が異なります。また、表示のレイアウトは NetMeister 側の更新によって変わる可能性があります。

本装置は以下のタブに対応しています。

タブ名	説明
装置概要	装置の詳細画面を表示します。 詳細はNetMeisterが提供する操作ガイドをご確認ください。
アラーム	温度異常/FAN 異常/CPU 異常/メモリ異常/異常再起動時にアラームを送信します。温度センサや FAN を持たない装置はそれらのアラームを送信することはありません。温度/FAN/CPU/メモリのしきい値はシステム管理の各種しきい値設定値に依存します。
コンフィグ	NetMeister 上にコンフィグを保存、装置の次回起動コンフィグとの比較、反映が可能です。
デバイスリスト	MAC テーブルと ARP テーブルを合わせた情報を表示します。
ログ	V7.3.49 を含む以降のソフトウェアで NetMiester prime 利用時に表示されます。 定期ログ送信を有効にし、時刻を指定して保存することで、NetMeister に定期的に装置情報一括取得(diag)データが保存されるようになります。
VLAN	display vlan コマンド、及び、displayinterface Vlan-interface brief コマンド相当の情報を表示します。
ポート状態	物理インタフェースの情報を表示します。

13.4 NetMeisterの設定例

I. ネットワーク要件

図 13-22に示すように、Device B を親機とし、子機である Device A の設定をします。

- あらかじめ NetMeister のサイトで「アカウント登録」をし、「グループ登録」としてグループ ID(aaa)とグループパスワード(bbb)が設定されていることとします。
- あらかじめ親機は外部ネットワークに接続するための設定を行い、グループ ID(aaa)に属していることとします。
- DNS サーバとして 10.0.0.254 が動作していることとします。

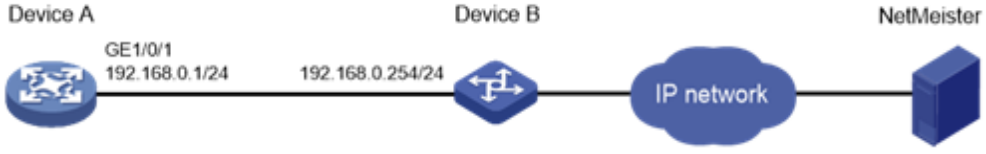


図 13-22 ネットワーク図

II. 設定手順

1)　外部ネットワークへの接続準備をします。

#VLAN インタフェースを作成し、IP アドレスをインタフェースに割り当てます。

```
<DeviceA> system-view
[DeviceA] vlan 1
[DeviceA-vlan1] port gigabitethernet 1/0/1
[DeviceA-vlan1] quit
[DeviceA] interface vlan-interface 1
[DeviceA -Vlan-interface1] ip address 192.168.0.1 24
[DeviceA -Vlan-interface1] quit
```

DNS サーバを指定します。

```
[DeviceA] dns server 10.0.0.254
```

ルーティング設定をします。

```
[DeviceA] ip route-static 0.0.0.0 0 192.168.0.254
```

2)　その他の追加機能の設定をします。

時刻とタイムゾーン(+9:00)の設定をします。

```
[DeviceA]  clock timezone JST add 09:00:00
[DeviceA]  ntp-service  enable
[DeviceA]  ntp-service  unicast-server  192.168.0.254
```

ssh と web コンソールアクセス用の設定をします。

```
[DeviceA]ssh  server  enable
[DeviceA]ip  https enable
[DeviceA]line  vty 0
[DeviceA-line-vty0]authentication-mode  scheme
[DeviceA-line-vty0]local-user  nec class manage
[DeviceA-luser-manage-nec]password  simple qx12345678
[DeviceA-luser-manage-nec]service-type  ssh https
[DeviceA-luser-manage-nec]authorization-attribute  user-role  network-admin
[DeviceA-luser-manage-nec]quit
```

lldp の有効化をします。

```
[DeviceA] lldp global enable
```

3)　NetMeister を利用するための設定をします。

グループ ID(aaa)とグループパスワード(bbb)を設定します。

```
[DeviceA] netmeister account aaa password simple bbb
```

親機の IP アドレスとポート番号(デフォルト:443)を指定します。

```
[DeviceA] netmeister parent ip 192.168.0.254 port 443
```

NetMeister 機能の有効化をします。

```
[DeviceA] netmeister enable
```

III. 設定の確認

1) 外部ネットワークと疎通ができることを確認するために、いずれかの外部ネットワークと ping の疎通ができることを確認します。

```
<SwitchA>ping 1.1.1.1
Ping 1.1.1.1 (1.1.1.1): 56 data bytes, press CTRL+C to break
56 bytes from 1.1.1.1: icmp_seq=0 ttl=52 time=68.584 ms
56 bytes from 1.1.1.1: icmp_seq=1 ttl=52 time=49.657 ms
56 bytes from 1.1.1.1: icmp_seq=2 ttl=52 time=48.447 ms
56 bytes from 1.1.1.1: icmp_seq=3 ttl=52 time=58.423 ms
56 bytes from 1.1.1.1: icmp_seq=4 ttl=52 time=59.423 ms

--- Ping statistics for 1.1.1.1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 48.447/56.907/68.584/7.336 ms
```

2) NetMeister および親機との接続状態を確認します。

```
<SwitchA> display netmeister
NetMeister state                          :  Enabled
Connection state with NetMeister          :  Connected
Account name                              :  aaa
Parent 1:
 IP address                               :  192.168.0.254
 Port number                              :  443
 Connection state                         :  Connected
```

13.5 NetMeister利用のトラブルシューティング

NetMeister 操作ガイドにも装置毎の機能対応一覧、及び、NetMeister 機能に関する注意事項、FAQ が記載されていますので参照して下さい。

13.5.1 NetMeister に QX が登録できない

I. 症状

QX で NetMeister を利用したいが NetMeister に装置が登録できない。

II. 解決策

親機モードで利用する場合

1) 同一グループに既に子機モードで登録されていないか確認し、登録されている場合は装置削除します。
2) NetMeister 上のライセンスの数が十分か確認します。
3) 外部ネットワークに DNS を使用した通信ができることを確認します。
4) 問題が解決しない場合、NetMeister のサイトから問い合わせをしてください。

子機モードで利用する場合

1) 同一グループに既に親機モードで登録されていないか確認し、登録されている場合は装置削除します。
2) 親機となる装置が NetMeister に接続できているか確認します。
3) 子機で設定したグループ ID およびパスワードが親機で設定しているものと同じであるか確認します。
4) 子機から外部ネットワークに DNS を使用した通信ができることを確認します。

5) 問題が解決しない場合、NetMeister のサイトから問い合わせをしてください。

13.5.2 NetMeister でグラフが正しく表示されない。

I. 症状

QXの装置詳細画面でグラフ情報が正しく表示されない。

II. 解決策

1) 装置にタイムゾーン(+9:00)が設定されていることを確認します。
2) 装置の時刻が正しいことを確認します。
3) NetMeister に装置登録した後に時刻設定を変更した場合は、周期的な装置情報更新のために、1 時間待つか NetMeister 機能を一度無効にし、再度有効にします。
4) 問題が解決しない場合、NetMeister のサイトから問い合わせてください。

13.5.3 NetMeister のリモートログインが使えない

I. 症状

QXにリモートログインができない。

II. 解決策

1) 同一拠点 ID にリモートログインの起点装置が存在することを確認します。詳細は NetMeister 操作ガイドを参照して下さい。
2) 装置に ssh または web コンソール接続の設定がされてあることを確認します。
3) リモートログインでのアクセスに利用する PC がプライベートアドレスではないことを確認します。
4) 操作 PC と対象の装置間でファイアウォールやフィルタなど、通信制限がない事を確認します。
5) 環境がプロキシやファイアウォールを利用していないことを確認します。
6) 問題が解決しない場合、NetMeister のサイトから問い合わせてください。

13.5.4 ファームウェア更新が成功しない

I. 症状

NetMeister で管理している装置のファームウェア更新(バージョンアップ)が成功しない。

II. 解決策

1) タスク一覧からタスクの状態を確認します。
2) タスク結果が失敗と表示され、詳細理由にディレクトリサイズが足りない、または、セットに失敗したと表示されている場合、装置のディレクトリサイズが不足していますので不要なファイルを削除します。

🕮 **メモ:**

ファームウェア更新をするためには、NetMeisterから取得するipe形式のソフトウェアと、それを bin ファイルに解凍する分のディレクトリの空き容量が必要です。
ソフトウェア v7.1.3 を含む以降のバージョンでは、NetMeister 機能[コマンド実行]によって、NetMeister からディレクトリ確認コマンド(**dir**)及び削除コマンド(**delete /unreserved**)等の実行が可能です。v7.1.3 以前のバージョンでは NetMeister 機能[リモートログイン]やコンソールケーブル接続等して、直接装置でコマンドを実行してください。

3) 問題が解決しない場合、NEC に問い合わせてください。

13.5.5 NetMeisterPrime 機能が使用できない

I. 症状

NetMeister に prime ライセンスを適用(またはトライアル)したが機能が使用できない。

II. 解決策

1) NetMeister メニューからライセンスの適用状態を確認し、適用されていない場合は適用操作をします。(NetMeister が提供する NetMeister 操作ガイド参照)
2) 子機モードの場合、手動で有償化操作をする必要があります。
3) prime 機能にはライセンス適用をして有償化装置になった時に即座に利用できるものと、周期的な装置情報更新のタイミングで識別され使用可能になる機能がありますので、1 時間待つか NetMeister 機能を一度無効にし、再度有効にします。
4) 問題が解決しない場合、NetMeister のサイトから問い合わせてください。

QX-S5100G シリーズ Ethernet スイッチ

オペレーションマニュアル

12. 謝辞

本マニュアルは以下に示す章で構成されています。

01-謝辞

目次

このセクションのページは **12-x-x** です。

1章 謝辞（Acknowledgments） **1-1**

1章 謝辞（Acknowledgments）

This document provides copyright information regarding the third-party software that are included, either in whole or in part, in this product.

Acknowledgements:
This product includes software developed by the University of California, Berkeley and its contributors.
This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/).
This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).
This product includes software developed by the University of California, Lawrence Berkeley Laboratory and its contributors.

This product contains third parties component softwares and they will be used and distributed under the specific license.
If you want to obtain source code of Open Source Software included in this product, please send a request to our support team: https://www.nec.com/, we will provide the source code included in this product in exchange for a fee no higher than the physical cost of providing the source code.

[boolean.h 1.19]
[COPYRIGHT]
Copyright (C) 2004-2007 Internet Systems Consortium, Inc. ("ISC")
Copyright (C) 1998-2001 Internet Software Consortium.

[LICENSE]
Permission to use, copy, modify, and/or distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ISC DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

[bootstrap 2.3.2]
[COPYRIGHT]
Copyright 2012 Twitter, Inc.

[LICENSE]
Apache License
Version 2.0, January 2004
http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition,

"control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the
   Work or Derivative Works thereof in any medium, with or without
   modifications, and in Source or Object form, provided that You
   meet the following conditions:

   (a) You must give any other recipients of the Work or
       Derivative Works a copy of this License; and

   (b) You must cause any modified files to carry prominent notices
       stating that You changed the files; and

   (c) You must retain, in the Source form of any Derivative Works
       that You distribute, all copyright, patent, trademark, and
       attribution notices from the Source form of the Work,
       excluding those notices that do not pertain to any part of
       the Derivative Works; and

   (d) If the Work includes a "NOTICE" text file as part of its
       distribution, then any Derivative Works that You distribute must
       include a readable copy of the attribution notices contained
       within such NOTICE file, excluding those notices that do not
       pertain to any part of the Derivative Works, in at least one
       of the following places: within a NOTICE text file distributed
       as part of the Derivative Works; within the Source form or
       documentation, if provided along with the Derivative Works; or,
       within a display generated by the Derivative Works, if and
       wherever such third-party notices normally appear. The contents
       of the NOTICE file are for informational purposes only and
       do not modify the License. You may add Your own attribution
       notices within Derivative Works that You distribute, alongside
       or as an addendum to the NOTICE text from the Work, provided
       that such additional attribution notices cannot be construed
       as modifying the License.

   You may add Your own copyright statement to Your modifications and
   may provide additional or different license terms and conditions
   for use, reproduction, or distribution of Your modifications, or
   for any such Derivative Works as a whole, provided Your use,
   reproduction, and distribution of the Work otherwise complies with
   the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise,
   any Contribution intentionally submitted for inclusion in the Work
   by You to the Licensor shall be under the terms and conditions of
   this License, without any additional terms or conditions.
   Notwithstanding the above, nothing herein shall supersede or modify
   the terms of any separate license agreement you may have executed
   with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade
   names, trademarks, service marks, or product names of the Licensor,
   except as required for reasonable and customary use in describing the
   origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or
   agreed to in writing, Licensor provides the Work (and each
   Contributor provides its Contributions) on an "AS IS" BASIS,
   WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or
   implied, including, without limitation, any warranties or conditions
   of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A
   PARTICULAR PURPOSE. You are solely responsible for determining the
   appropriateness of using or redistributing the Work and assume any
   risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory,
   whether in tort (including negligence), contract, or otherwise,
   unless required by applicable law (such as deliberate and grossly
   negligent acts) or agreed to in writing, shall any Contributor be
   liable to You for damages, including any direct, indirect, special,

incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

[bootstrap-datetimepicker 1.2]
[COPYRIGHT]
Copyright 2012 Stefan Petre

[LICENSE]

Apache License
Version 2.0, January 2004
http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain

separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

   (a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

   (b) You must cause any modified files to carry prominent notices stating that You changed the files; and

   (c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

   (d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and

wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

APPENDIX: How to apply the Apache License to your work.

To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets "[]" replaced with your own identifying information. (Don't include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a

```
      file or class name and description of purpose be included on the
      same "printed page" as the copyright notice for easier
      identification within third-party archives.

   Copyright 2012 Sebastien MALOT

   Licensed under the Apache License, Version 2.0 (the "License");
   you may not use this file except in compliance with the License.
   You may obtain a copy of the License at

       http://www.apache.org/licenses/LICENSE-2.0

   Unless required by applicable law or agreed to in writing, software
   distributed under the License is distributed on an "AS IS" BASIS,
   WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
   See the License for the specific language governing permissions and
   limitations under the License.
--------------------------------------------------------------------------
---
[bootstrap-dropdown 2.3.2]
[COPYRIGHT]
  Copyright 2013 Twitter, Inc.

[LICENSE]
                                 Apache License
                           Version 2.0, January 2004
                        http://www.apache.org/licenses/

   TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

   1. Definitions.

      "License" shall mean the terms and conditions for use, reproduction,
      and distribution as defined by Sections 1 through 9 of this document.

      "Licensor" shall mean the copyright owner or entity authorized by
      the copyright owner that is granting the License.

      "Legal Entity" shall mean the union of the acting entity and all
      other entities that control, are controlled by, or are under common
      control with that entity. For the purposes of this definition,
      "control" means (i) the power, direct or indirect, to cause the
      direction or management of such entity, whether by contract or
      otherwise, or (ii) ownership of fifty percent (50%) or more of the
      outstanding shares, or (iii) beneficial ownership of such entity.

      "You" (or "Your") shall mean an individual or Legal Entity
      exercising permissions granted by this License.

      "Source" form shall mean the preferred form for making modifications,
      including but not limited to software source code, documentation
      source, and configuration files.

      "Object" form shall mean any form resulting from mechanical
      transformation or translation of a Source form, including but
      not limited to compiled object code, generated documentation,
      and conversions to other media types.

      "Work" shall mean the work of authorship, whether in Source or
      Object form, made available under the License, as indicated by a
      copyright notice that is included in or attached to the work
      (an example is provided in the Appendix below).

      "Derivative Works" shall mean any work, whether in Source or Object
      form, that is based on (or derived from) the Work and for which the
      editorial revisions, annotations, elaborations, or other modifications
      represent, as a whole, an original work of authorship. For the purposes
      of this License, Derivative Works shall not include works that remain
      separable from, or merely link (or bind by name) to the interfaces of,
      the Work and Derivative Works thereof.
```

"Contribution" shall mean any work of authorship, including
the original version of the Work and any modifications or additions
to that Work or Derivative Works thereof, that is intentionally
submitted to Licensor for inclusion in the Work by the copyright owner
or by an individual or Legal Entity authorized to submit on behalf of
the copyright owner. For the purposes of this definition, "submitted"
means any form of electronic, verbal, or written communication sent
to the Licensor or its representatives, including but not limited to
communication on electronic mailing lists, source code control systems,
and issue tracking systems that are managed by, or on behalf of, the
Licensor for the purpose of discussing and improving the Work, but
excluding communication that is conspicuously marked or otherwise
designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity
on behalf of whom a Contribution has been received by Licensor and
subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of
this License, each Contributor hereby grants to You a perpetual,
worldwide, non-exclusive, no-charge, royalty-free, irrevocable
copyright license to reproduce, prepare Derivative Works of,
publicly display, publicly perform, sublicense, and distribute the
Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of
this License, each Contributor hereby grants to You a perpetual,
worldwide, non-exclusive, no-charge, royalty-free, irrevocable
(except as stated in this section) patent license to make, have made,
use, offer to sell, sell, import, and otherwise transfer the Work,
where such license applies only to those patent claims licensable
by such Contributor that are necessarily infringed by their
Contribution(s) alone or by combination of their Contribution(s)
with the Work to which such Contribution(s) was submitted. If You
institute patent litigation against any entity (including a
cross-claim or counterclaim in a lawsuit) alleging that the Work
or a Contribution incorporated within the Work constitutes direct
or contributory patent infringement, then any patent licenses
granted to You under this License for that Work shall terminate
as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the
Work or Derivative Works thereof in any medium, with or without
modifications, and in Source or Object form, provided that You
meet the following conditions:

   (a) You must give any other recipients of the Work or
       Derivative Works a copy of this License; and

   (b) You must cause any modified files to carry prominent notices
       stating that You changed the files; and

   (c) You must retain, in the Source form of any Derivative Works
       that You distribute, all copyright, patent, trademark, and
       attribution notices from the Source form of the Work,
       excluding those notices that do not pertain to any part of
       the Derivative Works; and

   (d) If the Work includes a "NOTICE" text file as part of its
       distribution, then any Derivative Works that You distribute must
       include a readable copy of the attribution notices contained
       within such NOTICE file, excluding those notices that do not
       pertain to any part of the Derivative Works, in at least one
       of the following places: within a NOTICE text file distributed
       as part of the Derivative Works; within the Source form or
       documentation, if provided along with the Derivative Works; or,
       within a display generated by the Derivative Works, if and
       wherever such third-party notices normally appear. The contents
       of the NOTICE file are for informational purposes only and

do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

APPENDIX: How to apply the Apache License to your work.

To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets "[]" replaced with your own identifying information. (Don't include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same "printed page" as the copyright notice for easier

identification within third-party archives.

Copyright 2012 Sebastien MALOT

Licensed under the Apache License, Version 2.0 (the "License");
you may not use this file except in compliance with the License.
You may obtain a copy of the License at

http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software
distributed under the License is distributed on an "AS IS" BASIS,
WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
See the License for the specific language governing permissions and
limitations under the License.

[bootstrap-modal 2.1]
[COPYRIGHT]
Copyright 2012 Jordan Schroter

[LICENSE]

Apache License
Version 2.0, January 2004
http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction,
and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by
the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all
other entities that control, are controlled by, or are under common
control with that entity. For the purposes of this definition,
"control" means (i) the power, direct or indirect, to cause the
direction or management of such entity, whether by contract or
otherwise, or (ii) ownership of fifty percent (50%) or more of the
outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity
exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications,
including but not limited to software source code, documentation
source, and configuration files.

"Object" form shall mean any form resulting from mechanical
transformation or translation of a Source form, including but
not limited to compiled object code, generated documentation,
and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or
Object form, made available under the License, as indicated by a
copyright notice that is included in or attached to the work
(an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object
form, that is based on (or derived from) the Work and for which the
editorial revisions, annotations, elaborations, or other modifications
represent, as a whole, an original work of authorship. For the purposes
of this License, Derivative Works shall not include works that remain
separable from, or merely link (or bind by name) to the interfaces of,
the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including

the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

   (a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

   (b) You must cause any modified files to carry prominent notices stating that You changed the files; and

   (c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

   (d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside

or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

APPENDIX: How to apply the Apache License to your work.

To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets "[]" replaced with your own identifying information. (Don't include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same "printed page" as the copyright notice for easier identification within third-party archives.

```
   Copyright 2012 Sebastien MALOT

   Licensed under the Apache License, Version 2.0 (the "License");
   you may not use this file except in compliance with the License.
   You may obtain a copy of the License at

       http://www.apache.org/licenses/LICENSE-2.0

   Unless required by applicable law or agreed to in writing, software
   distributed under the License is distributed on an "AS IS" BASIS,
   WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
   See the License for the specific language governing permissions and
   limitations under the License.
--------------------------------------------------------------------------------
---
[bootstrap-tab 2.3.2]
[COPYRIGHT]
  Copyright 2013 Twitter, Inc.

[LICENSE]
                                 Apache License
                           Version 2.0, January 2004
                        http://www.apache.org/licenses/

   TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

   1. Definitions.

      "License" shall mean the terms and conditions for use, reproduction,
      and distribution as defined by Sections 1 through 9 of this document.

      "Licensor" shall mean the copyright owner or entity authorized by
      the copyright owner that is granting the License.

      "Legal Entity" shall mean the union of the acting entity and all
      other entities that control, are controlled by, or are under common
      control with that entity. For the purposes of this definition,
      "control" means (i) the power, direct or indirect, to cause the
      direction or management of such entity, whether by contract or
      otherwise, or (ii) ownership of fifty percent (50%) or more of the
      outstanding shares, or (iii) beneficial ownership of such entity.

      "You" (or "Your") shall mean an individual or Legal Entity
      exercising permissions granted by this License.

      "Source" form shall mean the preferred form for making modifications,
      including but not limited to software source code, documentation
      source, and configuration files.

      "Object" form shall mean any form resulting from mechanical
      transformation or translation of a Source form, including but
      not limited to compiled object code, generated documentation,
      and conversions to other media types.

      "Work" shall mean the work of authorship, whether in Source or
      Object form, made available under the License, as indicated by a
      copyright notice that is included in or attached to the work
      (an example is provided in the Appendix below).

      "Derivative Works" shall mean any work, whether in Source or Object
      form, that is based on (or derived from) the Work and for which the
      editorial revisions, annotations, elaborations, or other modifications
      represent, as a whole, an original work of authorship. For the purposes
      of this License, Derivative Works shall not include works that remain
      separable from, or merely link (or bind by name) to the interfaces of,
      the Work and Derivative Works thereof.

      "Contribution" shall mean any work of authorship, including
      the original version of the Work and any modifications or additions
      to that Work or Derivative Works thereof, that is intentionally
```

submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

   (a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

   (b) You must cause any modified files to carry prominent notices stating that You changed the files; and

   (c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

   (d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed

as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

APPENDIX: How to apply the Apache License to your work.

To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets "[]" replaced with your own identifying information. (Don't include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same "printed page" as the copyright notice for easier identification within third-party archives.

Copyright 2012 Sebastien MALOT

Licensed under the Apache License, Version 2.0 (the "License");
you may not use this file except in compliance with the License.
You may obtain a copy of the License at

http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software
distributed under the License is distributed on an "AS IS" BASIS,
WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
See the License for the specific language governing permissions and
limitations under the License.

[bootstrapSwitch 1.3.0]
[COPYRIGHT]
bootstrapSwitch v1.3 by Larentis Mattia @spiritualGuru

[LICENSE]

Apache License
Version 2.0, January 2004
http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction,
and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by
the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all
other entities that control, are controlled by, or are under common
control with that entity. For the purposes of this definition,
"control" means (i) the power, direct or indirect, to cause the
direction or management of such entity, whether by contract or
otherwise, or (ii) ownership of fifty percent (50%) or more of the
outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity
exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications,
including but not limited to software source code, documentation
source, and configuration files.

"Object" form shall mean any form resulting from mechanical
transformation or translation of a Source form, including but
not limited to compiled object code, generated documentation,
and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or
Object form, made available under the License, as indicated by a
copyright notice that is included in or attached to the work
(an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object
form, that is based on (or derived from) the Work and for which the
editorial revisions, annotations, elaborations, or other modifications
represent, as a whole, an original work of authorship. For the purposes
of this License, Derivative Works shall not include works that remain
separable from, or merely link (or bind by name) to the interfaces of,
the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including
the original version of the Work and any modifications or additions
to that Work or Derivative Works thereof, that is intentionally
submitted to Licensor for inclusion in the Work by the copyright owner
or by an individual or Legal Entity authorized to submit on behalf of

the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

   (a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

   (b) You must cause any modified files to carry prominent notices stating that You changed the files; and

   (c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

   (d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

APPENDIX: How to apply the Apache License to your work.

To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets "[]" replaced with your own identifying information. (Don't include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same "printed page" as the copyright notice for easier identification within third-party archives.

Copyright 2012 Sebastien MALOT

Licensed under the Apache License, Version 2.0 (the "License");
you may not use this file except in compliance with the License.

You may obtain a copy of the License at

http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

[busybox 1.20.1]
[LICENSE]

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.
51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to

exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to

this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED

OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author
Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
This is free software, and you are welcome to redistribute it
under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than `show w' and `show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program `Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon>, 1 April 1989
Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Library General Public License instead of this License.

[cpio 2.11]
[COPYRIGHT]
Copyright (C) 1990, 1991, 1992, 2001, 2006, 2007, 2009, 2010 Free Software Foundation, Inc.

[LICENSE]

GNU GENERAL PUBLIC LICENSE
Version 3, 29 June 2007

Copyright (C) 2007 Free Software Foundation, Inc. <http://fsf.org/>
Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The GNU General Public License is a free, copyleft license for software and other kinds of works.

The licenses for most software and other practical works are designed to take away your freedom to share and change the works. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change all versions of a program--to make sure it remains free software for all its users. We, the Free Software Foundation, use the GNU General Public License for most of our software; it applies also to any other work released this way by its authors. You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for them if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you these rights or asking you to surrender the rights. Therefore, you have certain responsibilities if you distribute copies of the software, or if you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must pass on to the recipients the same freedoms that you received. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

Developers that use the GNU GPL protect your rights with two steps: (1) assert copyright on the software, and (2) offer you this License giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains that there is no warranty for this free software. For both users' and authors' sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.

Some devices are designed to deny users access to install or run modified versions of the software inside them, although the manufacturer can do so. This is fundamentally incompatible with the aim of protecting users' freedom to change the software. The systematic pattern of such abuse occurs in the area of products for individuals to

use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains, we stand ready to extend this provision to those domains in future versions of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents. States should not allow patents to restrict development and use of software on general-purpose computers, but in those that do, we wish to avoid the special danger that patents applied to a free program could make it effectively proprietary. To prevent this, the GPL assures that patents cannot be used to render the program non-free.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS

0. Definitions.

"This License" refers to version 3 of the GNU General Public License.

"Copyright" also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

"The Program" refers to any copyrightable work licensed under this License. Each licensee is addressed as "you". "Licensees" and "recipients" may be individuals or organizations.

To "modify" a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a "modified version" of the earlier work or a work "based on" the earlier work.

A "covered work" means either the unmodified Program or a work based on the Program.

To "propagate" a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well.

To "convey" a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays "Appropriate Legal Notices" to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

1. Source Code.

The "source code" for a work means the preferred form of the work for making modifications to it. "Object code" means any non-source form of a work.

A "Standard Interface" means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The "System Libraries" of an executable work include anything, other than the work as a whole, that (a) is included in the normal form of

packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A "Major Component", in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The "Corresponding Source" for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work's System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

2. Basic Permissions.

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered by this License only if the output, given its content, constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed; section 10 makes it unnecessary.

3. Protecting Users' Legal Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of technological measures.

4. Conveying Verbatim Copies.

You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice; keep intact all notices stating that this License and any non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

5. Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

a) The work must carry prominent notices stating that you modified it, and giving a relevant date.

b) The work must carry prominent notices stating that it is released under this License and any conditions added under section 7. This requirement modifies the requirement in section 4 to "keep intact all notices".

c) You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it.

d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.

A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution medium, is called an "aggregate" if the compilation and its resulting copyright are not used to limit the access or legal rights of the compilation's users beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate.

6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, in one of these ways:

a) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange.

b) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as long as you offer spare parts or customer support for that product model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical medium customarily used for software interchange, for a price no

more than your reasonable cost of physically performing this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge.

c) Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source. This alternative is allowed only occasionally and noncommercially, and only if you received the object code with such an offer, in accord with subsection 6b.

d) Convey the object code by offering access from a designated place (gratis or for a charge), and offer equivalent access to the Corresponding Source in the same way through the same place at no further charge. You need not require recipients to copy the Corresponding Source along with the object code. If the place to copy the object code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.

e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.

A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object code work.

A "User Product" is either (1) a "consumer product", which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, "normally used" refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

"Installation Information" for a User Product means any methods, procedures, authorization keys, or other information required to install and execute modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in ROM).

The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and

protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

7. Additional Terms.

"Additional permissions" are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

a) Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or

b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or

c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or

d) Limiting the use for publicity purposes of names of licensors or authors of the material; or

e) Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or

f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on those licensors and authors.

All other non-permissive additional terms are considered "further restrictions" within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions;

the above requirements apply either way.

8. Termination.

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

10. Automatic Licensing of Downstream Recipients.

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An "entity transaction" is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

11. Patents.

A "contributor" is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The

work thus licensed is called the contributor's "contributor version".

A contributor's "essential patent claims" are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For purposes of this definition, "control" includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a "patent license" is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To "grant" such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. "Knowingly relying" means you have actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient's use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is "discriminatory" if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement, or that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.

12. No Surrender of Others' Freedom.

If conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot convey a

covered work so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

13. Use with the GNU Affero General Public License.

Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed under version 3 of the GNU Affero General Public License into a single combined work, and to convey the resulting work. The terms of this License will continue to apply to the part which is the covered work, but the special requirements of the GNU Affero General Public License, section 13, concerning interaction through a network will apply to the combination as such.

14. Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of the GNU General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU General Public License, you may choose any version ever published by the Free Software Foundation.

If the Program specifies that a proxy can decide which future versions of the GNU General Public License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Program.

Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.

15. Disclaimer of Warranty.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

17. Interpretation of Sections 15 and 16.

If the disclaimer of warranty and limitation of liability provided

```
above cannot be given local legal effect according to their terms,
reviewing courts shall apply local law that most closely approximates
an absolute waiver of all civil liability in connection with the
Program, unless a warranty or assumption of liability accompanies a
copy of the Program in return for a fee.

                     END OF TERMS AND CONDITIONS

            How to Apply These Terms to Your New Programs

  If you develop a new program, and you want it to be of the greatest
possible use to the public, the best way to achieve this is to make it
free software which everyone can redistribute and change under these terms.

  To do so, attach the following notices to the program.  It is safest
to attach them to the start of each source file to most effectively
state the exclusion of warranty; and each file should have at least
the "copyright" line and a pointer to where the full notice is found.

    <one line to give the program's name and a brief idea of what it does.>
    Copyright (C) <year>  <name of author>

    This program is free software: you can redistribute it and/or modify
    it under the terms of the GNU General Public License as published by
    the Free Software Foundation, either version 3 of the License, or
    (at your option) any later version.

    This program is distributed in the hope that it will be useful,
    but WITHOUT ANY WARRANTY; without even the implied warranty of
    MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
    GNU General Public License for more details.

    You should have received a copy of the GNU General Public License
    along with this program.  If not, see <http://www.gnu.org/licenses/>.

Also add information on how to contact you by electronic and paper mail.

  If the program does terminal interaction, make it output a short
notice like this when it starts in an interactive mode:

    <program>  Copyright (C) <year>  <name of author>
    This program comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
    This is free software, and you are welcome to redistribute it
    under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate
parts of the General Public License.  Of course, your program's commands
might be different; for a GUI interface, you would use an "about box".

  You should also get your employer (if you work as a programmer) or school,
if any, to sign a "copyright disclaimer" for the program, if necessary.
For more information on this, and how to apply and follow the GNU GPL, see
<http://www.gnu.org/licenses/>.

  The GNU General Public License does not permit incorporating your program
into proprietary programs.  If your program is a subroutine library, you
may consider it more useful to permit linking proprietary applications with
the library.  If this is what you want to do, use the GNU Lesser General
Public License instead of this License.  But first, please read
<http://www.gnu.org/philosophy/why-not-lgpl.html>.

--------------------------------------------------------------------------
---
[curl 7.21.2]
[COPYRIGHT]
  Copyright (c) 1996 - 2010, Daniel Stenberg, <daniel@haxx.se>.
  All rights reserved.

[LICENSE]
 Permission to use, copy, modify, and distribute this software for any purpose
```

with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder.

[domain stack framework 8.0.0 (part of FreeBSD 8.0.0)]
[COPYRIGHT]
Copyright (c) 1992-2009 The FreeBSD Project. All rights reserved.

[LICENSE]
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The 4.4BSD and 4.4BSD-Lite software is distributed under the following terms:

All of the documentation and software included in the 4.4BSD and 4.4BSD-Lite Releases is copyrighted by The Regents of the University of California.

Copyright 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:
This product includes software developed by the University of California, Berkeley and its contributors.
4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND

ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The Institute of Electrical and Electronics Engineers and the American National Standards Committee X3, on Information Processing Systems have given us permission to reprint portions of their documentation.

In the following statement, the phrase ``this text'' refers to portions of the system documentation.

Portions of this text are reprinted and reproduced in electronic form in the second BSD Networking Software Release, from IEEE Std 1003.1-1988, IEEE Standard Portable Operating System Interface for Computer Environments (POSIX), copyright C 1988 by the Institute of Electrical and Electronics Engineers, Inc. In the event of any discrepancy between these versions and the original IEEE Standard, the original IEEE Standard is the referee document.

In the following statement, the phrase ``This material'' refers to portions of the system documentation.

This material is reproduced with permission from American National Standards Committee X3, on Information Processing Systems. Computer and Business Equipment Manufacturers Association (CBEMA), 311 First St., NW, Suite 500, Washington, DC 20001-2178. The developmental work of Programming Language C was completed by the X3J11 Technical Committee.

The views and conclusions contained in the software and documentation are those of the authors and should not be interpreted as representing official policies, either expressed or implied, of the Regents of the University of California.

NOTE: The copyright of UC Berkeley's Berkeley Software Distribution ("BSD") source has been updated. The copyright addendum may be found at ftp://ftp.cs.berkeley.edu/pub/4bsd/README.Impt.License.Change and is included below.

July 22, 1999

To All Licensees, Distributors of Any Version of BSD:

As you know, certain of the Berkeley Software Distribution ("BSD") source code files require that further distributions of products containing all or portions of the software, acknowledge within their advertising materials that such products contain software developed by UC Berkeley and its contributors.

Specifically, the provision reads:

```
"     * 3. All advertising materials mentioning features or use of this software
       *    must display the following acknowledgement:
       *    This product includes software developed by the University of
       *    California, Berkeley and its contributors."
```

Effective immediately, licensees and distributors are no longer required to include the acknowledgement within advertising materials. Accordingly, the foregoing paragraph of those BSD Unix files containing it is hereby deleted in its entirety.

William Hoskins
Director, Office of Technology Licensing

University of California, Berkeley

[dosfstools 3.0.12]
[COPYRIGHT]
Copyright (C) 1998-2005 Roman Hodek <Roman.Hodek@informatik.uni-erlangen.de>

[LICENSE]
GNU GENERAL PUBLIC LICENSE
Version 3, 29 June 2007

Copyright (C) 2007 Free Software Foundation, Inc. <http://fsf.org/>
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The GNU General Public License is a free, copyleft license for software and other kinds of works.

The licenses for most software and other practical works are designed to take away your freedom to share and change the works. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change all versions of a program--to make sure it remains free software for all its users. We, the Free Software Foundation, use the GNU General Public License for most of our software; it applies also to any other work released this way by its authors. You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for them if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you these rights or asking you to surrender the rights. Therefore, you have certain responsibilities if you distribute copies of the software, or if you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must pass on to the recipients the same freedoms that you received. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

Developers that use the GNU GPL protect your rights with two steps: (1) assert copyright on the software, and (2) offer you this License giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains that there is no warranty for this free software. For both users' and authors' sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.

Some devices are designed to deny users access to install or run modified versions of the software inside them, although the manufacturer can do so. This is fundamentally incompatible with the aim of protecting users' freedom to change the software. The systematic pattern of such abuse occurs in the area of products for individuals to use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains, we stand ready to extend this provision to those domains in future versions of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents. States should not allow patents to restrict development and use of

software on general-purpose computers, but in those that do, we wish to avoid the special danger that patents applied to a free program could make it effectively proprietary. To prevent this, the GPL assures that patents cannot be used to render the program non-free.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS

0. Definitions.

"This License" refers to version 3 of the GNU General Public License.

"Copyright" also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

"The Program" refers to any copyrightable work licensed under this License. Each licensee is addressed as "you". "Licensees" and "recipients" may be individuals or organizations.

To "modify" a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a "modified version" of the earlier work or a work "based on" the earlier work.

A "covered work" means either the unmodified Program or a work based on the Program.

To "propagate" a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well.

To "convey" a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays "Appropriate Legal Notices" to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

1. Source Code.

The "source code" for a work means the preferred form of the work for making modifications to it. "Object code" means any non-source form of a work.

A "Standard Interface" means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The "System Libraries" of an executable work include anything, other than the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A "Major Component", in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The "Corresponding Source" for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work's System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

2. Basic Permissions.

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered by this License only if the output, given its content, constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed; section 10 makes it unnecessary.

3. Protecting Users' Legal Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of technological measures.

4. Conveying Verbatim Copies.

You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice; keep intact all notices stating that this License and any non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all

recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

5. Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

a) The work must carry prominent notices stating that you modified it, and giving a relevant date.

b) The work must carry prominent notices stating that it is released under this License and any conditions added under section 7. This requirement modifies the requirement in section 4 to "keep intact all notices".

c) You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it.

d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.

A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution medium, is called an "aggregate" if the compilation and its resulting copyright are not used to limit the access or legal rights of the compilation's users beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate.

6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, in one of these ways:

a) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange.

b) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as long as you offer spare parts or customer support for that product model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical medium customarily used for software interchange, for a price no more than your reasonable cost of physically performing this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge.

c) Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source. This alternative is allowed only occasionally and noncommercially, and only if you received the object code with such an offer, in accord

with subsection 6b.

d) Convey the object code by offering access from a designated place (gratis or for a charge), and offer equivalent access to the Corresponding Source in the same way through the same place at no further charge. You need not require recipients to copy the Corresponding Source along with the object code. If the place to copy the object code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.

e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.

A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object code work.

A "User Product" is either (1) a "consumer product", which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, "normally used" refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

"Installation Information" for a User Product means any methods, procedures, authorization keys, or other information required to install and execute modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in ROM).

The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

7. Additional Terms.

"Additional permissions" are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

a) Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or

b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or

c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or

d) Limiting the use for publicity purposes of names of licensors or authors of the material; or

e) Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or

f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on those licensors and authors.

All other non-permissive additional terms are considered "further restrictions" within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions; the above requirements apply either way.

8. Termination.

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third

paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

10. Automatic Licensing of Downstream Recipients.

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An "entity transaction" is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

11. Patents.

A "contributor" is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's "contributor version".

A contributor's "essential patent claims" are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For

purposes of this definition, "control" includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a "patent license" is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To "grant" such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. "Knowingly relying" means you have actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient's use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is "discriminatory" if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement, or that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.

12. No Surrender of Others' Freedom.

If conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot convey a covered work so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

13. Use with the GNU Affero General Public License.

Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed under version 3 of the GNU Affero General Public License into a single combined work, and to convey the resulting work. The terms of this License will continue to apply to the part which is the covered work, but the special requirements of the GNU Affero General Public License, section 13, concerning interaction through a network will apply to the combination as such.

14. Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of the GNU General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU General Public License, you may choose any version ever published by the Free Software Foundation.

If the Program specifies that a proxy can decide which future versions of the GNU General Public License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Program.

Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.

15. Disclaimer of Warranty.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

17. Interpretation of Sections 15 and 16.

If the disclaimer of warranty and limitation of liability provided above cannot be given local legal effect according to their terms, reviewing courts shall apply local law that most closely approximates an absolute waiver of all civil liability in connection with the Program, unless a warranty or assumption of liability accompanies a copy of the Program in return for a fee.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively state the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

```
    <one line to give the program's name and a brief idea of what it does.>
    Copyright (C) <year>  <name of author>

    This program is free software: you can redistribute it and/or modify
    it under the terms of the GNU General Public License as published by
    the Free Software Foundation, either version 3 of the License, or
    (at your option) any later version.

    This program is distributed in the hope that it will be useful,
    but WITHOUT ANY WARRANTY; without even the implied warranty of
    MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
    GNU General Public License for more details.

    You should have received a copy of the GNU General Public License
    along with this program.  If not, see <http://www.gnu.org/licenses/>.
```

Also add information on how to contact you by electronic and paper mail.

If the program does terminal interaction, make it output a short notice like this when it starts in an interactive mode:

```
    <program>  Copyright (C) <year>  <name of author>
    This program comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
    This is free software, and you are welcome to redistribute it
    under certain conditions; type `show c' for details.
```

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, your program's commands might be different; for a GUI interface, you would use an "about box".

You should also get your employer (if you work as a programmer) or school, if any, to sign a "copyright disclaimer" for the program, if necessary. For more information on this, and how to apply and follow the GNU GPL, see <http://www.gnu.org/licenses/>.

The GNU General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Lesser General Public License instead of this License. But first, please read <http://www.gnu.org/philosophy/why-not-lgpl.html>.

[dynamic linking loader 0.9.32 (part of uclibc 0.9.32)]

[LICENSE]

GNU LESSER GENERAL PUBLIC LICENSE
Version 2.1, February 1999

```
 Copyright (C) 1991, 1999 Free Software Foundation, Inc.
     51 Franklin St, Fifth Floor, Boston, MA  02110-1301  USA
 Everyone is permitted to copy and distribute verbatim copies
 of this license document, but changing it is not allowed.
```

[This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less

of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an

appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for

that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked

with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or

distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free

programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the library's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA

Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the library, if necessary. Here is a sample; alter the names:

```
  Yoyodyne, Inc., hereby disclaims all copyright interest in the
  library `Frob' (a library for tweaking knobs) written by James Random Hacker.

  <signature of Ty Coon>, 1 April 1990
  Ty Coon, President of Vice

That's all there is to it!


------------------------------------------------------------------------------
---
[freeradius-server3.0.10]
[COPYRIGHT]
  Copyright (C) 1999-2015 The FreeRADIUS Server Project

  Copyright (C) 1999, 2000, 2001, 2002, 2003, 2004, 2005, 2006, 2007, 2008, 2009
Alan DeKok
  <aland@deployingradius.com>

  Copyright (C) 1996, 1997, 1999, 2000, 2002, 2003, 2004, 2005 Free
  Software Foundation, Inc.

  Copyright (C) 2011-2015 Arran Cudbard-Bell <a.cudbardb@freeradius.org>

  Copyright (C) 2003, 2004, 2005 Kostas Kalevras <kkalev@noc.ntua.gr>

  Copyright (C) 2004  Cladju Consulting, Inc.

  Copyright (C) 2001, 2002, 2003, 2004, 2005 Google, Inc.

  Copyright (C) 2003, 2004  Michael Richardson <mcr@sandelman.ottawa.on.ca>

  Copyright (C) 2002, 2003, 2004 Novell, Inc.

  Copyright (C) 2002  Miguel A.L. Paraz <mparaz@mparaz.com>

  Copyright (C) 2002 Simon Ekstrand <simon@routemeister.net>

  Copyright (C) 2001  Chad Miller <cmiller@surfsouth.com>

  Copyright (C) 2001 hereUare Communications, Inc.

  Copyright (C) 2000 Jochen Friedrich <jochen@scram.de>

  Copyright (C) 2000, 2002 Miquel van Smoorenburg

  Copyright (C) 2000  Jeff Carneal <jeff@apex.net>

  Copyright (C) 2000  Alan Curry <pacman@world.std.com>

  Copyright (C) 2000  David Kerry <davidk@snti.com>

  Copyright (C) 2000  Dmitri Ageev <d_ageev@ortcc.ru>

  Copyright (C) 2000  Nathan Neulinger <nneul@umr.edu>

  Copyright (C) 2000  Mike Machado <mike@innercite.com>

  Copyright (C) 2000, 2001  Chad Miller <cmiller@surfsouth.com>

  Copyright (C) 1997, 1998, 1999 Cistron Internet Services B.V.

  Copyright (C) 1999 Kunihiro Ishiguro <kunihiro@zebra.org>

[LICENSE]
                    GNU GENERAL PUBLIC LICENSE
                       Version 2, June 1991

 Copyright (C) 1989, 1991 Free Software Foundation, Inc.
                       51 Franklin St, Fifth Floor, Boston, MA  02110-1301  USA
```

Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program

is covered only if its contents constitute a work based on the
Program (independent of having been made by running the Program).
Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's
source code as you receive it, in any medium, provided that you
conspicuously and appropriately publish on each copy an appropriate
copyright notice and disclaimer of warranty; keep intact all the
notices that refer to this License and to the absence of any warranty;
and give any other recipients of the Program a copy of this License
along with the Program.

You may charge a fee for the physical act of transferring a copy, and
you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion
of it, thus forming a work based on the Program, and copy and
distribute such modifications or work under the terms of Section 1
above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices
stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in
whole or in part contains or is derived from the Program or any
part thereof, to be licensed as a whole at no charge to all third
parties under the terms of this License.

c) If the modified program normally reads commands interactively
when run, you must cause it, when started running for such
interactive use in the most ordinary way, to print or display an
announcement including an appropriate copyright notice and a
notice that there is no warranty (or else, saying that you provide
a warranty) and that users may redistribute the program under
these conditions, and telling the user how to view a copy of this
License. (Exception: if the Program itself is interactive but
does not normally print such an announcement, your work based on
the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If
identifiable sections of that work are not derived from the Program,
and can be reasonably considered independent and separate works in
themselves, then this License, and its terms, do not apply to those
sections when you distribute them as separate works. But when you
distribute the same sections as part of a whole which is a work based
on the Program, the distribution of the whole must be on the terms of
this License, whose permissions for other licensees extend to the
entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest
your rights to work written entirely by you; rather, the intent is to
exercise the right to control the distribution of derivative or
collective works based on the Program.

In addition, mere aggregation of another work not based on the Program
with the Program (or with a work based on the Program) on a volume of
a storage or distribution medium does not bring the other work under
the scope of this License.

3. You may copy and distribute the Program (or a work based on it,
under Section 2) in object code or executable form under the terms of
Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable
source code, which must be distributed under the terms of Sections
1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three
years, to give any third party, for a charge no more than your

cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other

circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

```
    <one line to give the program's name and a brief idea of what it does.>
    Copyright (C) <year>  <name of author>

    This program is free software; you can redistribute it and/or modify
    it under the terms of the GNU General Public License as published by
    the Free Software Foundation; either version 2 of the License, or
    (at your option) any later version.

    This program is distributed in the hope that it will be useful,
    but WITHOUT ANY WARRANTY; without even the implied warranty of
    MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
    GNU General Public License for more details.

    You should have received a copy of the GNU General Public License
    along with this program; if not, write to the Free Software
    Foundation, Inc., 51 Franklin St, Fifth Floor, Boston, MA  02110-1301  USA
```

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

```
    Gnomovision version 69, Copyright (C) year name of author
    Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
    This is free software, and you are welcome to redistribute it
    under certain conditions; type `show c' for details.
```

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than `show w' and `show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

```
  Yoyodyne, Inc., hereby disclaims all copyright interest in the program
  `Gnomovision' (which makes passes at compilers) written by James Hacker.

  <signature of Ty Coon>, 1 April 1989
  Ty Coon, President of Vice
```

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Library General Public License instead of this License.

[freescale-openflow-controller 1.0]

[COPYRIGHT]

Copyright (c) 2012, 2013 Freescale.

[LICENSE]

Apache License
Version 2.0, January 2004
http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

   "License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

   "Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

   "Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

   "You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

   "Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

   "Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

   "Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

   "Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

   "Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

   "Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of

this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

   (a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

   (b) You must cause any modified files to carry prominent notices stating that You changed the files; and

   (c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

   (d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

   You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or

```
      agreed to in writing, Licensor provides the Work (and each
      Contributor provides its Contributions) on an "AS IS" BASIS,
      WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or
      implied, including, without limitation, any warranties or conditions
      of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A
      PARTICULAR PURPOSE. You are solely responsible for determining the
      appropriateness of using or redistributing the Work and assume any
      risks associated with Your exercise of permissions under this License.

   8. Limitation of Liability. In no event and under no legal theory,
      whether in tort (including negligence), contract, or otherwise,
      unless required by applicable law (such as deliberate and grossly
      negligent acts) or agreed to in writing, shall any Contributor be
      liable to You for damages, including any direct, indirect, special,
      incidental, or consequential damages of any character arising as a
      result of this License or out of the use or inability to use the
      Work (including but not limited to damages for loss of goodwill,
      work stoppage, computer failure or malfunction, or any and all
      other commercial damages or losses), even if such Contributor
      has been advised of the possibility of such damages.

   9. Accepting Warranty or Additional Liability. While redistributing
      the Work or Derivative Works thereof, You may choose to offer,
      and charge a fee for, acceptance of support, warranty, indemnity,
      or other liability obligations and/or rights consistent with this
      License. However, in accepting such obligations, You may act only
      on Your own behalf and on Your sole responsibility, not on behalf
      of any other Contributor, and only if You agree to indemnify,
      defend, and hold each Contributor harmless for any liability
      incurred by, or claims asserted against, such Contributor by reason
      of your accepting any such warranty or additional liability.

   END OF TERMS AND CONDITIONS

   APPENDIX: How to apply the Apache License to your work.

      To apply the Apache License to your work, attach the following
      boilerplate notice, with the fields enclosed by brackets "[]"
      replaced with your own identifying information. (Don't include
      the brackets!)  The text should be enclosed in the appropriate
      comment syntax for the file format. We also recommend that a
      file or class name and description of purpose be included on the
      same "printed page" as the copyright notice for easier
      identification within third-party archives.

   Copyright 2012 Sebastien MALOT

   Licensed under the Apache License, Version 2.0 (the "License");
   you may not use this file except in compliance with the License.
   You may obtain a copy of the License at

       http://www.apache.org/licenses/LICENSE-2.0

   Unless required by applicable law or agreed to in writing, software
   distributed under the License is distributed on an "AS IS" BASIS,
   WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
   See the License for the specific language governing permissions and
   limitations under the License.
-------------------------------------------------------------------------------
---
[ftp client 8.0.0 (part of FreeBSD 8.0.0)]
[COPYRIGHT]
  Copyright (c) 1992-2009 The FreeBSD Project. All rights reserved.

[LICENSE]
Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:
1. Redistributions of source code must retain the above copyright
   notice, this list of conditions and the following disclaimer.
```

2. Redistributions in binary form must reproduce the above copyright
   notice, this list of conditions and the following disclaimer in the
   documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS ``AS IS'' AND
ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
SUCH DAMAGE.

The 4.4BSD and 4.4BSD-Lite software is distributed under the following
terms:

All of the documentation and software included in the 4.4BSD and 4.4BSD-Lite
Releases is copyrighted by The Regents of the University of California.

Copyright 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
         The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:
1. Redistributions of source code must retain the above copyright
   notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright
   notice, this list of conditions and the following disclaimer in the
   documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software
   must display the following acknowledgement:
This product includes software developed by the University of
California, Berkeley and its contributors.
4. Neither the name of the University nor the names of its contributors
   may be used to endorse or promote products derived from this software
   without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND
ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE
FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
SUCH DAMAGE.

The Institute of Electrical and Electronics Engineers and the American
National Standards Committee X3, on Information Processing Systems have
given us permission to reprint portions of their documentation.

In the following statement, the phrase ``this text'' refers to portions
of the system documentation.

Portions of this text are reprinted and reproduced in electronic form in
the second BSD Networking Software Release, from IEEE Std 1003.1-1988, IEEE
Standard Portable Operating System Interface for Computer Environments
(POSIX), copyright C 1988 by the Institute of Electrical and Electronics
Engineers, Inc. In the event of any discrepancy between these versions
and the original IEEE Standard, the original IEEE Standard is the referee
document.

In the following statement, the phrase ``This material'' refers to portions
of the system documentation.

This material is reproduced with permission from American National Standards Committee X3, on Information Processing Systems. Computer and Business Equipment Manufacturers Association (CBEMA), 311 First St., NW, Suite 500, Washington, DC 20001-2178. The developmental work of Programming Language C was completed by the X3J11 Technical Committee.

The views and conclusions contained in the software and documentation are those of the authors and should not be interpreted as representing official policies, either expressed or implied, of the Regents of the University of California.

NOTE: The copyright of UC Berkeley's Berkeley Software Distribution ("BSD") source has been updated. The copyright addendum may be found at ftp://ftp.cs.berkeley.edu/pub/4bsd/README.Impt.License.Change and is included below.

July 22, 1999

To All Licensees, Distributors of Any Version of BSD:

As you know, certain of the Berkeley Software Distribution ("BSD") source code files require that further distributions of products containing all or portions of the software, acknowledge within their advertising materials that such products contain software developed by UC Berkeley and its contributors.

Specifically, the provision reads:

" * 3. All advertising materials mentioning features or use of this software
 * must display the following acknowledgement:
 * This product includes software developed by the University of
 * California, Berkeley and its contributors."

Effective immediately, licensees and distributors are no longer required to include the acknowledgement within advertising materials. Accordingly, the foregoing paragraph of those BSD Unix files containing it is hereby deleted in its entirety.

William Hoskins
Director, Office of Technology Licensing
University of California, Berkeley

[grpc 1.4.2]
[COPYRIGHT]
Copyright 2015, Google Inc.
All rights reserved.

[LICENSE]
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
* Neither the name of Google Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,

```
SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT
LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE,
DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY
THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT
(INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE
OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
--------------------------------------------------------------------------
---
[inet stack 8.0.0 (part of FreeBSD 8.0.0)]
[COPYRIGHT]
  Copyright (c) 1992-2009 The FreeBSD Project. All rights reserved.

[LICENSE]
Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:
1. Redistributions of source code must retain the above copyright
   notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright
   notice, this list of conditions and the following disclaimer in the
   documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS ``AS IS'' AND
ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
ARE DISCLAIMED.  IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
SUCH DAMAGE.

The 4.4BSD and 4.4BSD-Lite software is distributed under the following
terms:

All of the documentation and software included in the 4.4BSD and 4.4BSD-Lite
Releases is copyrighted by The Regents of the University of California.

Copyright 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
         The Regents of the University of California.  All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:
1. Redistributions of source code must retain the above copyright
   notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright
   notice, this list of conditions and the following disclaimer in the
   documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software
   must display the following acknowledgement:
This product includes software developed by the University of
California, Berkeley and its contributors.
4. Neither the name of the University nor the names of its contributors
   may be used to endorse or promote products derived from this software
   without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND
ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
ARE DISCLAIMED.  IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE
FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
SUCH DAMAGE.
```

The Institute of Electrical and Electronics Engineers and the American National Standards Committee X3, on Information Processing Systems have given us permission to reprint portions of their documentation.

In the following statement, the phrase ``this text'' refers to portions of the system documentation.

Portions of this text are reprinted and reproduced in electronic form in the second BSD Networking Software Release, from IEEE Std 1003.1-1988, IEEE Standard Portable Operating System Interface for Computer Environments (POSIX), copyright C 1988 by the Institute of Electrical and Electronics Engineers, Inc. In the event of any discrepancy between these versions and the original IEEE Standard, the original IEEE Standard is the referee document.

In the following statement, the phrase ``This material'' refers to portions of the system documentation.

This material is reproduced with permission from American National Standards Committee X3, on Information Processing Systems. Computer and Business Equipment Manufacturers Association (CBEMA), 311 First St., NW, Suite 500, Washington, DC 20001-2178. The developmental work of Programming Language C was completed by the X3J11 Technical Committee.

The views and conclusions contained in the software and documentation are those of the authors and should not be interpreted as representing official policies, either expressed or implied, of the Regents of the University of California.

NOTE: The copyright of UC Berkeley's Berkeley Software Distribution ("BSD") source has been updated. The copyright addendum may be found at ftp://ftp.cs.berkeley.edu/pub/4bsd/README.Impt.License.Change and is included below.

July 22, 1999

To All Licensees, Distributors of Any Version of BSD:

As you know, certain of the Berkeley Software Distribution ("BSD") source code files require that further distributions of products containing all or portions of the software, acknowledge within their advertising materials that such products contain software developed by UC Berkeley and its contributors.

Specifically, the provision reads:

```
"     * 3. All advertising materials mentioning features or use of this software
       *    must display the following acknowledgement:
       *    This product includes software developed by the University of
       *    California, Berkeley and its contributors."
```

Effective immediately, licensees and distributors are no longer required to include the acknowledgement within advertising materials. Accordingly, the foregoing paragraph of those BSD Unix files containing it is hereby deleted in its entirety.

William Hoskins
Director, Office of Technology Licensing
University of California, Berkeley

[jquery-ui 1.9.2]
[COPYRIGHT]
Copyright 2012 jQuery Foundation and other contributors,
http://jqueryui.com/

[LICENSE]
This software consists of voluntary contributions made by many

```
individuals (AUTHORS.txt, http://jqueryui.com/about) For exact
contribution history, see the revision history and logs, available
at http://jquery-ui.googlecode.com/svn/

Permission is hereby granted, free of charge, to any person obtaining
a copy of this software and associated documentation files (the
"Software"), to deal in the Software without restriction, including
without limitation the rights to use, copy, modify, merge, publish,
distribute, sublicense, and/or sell copies of the Software, and to
permit persons to whom the Software is furnished to do so, subject to
the following conditions:

The above copyright notice and this permission notice shall be
included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND,
EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF
MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND
NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE
LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION
OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION
WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

--------------------------------------------------------------------------
---
[jquery.event.drag 2.2]
[COPYRIGHT]
  Copyright (c) 2008-2021 ThreeDubMedia

[LICENSE]
Permission is hereby granted, free of charge, to any person
obtaining a copy of this software and associated documentation
files (the "Software"), to deal in the Software without
restriction, including without limitation the rights to use,
copy, modify, merge, publish, distribute, sublicense, and/or sell
copies of the Software, and to permit persons to whom the
Software is furnished to do so, subject to the following
conditions:

The above copyright notice and this permission notice shall be
included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND,
EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES
OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND
NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT
HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY,
WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING
FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR
OTHER DEALINGS IN THE SOFTWARE.
--------------------------------------------------------------------------
---
[json c 0.12]
[COPYRIGHT]
  Copyright (c) 2009-2012 Eric Haszlakiewicz

[LICENSE]
Permission is hereby granted, free of charge, to any person obtaining a
copy of this software and associated documentation files (the "Software"),
to deal in the Software without restriction, including without limitation
the rights to use, copy, modify, merge, publish, distribute, sublicense,
and/or sell copies of the Software, and to permit persons to whom the
Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included
in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,
FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE
```

AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER
LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,
OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE
SOFTWARE.

[COPYRIGHT]
Copyright (c) 2004, 2005 Metaparadigm Pte Ltd

[LICENSE]
Permission is hereby granted, free of charge, to any person obtaining a
copy of this software and associated documentation files (the "Software"),
to deal in the Software without restriction, including without limitation
the rights to use, copy, modify, merge, publish, distribute, sublicense,
and/or sell copies of the Software, and to permit persons to whom the
Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included
in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,
FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE
AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER
LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,
OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE
SOFTWARE.

[jstree 3.0.0]
[COPYRIGHT]
  Copyright (c) 2013 Ivan Bozhanov

[LICENSE]
Permission is hereby granted, free of charge, to any person
obtaining a copy of this software and associated documentation
files (the "Software"), to deal in the Software without
restriction, including without limitation the rights to use,
copy, modify, merge, publish, distribute, sublicense, and/or sell
copies of the Software, and to permit persons to whom the
Software is furnished to do so, subject to the following
conditions:

The above copyright notice and this permission notice shall be
included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND,
EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES
OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND
NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT
HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY,
WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING
FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR
OTHER DEALINGS IN THE SOFTWARE.

[libiconv 1.13.1]
[LICENSE]
                  GNU LIBRARY GENERAL PUBLIC LICENSE
                       Version 2, June 1991

 Copyright (C) 1991 Free Software Foundation, Inc.
 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA
 Everyone is permitted to copy and distribute verbatim copies
 of this license document, but changing it is not allowed.

[This is the first released version of the library GPL. It is
 numbered 2 because it goes with version 2 of the ordinary GPL.]

                            Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Library General Public License, applies to some specially designated Free Software Foundation software, and to any other libraries whose authors decide to use it. You can use it for your libraries, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library, or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link a program with the library, you must provide complete object files to the recipients so that they can relink them with the library, after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

Our method of protecting your rights has two steps: (1) copyright the library, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the library.

Also, for each distributor's protection, we want to make certain that everyone understands that there is no warranty for this free library. If the library is modified by someone else and passed on, we want its recipients to know that what they have is not the original version, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that companies distributing free software will individually obtain patent licenses, thus in effect transforming the program into proprietary software. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License, which was designed for utility programs. This license, the GNU Library General Public License, applies to certain designated libraries. This license is quite different from the ordinary one; be sure to read it in full, and don't assume that anything in it is the same as in the ordinary license.

The reason we have a separate public license for some libraries is that they blur the distinction we usually make between modifying or adding to a program and simply using it. Linking a program with a library, without changing the library, is in some sense simply using the library, and is analogous to running a utility program or application program. However, in a textual and legal sense, the linked executable is a combined work, a derivative of the original library, and the ordinary General Public License treats it as such.

Because of this blurred distinction, using the ordinary General Public License for libraries did not effectively promote software sharing, because most developers did not use the libraries. We concluded that weaker conditions might promote sharing better.

However, unrestricted linking of non-free programs would deprive the users of those programs of all benefit from the free status of the libraries themselves. This Library General Public License is intended to permit developers of non-free programs to use free libraries, while preserving your freedom as a user of such programs to change the free libraries that are incorporated in them. (We have not seen how to achieve this as regards changes in header files, but we have achieved it as regards changes in the actual functions of the Library.) The hope is that this will lead to faster development of free libraries.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, while the latter only works together with the library.

Note that it is possible for a library to be covered by the ordinary General Public License rather than by this special one.

GNU LIBRARY GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Library General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion

of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a

medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also compile or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more

than the cost of performing this distribution.

c) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

d) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or

otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Library General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

Appendix: How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the library's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Library General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Library General Public License for more details.

You should have received a copy of the GNU Library General Public License along with this library; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA

Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the library, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the library `Frob' (a library for tweaking knobs) written by James Random Hacker.

<signature of Ty Coon>, 1 April 1990
Ty Coon, President of Vice

That's all there is to it!

[libpcap 1.2.0]
[LICENSE]
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright

```
     notice, this list of conditions and the following disclaimer in
     the documentation and/or other materials provided with the
     distribution.
  3. The names of the authors may not be used to endorse or promote
     products derived from this software without specific prior
     written permission.

THIS SOFTWARE IS PROVIDED ``AS IS'' AND WITHOUT ANY EXPRESS OR
IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED
WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.
--------------------------------------------------------------------------------
---
[libssh2 1.4.3]
[COPYRIGHT]
  Copyright (c) 2004-2007 Sara Golemon <sarag@libssh2.org>
  Copyright (c) 2005,2006 Mikhail Gusarov <dottedmag@dottedmag.net>
  Copyright (c) 2006-2007 The Written Word, Inc.
  Copyright (c) 2007 Eli Fant <elifantu@mail.ru>
  Copyright (c) 2009 Daniel Stenberg
  Copyright (C) 2008, 2009 Simon Josefsson
  All rights reserved.

[LICENSE]
  Redistribution and use in source and binary forms,
  with or without modification, are permitted provided
  that the following conditions are met:

    Redistributions of source code must retain the above
    copyright notice, this list of conditions and the
    following disclaimer.

    Redistributions in binary form must reproduce the above
    copyright notice, this list of conditions and the following
    disclaimer in the documentation and/or other materials
    provided with the distribution.

    Neither the name of the copyright holder nor the names
    of any other contributors may be used to endorse or
    promote products derived from this software without
    specific prior written permission.

  THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND
  CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES,
  INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES
  OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
  ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR
  CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
  SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING,
  BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR
  SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS
  INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY,
  WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING
  NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE
  USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY
  OF SUCH DAMAGE.


--------------------------------------------------------------------------------
---
[liburcu 0.6.8]
[COPYRIGHT]
  Copyright (c) 2009 Mathieu Desnoyers <mathieu.desnoyers@efficios.com>
  Copyright (c) 2009 Paul E. McKenney, IBM Corporation.

[LICENSE]
  This library is free software; you can redistribute it and/or
  modify it under the terms of the GNU Lesser General Public
  License as published by the Free Software Foundation; either
  version 2.1 of the License, or (at your option) any later version.
```

```
  This library is distributed in the hope that it will be useful,
  but WITHOUT ANY WARRANTY; without even the implied warranty of
  MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the GNU
  Lesser General Public License for more details.

  You should have received a copy of the GNU Lesser General Public
  License along with this library; if not, write to the Free Software
  Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

  IBM's contributions to this file may be relicensed under LGPLv2 or later.

--------------------------------------------------------------------------------
---
[multiselect 0.9.5]
[COPYRIGHT]
  Copyright (c) 2012 Louis Cuny

[LICENSE]
            DO WHAT THE FUCK YOU WANT TO PUBLIC LICENSE
                    Version 2, December 2004

 Copyright (C) 2004 Sam Hocevar <sam@hocevar.net>

 Everyone is permitted to copy and distribute verbatim or modified
 copies of this license document, and changing it is allowed as long
 as the name is changed.

            DO WHAT THE FUCK YOU WANT TO PUBLIC LICENSE
   TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

  0. You just DO WHAT THE FUCK YOU WANT TO.
--------------------------------------------------------------------------------
---
[ncurses 5.7]
[COPYRIGHT]
  Copyright (c) 1998-2004,2006 Free Software Foundation, Inc.

[LICENSE]
--                                                                          --
-- Permission is hereby granted, free of charge, to any person obtaining a  --
-- copy of this software and associated documentation files (the            --
-- "Software"), to deal in the Software without restriction, including      --
-- without limitation the rights to use, copy, modify, merge, publish,      --
-- distribute, distribute with modifications, sublicense, and/or sell copies --
-- of the Software, and to permit persons to whom the Software is furnished --
-- to do so, subject to the following conditions:                           --
--                                                                          --
-- The above copyright notice and this permission notice shall be included  --
-- in all copies or substantial portions of the Software.                   --
--                                                                          --
-- THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS  --
-- OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF               --
-- MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN --
-- NO EVENT SHALL THE ABOVE COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM,      --
-- DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR    --
-- OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE --
-- USE OR OTHER DEALINGS IN THE SOFTWARE.                                   --
--                                                                          --
-- Except as contained in this notice, the name(s) of the above copyright   --
-- holders shall not be used in advertising or otherwise to promote the     --
-- sale, use or other dealings in this Software without prior written       --
-- authorization.                                                           --
--------------------------------------------------------------------------------
---
[net-snmp 5.4.3]
Various copyrights apply to this package, listed in various separate
parts below.  Please make sure that you read all the parts.

---- Part 1: CMU/UCD copyright notice: (BSD like) -----
```

Copyright 1989, 1991, 1992 by Carnegie Mellon University

Derivative Work - 1996, 1998-2000
Copyright 1996, 1998-2000 The Regents of the University of California

All Rights Reserved

Permission to use, copy, modify and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appears in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of CMU and The Regents of the University of California not be used in advertising or publicity pertaining to distribution of the software without specific written permission.

CMU AND THE REGENTS OF THE UNIVERSITY OF CALIFORNIA DISCLAIM ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL CMU OR THE REGENTS OF THE UNIVERSITY OF CALIFORNIA BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM THE LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

---- Part 2: Networks Associates Technology, Inc copyright notice (BSD) -----

Copyright (c) 2001-2003, Networks Associates Technology, Inc
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of the Networks Associates Technology, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 3: Cambridge Broadband Ltd. copyright notice (BSD) -----

Portions of this code are copyright (c) 2001-2003, Cambridge Broadband Ltd.
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright
  notice, this list of conditions and the following disclaimer in the
  documentation and/or other materials provided with the distribution.

* The name of Cambridge Broadband Ltd. may not be used to endorse or
  promote products derived from this software without specific prior
  written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER ``AS IS'' AND ANY
EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE
LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF
SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR
BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY,
WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE
OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN
IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 4: Sun Microsystems, Inc. copyright notice (BSD) -----

Copyright ?2003 Su Microsystems, Inc., 4150 Network Circle, Santa Clara,
California 95054, U.S.A. All rights reserved.

Use is subject to license terms below.

This distribution may include materials developed by third parties.

Sun, Sun Microsystems, the Sun logo and Solaris are trademarks or registered
trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice,
  this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright
  notice, this list of conditions and the following disclaimer in the
  documentation and/or other materials provided with the distribution.

* Neither the name of the Sun Microsystems, Inc. nor the
  names of its contributors may be used to endorse or promote
  products derived from this software without specific prior written
  permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS
IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO,
THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR
CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL,
EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,
PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS;
OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY,
WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR
OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF
ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 5: Sparta, Inc copyright notice (BSD) -----

Copyright (c) 2003-2010, Sparta, Inc
All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice,
  this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright
notice, this list of conditions and the following disclaimer in the
documentation and/or other materials provided with the distribution.

* Neither the name of Sparta, Inc nor the names of its contributors may
be used to endorse or promote products derived from this software
without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS
IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO,
THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR
CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL,
EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,
PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS;
OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY,
WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR
OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF
ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 6: Cisco/BUPTNIC copyright notice (BSD) -----

Copyright (c) 2004, Cisco, Inc and Information Network
Center of Beijing University of Posts and Telecommunications.
All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice,
this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright
notice, this list of conditions and the following disclaimer in the
documentation and/or other materials provided with the distribution.

* Neither the name of Cisco, Inc, Beijing University of Posts and
Telecommunications, nor the names of their contributors may
be used to endorse or promote products derived from this software
without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS
IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO,
THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR
CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL,
EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,
PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS;
OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY,
WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR
OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF
ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 7: Fabasoft R&D Software GmbH & Co KG copyright notice (BSD) -----

Copyright (c) Fabasoft R&D Software GmbH & Co KG, 2003
oss@fabasoft.com
Author: Bernhard Penz <bernhard.penz@fabasoft.com>

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice,
this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright
notice, this list of conditions and the following disclaimer in the
documentation and/or other materials provided with the distribution.

```
*  The name of Fabasoft R&D Software GmbH & Co KG or any of its subsidiaries,
   brand or product names may not be used to endorse or promote products
   derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER ``AS IS'' AND ANY
EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE COPYRIGHT HOLDER BE
LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF
SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR
BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY,
WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE
OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN
IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

--------------------------------------------------------------------------------
---
[ntp 4.2 6p2-RC4]
This file is automatically generated from html/copyright.html

  Copyright Notice

   jpg "Clone me," says Dolly sheepishly.

   Last update: 11-May-2010 04:41 UTC

     ____________________________________________________________________

   The following copyright notice applies to all files collectively
   called the Network Time Protocol Version 4 Distribution. Unless
   specifically declared otherwise in an individual file, this notice
   applies as if the text was explicitly included in the file.
**********************************************************************
*                                                                    *
* Copyright (c) University of Delaware 1992-2010                     *
*                                                                    *
* Permission to use, copy, modify, and distribute this software and  *
* its documentation for any purpose with or without fee is hereby    *
* granted, provided that the above copyright notice appears in all   *
* copies and that both the copyright notice and this permission      *
* notice appear in supporting documentation, and that the name       *
* University of Delaware not be used in advertising or publicity     *
* pertaining to distribution of the software without specific,       *
* written prior permission. The University of Delaware makes no      *
* representations about the suitability this software for any        *
* purpose. It is provided "as is" without express or implied         *
* warranty.                                                          *
*                                                                    *
**********************************************************************

   The following individuals contributed in part to the Network Time
   Protocol Distribution Version 4 and are acknowledged as authors of
   this work.
    1. [1]Mark Andrews <mark_andrews@isc.org> Leitch atomic clock
       controller
    2. [2]Bernd Altmeier <altmeier@atlsoft.de> hopf Elektronik serial
       line and PCI-bus devices
    3. [3]Viraj Bais <vbais@mailman1.intel.com> and [4]Clayton Kirkwood
       <kirkwood@striderfm.intel.com> port to WindowsNT 3.5
    4. [5]Michael Barone <michael,barone@lmco.com> GPSVME fixes
    5. [6]Karl Berry <karl@owl.HQ.ileaf.com> syslog to file option
    6. [7]Greg Brackley <greg.brackley@bigfoot.com> Major rework of WINNT
       port. Clean up recvbuf and iosignal code into separate modules.
    7. [8]Marc Brett <Marc.Brett@westgeo.com> Magnavox GPS clock driver
    8. [9]Piete Brooks <Piete.Brooks@cl.cam.ac.uk> MSF clock driver,
       Trimble PARSE support
    9. [10]Nelson B Bolyard <nelson@bolyard.me> update and complete
       broadcast and crypto features in sntp
   10. [11]Jean-Francois Boudreault
       <Jean-Francois.Boudreault@viagenie.qc.ca> IPv6 support
```

11. [12]Reg Clemens <reg@dwf.com> Oncore driver (Current maintainer)
12. [13]Steve Clift <clift@ml.csiro.au> OMEGA clock driver
13. [14]Casey Crellin <casey@csc.co.za> vxWorks (Tornado) port and help with target configuration
14. [15]Sven Dietrich <sven_dietrich@trimble.com> Palisade reference clock driver, NT adj. residuals, integrated Greg's Winnt port.
15. [16]John A. Dundas III <dundas@salt.jpl.nasa.gov> Apple A/UX port
16. [17]Torsten Duwe <duwe@immd4.informatik.uni-erlangen.de> Linux port
17. [18]Dennis Ferguson <dennis@mrbill.canet.ca> foundation code for NTP Version 2 as specified in RFC-1119
18. [19]John Hay <jhay@icomtek.csir.co.za> IPv6 support and testing
19. [20]Dave Hart <davehart@davehart.com> General maintenance, Windows port interpolation rewrite
20. [21]Claas Hilbrecht <neoclock4x@linum.com> NeoClock4X clock driver
21. [22]Glenn Hollinger <glenn@herald.usask.ca> GOES clock driver
22. [23]Mike Iglesias <iglesias@uci.edu> DEC Alpha port
23. [24]Jim Jagielski <jim@jagubox.gsfc.nasa.gov> A/UX port
24. [25]Jeff Johnson <jbj@chatham.usdesign.com> massive prototyping overhaul
25. [26]Hans Lambermont <Hans.Lambermont@nl.origin-it.com> or [27]<H.Lambermont@chello.nl> ntpsweep
26. [28]Poul-Henning Kamp <phk@FreeBSD.ORG> Oncore driver (Original author)
27. [29]Frank Kardel [30]<kardel (at) ntp (dot) org> PARSE <GENERIC> driver (>14 reference clocks), STREAMS modules for PARSE, support scripts, syslog cleanup, dynamic interface handling
28. [31]William L. Jones <jones@hermes.chpc.utexas.edu> RS/6000 AIX modifications, HPUX modifications
29. [32]Dave Katz <dkatz@cisco.com> RS/6000 AIX port
30. [33]Craig Leres <leres@ee.lbl.gov> 4.4BSD port, ppsclock, Magnavox GPS clock driver
31. [34]George Lindholm <lindholm@ucs.ubc.ca> SunOS 5.1 port
32. [35]Louis A. Mamakos <louie@ni.umd.edu> MD5-based authentication
33. [36]Lars H. Mathiesen <thorinn@diku.dk> adaptation of foundation code for Version 3 as specified in RFC-1305
34. [37]Danny Mayer <mayer@ntp.org>Network I/O, Windows Port, Code Maintenance
35. [38]David L. Mills <mills@udel.edu> Version 4 foundation: clock discipline, authentication, precision kernel; clock drivers: Spectracom, Austron, Arbiter, Heath, ATOM, ACTS, KSI/Odetics; audio clock drivers: CHU, WWV/H, IRIG
36. [39]Wolfgang Moeller <moeller@gwdgv1.dnet.gwdg.de> VMS port
37. [40]Jeffrey Mogul <mogul@pa.dec.com> ntptrace utility
38. [41]Tom Moore <tmoore@fievel.daytonoh.ncr.com> i386 svr4 port
39. [42]Kamal A Mostafa <kamal@whence.com> SCO OpenServer port
40. [43]Derek Mulcahy <derek@toybox.demon.co.uk> and [44]Damon Hart-Davis <d@hd.org> ARCRON MSF clock driver
41. [45]Rob Neal <neal@ntp.org> Bancomm refclock and config/parse code maintenance
42. [46]Rainer Pruy <Rainer.Pruy@informatik.uni-erlangen.de> monitoring/trap scripts, statistics file handling
43. [47]Dirce Richards <dirce@zk3.dec.com> Digital UNIX V4.0 port
44. [48]Wilfredo S 疣 chez <wanchez@apple.com> added support for NetInfo
45. [49]Nick Sayer <mrapple@quack.kfu.com> SunOS streams modules
46. [50]Jack Sasportas <jack@innovativeinternet.com> Saved a Lot of space on the stuff in the html/pic/ subdirectory
47. [51]Ray Schnitzler <schnitz@unipress.com> Unixware1 port
48. [52]Michael Shields <shields@tembel.org> USNO clock driver
49. [53]Jeff Steinman <jss@pebbles.jpl.nasa.gov> Datum PTS clock driver
50. [54]Harlan Stenn <harlan@pfcs.com> GNU automake/autoconfigure makeover, various other bits (see the ChangeLog)
51. [55]Kenneth Stone <ken@sdd.hp.com> HP-UX port
52. [56]Ajit Thyagarajan <ajit@ee.udel.edu>IP multicast/anycast support
53. [57]Tomoaki TSURUOKA <tsuruoka@nc.fukuoka-u.ac.jp>TRAK clock driver
54. [58]Paul A Vixie <vixie@vix.com> TrueTime GPS driver, generic

```
      TrueTime clock driver
   55. [59]Ulrich Windl <Ulrich.Windl@rz.uni-regensburg.de> corrected and
       validated HTML documents according to the HTML DTD

    ____________________________________________________________________

References

   1. mailto:%20mark_andrews@isc.org
   2. mailto:%20altmeier@atlsoft.de
   3. mailto:%20vbais@mailman1.intel.co
   4. mailto:%20kirkwood@striderfm.intel.com
   5. mailto:%20michael.barone@lmco.com
   6. mailto:%20karl@owl.HQ.ileaf.com
   7. mailto:%20greg.brackley@bigfoot.com
   8. mailto:%20Marc.Brett@westgeo.com
   9. mailto:%20Piete.Brooks@cl.cam.ac.uk
  10. mailto:%20nelson@bolyard.me
  11. mailto:%20Jean-Francois.Boudreault@viagenie.qc.ca
  12. mailto:%20reg@dwf.com
  13. mailto:%20clift@ml.csiro.au
  14. mailto:casey@csc.co.za
  15. mailto:%20Sven_Dietrich@trimble.COM
  16. mailto:%20dundas@salt.jpl.nasa.gov
  17. mailto:%20duwe@immd4.informatik.uni-erlangen.de
  18. mailto:%20dennis@mrbill.canet.ca
  19. mailto:%20jhay@icomtek.csir.co.za
  20. mailto:%20davehart@davehart.com
  21. mailto:%20neoclock4x@linum.com
  22. mailto:%20glenn@herald.usask.ca
  23. mailto:%20iglesias@uci.edu
  24. mailto:%20jagubox.gsfc.nasa.gov
  25. mailto:%20jbj@chatham.usdesign.com
  26. mailto:Hans.Lambermont@nl.origin-it.com
  27. mailto:H.Lambermont@chello.nl
  28. mailto:%20phk@FreeBSD.ORG
  29. http://www4.informatik.uni-erlangen.de/%7ekardel
  30. mailto:%20kardel(at)ntp(dot)org
  31. mailto:%20jones@hermes.chpc.utexas.edu
  32. mailto:%20dkatz@cisco.com
  33. mailto:%20leres@ee.lbl.gov
  34. mailto:%20lindholm@ucs.ubc.ca
  35. mailto:%20louie@ni.umd.edu
  36. mailto:%20thorinn@diku.dk
  37. mailto:%20mayer@ntp.org
  38. mailto:%20mills@udel.edu
  39. mailto:%20moeller@gwdgv1.dnet.gwdg.de
  40. mailto:%20mogul@pa.dec.com
  41. mailto:%20tmoore@fievel.daytonoh.ncr.com
  42. mailto:%20kamal@whence.com
  43. mailto:%20derek@toybox.demon.co.uk
  44. mailto:%20d@hd.org
  45. mailto:%20neal@ntp.org
  46. mailto:%20Rainer.Pruy@informatik.uni-erlangen.de
  47. mailto:%20dirce@zk3.dec.com
  48. mailto:%20wsanchez@apple.com
  49. mailto:%20mrapple@quack.kfu.com
  50. mailto:%20jack@innovativeinternet.com
  51. mailto:%20schnitz@unipress.com
  52. mailto:%20shields@tembel.org
  53. mailto:%20pebbles.jpl.nasa.gov
  54. mailto:%20harlan@pfcs.com
  55. mailto:%20ken@sdd.hp.com
  56. mailto:%20ajit@ee.udel.edu
  57. mailto:%20tsuruoka@nc.fukuoka-u.ac.jp
  58. mailto:%20vixie@vix.com
  59. mailto:%20Ulrich.Windl@rz.uni-regensburg.de
--------------------------------------------------------------------------
---
[openldap 2.4.45]
[COPYRIGHT]
```

```
  Copyright 1998-2017 The OpenLDAP Foundation
  All rights reserved.

[NOTE]
Redistribution and use in source and binary forms, with or without
modification, are permitted only as authorized by the OpenLDAP
Public License.

A copy of this license is available in the file LICENSE in the
top-level directory of the distribution or, alternatively, at
<http://www.OpenLDAP.org/license.html>.

OpenLDAP is a registered trademark of the OpenLDAP Foundation.

Individual files and/or contributed packages may be copyright by
other parties and/or subject to additional restrictions.

This work is derived from the University of Michigan LDAP v3.3
distribution.  Information concerning this software is available
at <http://www.umich.edu/~dirsvcs/ldap/ldap.html>.

This work also contains materials derived from public sources.

Additional information about OpenLDAP can be obtained at
<http://www.openldap.org/>.

---

Portions Copyright 1998-2012 Kurt D. Zeilenga.
Portions Copyright 1998-2006 Net Boolean Incorporated.
Portions Copyright 2001-2006 IBM Corporation.
All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted only as authorized by the OpenLDAP
Public License.

---

Portions Copyright 1999-2008 Howard Y.H. Chu.
Portions Copyright 1999-2008 Symas Corporation.
Portions Copyright 1998-2003 Hallvard B. Furuseth.
Portions Copyright 2007-2011 Gavin Henry.
Portions Copyright 2007-2011 Suretec Systems Ltd.
All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that this notice is preserved.
The names of the copyright holders may not be used to endorse or
promote products derived from this software without their specific
prior written permission.  This software is provided ``as is''
without express or implied warranty.

---

Portions Copyright (c) 1992-1996 Regents of the University of Michigan.
All rights reserved.

Redistribution and use in source and binary forms are permitted
provided that this notice is preserved and that due credit is given
to the University of Michigan at Ann Arbor.  The name of the
University may not be used to endorse or promote products derived
from this software without specific prior written permission.  This
software is provided ``as is'' without express or implied warranty.

[LICENSE]
The OpenLDAP Public License
  Version 2.8, 17 August 2003

Redistribution and use of this software and associated documentation
```

```
("Software"), with or without modification, are permitted provided
that the following conditions are met:

1. Redistributions in source form must retain copyright statements
   and notices,

2. Redistributions in binary form must reproduce applicable copyright
   statements and notices, this list of conditions, and the following
   disclaimer in the documentation and/or other materials provided
   with the distribution, and

3. Redistributions must contain a verbatim copy of this document.

The OpenLDAP Foundation may revise this license from time to time.
Each revision is distinguished by a version number.  You may use
this Software under terms of this license revision or under the
terms of any subsequent revision of the license.

THIS SOFTWARE IS PROVIDED BY THE OPENLDAP FOUNDATION AND ITS
CONTRIBUTORS ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES,
INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED.  IN NO EVENT
SHALL THE OPENLDAP FOUNDATION, ITS CONTRIBUTORS, OR THE AUTHOR(S)
OR OWNER(S) OF THE SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT,
INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING,
BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER
CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN
ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE
POSSIBILITY OF SUCH DAMAGE.

The names of the authors and copyright holders must not be used in
advertising or otherwise to promote the sale, use or other dealing
in this Software without specific, written prior permission.  Title
to copyright in this Software shall at all times remain with copyright
holders.

OpenLDAP is a registered trademark of the OpenLDAP Foundation.

Copyright 1999-2003 The OpenLDAP Foundation, Redwood City,
California, USA.  All Rights Reserved.  Permission to copy and
distribute verbatim copies of this document is granted.
--------------------------------------------------------------------------
---
[openpam 20071221]
[COPYRIGHT]
  Copyright (c) 2002-2003 Networks Associates Technology, Inc.
  Copyright (c) 2004-2007 Dag-Erling Sm テク rgrav
  All rights reserved.

[LICENSE]
This software was developed for the FreeBSD Project by ThinkSec AS and
Network Associates Laboratories, the Security Research Division of
Network Associates, Inc.  under DARPA/SPAWAR contract N66001-01-C-8035
("CBOSS"), as part of the DARPA CHATS research program.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:
1. Redistributions of source code must retain the above copyright
   notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright
   notice, this list of conditions and the following disclaimer in the
   documentation and/or other materials provided with the distribution.
3. The name of the author may not be used to endorse or promote
   products derived from this software without specific prior written
   permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS ``AS IS'' AND
```

```
ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
ARE DISCLAIMED.  IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
SUCH DAMAGE.

--------------------------------------------------------------------------
---
[openssh 5.3p1]
The licences which components of this software fall under are as
follows.  First, we will summarize and say that all components
are under a BSD licence, or a licence more free than that.

OpenSSH contains no GPL code.

1)
     * Copyright (c) 1995 Tatu Ylonen <ylo@cs.hut.fi>, Espoo, Finland
     *                    All rights reserved
     *
     * As far as I am concerned, the code I have written for this software
     * can be used freely for any purpose.  Any derived versions of this
     * software must be clearly marked as such, and if the derived work is
     * incompatible with the protocol description in the RFC file, it must be
     * called by a name other than "ssh" or "Secure Shell".

    [Tatu continues]
     *  However, I am not implying to give any licenses to any patents or
     * copyrights held by third parties, and the software includes parts that
     * are not under my direct control.  As far as I know, all included
     * source code is used in accordance with the relevant license agreements
     * and can be used freely for any purpose (the GNU license being the most
     * restrictive); see below for details.

    [However, none of that term is relevant at this point in time.  All of
    these restrictively licenced software components which he talks about
    have been removed from OpenSSH, i.e.,

     - RSA is no longer included, found in the OpenSSL library
     - IDEA is no longer included, its use is deprecated
     - DES is now external, in the OpenSSL library
     - GMP is no longer used, and instead we call BN code from OpenSSL
     - Zlib is now external, in a library
     - The make-ssh-known-hosts script is no longer included
     - TSS has been removed
     - MD5 is now external, in the OpenSSL library
     - RC4 support has been replaced with ARC4 support from OpenSSL
     - Blowfish is now external, in the OpenSSL library

    [The licence continues]

    Note that any information and cryptographic algorithms used in this
    software are publicly available on the Internet and at any major
    bookstore, scientific library, and patent office worldwide.  More
    information can be found e.g. at "http://www.cs.hut.fi/crypto".

    The legal status of this program is some combination of all these
    permissions and restrictions.  Use only at your own responsibility.
    You will be responsible for any legal consequences yourself; I am not
    making any claims whether possessing or using this is legal or not in
    your country, and I am not taking any responsibility on your behalf.


                                NO WARRANTY

    BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY
```

```
FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW.  EXCEPT WHEN
OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES
PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED
OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF
MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.  THE ENTIRE RISK AS
TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU.  SHOULD THE
PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING,
REPAIR OR CORRECTION.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING
WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR
REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES,
INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING
OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED
TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY
YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER
PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE
POSSIBILITY OF SUCH DAMAGES.
```

2)

```
The 32-bit CRC compensation attack detector in deattack.c was
contributed by CORE SDI S.A. under a BSD-style license.

 * Cryptographic attack detector for ssh - source code
 *
 * Copyright (c) 1998 CORE SDI S.A., Buenos Aires, Argentina.
 *
 * All rights reserved. Redistribution and use in source and binary
 * forms, with or without modification, are permitted provided that
 * this copyright notice is retained.
 *
 * THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESS OR IMPLIED
 * WARRANTIES ARE DISCLAIMED. IN NO EVENT SHALL CORE SDI S.A. BE
 * LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY OR
 * CONSEQUENTIAL DAMAGES RESULTING FROM THE USE OR MISUSE OF THIS
 * SOFTWARE.
 *
 * Ariel Futoransky <futo@core-sdi.com>
 * <http://www.core-sdi.com>
```

3)

```
ssh-keyscan was contributed by David Mazieres under a BSD-style
license.

 * Copyright 1995, 1996 by David Mazieres <dm@lcs.mit.edu>.
 *
 * Modification and redistribution in source and binary forms is
 * permitted provided that due credit is given to the author and the
 * OpenBSD project by leaving this copyright notice intact.
```

4)

```
The Rijndael implementation by Vincent Rijmen, Antoon Bosselaers
and Paulo Barreto is in the public domain and distributed
with the following license:

 * @version 3.0 (December 2000)
 *
 * Optimised ANSI C code for the Rijndael cipher (now AES)
 *
 * @author Vincent Rijmen <vincent.rijmen@esat.kuleuven.ac.be>
 * @author Antoon Bosselaers <antoon.bosselaers@esat.kuleuven.ac.be>
 * @author Paulo Barreto <paulo.barreto@terra.com.br>
 *
 * This code is hereby placed in the public domain.
 *
 * THIS SOFTWARE IS PROVIDED BY THE AUTHORS ''AS IS'' AND ANY EXPRESS
 * OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED
 * WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
 * ARE DISCLAIMED.  IN NO EVENT SHALL THE AUTHORS OR CONTRIBUTORS BE
 * LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
```

```
 * CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF
 * SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR
 * BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY,
 * WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE
 * OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE,
 * EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
```

5)

One component of the ssh source code is under a 3-clause BSD license, held by the University of California, since we pulled these parts from original Berkeley code.

```
 * Copyright (c) 1983, 1990, 1992, 1993, 1995
 *      The Regents of the University of California.  All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 * 1. Redistributions of source code must retain the above copyright
 *    notice, this list of conditions and the following disclaimer.
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in the
 *    documentation and/or other materials provided with the distribution.
 * 3. Neither the name of the University nor the names of its contributors
 *    may be used to endorse or promote products derived from this software
 *    without specific prior written permission.
 *
 * THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND
 * ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
 * ARE DISCLAIMED.  IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE
 * FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
 * DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
 * OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
 * LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
 * OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
 * SUCH DAMAGE.
```

6)

Remaining components of the software are provided under a standard 2-term BSD licence with the following names as copyright holders:

```
     Markus Friedl
     Theo de Raadt
     Niels Provos
     Dug Song
     Aaron Campbell
     Damien Miller
     Kevin Steves
     Daniel Kouril
     Wesley Griffin
     Per Allansson
     Nils Nordman
     Simon Wilkinson
```

Portable OpenSSH additionally includes code from the following copyright holders, also under the 2-term BSD license:

```
     Ben Lindstrom
     Tim Rice
     Andre Lucas
     Chris Adams
     Corinna Vinschen
     Cray Inc.
     Denis Parker
     Gert Doering
     Jakob Schlyter
     Jason Downs
     Juha Yrj □?      Michael Stone
```

```
    NetworksAssociates Technology, Inc.
    Solar Designer
    Todd C. Miller
    Wayne Schroeder
    William Jones
    Darren Tucker
    Sun Microsystems
    The SCO Group
    Daniel Walsh

 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 * 1. Redistributions of source code must retain the above copyright
 *    notice, this list of conditions and the following disclaimer.
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in the
 *    documentation and/or other materials provided with the distribution.
 *
 * THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS'' AND ANY EXPRESS OR
 * IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES
 * OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED.
 * IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT,
 * INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
 * NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE,
 * DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY
 * THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT
 * (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF
 * THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

8) Portable OpenSSH contains the following additional licenses:

    a) md5crypt.c, md5crypt.h

        * "THE BEER-WARE LICENSE" (Revision 42):
        * <phk@login.dknet.dk> wrote this file.  As long as you retain this
        * notice you can do whatever you want with this stuff. If we meet
        * some day, and you think this stuff is worth it, you can buy me a
        * beer in return.   Poul-Henning Kamp

    b) snprintf replacement

       * Copyright Patrick Powell 1995
       * This code is based on code written by Patrick Powell
       * (papowell@astart.com) It may be used for any purpose as long as this
       * notice remains intact on all source code distributions

    c) Compatibility code (openbsd-compat)

       Apart from the previously mentioned licenses, various pieces of code
       in the openbsd-compat/ subdirectory are licensed as follows:

       Some code is licensed under a 3-term BSD license, to the following
       copyright holders:

         Todd C. Miller
         Theo de Raadt
         Damien Miller
         Eric P. Allman
         The Regents of the University of California
         Constantin S. Svintsoff

         * Redistribution and use in source and binary forms, with or without
         * modification, are permitted provided that the following conditions
         * are met:
         * 1. Redistributions of source code must retain the above copyright
         *    notice, this list of conditions and the following disclaimer.
         * 2. Redistributions in binary form must reproduce the above copyright
         *   notice, this list of conditions and the following disclaimer in the
         *   documentation and/or other materials provided with the distribution.
```

```
         * 3. Neither the name of the University nor the names of its contributors
         *    may be used to endorse or promote products derived from this software
         *     without specific prior written permission.
         *
         * THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS''
AND
         * ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
         * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE
         * ARE DISCLAIMED.  IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE
         *  FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
CONSEQUENTIAL
         * DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
         * OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
         * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
STRICT
         * LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY
WAY
         * OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY
OF
         * SUCH DAMAGE.

       Some code is licensed under an ISC-style license, to the following
       copyright holders:

         Internet Software Consortium.
         Todd C. Miller
         Reyk Floeter
         Chad Mynhier

         * Permission to use, copy, modify, and distribute this software for any
         * purpose with or without fee is hereby granted, provided that the above
         * copyright notice and this permission notice appear in all copies.
         *
         * THE SOFTWARE IS PROVIDED "AS IS" AND TODD C. MILLER DISCLAIMS ALL
         *  WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED
WARRANTIES
         * OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL TODD C. MILLER BE
LIABLE
         * FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY
DAMAGES
         * WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN
ACTION
         * OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR
IN
         * CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

       Some code is licensed under a MIT-style license to the following
       copyright holders:

         Free Software Foundation, Inc.

         * Permission is hereby granted, free of charge, to any person obtaining
a  *
         * copy of this software and associated documentation files (the        *
         * "Software"), to deal in the Software without restriction, including
*
         * without limitation the rights to use, copy, modify, merge, publish,
*
         * distribute, distribute with modifications, sublicense, and/or sell
*
         * copies of the Software, and to permit persons to whom the Software is
*
         * furnished to do so, subject to the following conditions:            *
         *                                                                     *
         * The above copyright notice and this permission notice shall be included
*
         * in all copies or substantial portions of the Software.              *
         *                                                                     *
```

```
         * THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS
*
         * OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF           *
         * MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT.
*
         * IN NO EVENT SHALL THE ABOVE COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM,
*
         * DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR
*
         * OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR
*
         * THE USE OR OTHER DEALINGS IN THE SOFTWARE.                           *
         *                                                                      *
         * Except as contained in this notice, the name(s) of the above copyright
*
         * holders shall not be used in advertising or otherwise to promote the
*
         * sale, use or other dealings in this Software without prior written    *
         * authorization.                                                       *

*************************************************************************/

------------------------------------------------------------------------------
---
[openssl 1.0.2n]
  LICENSE ISSUES
  ==============

  The OpenSSL toolkit stays under a double license, i.e. both the conditions of
  the OpenSSL License and the original SSLeay license apply to the toolkit.
  See below for the actual license texts. Actually both licenses are BSD-style
  Open Source licenses. In case of any license issues related to OpenSSL
  please contact openssl-core@openssl.org.

  OpenSSL License
  ---------------

/* ====================================================================
 * Copyright (c) 1998-2017 The OpenSSL Project.  All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 *
 * 1. Redistributions of source code must retain the above copyright
 *    notice, this list of conditions and the following disclaimer.
 *
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in
 *    the documentation and/or other materials provided with the
 *    distribution.
 *
 * 3. All advertising materials mentioning features or use of this
 *    software must display the following acknowledgment:
 *    "This product includes software developed by the OpenSSL Project
 *    for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
 *
 * 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
 *    endorse or promote products derived from this software without
 *    prior written permission. For written permission, please contact
 *    openssl-core@openssl.org.
 *
 * 5. Products derived from this software may not be called "OpenSSL"
 *    nor may "OpenSSL" appear in their names without prior written
 *    permission of the OpenSSL Project.
 *
 * 6. Redistributions of any form whatsoever must retain the following
 *    acknowledgment:
 *    "This product includes software developed by the OpenSSL Project
 *    for use in the OpenSSL Toolkit (http://www.openssl.org/)"
```

```
 *
 * THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
 * EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
 * PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE OpenSSL PROJECT OR
 * ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
 * SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
 * NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
 * LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
 * STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
 * ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
 * OF THE POSSIBILITY OF SUCH DAMAGE.
 * ====================================================================
 *
 * This product includes cryptographic software written by Eric Young
 * (eay@cryptsoft.com).  This product includes software written by Tim
 * Hudson (tjh@cryptsoft.com).
 *
 */

 Original SSLeay License
 -----------------------

/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
 * All rights reserved.
 *
 * This package is an SSL implementation written
 * by Eric Young (eay@cryptsoft.com).
 * The implementation was written so as to conform with Netscapes SSL.
 *
 * This library is free for commercial and non-commercial use as long as
 * the following conditions are aheared to.  The following conditions
 * apply to all code found in this distribution, be it the RC4, RSA,
 * lhash, DES, etc., code; not just the SSL code.  The SSL documentation
 * included with this distribution is covered by the same copyright terms
 * except that the holder is Tim Hudson (tjh@cryptsoft.com).
 *
 * Copyright remains Eric Young's, and as such any Copyright notices in
 * the code are not to be removed.
 * If this package is used in a product, Eric Young should be given attribution
 * as the author of the parts of the library used.
 * This can be in the form of a textual message at program startup or
 * in documentation (online or textual) provided with the package.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 * 1. Redistributions of source code must retain the copyright
 *    notice, this list of conditions and the following disclaimer.
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in the
 *    documentation and/or other materials provided with the distribution.
 * 3. All advertising materials mentioning features or use of this software
 *    must display the following acknowledgement:
 *    "This product includes cryptographic software written by
 *     Eric Young (eay@cryptsoft.com)"
 *    The word 'cryptographic' can be left out if the rouines from the library
 *    being used are not cryptographic related :-).
 * 4. If you include any Windows specific code (or a derivative thereof) from
 *   the apps directory (application code) you must include an acknowledgement:
 *   "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"
 *
 * THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND
 * ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
 * ARE DISCLAIMED.  IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
 * FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
 * DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
 * OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
```

```
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
 * LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
 * OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
 * SUCH DAMAGE.
 *
 * The licence and distribution terms for any publically available version or
 * derivative of this code cannot be changed.  i.e. this code cannot simply be
 * copied and put under another distribution licence
 * [including the GNU Public Licence.]
 */

------------------------------------------------------------------------------
---
[ovsdb 2.1.0 (part of openvswitch 2.1.0)]
[COPYRIGHT]
  Copyright (c) 2009, 2010, 2011, 2012, 2013 Nicira, Inc.

[LICENSE]
                                 Apache License
                           Version 2.0, January 2004
                        http://www.apache.org/licenses/

   TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

   1. Definitions.

      "License" shall mean the terms and conditions for use, reproduction,
      and distribution as defined by Sections 1 through 9 of this document.

      "Licensor" shall mean the copyright owner or entity authorized by
      the copyright owner that is granting the License.

      "Legal Entity" shall mean the union of the acting entity and all
      other entities that control, are controlled by, or are under common
      control with that entity. For the purposes of this definition,
      "control" means (i) the power, direct or indirect, to cause the
      direction or management of such entity, whether by contract or
      otherwise, or (ii) ownership of fifty percent (50%) or more of the
      outstanding shares, or (iii) beneficial ownership of such entity.

      "You" (or "Your") shall mean an individual or Legal Entity
      exercising permissions granted by this License.

      "Source" form shall mean the preferred form for making modifications,
      including but not limited to software source code, documentation
      source, and configuration files.

      "Object" form shall mean any form resulting from mechanical
      transformation or translation of a Source form, including but
      not limited to compiled object code, generated documentation,
      and conversions to other media types.

      "Work" shall mean the work of authorship, whether in Source or
      Object form, made available under the License, as indicated by a
      copyright notice that is included in or attached to the work
      (an example is provided in the Appendix below).

      "Derivative Works" shall mean any work, whether in Source or Object
      form, that is based on (or derived from) the Work and for which the
      editorial revisions, annotations, elaborations, or other modifications
      represent, as a whole, an original work of authorship. For the purposes
      of this License, Derivative Works shall not include works that remain
      separable from, or merely link (or bind by name) to the interfaces of,
      the Work and Derivative Works thereof.

      "Contribution" shall mean any work of authorship, including
      the original version of the Work and any modifications or additions
      to that Work or Derivative Works thereof, that is intentionally
      submitted to Licensor for inclusion in the Work by the copyright owner
      or by an individual or Legal Entity authorized to submit on behalf of
```

the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

   (a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

   (b) You must cause any modified files to carry prominent notices stating that You changed the files; and

   (c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

   (d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and
may provide additional or different license terms and conditions
for use, reproduction, or distribution of Your modifications, or
for any such Derivative Works as a whole, provided Your use,
reproduction, and distribution of the Work otherwise complies with
the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise,
any Contribution intentionally submitted for inclusion in the Work
by You to the Licensor shall be under the terms and conditions of
this License, without any additional terms or conditions.
Notwithstanding the above, nothing herein shall supersede or modify
the terms of any separate license agreement you may have executed
with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade
names, trademarks, service marks, or product names of the Licensor,
except as required for reasonable and customary use in describing the
origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or
agreed to in writing, Licensor provides the Work (and each
Contributor provides its Contributions) on an "AS IS" BASIS,
WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or
implied, including, without limitation, any warranties or conditions
of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A
PARTICULAR PURPOSE. You are solely responsible for determining the
appropriateness of using or redistributing the Work and assume any
risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory,
whether in tort (including negligence), contract, or otherwise,
unless required by applicable law (such as deliberate and grossly
negligent acts) or agreed to in writing, shall any Contributor be
liable to You for damages, including any direct, indirect, special,
incidental, or consequential damages of any character arising as a
result of this License or out of the use or inability to use the
Work (including but not limited to damages for loss of goodwill,
work stoppage, computer failure or malfunction, or any and all
other commercial damages or losses), even if such Contributor
has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing
the Work or Derivative Works thereof, You may choose to offer,
and charge a fee for, acceptance of support, warranty, indemnity,
or other liability obligations and/or rights consistent with this
License. However, in accepting such obligations, You may act only
on Your own behalf and on Your sole responsibility, not on behalf
of any other Contributor, and only if You agree to indemnify,
defend, and hold each Contributor harmless for any liability
incurred by, or claims asserted against, such Contributor by reason
of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

[ping 8.0.0 (part of FreeBSD 8.0.0)]
[COPYRIGHT]
Copyright (c) 1992-2009 The FreeBSD Project. All rights reserved.

[LICENSE]
Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:
1. Redistributions of source code must retain the above copyright
notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright
notice, this list of conditions and the following disclaimer in the
documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS ``AS IS'' AND
ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
SUCH DAMAGE.

The 4.4BSD and 4.4BSD-Lite software is distributed under the following
terms:

All of the documentation and software included in the 4.4BSD and 4.4BSD-Lite
Releases is copyrighted by The Regents of the University of California.

Copyright 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:
1. Redistributions of source code must retain the above copyright
   notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright
   notice, this list of conditions and the following disclaimer in the
   documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software
   must display the following acknowledgement:
This product includes software developed by the University of
California, Berkeley and its contributors.
4. Neither the name of the University nor the names of its contributors
   may be used to endorse or promote products derived from this software
   without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND
ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE
FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
SUCH DAMAGE.

The Institute of Electrical and Electronics Engineers and the American
National Standards Committee X3, on Information Processing Systems have
given us permission to reprint portions of their documentation.

In the following statement, the phrase ``this text'' refers to portions
of the system documentation.

Portions of this text are reprinted and reproduced in electronic form in
the second BSD Networking Software Release, from IEEE Std 1003.1-1988, IEEE
Standard Portable Operating System Interface for Computer Environments
(POSIX), copyright C 1988 by the Institute of Electrical and Electronics
Engineers, Inc. In the event of any discrepancy between these versions
and the original IEEE Standard, the original IEEE Standard is the referee
document.

In the following statement, the phrase ``This material'' refers to portions
of the system documentation.

This material is reproduced with permission from American National
Standards Committee X3, on Information Processing Systems. Computer and
Business Equipment Manufacturers Association (CBEMA), 311 First St., NW,

```
Suite 500, Washington, DC 20001-2178.  The developmental work of
Programming Language C was completed by the X3J11 Technical Committee.

The views and conclusions contained in the software and documentation are
those of the authors and should not be interpreted as representing official
policies, either expressed or implied, of the Regents of the University
of California.


NOTE: The copyright of UC Berkeley's Berkeley Software Distribution ("BSD")
source has been updated.  The copyright addendum may be found at
ftp://ftp.cs.berkeley.edu/pub/4bsd/README.Impt.License.Change and is
included below.

July 22, 1999

To All Licensees, Distributors of Any Version of BSD:

As you know, certain of the Berkeley Software Distribution ("BSD") source
code files require that further distributions of products containing all or
portions of the software, acknowledge within their advertising materials
that such products contain software developed by UC Berkeley and its
contributors.

Specifically, the provision reads:

"     * 3. All advertising materials mentioning features or use of this software
       *    must display the following acknowledgement:
       *    This product includes software developed by the University of
       *    California, Berkeley and its contributors."

Effective immediately, licensees and distributors are no longer required to
include the acknowledgement within advertising materials.  Accordingly, the
foregoing paragraph of those BSD Unix files containing it is hereby deleted
in its entirety.

William Hoskins
Director, Office of Technology Licensing
University of California, Berkeley
------------------------------------------------------------------------------
---
[ping6 8.0.0 (part of FreeBSD 8.0.0)]
[COPYRIGHT]
  Copyright (c) 1992-2009 The FreeBSD Project. All rights reserved.

[LICENSE]
Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:
1. Redistributions of source code must retain the above copyright
   notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright
   notice, this list of conditions and the following disclaimer in the
   documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS ``AS IS'' AND
ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
ARE DISCLAIMED.  IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
SUCH DAMAGE.

The 4.4BSD and 4.4BSD-Lite software is distributed under the following
terms:
```

All of the documentation and software included in the 4.4BSD and 4.4BSD-Lite Releases is copyrighted by The Regents of the University of California.

Copyright 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:
This product includes software developed by the University of California, Berkeley and its contributors.
4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The Institute of Electrical and Electronics Engineers and the American National Standards Committee X3, on Information Processing Systems have given us permission to reprint portions of their documentation.

In the following statement, the phrase ``this text'' refers to portions of the system documentation.

Portions of this text are reprinted and reproduced in electronic form in the second BSD Networking Software Release, from IEEE Std 1003.1-1988, IEEE Standard Portable Operating System Interface for Computer Environments (POSIX), copyright C 1988 by the Institute of Electrical and Electronics Engineers, Inc. In the event of any discrepancy between these versions and the original IEEE Standard, the original IEEE Standard is the referee document.

In the following statement, the phrase ``This material'' refers to portions of the system documentation.

This material is reproduced with permission from American National Standards Committee X3, on Information Processing Systems. Computer and Business Equipment Manufacturers Association (CBEMA), 311 First St., NW, Suite 500, Washington, DC 20001-2178. The developmental work of Programming Language C was completed by the X3J11 Technical Committee.

The views and conclusions contained in the software and documentation are those of the authors and should not be interpreted as representing official policies, either expressed or implied, of the Regents of the University of California.

NOTE: The copyright of UC Berkeley's Berkeley Software Distribution ("BSD") source has been updated. The copyright addendum may be found at ftp://ftp.cs.berkeley.edu/pub/4bsd/README.Impt.License.Change and is included below.

July 22, 1999

To All Licensees, Distributors of Any Version of BSD:

As you know, certain of the Berkeley Software Distribution ("BSD") source code files require that further distributions of products containing all or portions of the software, acknowledge within their advertising materials that such products contain software developed by UC Berkeley and its contributors.

Specifically, the provision reads:

```
"    * 3. All advertising materials mentioning features or use of this software
      *    must display the following acknowledgement:
      *    This product includes software developed by the University of
      *    California, Berkeley and its contributors."
```

Effective immediately, licensees and distributors are no longer required to include the acknowledgement within advertising materials. Accordingly, the foregoing paragraph of those BSD Unix files containing it is hereby deleted in its entirety.

William Hoskins
Director, Office of Technology Licensing
University of California, Berkeley

[pthread 0.9.32 (part of uclibc 0.9.32)]
[LICENSE]

GNU LESSER GENERAL PUBLIC LICENSE
Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.
51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source

code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The

former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or

table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the

library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF

SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the library's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA

Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the library, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the library `Frob' (a library for tweaking knobs) written by James Random Hacker.

<signature of Ty Coon>, 1 April 1990
Ty Coon, President of Vice

That's all there is to it!

[pure-ftpd 1.0.29]
[COPYRIGHT]
Copyright (c) 2001 - 2010
Frank Denis <j at pureftpd dot org> with help of contributors.

[LICENSE]
Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND THE AUTHOR DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

```
--------------------------------------------------------------------------
---
[python 2.7.18]
[COPYRIGHT]
  Copyright (c) 2001, 2002, 2003, 2004, 2005, 2006, 2007, 2008, 2009, 2010, 2011,
  2012, 2013, 2014, 2015, 2016, 2017, 2018, 2019, 2020 Python Software Foundation.
All
  rights reserved.

  Copyright (c) 2000 BeOpen.com.
  All rights reserved.

  Copyright (c) 1995-2001 Corporation for National Research Initiatives.
  All rights reserved.

  Copyright (c) 1991-1995 Stichting Mathematisch Centrum.
  All rights reserved.

[LICENSE]
PYTHON SOFTWARE FOUNDATION LICENSE VERSION 2
--------------------------------------------

1. This LICENSE AGREEMENT is between the Python Software Foundation
("PSF"), and the Individual or Organization ("Licensee") accessing and
otherwise using this software ("Python") in source or binary form and
its associated documentation.

2. Subject to the terms and conditions of this License Agreement, PSF hereby
grants Licensee a nonexclusive, royalty-free, world-wide license to reproduce,
analyze, test, perform and/or display publicly, prepare derivative works,
distribute, and otherwise use Python alone or in any derivative version,
provided, however, that PSF's License Agreement and PSF's notice of copyright,
i.e., "Copyright (c) 2001, 2002, 2003, 2004, 2005, 2006, 2007, 2008, 2009, 2010,
2011, 2012, 2013, 2014, 2015, 2016, 2017, 2018, 2019, 2020 Python Software
Foundation;
All Rights Reserved" are retained in Python alone or in any derivative version
prepared by Licensee.

3. In the event Licensee prepares a derivative work that is based on
or incorporates Python or any part thereof, and wants to make
the derivative work available to others as provided herein, then
Licensee hereby agrees to include in any such work a brief summary of
the changes made to Python.

4. PSF is making Python available to Licensee on an "AS IS"
basis.  PSF MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR
IMPLIED.  BY WAY OF EXAMPLE, BUT NOT LIMITATION, PSF MAKES NO AND
DISCLAIMS ANY REPRESENTATION OR WARRANTY OF MERCHANTABILITY OR FITNESS
FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF PYTHON WILL NOT
INFRINGE ANY THIRD PARTY RIGHTS.

5. PSF SHALL NOT BE LIABLE TO LICENSEE OR ANY OTHER USERS OF PYTHON
FOR ANY INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES OR LOSS AS
A RESULT OF MODIFYING, DISTRIBUTING, OR OTHERWISE USING PYTHON,
OR ANY DERIVATIVE THEREOF, EVEN IF ADVISED OF THE POSSIBILITY THEREOF.

6. This License Agreement will automatically terminate upon a material
breach of its terms and conditions.

7. Nothing in this License Agreement shall be deemed to create any
relationship of agency, partnership, or joint venture between PSF and
Licensee.  This License Agreement does not grant permission to use PSF
trademarks or trade name in a trademark sense to endorse or promote
products or services of Licensee, or any third party.

8. By copying, installing or otherwise using Python, Licensee
agrees to be bound by the terms and conditions of this License
Agreement.
```

BEOPEN.COM LICENSE AGREEMENT FOR PYTHON 2.0

BEOPEN PYTHON OPEN SOURCE LICENSE AGREEMENT VERSION 1

1. This LICENSE AGREEMENT is between BeOpen.com ("BeOpen"), having an office at 160 Saratoga Avenue, Santa Clara, CA 95051, and the Individual or Organization ("Licensee") accessing and otherwise using this software in source or binary form and its associated documentation ("the Software").

2. Subject to the terms and conditions of this BeOpen Python License Agreement, BeOpen hereby grants Licensee a non-exclusive, royalty-free, world-wide license to reproduce, analyze, test, perform and/or display publicly, prepare derivative works, distribute, and otherwise use the Software alone or in any derivative version, provided, however, that the BeOpen Python License is retained in the Software, alone or in any derivative version prepared by Licensee.

3. BeOpen is making the Software available to Licensee on an "AS IS" basis. BEOPEN MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED. BY WAY OF EXAMPLE, BUT NOT LIMITATION, BEOPEN MAKES NO AND DISCLAIMS ANY REPRESENTATION OR WARRANTY OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF THE SOFTWARE WILL NOT INFRINGE ANY THIRD PARTY RIGHTS.

4. BEOPEN SHALL NOT BE LIABLE TO LICENSEE OR ANY OTHER USERS OF THE SOFTWARE FOR ANY INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES OR LOSS AS A RESULT OF USING, MODIFYING OR DISTRIBUTING THE SOFTWARE, OR ANY DERIVATIVE THEREOF, EVEN IF ADVISED OF THE POSSIBILITY THEREOF.

5. This License Agreement will automatically terminate upon a material breach of its terms and conditions.

6. This License Agreement shall be governed by and interpreted in all respects by the law of the State of California, excluding conflict of law provisions. Nothing in this License Agreement shall be deemed to create any relationship of agency, partnership, or joint venture between BeOpen and Licensee. This License Agreement does not grant permission to use BeOpen trademarks or trade names in a trademark sense to endorse or promote products or services of Licensee, or any third party. As an exception, the "BeOpen Python" logos available at http://www.pythonlabs.com/logos.html may be used according to the permissions granted on that web page.

7. By copying, installing or otherwise using the software, Licensee agrees to be bound by the terms and conditions of this License Agreement.

CNRI LICENSE AGREEMENT FOR PYTHON 1.6.1
---

1. This LICENSE AGREEMENT is between the Corporation for National Research Initiatives, having an office at 1895 Preston White Drive, Reston, VA 20191 ("CNRI"), and the Individual or Organization ("Licensee") accessing and otherwise using Python 1.6.1 software in source or binary form and its associated documentation.

2. Subject to the terms and conditions of this License Agreement, CNRI hereby grants Licensee a nonexclusive, royalty-free, world-wide license to reproduce, analyze, test, perform and/or display publicly, prepare derivative works, distribute, and otherwise use Python 1.6.1 alone or in any derivative version, provided, however, that CNRI's License Agreement and CNRI's notice of copyright, i.e., "Copyright (c) 1995-2001 Corporation for National Research Initiatives; All Rights Reserved" are retained in Python 1.6.1 alone or in any derivative version prepared by Licensee. Alternately, in lieu of CNRI's License Agreement, Licensee may substitute the following text (omitting the

quotes): "Python 1.6.1 is made available subject to the terms and conditions in CNRI's License Agreement. This Agreement together with Python 1.6.1 may be located on the Internet using the following unique, persistent identifier (known as a handle): 1895.22/1013. This Agreement may also be obtained from a proxy server on the Internet using the following URL: http://hdl.handle.net/1895.22/1013".

3. In the event Licensee prepares a derivative work that is based on or incorporates Python 1.6.1 or any part thereof, and wants to make the derivative work available to others as provided herein, then Licensee hereby agrees to include in any such work a brief summary of the changes made to Python 1.6.1.

4. CNRI is making Python 1.6.1 available to Licensee on an "AS IS" basis. CNRI MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED. BY WAY OF EXAMPLE, BUT NOT LIMITATION, CNRI MAKES NO AND DISCLAIMS ANY REPRESENTATION OR WARRANTY OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF PYTHON 1.6.1 WILL NOT INFRINGE ANY THIRD PARTY RIGHTS.

5. CNRI SHALL NOT BE LIABLE TO LICENSEE OR ANY OTHER USERS OF PYTHON 1.6.1 FOR ANY INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES OR LOSS AS A RESULT OF MODIFYING, DISTRIBUTING, OR OTHERWISE USING PYTHON 1.6.1, OR ANY DERIVATIVE THEREOF, EVEN IF ADVISED OF THE POSSIBILITY THEREOF.

6. This License Agreement will automatically terminate upon a material breach of its terms and conditions.

7. This License Agreement shall be governed by the federal intellectual property law of the United States, including without limitation the federal copyright law, and, to the extent such U.S. federal law does not apply, by the law of the Commonwealth of Virginia, excluding Virginia's conflict of law provisions. Notwithstanding the foregoing, with regard to derivative works based on Python 1.6.1 that incorporate non-separable material that was previously distributed under the GNU General Public License (GPL), the law of the Commonwealth of Virginia shall govern this License Agreement only as to issues arising under or with respect to Paragraphs 4, 5, and 7 of this License Agreement. Nothing in this License Agreement shall be deemed to create any relationship of agency, partnership, or joint venture between CNRI and Licensee. This License Agreement does not grant permission to use CNRI trademarks or trade name in a trademark sense to endorse or promote products or services of Licensee, or any third party.

8. By clicking on the "ACCEPT" button where indicated, or by copying, installing or otherwise using Python 1.6.1, Licensee agrees to be bound by the terms and conditions of this License Agreement.

ACCEPT

CWI LICENSE AGREEMENT FOR PYTHON 0.9.0 THROUGH 1.2

Copyright (c) 1991 - 1995, Stichting Mathematisch Centrum Amsterdam, The Netherlands. All rights reserved.

Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of Stichting Mathematisch Centrum or CWI not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission.

STICHTING MATHEMATISCH CENTRUM DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL STICHTING MATHEMATISCH CENTRUM BE LIABLE

```
FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES
WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN
ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT
OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.
------------------------------------------------------------------------------
---
[respond 1.3.1]
[COPYRIGHT]
  copyright (c) 2012: Scott Jehl, Paul Irish, Nicholas Zakas.

[LICENSE]
  Dual MIT/BSD license


------------------------------------------------------------------------------
---
[result.h 1.73]
[COPYRIGHT]
  Copyright (C) 2004-2009, 2012, 2014  Internet Systems Consortium, Inc. ("ISC")
  Copyright (C) 1998-2001, 2003  Internet Software Consortium.

[LICENSE]
  Permission to use, copy, modify, and/or distribute this software for any
  purpose with or without fee is hereby granted, provided that the above
  copyright notice and this permission notice appear in all copies.

  THE SOFTWARE IS PROVIDED "AS IS" AND ISC DISCLAIMS ALL WARRANTIES WITH
  REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
  AND FITNESS.  IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT,
  INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
  LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
  OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
  PERFORMANCE OF THIS SOFTWARE.

------------------------------------------------------------------------------
---
[rpcapd 4.1.2 (part of winpcap 4.1.2)]
[COPYRIGHT]
  Copyright (c) 1999 - 2005 NetGroup, Politecnico di Torino (Italy).
  Copyright (c) 2005 - 2010 CACE Technologies, Davis (California).
  All rights reserved.

[LICENSE]
Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:

1. Redistributions of source code must retain the above copyright
   notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright
   notice, this list of conditions and the following disclaimer in the
   documentation and/or other materials provided with the distribution.
3. Neither the name of the Politecnico di Torino, CACE Technologies nor
   the names of its contributors may be used to endorse or promote products
   derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS"
AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE
FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
SUCH DAMAGE.

This product includes software developed by the University of California,
Lawrence Berkeley Laboratory and its contributors.
```

[COPYRIGHT]
Portions Copyright (c) 1990, 1991, 1992, 1993, 1994, 1995, 1996, 1997
The Regents of the University of California. All rights reserved.

[LICENSE]
Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:
1. Redistributions of source code must retain the above copyright
   notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright
   notice, this list of conditions and the following disclaimer in the
   documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software
   must display the following acknowledgement: "This product includes software
   developed by the University of California, Berkeley and its contributors."
4. Neither the name of the University nor the names of its contributors
   may be used to endorse or promote products derived from this software without
   specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE INSTITUTE AND CONTRIBUTORS ``AS IS'' AND
ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE
FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
SUCH DAMAGE.

[COPYRIGHT]
Portions Copyright (c) 1983 Regents of the University of California.
All rights reserved.

[LICENSE]
Redistribution and use in source and binary forms are permitted provided that
the above copyright notice and this paragraph are duplicated in all such forms
and that any documentation, advertising materials, and other materials related
to such distribution and use acknowledge that the software was developed by the
University of California, Berkeley. The name of the University may not be used
to endorse or promote products derived from this software without specific prior
written permission.

THIS SOFTWARE IS PROVIDED ``AS IS'' AND WITHOUT ANY EXPRESS OR IMPLIED
WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF
MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE.

[ruby 2.0.0]
[COPYRIGHT]
  Copyright (C) 1993-2013 Yukihiro Matsumoto. All rights reserved.

[LICENSE]
Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:
1. Redistributions of source code must retain the above copyright
notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright
notice, this list of conditions and the following disclaimer in the
documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS ``AS IS'' AND
ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE

```
FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
SUCH DAMAGE.
--------------------------------------------------------------------------
---
[slickgrid 2.1]
[COPYRIGHT]
  Copyright (c) 2010 Michael Leibman, http://github.com/mleibman/slickgrid

[LICENSE]
Permission is hereby granted, free of charge, to any person obtaining
a copy of this software and associated documentation files (the
"Software"), to deal in the Software without restriction, including
without limitation the rights to use, copy, modify, merge, publish,
distribute, sublicense, and/or sell copies of the Software, and to
permit persons to whom the Software is furnished to do so, subject to
the following conditions:

The above copyright notice and this permission notice shall be
included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND,
EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF
MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND
NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE
LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION
OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION
WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.
--------------------------------------------------------------------------
---
[sqlite3 3.35.5]
** 2006 June 7
**
** The author disclaims copyright to this source code.  In place of
** a legal notice, here is a blessing:
**
**    May you do good and not evil.
**    May you find forgiveness for yourself and forgive others.
**    May you share freely, never taking more than you give.
**
*************************************************************************
------------------------------------------------------------------------------
---
[tcl-snmptools 1.0]
[COPYRIGHT]
  Copyright (C) 2008  Alexandros Stergiakis

[LICENSE]
                    GNU GENERAL PUBLIC LICENSE
                       Version 3, 29 June 2007

 Copyright (C) 2007 Free Software Foundation, Inc. <http://fsf.org/>
 Everyone is permitted to copy and distribute verbatim copies
 of this license document, but changing it is not allowed.

                            Preamble

  The GNU General Public License is a free, copyleft license for
software and other kinds of works.

  The licenses for most software and other practical works are designed
to take away your freedom to share and change the works.  By contrast,
the GNU General Public License is intended to guarantee your freedom to
share and change all versions of a program--to make sure it remains free
software for all its users.  We, the Free Software Foundation, use the
GNU General Public License for most of our software; it applies also to
```

any other work released this way by its authors. You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for them if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you these rights or asking you to surrender the rights. Therefore, you have certain responsibilities if you distribute copies of the software, or if you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must pass on to the recipients the same freedoms that you received. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

Developers that use the GNU GPL protect your rights with two steps: (1) assert copyright on the software, and (2) offer you this License giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains that there is no warranty for this free software. For both users' and authors' sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.

Some devices are designed to deny users access to install or run modified versions of the software inside them, although the manufacturer can do so. This is fundamentally incompatible with the aim of protecting users' freedom to change the software. The systematic pattern of such abuse occurs in the area of products for individuals to use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains, we stand ready to extend this provision to those domains in future versions of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents. States should not allow patents to restrict development and use of software on general-purpose computers, but in those that do, we wish to avoid the special danger that patents applied to a free program could make it effectively proprietary. To prevent this, the GPL assures that patents cannot be used to render the program non-free.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS

0. Definitions.

"This License" refers to version 3 of the GNU General Public License.

"Copyright" also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

"The Program" refers to any copyrightable work licensed under this License. Each licensee is addressed as "you". "Licensees" and "recipients" may be individuals or organizations.

To "modify" a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a "modified version" of the earlier work or a work "based on" the earlier work.

A "covered work" means either the unmodified Program or a work based on the Program.

To "propagate" a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well.

To "convey" a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays "Appropriate Legal Notices" to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

1. Source Code.

The "source code" for a work means the preferred form of the work for making modifications to it. "Object code" means any non-source form of a work.

A "Standard Interface" means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The "System Libraries" of an executable work include anything, other than the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A "Major Component", in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The "Corresponding Source" for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work's System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

2. Basic Permissions.

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited

permission to run the unmodified Program. The output from running a covered work is covered by this License only if the output, given its content, constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed; section 10 makes it unnecessary.

3. Protecting Users' Legal Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of technological measures.

4. Conveying Verbatim Copies.

You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice; keep intact all notices stating that this License and any non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

5. Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

a) The work must carry prominent notices stating that you modified it, and giving a relevant date.

b) The work must carry prominent notices stating that it is released under this License and any conditions added under section 7. This requirement modifies the requirement in section 4 to "keep intact all notices".

c) You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it.

d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.

A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution medium, is called an "aggregate" if the compilation and its resulting copyright are not used to limit the access or legal rights of the compilation's users beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate.

6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, in one of these ways:

a) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange.

b) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as long as you offer spare parts or customer support for that product model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical medium customarily used for software interchange, for a price no more than your reasonable cost of physically performing this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge.

c) Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source. This alternative is allowed only occasionally and noncommercially, and only if you received the object code with such an offer, in accord with subsection 6b.

d) Convey the object code by offering access from a designated place (gratis or for a charge), and offer equivalent access to the Corresponding Source in the same way through the same place at no further charge. You need not require recipients to copy the Corresponding Source along with the object code. If the place to copy the object code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.

e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.

A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object code work.

A "User Product" is either (1) a "consumer product", which means any tangible personal property which is normally used for personal, family,

or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, "normally used" refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

"Installation Information" for a User Product means any methods, procedures, authorization keys, or other information required to install and execute modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in ROM).

The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

7. Additional Terms.

"Additional permissions" are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

a) Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or

b) Requiring preservation of specified reasonable legal notices or

author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or

c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or

d) Limiting the use for publicity purposes of names of licensors or authors of the material; or

e) Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or

f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on those licensors and authors.

All other non-permissive additional terms are considered "further restrictions" within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions; the above requirements apply either way.

8. Termination.

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work

occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

10. Automatic Licensing of Downstream Recipients.

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An "entity transaction" is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

11. Patents.

A "contributor" is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's "contributor version".

A contributor's "essential patent claims" are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For purposes of this definition, "control" includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a "patent license" is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To "grant" such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. "Knowingly relying" means you have actual knowledge that, but for the patent license, your conveying the

covered work in a country, or your recipient's use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is "discriminatory" if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement, or that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.

12. No Surrender of Others' Freedom.

If conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot convey a covered work so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

13. Use with the GNU Affero General Public License.

Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed under version 3 of the GNU Affero General Public License into a single combined work, and to convey the resulting work. The terms of this License will continue to apply to the part which is the covered work, but the special requirements of the GNU Affero General Public License, section 13, concerning interaction through a network will apply to the combination as such.

14. Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of the GNU General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU General Public License, you may choose any version ever published by the Free Software Foundation.

If the Program specifies that a proxy can decide which future versions of the GNU General Public License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Program.

Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.

15. Disclaimer of Warranty.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

17. Interpretation of Sections 15 and 16.

If the disclaimer of warranty and limitation of liability provided above cannot be given local legal effect according to their terms, reviewing courts shall apply local law that most closely approximates an absolute waiver of all civil liability in connection with the Program, unless a warranty or assumption of liability accompanies a copy of the Program in return for a fee.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively state the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This program is free software: you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation, either version 3 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program. If not, see <http://www.gnu.org/licenses/>.

```
Also add information on how to contact you by electronic and paper mail.

  If the program does terminal interaction, make it output a short
notice like this when it starts in an interactive mode:

    <program>  Copyright (C) <year>  <name of author>
    This program comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
    This is free software, and you are welcome to redistribute it
    under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate
parts of the General Public License.  Of course, your program's commands
might be different; for a GUI interface, you would use an "about box".

  You should also get your employer (if you work as a programmer) or school,
if any, to sign a "copyright disclaimer" for the program, if necessary.
For more information on this, and how to apply and follow the GNU GPL, see
<http://www.gnu.org/licenses/>.

  The GNU General Public License does not permit incorporating your program
into proprietary programs.  If your program is a subroutine library, you
may consider it more useful to permit linking proprietary applications with
the library.  If this is what you want to do, use the GNU Lesser General
Public License instead of this License.  But first, please read
<http://www.gnu.org/philosophy/why-not-lgpl.html>.

--------------------------------------------------------------------------------
---
[tcltk 8.5.8]
[COPYRIGHT]
  Copyright (c) 1987-1994 The Regents of the University of California.
  Copyright (c) 1993-1996 Lucent Technologies.
  Copyright (c) 1994-1998 Sun Microsystems, Inc.
  Copyright (c) 1998-2000 by Scriptics Corporation.
  Copyright (c) 2002 by Kevin B. Kenny.  All rights reserved.

[LICENSE]
This software is copyrighted by the Regents of the University of
California, Sun Microsystems, Inc., Scriptics Corporation, ActiveState
Corporation and other parties.  The following terms apply to all files
associated with the software unless explicitly disclaimed in
individual files.

The authors hereby grant permission to use, copy, modify, distribute,
and license this software and its documentation for any purpose, provided
that existing copyright notices are retained in all copies and that this
notice is included verbatim in any distributions. No written agreement,
license, or royalty fee is required for any of the authorized uses.
Modifications to this software may be copyrighted by their authors
and need not follow the licensing terms described here, provided that
the new terms are clearly indicated on the first page of each file where
they apply.

IN NO EVENT SHALL THE AUTHORS OR DISTRIBUTORS BE LIABLE TO ANY PARTY
FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES
ARISING OUT OF THE USE OF THIS SOFTWARE, ITS DOCUMENTATION, OR ANY
DERIVATIVES THEREOF, EVEN IF THE AUTHORS HAVE BEEN ADVISED OF THE
POSSIBILITY OF SUCH DAMAGE.

THE AUTHORS AND DISTRIBUTORS SPECIFICALLY DISCLAIM ANY WARRANTIES,
INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY,
FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT.  THIS SOFTWARE
IS PROVIDED ON AN "AS IS" BASIS, AND THE AUTHORS AND DISTRIBUTORS HAVE
NO OBLIGATION TO PROVIDE MAINTENANCE, SUPPORT, UPDATES, ENHANCEMENTS, OR
MODIFICATIONS.

GOVERNMENT USE: If you are acquiring this software on behalf of the
U.S. government, the Government shall have only "Restricted Rights"
in the software and related documentation as defined in the Federal
```

Acquisition Regulations (FARs) in Clause 52.227.19 (c) (2). If you
are acquiring the software on behalf of the Department of Defense, the
software shall be classified as "Commercial Computer Software" and the
Government shall have only "Restricted Rights" as defined in Clause
252.227-7013 (c) (1) of DFARs. Notwithstanding the foregoing, the
authors grant the U.S. Government and others acting in its behalf
permission to use and distribute the software in accordance with the
terms specified in this license.

[telnet 7.2.0 (part of FreeBSD 7.2.0)]
[COPYRIGHT]
Copyright (c) 1992-2009 The FreeBSD Project. All rights reserved.

[LICENSE]
Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:
1. Redistributions of source code must retain the above copyright
notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright
notice, this list of conditions and the following disclaimer in the
documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY AUTHOR AND CONTRIBUTORS ``AS IS'' AND
ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
ARE DISCLAIMED. IN NO EVENT SHALL AUTHOR OR CONTRIBUTORS BE LIABLE
FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
SUCH DAMAGE.

The 4.4BSD and 4.4BSD-Lite software is distributed under the following
terms:

All of the documentation and software included in the 4.4BSD and 4.4BSD-Lite
Releases is copyrighted by The Regents of the University of California.

Copyright 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:
1. Redistributions of source code must retain the above copyright
notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright
notice, this list of conditions and the following disclaimer in the
documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software
must display the following acknowledgement:
This product includes software developed by the University of
California, Berkeley and its contributors.
4. Neither the name of the University nor the names of its contributors
may be used to endorse or promote products derived from this software
without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND
ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE
FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY

OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
SUCH DAMAGE.

The Institute of Electrical and Electronics Engineers and the American
National Standards Committee X3, on Information Processing Systems have
given us permission to reprint portions of their documentation.

In the following statement, the phrase ``this text'' refers to portions
of the system documentation.

Portions of this text are reprinted and reproduced in electronic form in
the second BSD Networking Software Release, from IEEE Std 1003.1-1988, IEEE
Standard Portable Operating System Interface for Computer Environments
(POSIX), copyright C 1988 by the Institute of Electrical and Electronics
Engineers, Inc. In the event of any discrepancy between these versions
and the original IEEE Standard, the original IEEE Standard is the referee
document.

In the following statement, the phrase ``This material'' refers to portions
of the system documentation.

This material is reproduced with permission from American National
Standards Committee X3, on Information Processing Systems. Computer and
Business Equipment Manufacturers Association (CBEMA), 311 First St., NW,
Suite 500, Washington, DC 20001-2178. The developmental work of
Programming Language C was completed by the X3J11 Technical Committee.

The views and conclusions contained in the software and documentation are
those of the authors and should not be interpreted as representing official
policies, either expressed or implied, of the Regents of the University
of California.

NOTE: The copyright of UC Berkeley's Berkeley Software Distribution ("BSD")
source has been updated. The copyright addendum may be found at
ftp://ftp.cs.berkeley.edu/pub/4bsd/README.Impt.License.Change and is
included below.

July 22, 1999

To All Licensees, Distributors of Any Version of BSD:

As you know, certain of the Berkeley Software Distribution ("BSD") source
code files require that further distributions of products containing all or
portions of the software, acknowledge within their advertising materials
that such products contain software developed by UC Berkeley and its
contributors.

Specifically, the provision reads:

```
"     * 3. All advertising materials mentioning features or use of this software
       *    must display the following acknowledgement:
       *    This product includes software developed by the University of
       *    California, Berkeley and its contributors."
```

Effective immediately, licensees and distributors are no longer required to
include the acknowledgement within advertising materials. Accordingly, the
foregoing paragraph of those BSD Unix files containing it is hereby deleted
in its entirety.

William Hoskins
Director, Office of Technology Licensing
University of California, Berkeley

[tftp-hpa 5.2]
[COPYRIGHT]
  Copyright (c) 1983 Regents of the University of California.
  Copyright (c) 1999-2009 H. Peter Anvin
  Copyright (c) 2011 Intel Corporation; author: H. Peter Anvin

All rights reserved.

[LICENSE]
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:
This product includes software developed by the University of California, Berkeley and its contributors.
4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

[timer 0.9.32 (part of uclibc 0.9.32)]
[LICENSE]

GNU LESSER GENERAL PUBLIC LICENSE
Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.
51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the

Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not

excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the library's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA

Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the library, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the library `Frob' (a library for tweaking knobs) written by James Random Hacker.

<signature of Ty Coon>, 1 April 1990
Ty Coon, President of Vice

That's all there is to it!

[traceroute 8.0.0 (part of FreeBSD 8.0.0)]
[COPYRIGHT]
Copyright (c) 1992-2009 The FreeBSD Project. All rights reserved.

[LICENSE]
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright

notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright
notice, this list of conditions and the following disclaimer in the
documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS ``AS IS'' AND
ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
SUCH DAMAGE.

The 4.4BSD and 4.4BSD-Lite software is distributed under the following
terms:

All of the documentation and software included in the 4.4BSD and 4.4BSD-Lite
Releases is copyrighted by The Regents of the University of California.

Copyright 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:
1. Redistributions of source code must retain the above copyright
notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright
notice, this list of conditions and the following disclaimer in the
documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software
must display the following acknowledgement:
This product includes software developed by the University of
California, Berkeley and its contributors.
4. Neither the name of the University nor the names of its contributors
may be used to endorse or promote products derived from this software
without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND
ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE
FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
SUCH DAMAGE.

The Institute of Electrical and Electronics Engineers and the American
National Standards Committee X3, on Information Processing Systems have
given us permission to reprint portions of their documentation.

In the following statement, the phrase ``this text'' refers to portions
of the system documentation.

Portions of this text are reprinted and reproduced in electronic form in
the second BSD Networking Software Release, from IEEE Std 1003.1-1988, IEEE
Standard Portable Operating System Interface for Computer Environments
(POSIX), copyright C 1988 by the Institute of Electrical and Electronics
Engineers, Inc. In the event of any discrepancy between these versions
and the original IEEE Standard, the original IEEE Standard is the referee
document.

In the following statement, the phrase ``This material'' refers to portions

of the system documentation.

This material is reproduced with permission from American National Standards Committee X3, on Information Processing Systems. Computer and Business Equipment Manufacturers Association (CBEMA), 311 First St., NW, Suite 500, Washington, DC 20001-2178. The developmental work of Programming Language C was completed by the X3J11 Technical Committee.

The views and conclusions contained in the software and documentation are those of the authors and should not be interpreted as representing official policies, either expressed or implied, of the Regents of the University of California.

NOTE: The copyright of UC Berkeley's Berkeley Software Distribution ("BSD") source has been updated. The copyright addendum may be found at ftp://ftp.cs.berkeley.edu/pub/4bsd/README.Impt.License.Change and is included below.

July 22, 1999

To All Licensees, Distributors of Any Version of BSD:

As you know, certain of the Berkeley Software Distribution ("BSD") source code files require that further distributions of products containing all or portions of the software, acknowledge within their advertising materials that such products contain software developed by UC Berkeley and its contributors.

Specifically, the provision reads:

" * 3. All advertising materials mentioning features or use of this software
 * must display the following acknowledgement:
 * This product includes software developed by the University of
 * California, Berkeley and its contributors."

Effective immediately, licensees and distributors are no longer required to include the acknowledgement within advertising materials. Accordingly, the foregoing paragraph of those BSD Unix files containing it is hereby deleted in its entirety.

William Hoskins
Director, Office of Technology Licensing
University of California, Berkeley

[traceroute6 8.0.0 (part of FreeBSD 8.0.0)]
[COPYRIGHT]
Copyright (c) 1992-2009 The FreeBSD Project. All rights reserved.

[LICENSE]
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF

SUCH DAMAGE.

The 4.4BSD and 4.4BSD-Lite software is distributed under the following terms:

All of the documentation and software included in the 4.4BSD and 4.4BSD-Lite Releases is copyrighted by The Regents of the University of California.

Copyright 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:
This product includes software developed by the University of California, Berkeley and its contributors.
4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The Institute of Electrical and Electronics Engineers and the American National Standards Committee X3, on Information Processing Systems have given us permission to reprint portions of their documentation.

In the following statement, the phrase ``this text'' refers to portions of the system documentation.

Portions of this text are reprinted and reproduced in electronic form in the second BSD Networking Software Release, from IEEE Std 1003.1-1988, IEEE Standard Portable Operating System Interface for Computer Environments (POSIX), copyright C 1988 by the Institute of Electrical and Electronics Engineers, Inc. In the event of any discrepancy between these versions and the original IEEE Standard, the original IEEE Standard is the referee document.

In the following statement, the phrase ``This material'' refers to portions of the system documentation.

This material is reproduced with permission from American National Standards Committee X3, on Information Processing Systems. Computer and Business Equipment Manufacturers Association (CBEMA), 311 First St., NW, Suite 500, Washington, DC 20001-2178. The developmental work of Programming Language C was completed by the X3J11 Technical Committee.

The views and conclusions contained in the software and documentation are those of the authors and should not be interpreted as representing official policies, either expressed or implied, of the Regents of the University of California.

NOTE: The copyright of UC Berkeley's Berkeley Software Distribution ("BSD")

source has been updated. The copyright addendum may be found at
ftp://ftp.cs.berkeley.edu/pub/4bsd/README.Impt.License.Change and is
included below.

July 22, 1999

To All Licensees, Distributors of Any Version of BSD:

As you know, certain of the Berkeley Software Distribution ("BSD") source
code files require that further distributions of products containing all or
portions of the software, acknowledge within their advertising materials
that such products contain software developed by UC Berkeley and its
contributors.

Specifically, the provision reads:

"   * 3. All advertising materials mentioning features or use of this software
      *   must display the following acknowledgement:
      *   This product includes software developed by the University of
      *   California, Berkeley and its contributors."

Effective immediately, licensees and distributors are no longer required to
include the acknowledgement within advertising materials. Accordingly, the
foregoing paragraph of those BSD Unix files containing it is hereby deleted
in its entirety.

William Hoskins
Director, Office of Technology Licensing
University of California, Berkeley

[u-boot 1.1.4]
[COPYRIGHT]
   (C) Copyright 2000 - 2005
   Wolfgang Denk, DENX Software Engineering, wd@denx.de.

[NOTE]
  NOTE! This copyright does *not* cover the so-called "standalone"
applications that use U-Boot services by means of the jump table
provided by U-Boot exactly for this purpose - this is merely
considered normal use of U-Boot, and does *not* fall under the
heading of "derived work".

  The header files "include/image.h" and "include/asm-*/u-boot.h"
define interfaces to U-Boot. Including these (unmodified) header
files in another file is considered normal use of U-Boot, and does
not fall under the heading of "derived work".

  Also note that the GPL below is copyrighted by the Free Software
Foundation, but the instance of code that it refers to (the U-Boot
source code) is copyrighted by me and others who actually wrote it.
-- Wolfgang Denk

[LICENSE]
                    GNU GENERAL PUBLIC LICENSE
                       Version 2, June 1991

 Copyright (C) 1989, 1991 Free Software Foundation, Inc.
     59 Temple Place, Suite 330, Boston, MA 02111-1307 USA
 Everyone is permitted to copy and distribute verbatim copies
 of this license document, but changing it is not allowed.

                            Preamble

  The licenses for most software are designed to take away your
freedom to share and change it. By contrast, the GNU General Public
License is intended to guarantee your freedom to share and change free
software--to make sure the software is free for all its users. This
General Public License applies to most of the Free Software
Foundation's software and to any other program whose authors commit to

using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot

impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

[uclibc 0.9.32 (part of uclibc 0.9.32)]
[LICENSE]

GNU LESSER GENERAL PUBLIC LICENSE
Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.
51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General

Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for

writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the

ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one

of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your

rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by

the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the library's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA

```
Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or your
school, if any, to sign a "copyright disclaimer" for the library, if
necessary.  Here is a sample; alter the names:

  Yoyodyne, Inc., hereby disclaims all copyright interest in the
  library `Frob' (a library for tweaking knobs) written by James Random Hacker.

  <signature of Ty Coon>, 1 April 1990
  Ty Coon, President of Vice

That's all there is to it!


------------------------------------------------------------------------------
---
[unix stack 8.0.0 (part of FreeBSD 8.0.0)]
[COPYRIGHT]
  Copyright (c) 1992-2009 The FreeBSD Project. All rights reserved.

[LICENSE]
Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:
1. Redistributions of source code must retain the above copyright
   notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright
   notice, this list of conditions and the following disclaimer in the
   documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS ``AS IS'' AND
ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
ARE DISCLAIMED.  IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
SUCH DAMAGE.

The 4.4BSD and 4.4BSD-Lite software is distributed under the following
terms:

All of the documentation and software included in the 4.4BSD and 4.4BSD-Lite
Releases is copyrighted by The Regents of the University of California.

Copyright 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
         The Regents of the University of California.  All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:
1. Redistributions of source code must retain the above copyright
   notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright
   notice, this list of conditions and the following disclaimer in the
   documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software
   must display the following acknowledgement:
This product includes software developed by the University of
California, Berkeley and its contributors.
4. Neither the name of the University nor the names of its contributors
   may be used to endorse or promote products derived from this software
   without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND
ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
```

IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The Institute of Electrical and Electronics Engineers and the American National Standards Committee X3, on Information Processing Systems have given us permission to reprint portions of their documentation.

In the following statement, the phrase ``this text'' refers to portions of the system documentation.

Portions of this text are reprinted and reproduced in electronic form in the second BSD Networking Software Release, from IEEE Std 1003.1-1988, IEEE Standard Portable Operating System Interface for Computer Environments (POSIX), copyright C 1988 by the Institute of Electrical and Electronics Engineers, Inc. In the event of any discrepancy between these versions and the original IEEE Standard, the original IEEE Standard is the referee document.

In the following statement, the phrase ``This material'' refers to portions of the system documentation.

This material is reproduced with permission from American National Standards Committee X3, on Information Processing Systems. Computer and Business Equipment Manufacturers Association (CBEMA), 311 First St., NW, Suite 500, Washington, DC 20001-2178. The developmental work of Programming Language C was completed by the X3J11 Technical Committee.

The views and conclusions contained in the software and documentation are those of the authors and should not be interpreted as representing official policies, either expressed or implied, of the Regents of the University of California.

NOTE: The copyright of UC Berkeley's Berkeley Software Distribution ("BSD") source has been updated. The copyright addendum may be found at ftp://ftp.cs.berkeley.edu/pub/4bsd/README.Impt.License.Change and is included below.

July 22, 1999

To All Licensees, Distributors of Any Version of BSD:

As you know, certain of the Berkeley Software Distribution ("BSD") source code files require that further distributions of products containing all or portions of the software, acknowledge within their advertising materials that such products contain software developed by UC Berkeley and its contributors.

Specifically, the provision reads:

```
"     * 3. All advertising materials mentioning features or use of this software
       *    must display the following acknowledgement:
       *    This product includes software developed by the University of
       *    California, Berkeley and its contributors."
```

Effective immediately, licensees and distributors are no longer required to include the acknowledgement within advertising materials. Accordingly, the foregoing paragraph of those BSD Unix files containing it is hereby deleted in its entirety.

William Hoskins
Director, Office of Technology Licensing
University of California, Berkeley

```
------------------------------------------------------------------------------
---
[wireshark 2.4.6]
This text consists of three parts:

Part I: Some remarks regarding the license given in
Part II: The actual license that covers Wireshark.
Part III: Other applicable licenses.

When in doubt: Part II/III is the legally binding part, Part I is just
there to make it easier for people that are not familiar with the GPLv2.


------------------------------------------------------------------------
Part I:

Wireshark is distributed under the GNU GPLv2. There are no restrictions
on its use. There are restrictions on its distribution in source or
binary form.

Most parts of Wireshark are covered by a "GPL version 2 or later" license.
Some files are covered by different licenses that are compatible with
the GPLv2.

As a notable exception, some utilities distributed with the Wireshark source are
covered by other licenses that are not themselves directly compatible with the
GPLv2. This is OK, as only the tools themselves are licensed this way, the
output of the tools is not considered a derived work, and so can be safely
licensed for Wireshark's use. An incomplete selection of these tools includes:
 - the pidl utility (tools/pidl) is licensed under the GPLv3+.

Parts of Wireshark can be built and distributed as libraries. These
parts are still covered by the GPL, and NOT by the Lesser General Public
License or any other license.

If you integrate all or part of Wireshark into your own application, then
that application must be released under a license compatible with the GPL.

The full text of the GNU GPL and some of the other applicable licenses follows.

------------------------------------------------------------------------
Part II:

                    GNU GENERAL PUBLIC LICENSE
                       Version 2, June 1991

 Copyright (C) 1989, 1991 Free Software Foundation, Inc.,
 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA
 Everyone is permitted to copy and distribute verbatim copies
 of this license document, but changing it is not allowed.

                            Preamble

  The licenses for most software are designed to take away your
freedom to share and change it.  By contrast, the GNU General Public
License is intended to guarantee your freedom to share and change free
software--to make sure the software is free for all its users.  This
General Public License applies to most of the Free Software
Foundation's software and to any other program whose authors commit to
using it.  (Some other Free Software Foundation software is covered by
the GNU Lesser General Public License instead.)  You can apply it to
your programs, too.

  When we speak of free software, we are referring to freedom, not
price.  Our General Public Licenses are designed to make sure that you
have the freedom to distribute copies of free software (and charge for
this service if you wish), that you receive source code or can get it
if you want it, that you can change the software or use pieces of it
in new free programs; and that you know you can do these things.
```

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent

access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions

of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc.,

```
    51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this
when it starts in an interactive mode:

    Gnomovision version 69, Copyright (C) year name of author
    Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
    This is free software, and you are welcome to redistribute it
    under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate
parts of the General Public License.  Of course, the commands you use may
be called something other than `show w' and `show c'; they could even be
mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your
school, if any, to sign a "copyright disclaimer" for the program, if
necessary.  Here is a sample; alter the names:

  Yoyodyne, Inc., hereby disclaims all copyright interest in the program
  `Gnomovision' (which makes passes at compilers) written by James Hacker.

  <signature of Ty Coon>, 1 April 1989
  Ty Coon, President of Vice

This General Public License does not permit incorporating your program into
proprietary programs.  If your program is a subroutine library, you may
consider it more useful to permit linking proprietary applications with the
library.  If this is what you want to do, use the GNU Lesser General
Public License instead of this License.

------------------------------------------------------------------------
Part III:

Parts of this software are licensed as follows

   Copyright (c) 1988, 1992, 1993
        The Regents of the University of California.  All rights reserved.

   Redistribution and use in source and binary forms, with or without
   modification, are permitted provided that the following conditions
   are met:
   1. Redistributions of source code must retain the above copyright
      notice, this list of conditions and the following disclaimer.
   2. Redistributions in binary form must reproduce the above copyright
      notice, this list of conditions and the following disclaimer in the
      documentation and/or other materials provided with the distribution.
   3. Neither the name of the University nor the names of its contributors
      may be used to endorse or promote products derived from this software
      without specific prior written permission.

   THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND
   ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
   IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
   ARE DISCLAIMED.  IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE
   FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
   DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
   OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
   HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
   LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
   OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
   SUCH DAMAGE.


   Copyright (c) 2003 Markus Friedl.  All rights reserved.

   Redistribution and use in source and binary forms, with or without
   modification, are permitted provided that the following conditions
```

are met:
1. Redistributions of source code must retain the above copyright
notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright
notice, this list of conditions and the following disclaimer in the
documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS'' AND ANY EXPRESS OR
IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES
OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED.
IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT,
INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE,
DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY
THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT
(INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF
THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright (c) 2003 Endace Technology Ltd, Hamilton, New Zealand.
All rights reserved.

This software and documentation has been developed by Endace Technology Ltd.
along with the DAG PCI network capture cards. For further information please
visit http://www.endace.com/.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice,
this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright
notice, this list of conditions and the following disclaimer in the
documentation and/or other materials provided with the distribution.

3. The name of Endace Technology Ltd may not be used to endorse or promote
products derived from this software without specific prior written
permission.

THIS SOFTWARE IS PROVIDED BY ENDACE TECHNOLOGY LTD ``AS IS'' AND ANY EXPRESS
OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES
OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO
EVENT SHALL ENDACE TECHNOLOGY LTD BE LIABLE FOR ANY DIRECT, INDIRECT,
INCIDENTAL,
SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,
PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS;
OR
BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER
IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE
POSSIBILITY OF SUCH DAMAGE.

Copyright (C) 1995, 1996, 1997, and 1998 WIDE Project.
All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:
1. Redistributions of source code must retain the above copyright
notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright
notice, this list of conditions and the following disclaimer in the
documentation and/or other materials provided with the distribution.
3. Neither the name of the project nor the names of its contributors
may be used to endorse or promote products derived from this software
without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE PROJECT AND CONTRIBUTORS ``AS IS'' AND

ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
ARE DISCLAIMED. IN NO EVENT SHALL THE PROJECT OR CONTRIBUTORS BE LIABLE
FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
SUCH DAMAGE.

Copyright (c) 1997, 1999 Hellmuth Michaelis. All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:
1. Redistributions of source code must retain the above copyright
   notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright
   notice, this list of conditions and the following disclaimer in the
   documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS ``AS IS'' AND
ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
SUCH DAMAGE.

[wpa_supplicant 2.6]
[COPYRIGHT]
Copyright (c) 2002-2016, Jouni Malinen <j@w1.fi> and contributors
All Rights Reserved.

[LICENSE]
This software may be distributed, used, and modified under the terms of
BSD license:

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions are
met:

1. Redistributions of source code must retain the above copyright
   notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright
   notice, this list of conditions and the following disclaimer in the
   documentation and/or other materials provided with the distribution.

3. Neither the name(s) of the above-listed copyright holder(s) nor the
   names of its contributors may be used to endorse or promote products
   derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS
"AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT
LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR
A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT
OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT
LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE,
DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY
THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT
(INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE

```
OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
------------------------------------------------------------------------------
---
[xzdec 5.2.2(part of xz 5.2.2)]
////////////////////////////////////////////////////////////////////////////
//
//
/// \file       xzdec.c
/// \brief      Simple single-threaded tool to uncompress .xz or .lzma files
//
//  Author:     Lasse Collin
//
//  This file has been put into the public domain.
//  You can do whatever you want with this file.
//
////////////////////////////////////////////////////////////////////////////
//
------------------------------------------------------------------------------
---
[zlib 1.2.3]
[COPYRIGHT]
  Copyright (C) 1995-2005 Jean-loup Gailly and Mark Adler

[LICENSE]
  This software is provided 'as-is', without any express or implied
  warranty.  In no event will the authors be held liable for any damages
  arising from the use of this software.

  Permission is granted to anyone to use this software for any purpose,
  including commercial applications, and to alter it and redistribute it
  freely, subject to the following restrictions:

  1. The origin of this software must not be misrepresented; you must not
     claim that you wrote the original software. If you use this software
     in a product, an acknowledgment in the product documentation would be
     appreciated but is not required.
  2. Altered source versions must be plainly marked as such, and must not be
     misrepresented as being the original software.
  3. This notice may not be removed or altered from any source distribution.

  Jean-loup Gailly        Mark Adler
  jloup@gzip.org          madler@alumni.caltech.edu


------------------------------------------------------------------------------
---
```