NEC

GVT-125431-001-00 1.10

QX-S1100G シリーズ

Ethernet スイッチ オペレーションマニュアル

改版履歴

版数	日付	改版内容
1.0	2020/04	初版発行
1.1	2020/07/31	・09-システム管理の 11 章 NetMeister に NetMeister proxy を追加しました。
1.2	2021/01	・07-セキュリティの 3 章 802.1X のメモを変更 ・07-セキュリティの 4 章 MAC アドレス認証のメモを変更 ・誤記修正
1.3	2021/05	・07-セキュリティの 11 章 パスワード管理を追加 ・誤記修正
1.4	2021/07	・01-はじめにの 14 章 装置管理に locator blink コマンドに関する記載（装置の特定）を追加しました。 ・09- システム管理の 11 章 NetMeister にプロキシ関連の記載、ゼロタッチプロビジョニングに関する記載、トラブルシューティングを追加しました。
1.5	2022/07	・07-セキュリティの3章802.1Xに802.1 Xユニキャストトリガーサイレント機能を追加しました。 ・07-セキュリティの 5 章ポートセキュリティに 7.12 ポートでの認証方式のトリガー順序の設定を追加しました。 ・09-システム管理の 11 章 NetMeister に IRF 対応に関する記載を追加しました。 ・誤記訂正
1.6	2023/02	・02-アクセスの 9 章 ループ検出について誤記修正しました。 ・03.IP サービスの 5 章 DHCP サーバの設定の「カスタマイズ DHCP オプションの設定」にオプショングループでのカスタマイズ DHCP オプションの設定手順を追記しました。 ・06-ACL and QoS の 1 章 ACL の rule (IPv6 advanced ACL view)コマンドにポイントを追加しました。 ・06-ACL and QoS の 5 章ラインレートについて、色ごとのアクション設定は未サポートのため、誤記修正しました。 ・07-セキュリティの 5 章ポートセキュリティの port-security port-mode コマンドに mac-and-userlogin-secure-ext オプションを追加しました。 ・07-セキュリティの 11 章パスワード管理の表 11-1 特殊文字について誤記修正しました。 ・09-システム管理の 11 章 NetMeister に親機モード運用時の設定を追加しました。

版数	日付	改版内容
1.7	2025/05	・表紙ロゴ色、配置の変更 ・01-はじめにの 4 章 CLI によるログインの 4.2 コンソールポートからのローカルログインを更新しました。 ・01-はじめに の 14 章 装置管理 の 14.11.2 トランシーバの診断 は未サポートのため修正しました。 ・02-アクセス　の　8 章 STP　の 8.27.2. BPDU ガードの設定 に、検出の間隔を設定するコマンドの案内文を追加しました。 ・02-アクセス　の　8 章 STP　の 8.27.7. BPDU ドロップ機能の有効化 に、制限とガイドラインを追加しました。 ・06-ACL and QoS の 1 章 ACL の 1.4.2 拡張 IPv6 ACL の設定 のポイントに説明を追記しました。 ・07-セキュリティの 9 章 ARP アタックプロテクション に 9.3 ARP パケットレートリミットの設定 を追加しました。 ・08-高可用性の 1 章 DLPP の 1.2 設定の制限とガイドラインを更新しました。 ・08-高可用性の 4 章 Track の 4.4Track 設定作業リストに、PoE との関連付けを追加しました。 ・09-システム管理 10 章 PoE 行頭メモに poe high-inrush に対応していることを記載しました。 10.4 PD による突入電力の許容（high-inrush のやり方）を追加しました。
1.8	2025/07	・06-ACL and QoS の8 章 プライオリティマーキング の「8.2. 設定手順」を誤記修正しました。 ・10-謝辞を更新しました。
1.9	2026/02	・07-セキュリティの4章 MACアドレス認証の概要に、対応する認証方式のメモを追加しました。
1.10	2026/10	・QX-S1100Gシリーズ Ethernet スイッチマニュアル訂正資料 5.0版の修正内容を反映しました。

Copyright © NEC Corporation 2020-2026

All Rights Reserved

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

商標

本マニュアルに記載されているその他の商標は、各社が保有します。

注意

- 本装置は *QX-S1100G シリーズ Ethernet スイッチ コマンドマニュアル*に記載されているコマンドのみ使用することができます。*QX-S1100G シリーズ Ethernet スイッチ コマンドマニュアル*に記載されていないコマンドを使用した場合の動作については保証しません。
- 本マニュアルの内容は、予告なく変更されることがあります。本マニュアルのすべての記述、情報、および推奨事項は、明示的か暗黙的かにかかわらず、いかなる種類の保証の対象になりません。

本マニュアルについて

関連マニュアル

次のマニュアルには、QX-S1100G シリーズ Ethernet スイッチに関する詳細な説明があります。

マニュアル	内容
QX-S1100G シリーズ Ethernet スイッチ インスタレーションマニュアル	システムのインストールについて説明しています。
QX-S1100G シリーズ Ethernet スイッチ オペレーションマニュアル	機能の設定について説明しています。
QX-S1100G シリーズ Ethernet スイッチ コマンドマニュアル	機能に関するコマンドについて説明しています。
QX-S1100G シリーズ Ethernet スイッチ Web コンソール操作マニュアル	Web コンソールからの装置設定、状態確認等についての操作を記述しています。

マニュアルの構成

このオペレーションマニュアルは以下のセクションで構成されます。

- **はじめに**

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

- **アクセス**

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

- **IP サービス**

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

- **ルーティングプロトコル**

  各種ルーティングプロトコル（IPv4＆IPv6）の設定について説明します。

- **マルチキャスト**

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

- **ACL and QoS**

  QoS、ACL の設定について説明します。

- **セキュリティ**

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

- **高可用性**

  DLDP 等の設定について説明します。

- **システム管理**

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

- **謝辞**

表記規則

本マニュアルでは、次の表記規則を使用しています。

I. コマンド表記規則

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

II. GUI 表記規則

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

III. キーボード操作

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

IV. マウス操作

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

V. 記号

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

VI. ネットワークアイコン

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

VII. 設定例

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

VIII. セキュリティ強化

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

本マニュアルは以下に示す 10 個のセクションで構成されています。

01 - はじめに

02 - アクセス

03 - IP サービス

04 - ルーティングプロトコル

05 - マルチキャスト

06 - ACL and QoS

07 - セキュリティ

08 - 高可用性

09 - システム管理

10 - 謝辞

QX-S1100G シリーズ Ethernet スイッチ

オペレーションマニュアル

1. はじめに

本マニュアルは以下に示す章で構成されています。

01-CLI

02-ログイン

03-コンソールポートによる最初のログイン

04-CLI によるログイン

05-Web コンソールによるログイン

06-SNMP によるアクセス

07-ログインユーザの制御

08-RBAC

09-FTP

10-TFTP

11-ファイルシステム管理

12-コンフィグレーションファイル管理

13-ソフトウェアのアップグレード

14-装置管理

15-Python

16-Auto Config

目次

このセクションのページは **1-x-x** です。

1 章 CLI 1-1
1.1 CLI view の記述 1-1
1.2 コマンドラインを使ったオンラインヘルプ 1-2
1.3 コマンドの取り消し 1-3
1.4 コマンドの実行 1-3
1.4.1 コマンドラインの編集 1-3
1.4.2 引数の文字列あるいはテキストタイプ値の入力 1-4
1.4.3 インタフェースタイプの固有の短縮文字列 1-4
1.4.4 コマンドの短縮入力と補完 1-5
1.4.5 コマンドエイリアスの設定と使用方法 1-5
1.4.6 ホットキーを使用した設定と使用方法 1-6
1.4.7 情報の同期出力 1-7
1.5 コマンドラインのエラーメッセージ 1-8
1.6 履歴コマンドの保存 1-8
1.7 CLI 表示の管理 1-9
1.7.1 スクリーン出力の停止 1-9
1.7.2 表示コマンドの各出力ラインの番号表示 1-10
1.7.3 出力のフィルタリング 1-10
1.7.4 display コマンドのファイルへの保存 1-13
1.7.5 display コマンドからの出力の有効的な表示、管理 1-14
1.8 稼働中の設定の保存 1-15

1章 CLI

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

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

[Switch]
```

図 1-1 CLI の例

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

1.1 CLI viewの記述

コマンドは機能によって入力可能な view が異なります。コマンドを使用する場合、その view に入る必要があります。

CLI view は図 1-2に示すような階層構造となっています。各 view は、プロンプトによってどの階層にいるかを確認できます。例えば、プロンプトが[Switch-vlan100]である場合、system-view で vlan100 を作成し、VLAN100 view にいることを示します。

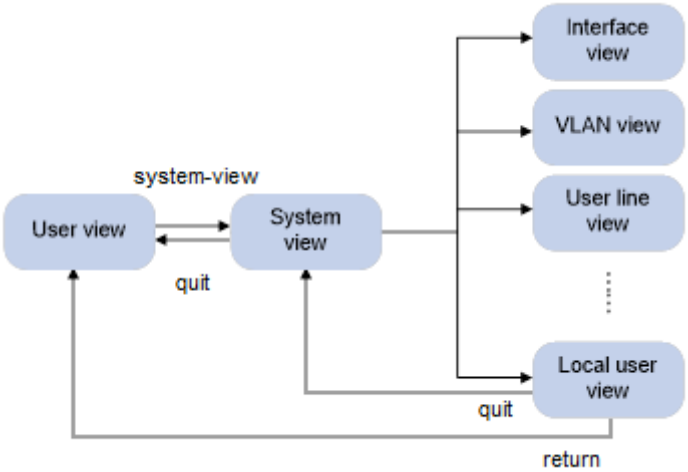


図 1-2 CLI view

CLI でログインした場合の最初の view は user view です。user view のプロンプトは <*Device-name*>です。(*Device-name* はデフォルトでは装置名であり、**sysname** コマンドを使用して変更することができます。)

user view では以下の操作を行うことができます。

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

system view では以下の操作を行うことができます。

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

- system view から **quit** コマンドによって user view に移行することができます。

各種設定毎の view からは、**quit** コマンドによって 1 階層前の view 移行することができ、**return** コマンドあるいはホットキー**Ctrl+Z** によって user view に移行することができます。

1.2 コマンドラインを使ったオンラインヘルプ

CLI で“?”を入力することで、現在の view で利用できるコマンドまたはパラメータを表示できます。

CLI オンラインヘルプは状況に応じてヘルプ情報が異なります。

- 各 view で “?”を入力することで、その view で利用できるすべてのコマンドの最初の文字列を表示します。

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

- コマンドの後ろにスペースを空けて“?”を入力することで、入力されているコマンドの後ろに設定可能なコマンドかパラメータが表示されます。

```
<Switch>system-view
System View: return to User View with Ctrl+Z.
[Switch]interface ?
  Vlan-interface       VLAN interface
[Switch]interface vlan-interface ?
  <1-4094>  Vlan-interface interface number
[Switch]interface vlan-interface 1 ?
  <cr>
[Switch]interface vlan-interface 1
```

<1-4094> は引数の範囲、<cr>はコマンドの末尾であることを示します。**Enter** キーを押すことでコマンドを実行することができます。

- コマンドの後ろにスペースを空けずに“?”を入力することで、その文字列から始まるコマンドが表示されます。

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

1.3 コマンドの取り消し

コマンドの先頭に **undo** をつけることで、以下のことができます。

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

例えば、Information Center を有効にするために、**info-center enable** コマンドが設定されている場合、**undo info-center enable** コマンドで Information Center を無効にします。

undo コマンドが使えない設定は、無効にするコマンドがそれぞれ用意されています。また、一部のコマンドは、**undo** コマンドによってデフォルトと異なる状態になる場合があります。**undo** コマンドが使えない設定、および、設定によってデフォルトとは異なる状態になるコマンドは、該当コマンドのコマンドマニュアルに説明が記載されています。

1.4 コマンドの実行

1.4.1 コマンドラインの編集

入力中のコマンドラインを編集するために、表 1-1に示すキーや表 1-4に示すホットキーを使用することができます。**Enter** を押すことでコマンドを実行されます。

表 1-1 コマンドラインの編集キー

キー	機能
コマンドキー	カーソルの位置に文字を挿入し、カーソルを右に移動します。編集可能なコマンドの最大文字数は、511文字です。最大の文字数を入力している場合、文字を挿入することができません。
Backspace	カーソルの左側の文字を削除し、1文字分カーソルを戻します。
左矢印キー (←)	カーソルが左に1文字分移動します。

キー	機能
右矢印キー (→)	カーソルが右に1文字分移動します。
上矢印キー (↑)	前に入力した履歴コマンドを表示します。
下矢印キー (↓)	次に入力した履歴コマンドを表示します。
Tab	文字列を入力した状態でTabキーを押した場合、入力済みの文字列を補完します。

1.4.2 引数の文字列あるいはテキストタイプ値の入力

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

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

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

引数のために特定の引数が必要となる場合があります。特定の引数が必要なコマンドについては、関連コマンドのコマンドマニュアルに記載をしています。

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

1.4.3 インタフェースタイプの固有の短縮文字列

インタフェースタイプには、固有の短縮文字列が存在します。コマンドの短縮入力以外に固有の短縮文字列での入力も可能です。

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

表 1-2 インタフェースのタイプのコマンドと短縮文字列

コマンド	固有の短縮文字列
Bridge-Aggregation	BAGG
GigabitEthernet	GE
InLoopBack	InLoop
LoopBack	Loop
M-GigabitEthernet	MGE
NULL	NULL
Ten-GigabitEthernet	XGE
Vlan-interface	Vlan-int

例えば、GigabitEthernet 1/0/1 の view に移行するために、下記のいずれのフォーマットも使用できます。

- interface gigabitethernet 1/0/1

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

インタフェースのタイプとインタフェースの間のスペースは無くても使用できます。

1.4.4 コマンドの短縮入力と補完

コマンドまたはパラメータは、入力された文字列から始まるコマンドが一意のコマンドまたはパラメータとして認識可能な場合、文字列を短縮して入力することができます。

例えば、user view において **s** から始まるコマンドは、**system-view** や **startup saved-configuration** などがあります。**system-view** を実行する場合、一意のコマンドになるように最低でも **sy** を入力すれば、短縮入力が可能です。**startup saved-configuration** を実行する場合、最低でも **st s** を入力する必要があります。

また、文字列を入力した状態で **Tab** キーを押すことで、システムは自動的に文字列を補完し、完全なコマンドを表示、入力することができます。

- **Tab** キーを押したとき、入力済みの文字列からはじまるコマンドが存在する場合、システムは完全なコマンドを次の行に表示します。
- 入力済みの文字列からはじまるコマンドが複数ある場合、Tab キーを押すたびに候補のコマンドが表示されます。
- 入力済みの文字列からはじまるコマンドがない場合、システムは文字列を補完せず、元の文字列を次の行に表示します。

1.4.5 コマンドエイリアスの設定と使用方法

コマンドエイリアスを使用することで、本来の文字列とは異なる文字列でのコマンド実行が可能です。

例えば、**display** のエイリアスとして **show** が設定されている場合、**display clock** コマンドの代わりに **show clock** コマンドを使用することができます。

また、**display ip routing-table** コマンドのために **display ip** のエイリアスを **shiprt** として設定してある場合、**display ip** から始まるすべてのコマンドを **shiprt** を使用して入力することができます。

I. ガイドライン

コマンドエイリアスで定義されたコマンドを実行しても、コンフィグ上にはオリジナルなコマンドで登録されます。

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

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

パラメータがあるコマンドのエイリアスを使用する場合、各パラメータの値を指定する必要があります。パラメータの指定が正しくない場合、コマンドの実行に失敗し、エイリアスで設定したコマンドの文字列がそのまま表示されます。

表 1-3にシステムであらかじめ定義されているコマンドエイリアスを示します。手動で新しいコマンドエイリアスを設定することもできます。システムで定義されているコマンドエイリアスは削除することができません。

表 1-3 システムで定義されているコマンドエイリアス

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

II. 設定手順

以下にコマンドエイリアスの設定を以下に示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. コマンドエイリアスを設定する	**alias** *alias command*	デフォルト： システムで定義されているコマンドエイリアスのみ
3. （オプション設定項目）コマンドエイリアスで定義されたコマンドを表示する	**display alias** [**alias**]	すべてのviewで実行可能です。

1.4.6 ホットキーを使用した設定と使用方法

CLI ではホットキーを使用できます。ホットキーを使用することで、定義された操作を容易に実行することができます。表 1-4にシステムで定義されているホットキーを示します。手動で新しいホットキーの定義を設定することもできます。

端末のソフトウェアによって既にこれらのキーに他の操作が定義されている可能性があります。その場合、端末のソフトウェアの定義が優先されます。

表 1-4 システムで定義されているホットキー

ホットキー	昨日
Ctrl+A	カーソルを現在の行の先頭に動かします。
Ctrl+B	カーソルを 1 文字分左に動かします。
Ctrl+C	コマンドの実行を停止させます。
Ctrl+D	現在カーソルがある位置の文字を削除します。
Ctrl+E	カーソルを現在の行の末尾に動かします。
Ctrl+F	カーソルを1文字分右に動かします。
Ctrl+H	カーソルの左側の文字を削除します。
Ctrl+N	履歴バッファの次のコマンドを表示します。
Ctrl+P	履歴バッファの前のコマンドを表示します。
Ctrl+R	現在の行のコマンドを再表示します。
Ctrl+W	カーソルの左側に続く文字列の文字をすべて削除します。
Ctrl+X	カーソルの左側の文字をすべて削除します。
Ctrl+Y	カーソルの右側の文字をすべて削除します。
Ctrl+Z	終了し、user viewに戻ります。
Ctrl+]	内部接続またはリダイレクト接続を終了します。
Esc+B	カーソルを左側に続く文字列の先頭の文字に移動します。
Esc+D	現在カーソルがある位置の文字列の文字および右側の文字をすべて削除します。
Esc+F	カーソルを右側に続く次の文字列の先頭に移動します。

以下の手順でホットキーを設定します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． コマンドをホットキーに割り当てる	**hotkey** { **ctrl_g** | **ctrl_l** | **ctrl_o** | **ctrl_t** | **ctrl_u** } *command*	デフォルト： ● **Ctrl+G**は**display current-configuration**コマンドを表示します。 ● **Ctrl+L**は**display ip routing-table**コマンドを表示します。 ● **Ctrl+O**は **undo debugging all**コマンドを表示します。 ● **Ctrl+T**コマンドと**Ctrl+U**コマンドは未割り当てです。
3． （オプション設定項目）ホットキーを表示する	**display hotkey**	すべてのviewで実行可能です。

1.4.7 情報の同期出力

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

以下の手順で情報の同期出力を設定します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． 情報の同期出力を有効にする	**info-center synchronous**	デフォルト：無効 詳細はコマンドマニュアルのセクション9 *システム管理*を参照してください。

1.5 コマンドラインのエラーメッセージ

コマンドラインにエラーがある場合、エラーメッセージを表示します。

表 1-5 コマンドラインのエラーメッセージの例

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

1.6 履歴コマンドの保存

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

- user line 用のコマンド履歴バッファ
- すべての user line 用のコマンド履歴バッファ

表 1-6に 2 つのコマンド履歴バッファの違いを示します。

表 1-6 コマンド履歴バッファの比較

アイテム	user line のコマンド履歴バッファ	すべての user line のコマンド履歴バッファ
バッファに保存されるコマンドの種類	user lineにログイン中のユーザによって実行されたコマンド	すべてのログインユーザによって実行されたコマンド
ユーザがログアウトしたときに履歴がクリアされるか？	Yes	No
履歴を表示するコマンド	**display history-command**コマンド	**display history-command all**コマンド
履歴を実行するために呼び出す方法	↑↓キーによって情報を呼び出し、Enterで実行します。	履歴を呼び出すことはできません。

アイテム	user line のコマンド履歴バッファ	すべての user line のコマンド履歴バッファ
バッファサイズの設定方法	user line view で **history-command max-size** *size-value* コマンドを使用します。 デフォルト：10コマンド	バッファサイズをデフォルトから変更することはできません。 デフォルト：1024コマンド
バッファを無効にする方法	バッファサイズの設定を0にします。	バッファを無効にすることはできません。

履歴のルールを示します。

- 実行に成功したコマンドがそのまま履歴に残ります。短縮入力の場合、短縮されたコマンドで保存されます。
- コマンドエイリアスで定義したコマンドは、履歴には本来のコマンドで残ります。
- 同一フォーマットのコマンドを連続して複数入力した場合、履歴コマンドには 1 回のみ履歴に残します。
- バッファがいっぱいの場合、新しいコマンドを履歴に残すために最も古いコマンドの履歴を削除します。

1.7 CLI表示の管理

1.7.1 スクリーン出力の停止

情報表示をしたときに、情報の表示量が 24 行を上回る場合、システムは表示を中断し、----more----を表示します。必要に応じて残りの情報を表示、または、表示の中止を行うことができます。一度に表示する行数は **screen-length** コマンドによって変更することもできます。

I. 出力管理キー

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

II. 一時的なスクリーン一括出力

一時的に、現在のセッション中のみ情報を中断することなく表示させるようにすることもできます。

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

1.7.2 表示コマンドの各出力ラインの番号表示

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

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

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

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

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

例：

VLAN 999 の情報を各出力ラインに番号付けして出力します。

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

1.7.3 出力のフィルタリング

display コマンドに、[**|** [**by-linenum**] { **begin** | **exclude** | **include** } *regular-expression*]&<1-128>オプションを使用して出力をフィルタリングすることができます。

- このオプションを使用して、最大 128 個のフィルタ条件を指定できます。システムは、すべての条件を満たす出力行のみを表示します
- **by-linenum**– 各出力行の前に数字を表示します。1 つのフィルタ条件でのみ指定する必要があります。
- **begin**– 指定した正規表現から後の情報を表示します。
- **exclude**– 指定した正規表現を含まない情報を表示します。
- **include**– 指定した正規表現を含む情報だけを表示します。
- *regular-expression*– 1～256 文字の文字列で、大文字と小文字を区別します。正規表現は表 1-7に示す特殊文字をサポートします。

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

表 1-7 サポートする正規表現の特殊文字

文字	意味	例
^	キャレット。この後の文字列が行の先頭にのみ現れる場合にマッチします。	正規表現“^user”は、”user”で始まる文字列にマッチします。”Auser”はマッチします。
$	ドル記号。この前の文字列が行の最後にのみ現れる場合にマッチします。	正規表現"user$”は、”user”で終わる文字列にマッチします。“userA”はマッチします。
. (period)	ピリオド。空白を含む任意の一文字を示します。	“.s”は“as”と“bs”どちらにもマッチします。
*	アスタリスク。直前の文字の 0回以上の繰り返しにマッチします。	”zo*”は“z”や“zoo”にマッチします。(zo)*は”zo”と”zozo”にマッチします。
+	プラス。直前の文字の1回以上の繰り返しにマッチします。	”zo+”は"zo"や”zoo”にマッチするが、"z" にはマッチしません。
|	パイプ。左または右の文字列にマッチします。	”def|int”は、”def”または”int”を含んでいる文字列とマッチします。
( )	括弧。文字列を指定します。"+”や“*”と一緒に使われます。	”(123A)”は文字列“123A”を意味し、“408(12)+”は”40812”” 408121212”にマッチします。”408”にはマッチしません。
\N	Nで表した回数の文字列の繰り返しを示します。文字列とは\の前の( )内の文字列です。 \の前の文字列が一文字の場合は、Nは1のみが指定できます。\の前の文字列がn個の場合、Nは1からnの指定ができます。	“(string)\1”は、stringstringを含む文字列にマッチします。“(string1)(string2)\2”はstring1string2string2を含む文字列にマッチします。“(string1)(string2)\1\2”はstring1string2string1string2を含む文字列にマッチします。
[ ]	ブラケットです。ブラケット内の1文字にマッチします。	“[16A]”は1、6、A、のいずれか1文字にマッチします。“1-36A”は1、2、3、6、Aのうちの1文字にマッチします。(-はハイフン)。“]”にマッチするためには“[”のすぐ後に“]”を入力します。たとえば“[]abc]”です。
[^]	[ ]内の文字列以外を指定します。	“[^16A]“は1、6、A以外で少なくとも1文字を含む文字列にマッチします（例”abc“）。1、6、Aを含む文字列(例”m16“)はマッチするが、1、6、Aのみの文字列（例1、16、16A）はマッチしません。
{n}	正の整数のn回の文字列にマッチします。	“o{2}”は“food”にマッチするが、“Bob”にマッチしません。
{n,}	正の整数のn回以上の文字列にマッチします。	“o{2,}”は“foooood”にマッチするが、“Bob”にマッチしません。
{n,m}	正の整数のnからm回以上の文字列にマッチします。mはnm以上の整数です。	“o{1,3}”は“fod”、“food”、“fooood“にマッチするが、“fd”にマッチしません。
\<	文字列の最初からマッチします。 \<の次の文字列のパターンを含みますが、英数字、アンダーバーは含まれません。	”\<do”は”domain”、”doa”にマッチします。
\>	文字列の最後からがstringにマッチします。\>の次の文字列のパターンを含みますが、英数字、アンダーバーは含まれません。	”do\>”は”undo”や"cdo"にマッチします。

文字	意味	例
\b	[^A- Za-z0-9_]に等しい文字列にマッチします。 英数字、アンダーラインは含みます。	“\ba”は“-a”にマッチするが、“2a”、“ba”にマッチしません。
\B	[A- Za-z0-9_]に等しい文字列にマッチします。 英数字、アンダーラインは含みません。	“\Bt”は“install”にマッチするが、“big top”にマッチしません。
\w	\Bと同一です。	“v\w”は“"vlan”、“service”にマッチします。
\W	\bと同一です。	“\Wa”は“-a”にマッチするが、"2a"、"ba"にマッチしません。
\	エスケープ文字です。この表に記載された特殊文字が\に続くと、その文字を取り除くことを意味します。	”\\”は、”\”を含む文字列にマッチします。”\^”は、”^”を含んでいる文字列にマッチ、”\\b”は”\b”を含んでいる文字列とマッチします。

例：

display current-configuration コマンドで**| begin line** を使用し、**line** を含むコマンド以降の display current-configuration 情報を表示します。デフォルトでは **line class aux** 以降が表示されます。

```
<Switch> display current-configuration | begin line
line class aux
 user-role network-admin
#
line class vty
 user-role network-operator
#
line aux 0
 user-role network-admin
#
line vty 0 63
 authentication-mode none
 user-role network-admin
 user-role network-operator
#
...
```

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

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

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

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

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

display logbuffer コマンドで**| include SHELL | include VTY** を使用し、**SHELL** と **VTY** の両方を含むログバッファのログエントリを表示します。

```
<Switch> display logbuffer | include SHELL | include VTY
%Sep   6 10:38:12:320 2018 Sysname SHELL/5/SHELL_LOGIN: VTY logged in from
169.254.100.171.
%Sep   6 10:52:32:576 2018 Sysname SHELL/5/SHELL_LOGOUT: VTY logged out from
169.254.100.171.
%Sep   6 16:03:27:100 2018 Sysname SHELL/5/SHELL_LOGIN: VTY logged in from
169.254.100.171.
%Sep   6 16:44:18:113 2018 Sysname SHELL/5/SHELL_LOGOUT: VTY logged out from
169.254.100.171.
```

1.7.4 display コマンドのファイルへの保存

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

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

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

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

操作	コマンド
コマンドからファイルを分離して出力を保存する	**display** *command* **>** *filename*
ファイルの最後に出力を追記する	**display** *command* **>>** *filename*

例：

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

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

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

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

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

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

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

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

1.7.5 display コマンドからの出力の有効的な表示、管理

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

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

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

操作	コマンド
displayコマンドからの出力の有効的な表示、管理を組み合わせる	**display** *command* [| [**by-linenum**] { **begin** | **exclude** | **include** } *regular-expression*]&<1-128> [**>** *filename* | **>>** *filename*]

例：

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

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

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

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

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

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

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

1.8 稼働中の設定の保存

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

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

目次

このセクションのページは **1-x-x** です。

2 章 ログイン.....2-1

2章 ログイン

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

表 2-1 ログイン方法の概要

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

ログイン方法	デフォルト設定、必要最低限の設定
SNMPからのアクセス	デフォルトではSNMPによるアクセスはできません。 SNMPによるアクセスを可能にする為には、以下の設定が必要です。 ● レイヤ3インタフェースにIPアドレスを設定し、インタフェースとNMS間で通信可能なことを確認します。 ● SNMPの基本パラメータを設定します。

目次

このセクションのページは **1-x-x** です。

3 章 コンソールポートによる最初のログイン 3-1

3章 コンソールポートによる最初のログイン

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

コンソールポートから装置にログインするには、コンソール端末（例 PC）と端末エミュレータ（例 Windows の HyperTerminal）などのユーザ端末の関連設定をコンソールポートと同じにしなければなりません。 Windows 8.1 などその他の Windows OS ではサードパーティの端末エミュレータを取得し、インストールする必要があります。ほかの端末エミュレータの使い方については、各ツールのユーザーズガイドあるいはオンラインヘルプを見てください。

コンソールポートでログインする場合は以下の手順に従ってください。

1) PC のシリアルポートに D-sub 9 ピンメスコネクタを接続します。
2) コンソールケーブルの RJ-45 コネクタを装置のコンソールポートに接続します。

⚠ **重要**：

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

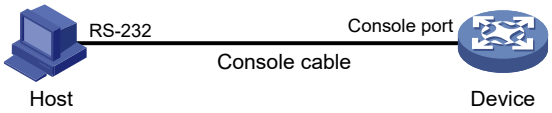


図 3-1 コンソールポートとの接続

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

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

図 3-2から図 3-4は Windows のハイパーターミナルでの設定を示します。Windows 8.1 などその他の Windows OS や、ほかの OS ではサードパーティの端末エミュレータを起動してください。

a) スタートボタンをクリックします。

b)　メニューからすべてのプログラム ＞ アクセサリ ＞ 通信 ＞ハイパーターミナルを選択します。

PC のシリアルポートと装置のコンソールポートにコンソールケーブルが接続されていることを確認します。

a)　デスクトップにあるマイコンピュータアイコンを右クリックします。

b)　コンピュータ管理ウィンドウ画面で管理を選択します。

c)　ナビゲーションツリーからシステムツール＞デバイスマネージャーを選択します。

d)　ポート（COM＆LPT）を選択します。



図 3-2 接続の作成



図 3-3 シリアルポートの設定

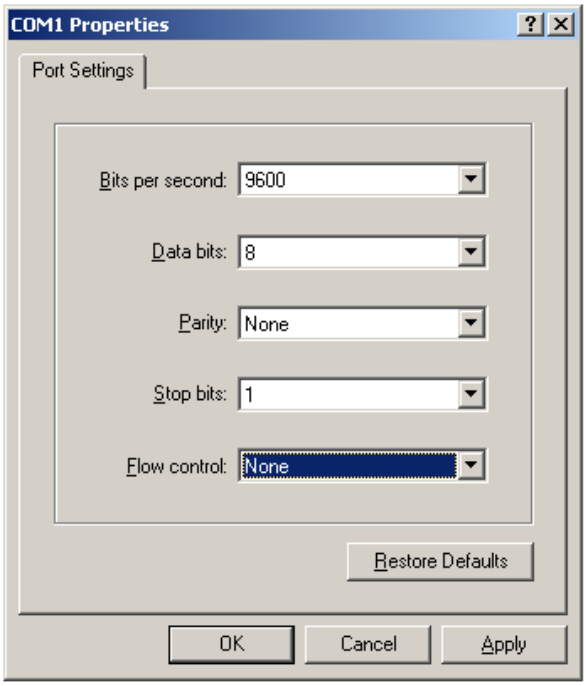


図 3-4 シリアルポートのプロパティの設定

5) 装置の電源を入れます。POST（power-on self test）が正常終了すると、**Enter** を押すように指示されます。

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

目次

このセクションのページは **1-x-x** です。

4章 CLIによるログイン 4-1
4.1 CLI概要 4-1
4.1.1 ユーザライン 4-1
4.1.2 ログイン認証モード 4-2
4.1.3 ユーザロール 4-2
4.2 コンソールポートからのローカルログイン 4-3
4.2.1 None認証の設定 4-4
4.2.2 Password認証の設定 4-4
4.2.3 Scheme認証の設定 4-5
4.2.4 AUXユーザラインの共通設定 4-6
4.3 Telnetからのログイン 4-8
4.3.1 装置のTelnetログインの設定 4-8
4.3.2 装置からTelnetサーバへのTelnet接続 4-14
4.4 SSHからのログイン 4-15
4.4.1 SSHログインの設定 4-15
4.4.2 装置からSSHサーバへのSSH接続 4-17
4.5 CLIログインの表示と維持 4-18

4章 CLI によるログイン

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

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

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

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

4.1 CLI概要

4.1.1 ユーザライン

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

ユーザは、表 4-1のようにログイン方法に依存した異なるユーザラインに割り当てられます。

表 4-1 CLI ログイン方法とユーザライン

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

I. ユーザラインの識別化

各ユーザラインは、識別化のため絶対値と相対値を持っています。

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

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

II. ユーザラインの割り当て

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

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

4.1.2 ログイン認証モード

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

装置は以下のログイン認証モードをサポートしています。

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

異なるログイン認証モードは、表 4-2のようにユーザラインで異なる設定が必要です。

表 4-2 異なるログイン認証で必要な設定

認証モード	操作
None	認証モードを**none**に設定します。
Password	1. 認証モードを **password** に設定します。 2. パスワードを設定します。
Scheme	1. 認証モードを **scheme** に設定します。 2. ISP domain view でログイン認証方法を設定します。詳細はオペレーションマニュアルのセクション *7 セキュリティ”AAA”* を参照してください。

4.1.3 ユーザロール

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

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

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

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

4.2 コンソールポートからのローカルログイン

図 4-1のように装置にログインし、管理するため、コンソールポートに端末を接続することができます。ログイン手順については、オペレーションマニュアルのセクション 1 *はじめに*”*コンソールポートによる最初のログイン*”を参照してください。

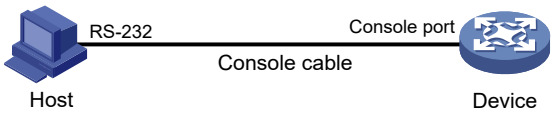


図 4-1 コンソールポートによるログイン

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

コンソールログインを設定するため、以下の作業が完了している必要があります。

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

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

4.2.1 None 認証の設定

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

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

4.2.2 Password 認証の設定

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

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

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

🕮 **メモ：**

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

4.2.3 Scheme 認証の設定

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

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

Scheme 認証を使用するため、以下の設定を完了してください。

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

詳細はオペレーションマニュアルのセクション 7 *セキュリティ*”*AAA*”を参照してください。

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

4.2.4 AUX ユーザラインの共通設定

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

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

以下に AUX ユーザラインの共通設定を示します。

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

操作	コマンド	備考
2. AUX line view あるいは class view に移行する	● AUX line viewに移行する： **line aux** *first-number* [*last-number*] ● AUX line class viewに移行する： **line class aux**	どちらか一方を使用します。 User line viewでの設定はユーザラインのみ適用されます。 User line class viewでの設定はclassのすべてのユーザに適用されます。 どちらかの設定がデフォルトから変更された場合、他のviewのデフォルト設定よりも優先されます。 User line viewの設定がデフォルトから変更された場合、user line class viewでデフォルトから変更された設定よりも優先されます。 user line viewでの設定はオンラインユーザにすぐに適用されます。 User line class viewでの設定は、設定が完了したのち、ログインしたユーザに適用されます。
3. ボーレートを設定する	**speed** *speed-value*	デフォルト：9600 bps このコマンドはAUX line class viewで設定できません。
4. パリティチェックモードを指定する	**parity** { **even** | **mark** | **none** | **odd** | **space** }	デフォルト：**none**（パリティチェックなし） このコマンドはAUX line class viewで設定できません。
5. ストップビットを設定する	**stopbits** { **1** | **1.5** | **2** }	デフォルト：**1** ストップビットは文字の最後を示すビットの長さを設定します。ストップビットが多いと転送が遅くなります。 このコマンドはAUX line class viewで設定できません。
6. データビットを設定する	**databits** { **5** | **6** | **7** | **8** }	デフォルト：**8** 文字コードタイプに依存します。たとえば7に設定されると標準ASCII文字が送信され、8に設定すると拡張ASCII文字が送信されます。 このコマンドはAUX line class viewで設定できません。
7. エスケープキーを設定する	**escape-key** { *key-string* | **default** }	デフォルト：CTRL+C
8. 端末タイプを設定する	**terminal type** { **ansi** | **vt100** }	デフォルト：ANSI 装置はANSIとvt100の2つの端末タイプをサポートします。端末で適した表示を保証するため、両方のタイプを設定し、装置と端末の両方のタイプをvt100に設定することを推奨します。 そうでなければコマンドラインが80文字超えてしまい、カーソル位置がエラーとなる場合や、異常な端末表示となる場合があります。
9. 画面に表示できる最大行数を設定する	**screen-length** *screen-length*	デフォルト：最大24行 出力の最大行を0とすると画面の表示は停止しません。

操作	コマンド	備考
10．コマンド履歴バッファのサイズを設定する	**history-command max-size** *value*	デフォルト：10
11．ユーザラインのタイムアウトの時間を設定する	**idle-timeout** *minutes* [*seconds*]	デフォルト：10分 タイムアウト時間内に、ユーザラインで何も実行されないと自動的にユーザラインの接続が終了します。タイムアウト機能を無効にする場合、0に設定してください。
12．ユーザが現在のuser lineにログインしたとき、自動で実行されるコマンドを設定する	**auto-execute command** *command*	デフォルト：無効 ユーザが現在のuser lineにログインしたとき、装置は自動で指定されたコマンドを実行します。コマンドが実行されたのち、ユーザの接続を切断します。 このコマンドはAUX line viewあるいはAUX line class viewでサポートしていません。
13．端末サービスを有効にする	**shell**	デフォルト：有効 AUX line viewあるいはAUX line class viewでコマンドは**undo shell**サポートしていません。

4.3 Telnetからのログイン

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

デフォルトでは Telnet からのログインはできません。Telnet を使用する場合、以下の作業を行ってください。

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

4.3.1 装置の Telnet ログインの設定

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

操作	備考
（オプション設定項目）VTYユーザラインの共通設定	–

I. Telnet サーバの有効化

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

II. None 認証の設定

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

None 認証モードを有効とすると、図 4-2のように次回 Telnet で装置にログインを行う場合、ユーザ名あるいはパスワードを必要としません。ログインユーザ数が最大である場合はログインに失敗し、"All user lines are used, Please try later!"のメッセージが表示されます。

```
<Switch>
```

図 4-2 None 認証の Telnet 接続

III. Password 認証の設定

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

Password 認証モードを有効とすると、図 4-3のように次回 Telnet で装置にログインを行う場合、パスワードが必要となります。ログインユーザ数が最大である場合はログインに失敗し、" All user lines are used, please try later!"のメッセージが表示されます。

```
Password:
<Switch>
```

図 4-3 Password 認証による Telnet 接続

IV. Scheme 認証の設定

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

Scheme 認証を行うため、以下の作業を完了してください。

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

詳細はオペレーションマニュアルのセクション7 *セキュリティ ”AAA”* を参照してください。

Scheme 認証の設定を行うと、図 4-4ように次回 Telnet で装置にログインを行う場合、ユーザ名、パスワードが必要となります。ログインユーザ数が最大である場合はログインに失敗し、"All lines are used, please try later!"のメッセージが表示されます。

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

図 4-4 Scheme 認証による Telnet 接続

V. 現在の Telnet ユーザの最大数の設定

操作	コマンド	備考
1. system view に移行する	**system-view**	―
2. 現在の Telnet ユーザの最大数を設定する	**aaa session-limit telnet** *max-sessions*	デフォルト：32 オンライン中のTelnetユーザには影響しません。現在のオンライン中のTelnetユーザ数が、新しく設定した最大数以上である場合、オンラインユーザがログアウトするまで新規にログインすることができません。このコマンドの詳細は、コマンドマニュアルのセクション7 *セキュリティ ”AAA”* を参照してください。

VI. 出力 telnet パケットの DSCP 値の設定

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

以下に出力 telnet パケットの DSCP 値の設定を示します。

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

VII. VTY ユーザラインの共通設定

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

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

以下に VTY ユーザラインの共通設定を示します。

操作	コマンド	備考
1. system view に移行する	**system-view**	―
2. VTY line view または VTY line class view に移行する	• VTY line viewに移行する：**line vty** *first-number* [*last-number*] • VTY line class viewに移行する：**line class vty**	どちらか一方を使用します。 User line viewでの設定はユーザラインのみ適用されます。 User line class viewでの設定はclassのすべてのユーザに適用されます。 どちらかの設定がデフォルトから変更された場合、他のviewのデフォルト設定よりも優先されます。 User line viewの設定がデフォルトから変更された場合、user line class viewでデフォルトから変更された設定よりも優先されます。 user line viewでの設定はオンラインユーザにすぐに適用されます。 User line class viewでの設定は、ログイン中のユーザには適用されません。次にログインするユーザのみ適用されます。
3. 端末サービスを有効にする	**shell**	デフォルト：有効
4. 指定したユーザラインでサポートするプロトコルを設定する	**protocol inbound** { **all** | **ssh** | **telnet** }	デフォルト：all 次回のログイン時に適用されます。 VTY line viewでは、**authentication-mode**コマンドに関連します。 • VTY line viewの設定がデフォルトから変更された場合、VTY line viewの他の設定が適用されます。 • VTY line viewで両方の設定がデフォルトである場合、VTY line class viewの設定が適用されます。
5. エスケープキーを設定する	**escape-key** { *key-string* | **default** }	デフォルト：CTRL+C

操作	コマンド	備考
6. 端末タイプを設定する	**terminal type** { **ansi** | **vt100** }	デフォルト：ANSI
7. 画面に表示できる最大数を設定する	**screen-length** *screen-length*	デフォルト：24行 出力の最大行を0とすると画面の表示は停止しません。
8. コマンド履歴のバッファサイズを設定する	**history-command max-size** *value*	デフォルト：10 コマンド履歴のバッファは最大10のコマンドを保存します。
9. ユーザラインのタイムアウト時間を設定する	**idle-timeout minutes** [***seconds***]	デフォルト：10分 タイムアウト時間内に、ユーザラインで何も実行されないと自動的にユーザラインの接続が終了します。 タイムアウト機能を無効にする場合、0に設定します。
10. ユーザラインにログイン後、自動で実行されるコマンドを指定する	**auto-execute command** *command*	デフォルト：ユーザがユーザラインにログインした際に自動的に実行されるコマンドはなし ⚠ **重要：** user lineにこのコマンドを実行すると、user lineによるCLIアクセスができなくなる可能性があります。このコマンドを設定する前に、異なるuser lineあるいはAUX user lineによってCLIにアクセスできることを確認してください。

4.3.2 装置から Telnet サーバへの Telnet 接続

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



図 4-5 装置から Telnet サーバへの Telnet 接続

以下に装置から Telnet サーバへのログインの設定を示します。

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

操作	コマンド	備考
2．（オプション設定項目） Telnet パケットの送信元 IPv4 アドレス/インタフェースを指定する	**telnet client source** { **interface** *interface-type interface-number* | **ip** *ip-address* }	デフォルト : 送信元IPv4アドレス/インタフェースは設定なし、送信元アドレスとして出力インタフェースのプライマリIPv4アドレスが使われます。
3． user view へ戻る	**quit**	—
4． Telnet サーバへのログインする	• IPv4 Telnet サーバへのログイン： **telnet** *remote-host* [*service-port*] [**source** { **interface** *interface-type interface-number* | **ip** *ip-address* }] [**dscp** *dscp-value*] • IPv6 Telnet サーバへのログイン： **telnet ipv6** *remote-host* [**-i** *interface-type interface-number*] [*port-number*] [**dscp** *dscp-value*]	—

4.4 SSHからのログイン

SSH は、より強固なセキュリティを持ったログイン方法です。強力な暗号化と認証機能によって IP スプーフィング攻撃、パスワード傍受なども防止することができます。詳細はオペレーションマニュアルのセクション 7 *セキュリティ*”*SSH*”を参照してください。

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

デフォルトでは SSH からのログインはできません。SSH を使用する場合、SSH 以外の他のログイン方法を用いて、初回に SSH からログインできるように設定を行う必要があります。

4.4.1 SSH ログインの設定

この章では SSH クライアント認証が password である場合の手順を示します。SSH、公開鍵認証の設定の詳細は、オペレーションマニュアルのセクション7 *セキュリティ*”*SSH*”、“*公開鍵*”を参照してください。

以下に装置から SSH ログインの設定を示します。

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

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

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

4.4.2 装置から SSH サーバへの SSH 接続

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



図 4-6 装置から SSH サーバへの SSH 接続

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

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

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

SSH サーバを動作させるためには、SSH クライアントの設定を行う必要があります。SSH クライアントの設定の詳細は、オペレーションマニュアルのセクション 7 *セキュリティ”SSH*”を参照してください。

4.5 CLIログインの表示と維持

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

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

目次

このセクションのページは **1-x-x** です。

5 章 Web コンソールによるログイン 5-1
5.1 HTTP ログインの設定 5-1
5.2 HTTPS ログインの設定 5-2
5.3 Web ログインの表示と維持 5-3
5.4 Web ログインの設定例 5-4
5.4.1 HTTP ログインの設定例 5-4

5章 Web コンソールによるログイン

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

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

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

5.1 HTTPログインの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. HTTP サービスを有効にする	**ip http enable**	デフォルト：無効
3. （オプション設定項目）HTTP サービスのポート番号を設定する	**ip http port** *port-number*	デフォルト：80
4. （オプション設定項目）Web ユーザの接続のタイムアウトタイマを設定する	**web idle-timeout** *idle-time*	デフォルト：10分
5. （オプション設定項目）オンライン HTTP ユーザの最大数を設定する	**aaa session-limit http** *max-sessions*	デフォルト：32 オンライン中のHTTPユーザには影響しません。現在のオンライン中のHTTPユーザ数が、新しく設定した最大数以上である場合、オンラインHTTPユーザがログアウトするまで新規にログインすることができません。詳細はコマンドマニュアルのセクション*7 セキュリティ”AAA”*を参照してください。
6. ローカルユーザを追加し、local user view に移行する	**local-user** *user-name* [**class manage**]	デフォルト：設定なし

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

5.2 HTTPSログインの設定

装置は HTTPS ログインモードをサポートします。

- **Simplified モード**—装置は自己署名の証明書（装置自身によって作成し署名された証明書）を使用します。装置で HTTPS サービスを有効にしたのち、Simplified モードで動作します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. HTTPS サービスを有効にする	**ip https enable**	デフォルト：無効 HTTPSサービスを有効にすると、SSLハンドシェイクネゴシエーションが開始します。 ● 装置でローカル認証がある場合、SSLハンドシェイクは成功し、HTTPSサービスが開始します。 装置でローカル証明書がない場合、証明書アプリケーション処理が開始します。証明書アプリケーション処理は時間がかかるため、SSLハンドシェイクのネゴシエーションが失敗し、HTTPSサービスが開始しない可能性があります。この問題に対応するためHTTPSサービスが有効になるまで再度コマンドを実行してください。
3. （オプション設定項目）HTTPS サービスのポート番号を設定する	**ip https port** *port-number*	デフォルト：443

操作	コマンド	補足
4．（オプション設定項目）Web 接続のタイムアウトタイマを設定する	**web idle-timeout** *idle-time*	デフォルト：10分
5．（オプション設定項目）オンライン HTTP ユーザの最大数を設定する	**aaa session-limit https** *max-sessions*	デフォルト：32 オンライン中のHTTPSユーザには影響しません。現在のオンライン中のHTTPSユーザ数が、新しく設定した最大数以上である場合、オンラインHTTPSユーザがログアウトするまで新規にログインすることができません。詳細はコマンドマニュアルのセクション*7 セキュリティ”AAA”*を参照してください。
6．ローカルユーザを追加し、local user view に移行する	**local-user user-name** [**class manage**]	デフォルト：設定なし
7．ローカルユーザのパスワードを設定する	**password** { **cipher** | **simple** } *string*	デフォルト: ローカルユーザのパスワードは設定されていません。 プレーンテキストで設定されたパスワードを含めたすべてのパスワードは、暗号化されて保存されます。 セキュリティのためローカルユーザのパスワードを設定してください。
8．ローカルユーザのユーザロールを設定する	**authorization-attribute user-role** *user-role*	デフォルト：network-operator
9．ローカルユーザのサービスタイプを指定する	**service-type https**	デフォルト：設定なし

5.3 Webログインの表示と維持

すべての view で実行可能です。

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

5.4 Webログインの設定例

5.4.1 HTTP ログインの設定例

I. ネットワーク要件

図 5-1に示すように IP ネットワークで通信可能な PC と Device を接続します。HTTP を使用して PC にログインします。



図 5-1 ネットワーク図

II. 設定手順

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

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

HTTP を有効にします。

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

III. 設定の確認

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

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

目次

このセクションのページは **1-x-x** です。

6 章 SNMP によるアクセス..... 6-1

6章 SNMP によるアクセス

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

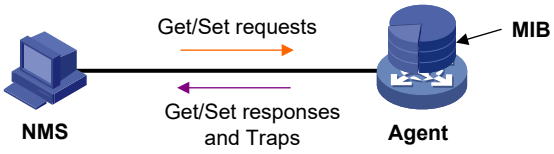


図 6-1 SNMP アクセス

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

SNMP に関する詳細は、オペレーションマニュアルのセクション 9 *システム管理 ”SNMP”* を参照してください。

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

目次

このセクションのページは **1-x-x** です。

7 章 ログインユーザの制御 7-1
7.1 Telnet/SSH ログインの制御 7-1
7.1.1 設定手順 7-1
7.1.2 設定例 7-2
7.2 Web ログインの制御 7-2
7.2.1 送信元 IP アドレスベースの Web ログインの制御 7-3
7.2.2 オンライン Web ユーザのログオフ 7-3
7.2.3 設定例 7-3
7.3 SNMP ログインの制御 7-4
7.3.1 設定手順 7-4
7.3.2 設定例 7-6

7章 ログインユーザの制御

不正なアクセスを防ぐため ACL(Access Control List)を使用し、ユーザのふるまいを監視および制御を行うため、コマンドの許可、アカウンティングの設定を行います。ACL の詳細は、オペレーションマニュアルのセクション 6 *ACL and QoS* ”*ACL*”を参照してください。

7.1 Telnet/SSHログインの制御

Telnet、SSH ログインをフィルタするため ACL を使用します。

- **標準 ACL（2000～2999）**－送信元 IP アドレスを使用します。
- **拡張 ACL（3000～3999）**－送信元 IP アドレス、宛先 IP アドレスを使用します。
- **L2 ACL（4000～4999）**－送信元 MAC アドレスを使用します。

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

7.1.1 設定手順

以下に Telnet ログインを制御する設定を示します。

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

以下に SSH ログインを制御する設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	－
2． SSH ログインをフィルタする ACL を適用する	• **ssh server acl** [**mac**] *acl-number* • **ssh server ipv6 acl** [**ipv6** | **mac**] *acl-number*	デフォルト：ACLはなし 詳細はコマンドマニュアルのセクション*7 セキュリティ* ”*SSH*”を参照してください。

メモ：

本設定によるフィルタリングでは暗黙の deny(拒否)が適用されます。

7.1.2 設定例

I. ネットワーク要件

図 7-1に装置が Host A と Host B からの Telnet パケットのみを許可するように設定します。

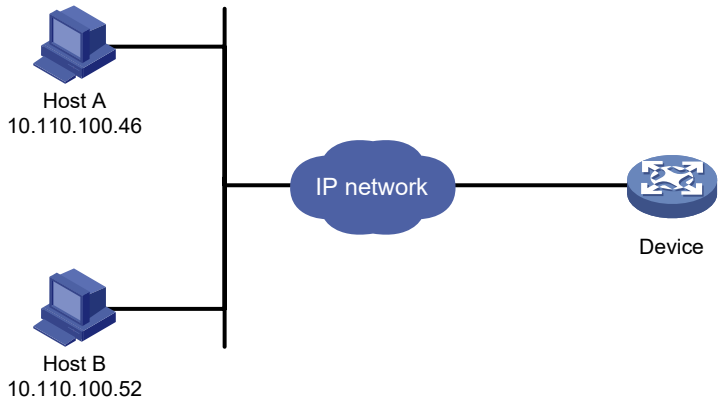


図 7-1 ネットワーク図

II. 設定手順

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

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

Telnet ログインをフィルタするため ACL を適用します。

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

7.2 Webログインの制御

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

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

ログインしている疑わしい Web ユーザをログオフすることもできます。

7.2.1 送信元 IP アドレスベースの Web ログインの制御

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

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

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

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

7.2.2 オンライン Web ユーザのログオフ

以下にオンライン Web ユーザをログオフする設定を示します。

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

7.2.3 設定例

I. ネットワーク要件

図 7-2に示すように Device は HTTP サーバです。Device は Host B のみに HTTP サービスを提供するように設定します。

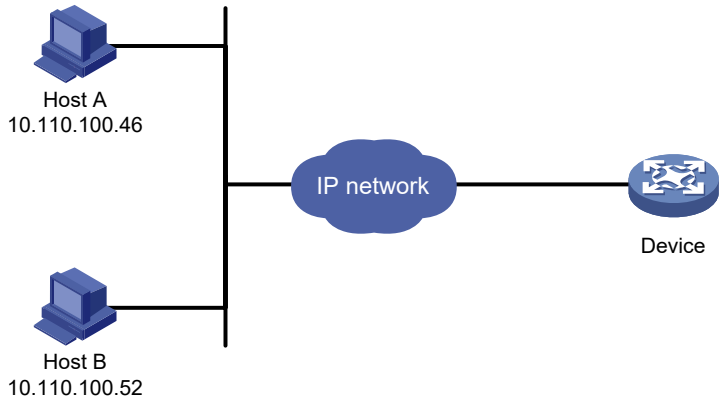


図 7-2 ネットワーク図

II. 設定手順

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

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

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

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

7.3 SNMPログインの制御

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

7.3.1 設定手順

以下に SNMPv1/v2c アクセスを制御する設定を示します。

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

操作	コマンド	補足
2． SNMP v1/v2 コミュニティ、グループ、ユーザに ACL を適用する	● SNMPコミュニティを作成し、ACLを適用する：**snmp-agent community** { **read** | **write** } [**simple** | **cipher**] *community-name* [**mib-view** *view-name*] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } | **acl ipv6** { *ipv6-acl-number* | **name** *ipv6-acl-name* }] * ● SNMPv1/v2cグループを作成し、グループにユーザを追加し、その後ACLを適用する：**snmp-agent group** { **v1** | **v2c** } *group-name* [**read-view** *view-name*] [**write-view** *view-name*] [**notify-view** *view-name*] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } | **acl ipv6** { *ipv6-acl-number* | **name** *ipv6-acl-name* }] * ● SNMPv1/v2cユーザ：**snmp-agent usm-user** { **v1** | **v2c** } *user-name group-name* [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } | **acl ipv6** { *ipv6-acl-number* | **name** *ipv6-acl-name* }] *	SNMPに関する詳細は、オペレーションマニュアルのセクション9 *システム管理" SNMP"* を参照してください。

以下に SNMPv3 アクセスを制御する設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． SNMPv3 グループに ACL を適用する	**snmp-agent group v3** *group-name* [**authentication** | **privacy**] [**read-view** *read-view*] [**write-view** *view-name*] [**notify-view** *view-name*] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } | **acl ipv6** { *ipv6-acl-number* | **name** *ipv6-acl-name* }] *	―
3． SNMPv3 ユーザに ACL を適用する	**snmp-agent usm-user v3** *user-name group-name* [{ **cipher** | **simple** } **authentication-mode** { **md5** | **sha** } *auth-password* [**privacy-mode** { **3des** | **aes128** | **des56** } *priv-password*]] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } | **acl ipv6** { *ipv6-acl-number* | **name** *ipv6-acl-name* }] *	SNMPに関する詳細は、オペレーションマニュアルのセクション9 *システム管理" SNMP"* を参照してください。

🕮 **メモ：**

本設定によるフィルタリングでは暗黙の deny(拒否)が適用されます。

7.3.2 設定例

I. ネットワーク要件

図 7-3のように Device が Host A と Host B からの SNMP のアクセスを許可するように設定します。

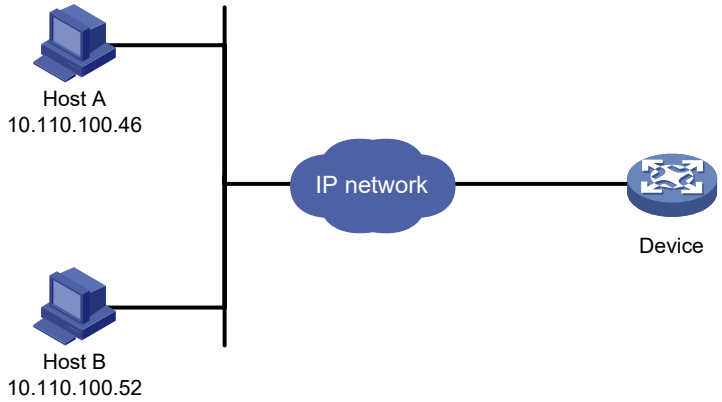


図 7-3 ネットワーク図

II. 設定手順

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

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

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

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

目次

このセクションのページは **1-x-x** です。

8 章 RBAC 8-1
8.1 概要 8-1
8.1.1 許可の割り当て 8-1
8.1.2 ユーザロールの割り当て 8-3
8.2 設定作業リスト 8-4
8.3 ユーザロールの作成 8-4
8.4 ユーザロールのルールの設定 8-5
8.4.1 設定の制限とガイドライン 8-5
8.4.2 設定手順 8-5
8.5 機能グループの設定 8-6
8.6 リソースアクセスポリシーの変更 8-6
8.6.1 ユーザロールのインタフェースポリシーの設定 8-7
8.6.2 ユーザロールの VLAN ポリシーの設定 8-7
8.7 ユーザロールの割り当て 8-7
8.7.1 デフォルトユーザロール機能の有効化 8-8
8.7.2 リモート AAA 認証ユーザへのユーザロールの割り当て 8-8
8.7.3 ローカル AAA 認証ユーザへのユーザロールの割り当て 8-8
8.7.4 ユーザラインで非 AAA 認証ユーザへのユーザロールの割り当て 8-9
8.8 一時的なユーザロールの許可設定 8-10
8.8.1 設定ガイドライン 8-10
8.8.2 ユーザロールの認証の設定 8-11
8.8.3 一時的なユーザロールの許可の取得 8-11
8.9 RBAC 設定の表示と維持 8-12
8.10 RBAC の設定例 8-13
8.10.1 ローカル AAA 認証ユーザの RBAC の設定例 8-13
8.10.2 RADIUS 認証ユーザの RBAC の設定例 8-15
8.10.3 RBAC の一時的なユーザロールの許可の設定例 8-19
8.11 RBAC のトラブルシューティング 8-22
8.11.1 ローカルユーザで許可していないコマンドにアクセスできる 8-22
8.11.2 RADIUS ユーザによるログインがいつも失敗する 8-23

8章 RBAC

8.1 概要

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

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

8.1.1 許可の割り当て

以下の方法により、ユーザロールに許可を割り当てることができます。

- アクセス可能か不可能か決定するためのルールを定義します。（オペレーションマニュアルのセクション 1 *はじめに ”RBAC”の ”ユーザロールのルール”* を参照してください。）
- リソースがユーザロールにアクセス可能かどうかを決定するためのリソースアクセスポリシーを定義します。（オペレーションマニュアルのセクション 1 *はじめに ”RBAC”の ”リモートアクセスポリシー”* を参照してください）

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

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

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

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

I. ユーザロールのルール

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

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

コマンドは以下のタイプによって制御します。

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

ユーザロールは、ユーザロールのルールで許可された指定コマンドセットにアクセスできます。ユーザロールは定義済みのユーザロール（*sys-n* で識別されます）とユーザ定義のユーザロールがあります。ユーザロールのルールの優先順位は、オペレーションマニュアルのセクション 1 *はじめに”RBAC”の”ユーザロールのルールの設定*”を参照してください。

II. リソースアクセスポリシー

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

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

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

III. 定義済みユーザロール

システムには定義済みのユーザロールがあります。すべてのユーザロールはすべてのシステムリソース（インタフェース、VLAN）にアクセスできますが、これらのコマンドはアクセス許可とは異なります。表 8-1を参照してください。

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

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

- Level-0～Level-14 のユーザは、**display history-command all** コマンドを除いて自身の許可を変更することができます。

表 8-1 定義済みユーザロールと許可

ユーザロール名	許可
network-admin	システムのすべての機能とリソースにアクセス可能です。**display security-logfile summary**コマンド、**info-center security-logfile directory**コマンド、 **security-logfile save**コマンドを除きます。
network-operator	• すべての機能の**display**コマンドとリソースにアクセス可能です。ユーザロールでアクセス可能なコマンドを表示する場合、**display role**コマンドを使用します。 • 自身のパスワードを変更するため、ローカルユーザへのローカル認証が有効です。
level-*n* (*n* = 0 ～ 15)	• **level-0**– **ping**、**tracert**、**telnet** 、**ssh2**、**super**コマンドを含む診断コマンドにアクセスできます。**level-0**のアクセス権は設定可能です。 • **level-1**– **level-0**のコマンドに加えて**display history-command all**コマンドを除く**display**コマンドとリソースが使用可能です。**level-0**のアクセス権は設定可能です。 • **level-2**～**level-8**、**level-10** ～**level-14**– デフォルトでアクセス権はありません。アクセス権は設定可能です。 • **level-9**– 以下の機能を除いたすべての機能とリソースにアクセス可能です。ユーザロールが**level-9**のローカルユーザアカウントのユーザにログインした場合、自身のアカウントのパスワードを変更することができます。**level-9**のアクセス権は設定可能です。 • RBAC-非デバッグコマンド • ローカルユーザ • ファイル管理 • 装置管理 • **display history-command all**コマンド • **level-15**– network-adminと同じアクセス権があります。

8.1.2 ユーザロールの割り当て

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

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

ユーザロールの割り当ては認証方法に応じて、以下の方法があります。

- **AAA 許可**– scheme 認証が使用されている場合、AAA モジュールはユーザロールの割り当てを操作できます。

- □ ユーザがローカル認証にパスした場合、装置はローカルユーザアカウントで指定されたユーザロールを割り当てます。
- □ ユーザがリモート認証にパスした場合、ユーザにサーバで指定したユーザロールを割り当てます。AAA サーバは RADIUS サーバを使用できます。

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

AAA、SSH の詳細は、オペレーションマニュアルのセクション 7 *セキュリティ*”*AAA*”、”*SSH*”を参照してください。ユーザラインの詳細は、オペレーションマニュアルのセクション 1 *はじめに*”*ログイン*”、”*CLI によるログイン*”を参照してください。

8.2 設定作業リスト

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

8.3 ユーザロールの作成

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

以下にユーザロールを作成する手順を示します。

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

8.4 ユーザロールのルールの設定

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

8.4.1 設定の制限とガイドライン

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

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

8.4.2 設定手順

以下にユーザロールのルールの設定を示します。

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

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

8.5 機能グループの設定

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

以下に機能グループの設定を示します。

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

8.6 リソースアクセスポリシーの変更

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

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

8.6.1 ユーザロールのインタフェースポリシーの設定

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

8.6.2 ユーザロールの VLAN ポリシーの設定

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

8.7 ユーザロールの割り当て

システムにユーザロールを管理するため、少なくとも 1 つのユーザロールを割り当てる必要があります。装置または、サーバによって少なくとも 1 つのユーザロールが割り当てられていることを確認してください。ユーザロールはリモート AAA 認証ユーザ、ローカル AAA 認証ユーザ、AAA 認証を行わないユーザで割り当てる手順が異なります。AAA 認証の詳細は、オペレーションマニュアルのセクション 7 *セキュリティ ”AAA”* を参照してください。

8.7.1 デフォルトユーザロール機能の有効化

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

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

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

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

8.7.2 リモート AAA 認証ユーザへのユーザロールの割り当て

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

🕮 **メモ：**

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

8.7.3 ローカル AAA 認証ユーザへのユーザロールの割り当て

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

以下にローカルユーザにユーザロールを割り当てる設定を示します。

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

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

8.7.4 ユーザラインで非 AAA 認証ユーザへのユーザロールの割り当て

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

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

ユーザラインの詳細は、オペレーションマニュアルのセクション 1 *はじめに*”*ログイン*”、”*CLI によるログイン*”を参照してください。SSH の詳細は、オペレーションマニュアルのセクション 7 *セキュリティ*”*SSH*”を参照してください。

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

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

8.8 一時的なユーザロールの許可設定

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

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

8.8.1 設定ガイドライン

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

- ユーザが装置に再接続をしないで別のユーザロールを取得するため、ユーザロール認証を設定する必要があります。表 8-2に有効な認証モードと設定要件を記載します。
- RADIUS 認証が使用されている場合、以下のルールを適用します。
  - 装置はユーザロールの認証を要求するためのユーザ名を使用せず、**$enab*n*$**のフォーマットを使用します。*n* はユーザロールレベルです。ドメイン名はユーザ名に含まれません。パスワードが正しい場合、ユーザロールの認証にパスすることができます。
  - level-*n* のユーザロールを取得するため、RADIUS サーバで**$enab*n*$**のフォーマットで level-*n* のユーザのユーザアカウントを作成する必要があります。*n* はターゲットのユーザロールのレベルです。たとえば、level-3 のユーザロールを取得する場合、ユーザ名を入力します。装置はサーバからユーザロール認証を要求するため、ユーザ名**$enab3$**を使用します。
  - 非 level-n のユーザロールを取得するため、以下の処理を行う必要があります。
    - サーバでユーザアカウント**$enab0$**を作成します。
    - **allowed-roles="***role***"**の形式のアカウントの cisco-av-pair 属性を設定します。変数のロールはターゲットのユーザロールを示します。
- 装置は以下の順番でユーザロール認証の認証ドメインを選択します。

a) 入力されたユーザ名が含まれるISPドメイン

b) デフォルトISPドメイン

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

表 8-2 ユーザロールの認証モード

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

キーワード	認証モード	記述
scheme	RADIUSによるリモートAAA認証（remote-only）	装置はリモート認証を行うためRADIUSサーバにユーザ名とパスワードを送信します。 このモードを使用するため、以下の設定を実行する必要があります。 ● 要求されたRADIUS scheme、ユーザのschemeを使用するISP domainを設定します。詳細は*オペレーションマニュアル*のセクション*7 セキュリティ”AAA””*を参照してください。 ● RADIUSサーバにユーザアカウントとパスワードを追加します。
local scheme	最初にローカルパスワード認証を行い、次にリモートAAA認証を行う（local-then-remote）	最初にローカルパスワード認証が実行されます。ローカルパスワードが設定されていない場合、以下となります。 ● 装置はVTYユーザ用にリモートAAA認証を実行します。 ● AUXユーザは文字列を入力するか、何も入力しないでEnterキーを押すことで一時的なユーザロールを取得することができます。
scheme local	最初にリモートAAA認証を行い、次にローカルパスワード認証を行う（remote-then-local）	最初にAAA認証が実行されます。ローカルパスワード認証は以下のいずれかの状況で実行されます。 ● リモートRADIUSサーバからの応答がありません。 ● 装置でのAAAの設定が無効です。

8.8.2 ユーザロールの認証の設定

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

8.8.3 一時的なユーザロールの許可の取得

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

user view で以下の設定を行います。

操作	コマンド	補足
ユーザロールを使用した一時的な許可を取得する	**super** [*role-name*]	[*role-name*]を指定しない場合一時的なユーザロールの許可のデフォルトターゲットユーザロールを取得します。 3回連続してパスワードの認証に失敗すると、ユーザロールの取得に失敗します。 現在のユーザロールが**super**コマンドを実行できることを確認してください。 次の両方の条件が存在する場合、非level-nのユーザロールへの切り替えに失敗する可能性があります。 ● ユーザロールスイッチング認証は、現在のログインユーザと同じISPドメインで実行されます。 ● ユーザロールスイッチング認証は、ISPドメイン用に設定されたログイン認証方法とは異なるAAA方法を使用します。 AAAの詳細は、オペレーションマニュアルのセクション7 *セキュリティ*を参照してください。

8.9 RBAC設定の表示と維持

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

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

8.10 RBACの設定例

8.10.1 ローカル AAA 認証ユーザの RBAC の設定例

I. ネットワーク要件

図 8-1に示すように、装置は Telnet ユーザ用にローカル AAA 認証を実行します。Telnet ユーザはユーザ名 **user1@bbb** を持ち、ユーザロール **role1** を割り当てます。

role1 に以下の許可を設定します。

- すべての機能の **read** コマンドを実行します。
- VLAN10～VLAN20 のみアクセスできるようにします。

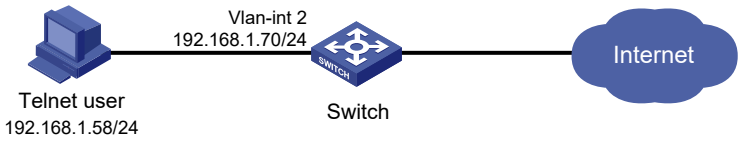


図 8-1 ネットワーク図

II. 設定手順

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

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

Telnet サーバを有効にします。

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

Telnet ユーザのユーザラインで scheme 認証を有効にします。

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

ISP ドメイン **bbb** 用にローカル認証、許可を有効にします。

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

ユーザロール **role1** を作成します。

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

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

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

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

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

VLAN ポリシーを変更して、ユーザロールが VLAN 10～VLAN 20 のみを設定できるようにします。

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

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

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

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

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

サービスタイプを Telnet に設定します。

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

ユーザにユーザロール **role1** を割り当てます。

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

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

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

III. 設定の確認

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

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

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

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

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

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

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

機能の書き込みあるいは実行コマンドが使用できないことを確認します。

```
<Switch> debugging role all
Permission denied.
<Switch> ping 192.168.1.58
Permission denied.
```

8.10.2 RADIUS 認証ユーザの RBAC の設定例

I. ネットワーク要件

図 8-2に示すように、装置は Free RADIUS サーバを使用し、Telnet ユーザを含むログインユーザに AAA サービスを提供します。Telnet ユーザはユーザ名 **hello@bbb** を持ち、ユーザロール **role2** が割り当てられます。

ユーザロール **role2** に以下の許可を設定します。

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

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

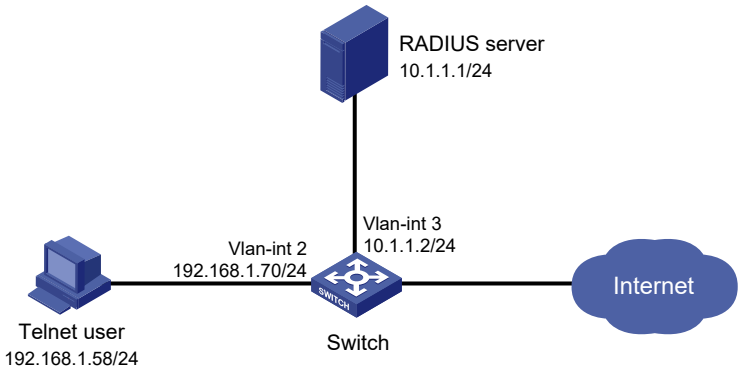


図 8-2 ネットワーク図

II. 設定手順

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

1)　Switch を設定します。

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

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

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

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

Telnet サーバを有効にします。

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

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

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

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

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

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

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

サーバに認証するサーバ用に scheme で専用の共有鍵を設定します。

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

ISP ドメイン **bbb** 用の認証、許可 scheme として scheme **rad** を指定し、ログインユーザのアカウンティングを実行しないように ISP ドメインを設定します。

⚠ **重要**：

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

```
[Switch] domain bbb
[Switch-isp-bbb] authentication login radius-scheme rad
[Switch-isp-bbb] authorization login radius-scheme rad
[Switch-isp-bbb] accounting login none
[Switch-isp-bbb] quit
```

機能グループ **fgroup1** を作成します。

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

機能グループに機能 **arp**、**radius** を追加します。

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

ユーザロール **role2** を作成します。

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2)　RADIUS サーバを設定します。

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

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

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

III. 設定の確認

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

ISP view で有効なすべてのコマンドが使用できることを確認します。

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

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

```
[Switch] radius scheme rad
[Switch-radius-rad] primary authentication 2.2.2.2
[Switch-radius-rad] display radius scheme rad
...
```

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

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

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

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

8.10.3 RBAC の一時的なユーザロールの許可の設定例

I. ネットワーク要件

図 8-3に示すように、装置はログインユーザ用にローカル認証を実行します。Telnet ユーザはユーザ名 **test@bbb** を持ち、ユーザロール **level-0** が割り当てられます。

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

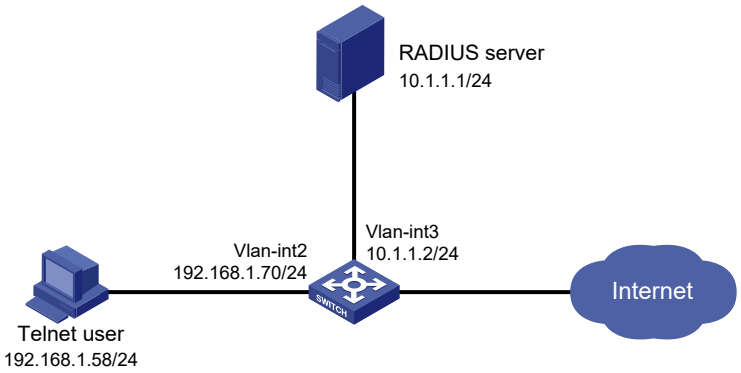


図 8-3 ネットワーク図

II. 設定手順

1)　Switch を設定します。

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

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

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

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

Telnet サーバを有効にします。

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

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

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

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

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

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

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

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

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

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

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

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

```
[Switch] domain bbb
```

ISP ドメイン **bbb** を設定して、ログインユーザ認証に RADIUS scheme **radius** を使用します。

```
[Switch-isp-bbb] authentication login radius-scheme radius
```

ISP ドメイン **bbb** を設定して、ログインユーザ許可に RADIUS scheme **radius** を使用します。

```
[Switch-isp-bbb] authorization login radius-scheme radius
```

ログインユーザのアカウンティングを実行しないように ISP ドメイン **bbb** を設定します。

```
[Switch-isp-bbb] accounting login none
```

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

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

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

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

2)　RADIUS サーバを設定します。

（詳細は省略します）

III. 設定の確認

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

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

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

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

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

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

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

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

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

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

出力はユーザロール network-admin を取得したことを示します。

8.11 RBACのトラブルシューティング

この章では、一般的な RBAC 問題と解決方法について記載します。

8.11.1 ローカルユーザで許可していないコマンドにアクセスできる

I. 症状

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

II. 分析

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

III. 解決策

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

8.11.2 RADIUS ユーザによるログインがいつも失敗する

I. 症状

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

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

II. 分析

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

III. 解決策

以下の方法で問題を解決します。

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

2) 問題が解決しない場合、NEC に問い合わせてください。

目次

このセクションのページは **1-x-x** です。

9 章 FTP 9-1
9.1 FTP サーバの使用 9-1
9.1.1 認証および許可の設定 9-2
9.1.2 FTP 接続の手動解放 9-3
9.1.3 FTP サーバの表示と維持 9-3
9.2 FTP クライアントの使用 9-3
9.2.1 FTP 接続の確立 9-3
9.2.2 FTP サーバのディレクトリの管理 9-4
9.2.3 FTP サーバの動作 9-4
9.2.4 別のユーザアカウントへの変更 9-5
9.2.5 FTP 接続の維持とトラブルシューティング 9-6
9.2.6 FTP 接続の終了 9-6
9.2.7 表示コマンドとヘルプ情報 9-6
9.2.8 FTP クライアントの表示と維持 9-6

9章 FTP

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

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



図 9-1 FTP アプリケーションのシナリオ

FTP は、2 つのモードでファイルを送信します。

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

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

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

FTP 動作モードは、以下のモードがあります。

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

FTP 動作モードは、FTP クライアントのプログラムによって変わります。

9.1 FTPサーバの使用

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

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. FTP を有効にする	**ftp server enable**	デフォルト：無効
3. （オプション設定項目）FTP サーバのアクセス管理を行うため ACL を使用する	**ftp server acl** { *ipv4-acl-number* | **ipv6** *ipv6-acl-number* }	デフォルト：設定なし

操作	コマンド	補足
4.　（オプション設定項目）idle-timeout タイマを設定する	**ftp timeout** *minutes*	デフォルト：30分 アイドルタイムアウト時間内にFTPサーバとFTPクライアント間で情報のやり取りがなければ、FTP接続は終了します。
5.　（オプション設定項目）送信 FTP パケットの DSCP 値を設定する	• IPv4で動作するFTPサーバ： **ftp server dscp** *dscp-value* • IPv6で動作するFTPサーバ： **ftp server ipv6 dscp** *dscp-value*	デフォルト：0
6.　（オプション設定項目）現在のログインユーザの最大数を設定する	**aaa session-limit ftp** *max-sessions*	デフォルト：32 この変更はオンラインユーザに影響しません。FTPユーザの現在の数が新しい設定の値以上ならば、オンラインユーザがログアウトするまで、どの追加のFTPユーザもログインすることができません。詳細はコマンドマニュアルのセクション7 *セキュリティ”AAA”*を参照してください。

9.1.1 認証および許可の設定

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

以下の認証モードが有効です。

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

以下の許可モードが有効です。

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

認証と許可の詳細は、コマンドマニュアルのセクション 7 *セキュリティ”AAA”*を参照してください。

9.1.2 FTP 接続の手動解放

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

9.1.3 FTP サーバの表示と維持

すべての view で **display** コマンドを実行できます。

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

9.2 FTPクライアントの使用

9.2.1 FTP 接続の確立

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

以下に IPv4 FTP 接続を確立する設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． （オプション設定項目）送信 FTP パケットの送信元 IP アドレスを設定する	**ftp client source** { **interface** *interface-type interface-number* | **ip** *source-ip-address* }	デフォルト：送信元IPアドレスは、出力インタフェースのプライマリIPアドレスが使用されます。
3． user view へ戻る	**quit**	―
4． FTP サーバにログインする	• （アプローチ1）user viewから直接FTPサーバにログインする： **ftp** [*ftp-server* [*service-port*] [**dscp** *dscp-value* | **source** { **interface** *interface-type interface-number* | **ip** *source-ip-address* }]] * • （アプローチ2） FTP client viewからFTPサーバにログインする： • **ftp** • **open** *server-address* [*service-port*]	**ftp**コマンドで指定された送信元IPアドレスは、**ftp client source**コマンドで指定されたアドレスより優先されます。

以下に IPv6 FTP 接続を確立する設定を示します。

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

9.2.2 FTP サーバのディレクトリの管理

操作	コマンド
FTPサーバのディレクトリあるいはファイル情報を表示する	● FTPサーバのディレクトリあるいはファイルの詳細情報を表示する： **dir** [*remotefile* [*localfile*]] ● FTPサーバのディレクトリ名あるいはファイル名を表示する： **ls** [*remotefile* [*localfile*]]
FTPサーバの作業ディレクトリを変更する	**cd** { *directory* | **..** | */* }
現在のディレクトリを終了して、上位レベルのディレクトリに移行する	**cdup**
FTPサーバの現在のディレクトリを表示する	**pwd**
FTPサーバにディレクトリを作成する	**mkdir** *directory*
リモートFTPサーバで指定した作業ディレクトリを削除する	**rmdir** *directory*

9.2.3 FTP サーバの動作

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

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

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

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

9.2.4 別のユーザアカウントへの変更

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

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

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

9.2.5 FTP 接続の維持とトラブルシューティング

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

9.2.6 FTP 接続の終了

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

9.2.7 表示コマンドとヘルプ情報

以下にサーバにログインした後、ヘルプ情報を表示するコマンドを示します。

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

9.2.8 FTP クライアントの表示と維持

すべての view で **display** コマンドを実行します。

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

目次

このセクションのページは **1-x-x** です。

10 章 TFTP 10-1
10.1 IPv4 TFTP クライアントの設定 10-1
10.2 IPv6 TFTP クライアントの設定 10-2

10章 TFTP

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

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



図 10-1 TFTP アプリケーションシナリオ

10.1 IPv4 TFTPクライアントの設定

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

10.2 IPv6 TFTPクライアントの設定

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

目次

このセクションのページは **1-x-x** です。

11 章 ファイルシステム管理 11-1
11.1 概要 11-1
11.1.1 ファイルシステム 11-1
11.1.2 ディレクトリ 11-2
11.1.3 ファイル 11-2
11.1.4 ディレクトリ、ファイル名の指定 11-3
11.2 ファイルシステムの管理の制限とガイドライン 11-4
11.3 ファイルシステムの管理 11-4
11.3.1 記憶媒体のフォーマット 11-4
11.3.2 記憶媒体の回復 11-4
11.4 ディレクトリの管理 11-4
11.4.1 ディレクトリ情報の表示 11-4
11.4.2 カレント作業ディレクトリの表示 11-5
11.4.3 カレント作業ディレクトリの変更 11-5
11.4.4 ディレクトリの作成 11-5
11.4.5 ディレクトリ名の変更 11-5
11.4.6 ディレクトリのアーカイブ（圧縮）/解凍 11-5
11.4.7 ディレクトリの削除 11-6
11.4.8 ディレクトリの動作モードの設定 11-6
11.5 ファイルの管理 11-6
11.5.1 ファイル情報の表示 11-6
11.5.2 テキストファイルの内容表示 11-6
11.5.3 ファイル名の変更 11-7
11.5.4 ファイルのコピー 11-7
11.5.5 ファイルの移動 11-7
11.5.6 ファイルの圧縮/解凍 11-7
11.5.7 ファイルのアーカイブ（圧縮）/解凍 11-7
11.5.8 ファイルの削除/回復 11-8
11.5.9 ごみ箱のファイルを削除する 11-8
11.5.10 ファイルの動作モードの設定 11-8

11章 ファイルシステム管理

11.1 概要

11.1.1 ファイルシステム

この章では、記録媒体、ディレクトリ（フォルダとも呼ばれます）、ファイルを含む装置のファイルシステムを管理する方法を示します。

⚠ **重要**：

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

⚠ **注意**：

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

I. 記憶媒体の命名ルール

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

⚠ **重要**：

- 記憶媒体の名前とスロットの文字列は、小文字で記憶媒体名を入力してください。
- ディレクトリ名とファイル名は大文字小文字を区別しません。

II. ファイルの位置情報

ファイルシステムの位置は **slot*n*#**形式で指定できます。n は装置のスロット番号を表し、1 に固定されています。

III. デフォルトファイルシステム

装置にログインしたのち、デフォルトではデフォルトファイルシステムで動作します。デフォルトファイルのファイルあるいはディレクトリを指定する場合、ファイルシステム名を指定する必要はありません。たとえば、ルートディレクトリに保存する場合、位置情報を指定する必要がありません。デフォルトファイルシステムを変更する場合、Boot ROM メニューを使用します。詳細は*インスタレーションマニュアル*を参照してください。

11.1.2 ディレクトリ

ファイルシステムのディレクトリはツリー形状に構成されます。

I. ルートディレクトリ

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

II. 作業ディレクトリ

作業ディレクトリはカレントディレクトリと呼ばれます。

III. ディレクトリ命名ルール

ディレクトリの名前を指定する場合、以下のルールに従ってください。

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

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

IV. 共通使用ディレクトリ

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

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

11.1.3 ファイル

I. ファイル命名ルール

ファイルの名前を指定する場合、以下のルールに従ってください。

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

アスタリスク（*）、垂直バー（|）、スラッシュ（/）、バックスラッシュ（\）、クエスチョンマーク（?）、左アングルブラケット（<）、右アングルブラケット（>）、ダブルクォーテーションマーク（"）、コロン（:）

- ドット（.）で始まるファイルは隠しファイルです。システムがファイルを隠さないようにするため、ドット（.）で始まるファイル名を指定しないでください。

II. 共通使用ファイル

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

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

11.1.4 ディレクトリ、ファイル名の指定

I. ディレクトリの指定

ディレクトリを指定する場合、絶対パスあるいは相対パスを使用することができます。たとえば、作業ディレクトリは **flash:/**です。図 11-1 の **test2** ディレクトリを指定する場合、以下の方法を使用することができます。

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



図 11-1 ディレクトリ階層の例

II. ファイルの指定

ファイルを指定する場合、以下の方法に従います。

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

たとえば、作業ディレクトリは **flash:/**です。ファイル **samplefile.cfg** は、図 11-1 の **test2** ディレクトリにあります。ファイル **samplefile.cfg** を指定する場合、以下の方法を使用することができます。

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

11.2 ファイルシステムの管理の制限とガイドライン

フォーマットまたは修復中の記憶媒体にはアクセスできません。

ファイルシステム、ディレクトリ、およびファイルを管理する前に、考えられる影響を確認してください。

11.3 ファイルシステムの管理

11.3.1 記憶媒体のフォーマット

注意：

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

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

user view で以下の操作を実行します。

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

11.3.2 記憶媒体の回復

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

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

user view で以下の操作を実行します。

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

11.4 ディレクトリの管理

11.4.1 ディレクトリ情報の表示

user view で以下の操作を実行します。

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

11.4.2 カレント作業ディレクトリの表示

user view で以下の操作を実行します。

操作	コマンド
カレント作業ディレクトリを表示する	**pwd**

11.4.3 カレント作業ディレクトリの変更

user view で以下の操作を実行します。

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

11.4.4 ディレクトリの作成

user view で以下の操作を実行します。

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

11.4.5 ディレクトリ名の変更

user view で以下の操作を実行します。

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

11.4.6 ディレクトリのアーカイブ（圧縮）/解凍

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

user view で実行可能です。

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

11.4.7 ディレクトリの削除

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

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

user view で以下の操作を実行します。

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

11.4.8 ディレクトリの動作モードの設定

ファイルシステムには、次のディレクトリの動作モードがあります。

- **alert**：ファイルの破損やデータの損失など、望ましくない結果をもたらす恐れのある操作についてシステムが警告を出します。
- **quiet**：ごみ箱を空にする操作以外のファイルまたはディレクトリ操作を実行する時に、システムは警告を出しません。

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

以下にディレクトリの動作モードの設定を示します。

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

11.5 ファイルの管理

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

11.5.1 ファイル情報の表示

user view で以下の操作を実行します。

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

11.5.2 テキストファイルの内容表示

user view で以下の操作を実行します。

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

11.5.3 ファイル名の変更

user view で以下の操作を実行します。

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

11.5.4 ファイルのコピー

user view で以下の操作を実行します。

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

11.5.5 ファイルの移動

user view で以下の操作を実行します。

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

11.5.6 ファイルの圧縮/解凍

user view で以下の操作を実行します。

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

11.5.7 ファイルのアーカイブ（圧縮）/解凍

tar extract コマンドに **screen** を指定するには、最初に **tar list** コマンドを使用してアーカイブファイルのタイプを識別します。ベストプラクティスとして、すべてのアーカイブファイルがテキストファイルである場合にのみ指定します。端末制御文字を含むアーカイブされた非テキストファイルのコンテンツを表示すると、文字化けが発生し、端末が正しく動作しなくなる場合があります。ターミナルを再度使用するには、現在の接続を閉じて、装置に再度ログインする必要があります。

user view で実行可能です。

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

操作	コマンド
アーカイブされたファイルのリストを表示する	**tar list archive-file** *file*

11.5.8 ファイルの削除/回復

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

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

user view で以下の操作を実行します。

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

⚠ **重要**：

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

11.5.9 ごみ箱のファイルを削除する

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

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

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

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

11.5.10 ファイルの動作モードの設定

ファイルシステムには、次のファイルの動作モードがあります。

- **alert**：ファイルの破損やデータの損失など、望ましくない結果をもたらす恐れのある操作についてシステムが警告を出します。
- **quiet**：ごみ箱を空にする操作以外のファイルまたはディレクトリ操作を実行する時に、システムは警告を出しません。

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

以下にファイルの動作モードの設定を示します。

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

目次

このセクションのページは **1-x-x** です。

12 章 コンフィグレーションファイル管理 12-1
12.1 概要 12-1
12.1.1 コンフィグレーションタイプ 12-1
12.1.2 次回の起動に使用するスタートアップコンフィグレーションファイルの冗長 . 12-2
12.1.3 コンフィグレーションファイルのフォーマット形式 12-2
12.1.4 スタートアップコンフィグレーションファイルの選択..... 12-2
12.1.5 コンフィグレーションファイルの内容とフォーマット..... 12-3
12.2 2 つのコンフィグレーション設定の差分表示 12-4
12.3 カレントコンフィグレーションの保存..... 12-4
12.3.1 カレントコンフィグレーションの保存方法..... 12-4
12.4 次回の起動に使用するスタートアップコンフィグレーションファイルの設定 12-5
12.5 TFTP サーバへスタートアップコンフィグレーションファイルのバックアップ 12-6
12.6 TFTP サーバからスタートアップコンフィグレーションファイルの復元 12-7
12.7 次回の起動で使用するスタートアップコンフィグレーションファイルの削除 12-7
12.8 コンフィグレーションファイルの表示と維持..... 12-8

12章 コンフィグレーションファイル管理

12.1 概要

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

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

12.1.1 コンフィグレーションタイプ

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

以下にコンフィグレーションファイルの種類を示します。

I. デフォルトコンフィグレーション

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

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

II. スタートアップコンフィグレーション

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

- 今回の起動に使用したスタートアップコンフィグレーションと次回の起動で使用するスタートアップコンフィグレーションの設定を表示するには、**display startup** コマンドを使用します。詳細な設定を表示する場合、**more** コマンドを使用します。
- 次回の起動で使用するスタートアップコンフィグレーションファイルの内容を表示するには、**display saved-configuration** コマンドを使用します。次回の起動で使用するコンフィグレーションファイルが保存されていない場合は表示されません。

III. カレントコンフィグレーション

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

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

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

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

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

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

12.1.3 コンフィグレーションファイルのフォーマット形式

コンフィグレーションファイルは、以下のフォーマット形式となります。

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

12.1.4 スタートアップコンフィグレーションファイルの選択

起動時、装置は以下の順番でコンフィグレーションファイルを識別します。

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

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

12.1.5 コンフィグレーションファイルの内容とフォーマット

⚠ **重要**：

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

コンフィグレーションファイルは以下の規則に従います。

- すべてのコマンドは省略されていない正しい形式のフォーマットで保存されます。
- 無効な文字を含むコマンドラインはありません。

⚠ **重要**：

一部のコマンドライン（**sysname** コマンドなど）には、疑問符（?）または水平タブ（\t）を含めることができません。システムが **sysname abc ??**を含むコンフィグレーションファイルを読み込む場合、起動時のコマンドラインでは、システムはコマンドラインを無視し、デフォルトのシステム名を使用します。システムがそのコンフィグレーションファイルを使用してロールバックまたは復元する場合、システム名はロールバックまたは復元されません。

- コマンドは異なる view 毎にセクションに分かれて区別されています。通常は system view、interface view、protocol view、line view などの順番です。
- セクションは、1 行または複数行のブランク行またはコメント行（#）で区切られます。
- 最後に **return** が付きます。

コンフィグレーションファイルを抜粋した例を以下に示します。

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

12.2 2つのコンフィグレーション設定の差分表示

2 つのコンフィグレーションファイルで設定の差分を表示することができます。

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

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

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

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

すべての view で **display** コマンドを実行します。

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

12.3 カレントコンフィグレーションの保存

12.3.1 カレントコンフィグレーションの保存方法

カレントコンフィグレーションを保存するとき、次回に起動するスタートアップコンフィグレーションファイルとして指定することができます。

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

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

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

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

操作	コマンド	補足
指定したファイルに現在の設定を保存します、しかし、コンフィグレーションファイルは次回起動時にファイルとしてセットされません。	**save** *file-url* [**all** | **slot** *slot-number*]	ー
現在の設定をコンフィグレーションファイルに保存し、次回の起動に使用するスタートアップコンフィグレーションファイルに指定する	**save** [**safely**] [**backup** | **main**] [**force**]	このコマンドは記憶媒体のルートディレクトリのファイルに設定を保存します。信頼性のあるファイルの保存を行うため、**safety**パラメータを使用することを推奨します。 **force**パラメータを指定した場合、設定は次回の起動に使用されるコンフィグレーションファイルに保存されます。 **force**パラメータを指定しない場合、次回の起動に使用するスタートアップコンフィグレーションファイルを新規作成します。

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

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

また **startup saved-configuration** *cfgfile* [**backup** | **main**]コマンドを使用して次回の起動で使用するメインあるいはバックアップのスタートアップコンフィグレーションファイルを指定することができます。指定したスタートアップコンフィグレーションファイル

が有効で、各メンバ装置のデフォルトの記憶領域のルートディレクトリに保存されることを確認してください。

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

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

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

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

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

バックアップを行う前に、以下の要件が完了していることを確認してください。

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

たとえば **reset saved-configuration backup** コマンドが行われると、バックアップの次回の起動で使用するスタートアップコンフィグレーションファイルの属性が NULL にな

り、ファイルがメインファイルとして使用されます。ファイルを削除する場合、**reset saved-configuration main** コマンドを行う必要があります。

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

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

12.8 コンフィグレーションファイルの表示と維持

すべての view で **display** コマンドを実行します。

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

目次

このセクションのページは **1-x-x** です。

13 章 ソフトウェアのアップグレード..... 13-1
13.1 概要..... 13-1
13.1.1 ソフトウェアタイプ..... 13-1
13.1.2 ソフトウェアファイル名の規則..... 13-1
13.1.3 Comware イメージの冗長性と読み込み手順..... 13-2
13.1.4 システム起動プロセス..... 13-2
13.2 アップグレード方法..... 13-3
13.3 アップグレードの準備..... 13-4
13.4 アップグレード設定作業リスト..... 13-4
13.5 Boot ROM の Boot ROM イメージへの読み込み..... 13-5
13.6 スタートアップソフトウェアイメージの指定とアップグレードの完了..... 13-5
13.7 ソフトウェア設定の表示と維持..... 13-5

13章 ソフトウェアのアップグレード

13.1 概要

ソフトウェアアップグレードは、新しい機能の追加や不具合を修正するために行います。アップグレードを行う前に、新しいソフトウェアのリリースメモを確認して、装置とソフトウェアの互換性およびアップグレードが与える影響を確認してください。

13.1.1 ソフトウェアタイプ

以下にソフトウェアタイプを示します。

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

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

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

13.1.2 ソフトウェアファイル名の規則

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

13.1.3 Comware イメージの冗長性と読み込み手順

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

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

システムは常にメインソフトウェアで起動を試みます。メインソフトウェアが存在しないあるいは無効である場合、システムはバックアップソフトウェアで起動を試みます。図 13-1に Comware イメージの読み込み手順の全体を示します。

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

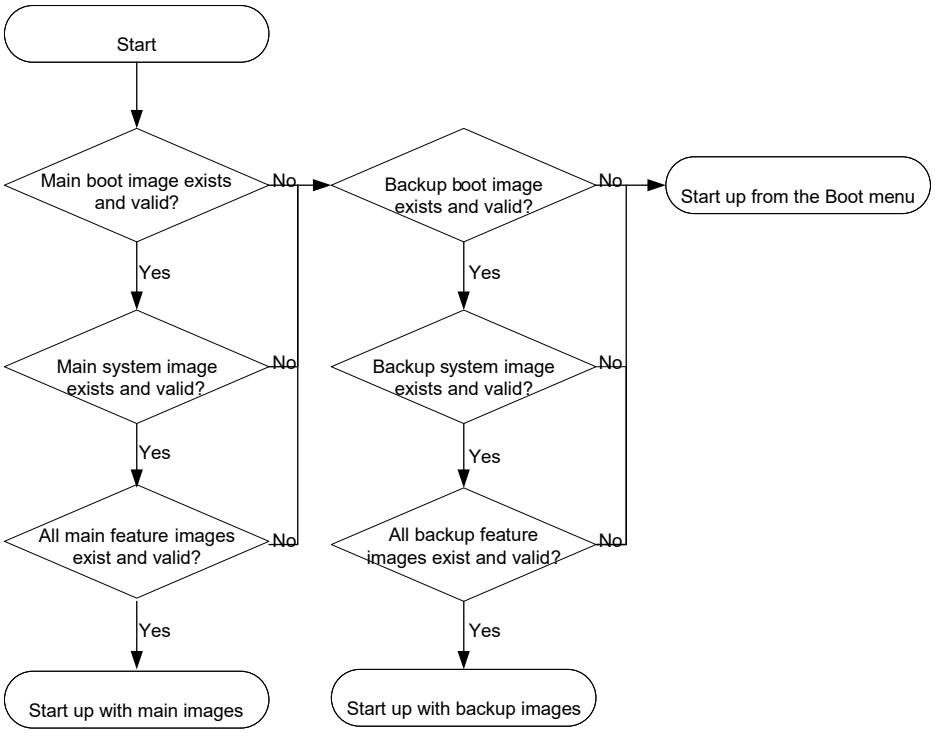


図 13-1 Comware イメージの読み込み手順の全体

13.1.4 システム起動プロセス

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

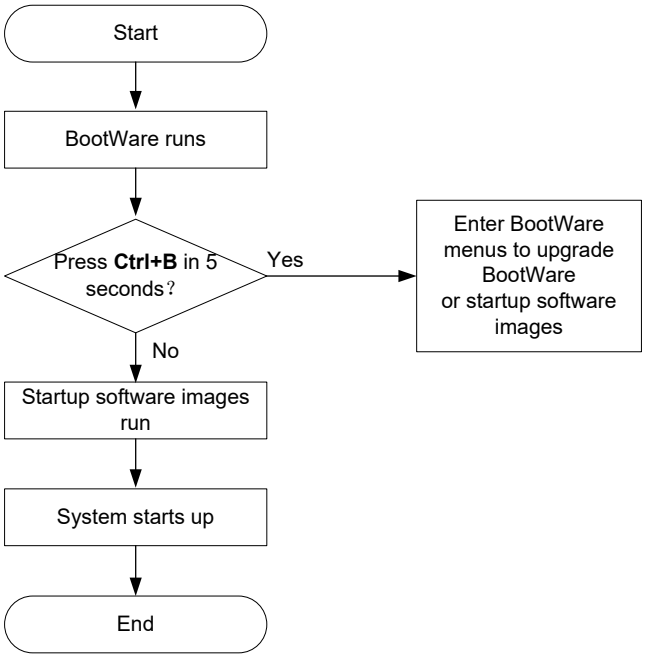


図 13-2 システム起動プロセス

13.2 アップグレード方法

アップグレード方法	ソフトウェアタイプ	補足
CLIからのアップグレード	• Boot ROMイメージ（BootWareイメージ） • Comwareイメージ	アップグレードを完了するため、再起動が必要となります。ネットワークサービスの中断が発生します。
再起動を伴うソフトウェアのアップグレード	• Comwareイメージ	アップグレードを行うため、装置全体の再起動を行ってください。サービスの中断が発生します。
Boot メニューからのアップグレード	• Boot ROMイメージ（BootWareイメージ） • Comwareイメージ	装置が正常に起動しないときに使用します。 最初にコンソールポートに接続し、装置の電源をONにします。その後BootWare メニューにアクセスするため <CTRL+B>を押下します。 BootWareメニューからのアップグレードの詳細は、*インストレーションマニュアル*を参照してください。 ⚠ **重要：** アップデートは、Bootメニューではなく CLIから行ってください。装置を1台ずつアップデートする必要があるため、Bootメニューではサービスの停止時間が増加します。

この章では CLI からのアップグレードのみ記載します。

13.3 アップグレードの準備

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

13.4 アップグレード設定作業リスト

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

13.5 Boot ROMのBoot ROMイメージへの読み込み

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

13.6 スタートアップソフトウェアイメージの指定とアップグレードの完了

user view で以下の操作を実行します。

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

13.7 ソフトウェア設定の表示と維持

すべての view で **display** コマンドを実行します。

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

目次

このセクションのページは **1-x-x** です。

14章 装置管理 14-1
14.1 装置名の設定 14-1
14.2 システムクロックの設定 14-1
14.2.1 システムクロックソースの設定 14-1
14.3 著作権情報表示の有効化 14-3
14.4 バナーの設定 14-3
14.4.1 バナーの種類 14-3
14.4.2 バナー入力モード 14-4
14.4.3 設定手順 14-5
14.5 装置の特定 14-5
14.5.1 装置の特定について 14-5
14.5.2 Power LEDの点滅開始 14-6
14.5.3 Power LEDの点滅停止 14-6
14.6 装置の再起動 14-6
14.6.1 CLIによる装置の即時再起動 14-7
14.6.2 パスワードリカバリ機能の無効化 14-7
14.7 検出間隔の設定 14-8
14.8 CPU使用率のモニタリングの設定 14-8
14.9 メモリ使用しきい値の設定 14-8
14.10 装置の温度アラームのしきい値の設定 14-10
14.11 トランシーバの情報表示と診断 14-13
14.11.1 トランシーバの情報表示 14-13
14.11.2 トランシーバの診断 14-13
14.12 装置管理の情報表示と維持 14-13

14章 装置管理

この章では装置の基本的なパラメータの設定、装置の管理について記載します。

この章の設定操作は、順番に関係なく実行できます。

14.1 装置名の設定

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

以下に装置名を設定する方法を示します。

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

14.2 システムクロックの設定

14.2.1 システムクロックソースの設定

正しいシステムクロックの設定はネットワーク管理と通信に不可欠です。ネットワーク上で使用する前に、システムクロックを正しく設定してください。装置はシステムクロックをローカルに設定するか、NTP クロックソースを使用して UTC 時間を設定することができます。

以下の方法で設定できます。

- **None**－ローカルシステム時間です。CLI を用いて手動でシステム時間を設定します。システム時間を維持するため、装置内部の水晶発振器によって生成されたクロック周波数を使用します。再起動を行うとローカルシステム時間はデフォルトの時刻に戻るため、再度コマンドで設定してください。
- **NTP**－NTP ソースから定期的に UTC 時間を取得し、UTC 時間、タイムゾーン、およびサマータイムを使用してシステム時間を計算します。NTP を使用した場合、手動でシステム時間を変更できません。NTP についての詳細は、オペレーションマニュアルのセクション 9 *システム管理”NTP*”を参照してください。

QX-S1100G シリーズは、電源 OFF/ON による再起動あるいは **reboot** コマンドを実行した場合、デフォルトの時刻に戻ります。手動でシステム時間を設定している場合は、再度システム時間を設定してください。

NTP クロックソースを使用した方が、ローカルシステムクロックをした場合より精度が高くなります。

以下にローカルシステム時間を使用する設定方法を示します。

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

以下にシステムクロックのソースとして NTP を使用する設定方法を示します。

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

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

14.3 著作権情報表示の有効化

著作権情報の表示を有効にすると、以下の場合、著作権情報が表示されます。

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

以下に著作権情報の表示例を示します。

```
**************************************************************************
* Copyright (c) 2004-2019 New H3C Technologies Co., Ltd. All rights reserved.*
* Without the owner's prior written consent,                             *
* no decompiling or reverse-engineering shall be allowed.                *
**************************************************************************
```

以下に著作権情報表示の有効化の手順を以下に示します。

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

14.4 バナーの設定

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

14.4.1 バナーの種類

装置は以下のバナーをサポートしています。

- **Legal** バナー － 認証情報とも呼ばれます。システムは著作権または権限情報を表示し、ユーザがログインする前にバナーを表示して、ユーザがログインするかどうか確認します。”Y”、または Enter キーを入力すると、ユーザはログインプロセスに入ります。”N”を入力すると、ユーザはログインプロセスを終了します。”Y”、”N”は、大文字でも小文字でもかまいません。

- **Message of the Day**（**MOTD**）バナー – 認証前に表示される welcome information です。legal バナーの後、login バナーの前に表示されます。
- **Login** バナー – ログイン認証時の welcome information です。パスワードと scheme 認証が設定されている場合に表示されます。
- **incoming** バナー – Modem ログインユーザが user view に移行する際に表示されます。認証が必要な場合、認証にパスしたのちバナーが表示されます。
- **Shell** バナー – ログインした後に表示します。

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

14.4.2 バナー入力モード

バナーを設定する場合、1 行入力モードあるいは複数入力モードを使用します。

- 1 行入力モード

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

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

- 複数入力モード

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

複数行を設定する場合以下のいずれかの方法を使用します。

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

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

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

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

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

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

14.4.3 設定手順

以下の手順に従ってバナーの設定を行います。

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

14.5 装置の特定

14.5.1 装置の特定について

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

14.5.2 Power LED の点滅開始

user view で以下のコマンドを実行します。

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

14.5.3 Power LED の点滅停止

user view で以下のコマンドを実行します。

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

🕮 **メモ:**

locator blink コマンドは Version 7.1.9 を含む以降のソフトウェアからサポートしています。

14.6 装置の再起動

⚠ **注意：**

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

以下の方法で装置を再起動できます。

- CLI によるスケジュールリブートを行います。指定した時間に自動的に再起動させることができます。
- CLI による再起動を即時行うことができます。
  この方法では、装置をリモートで再起動できます。
- 再起動中、装置は以下の処理を行います。
  - 装置内部のすべてのチップをリセットします。

- □ 圧縮されているイメージを解凍し、イメージを読み込みます。スタートアップソフトウェアを確認するため、BootWare を使用します。

- システムを初期設定します。
- 電源 ON/OFF による再起動を行います。電源を ON/OFF することでハードウェアも再起動させることができます。ただし、稼働中に装置電源を ON/OFF するため、ハードウェアに影響を及ぼす可能性があります。ハードウェアの再起動が必要な場合を除き、装置電源の ON/OFF は推奨できません。

遠隔ホストから CLI により装置を再起動することができます。

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

14.6.1 CLI による装置の即時再起動

user view で以下のコマンドを実行します。

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

14.6.2 パスワードリカバリ機能の無効化

パスワードリカバリ機能は Boot ROM メニューから装置構成と SDRAM へのアクセスを制御できます。

パスワードリカバリ機能が有効の場合、コンソールからのユーザは認証なしで装置にアクセスでき、新しいパスワードを設定することができます。

パスワードリカバリ機能が無効の場合、コンソールからのユーザは、新しいパスワードを設定する前に、工場出荷コンフィグレーションに戻す必要があります。工場出荷コンフィグレーションに戻すことで、次回に起動で使用するコンフィグレーションファイルを削除します。工場出荷コンフィグレーションはデフォルトコンフィグレーションを読み込んでいない設定になります。

次回起動時に使用するコンフィグレーションファイルにアクセスする不正なユーザからのアクセスを防ぐため、パスワードリカバリ機能を無効にできます。

以下にパスワードリカバリ機能を無効にする設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． パスワードリカバリ機能を無効にする	**undo password-recovery enable**	デフォルト：有効

14.7 検出間隔の設定

特定の環境において、いくつかのプロトコルはポートをシャットダウンします。ポートがシャットダウンした後、装置は検出間隔タイマを開始します。検出間隔が経過した際にポートがまだダウンされている場合、物理的にポートを復旧させます。

以下に検出間隔を設定する方法を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． 検出間隔を設定する	**shutdown-interval** *time*	デフォルト：30秒

14.8 CPU使用率のモニタリングの設定

CPU 使用率を検出するため、装置は以下の処理を行います。

- サンプリング間隔は 1 分間隔です。CPU 使用率のしきい値と CPU 使用率をサンプリングし、サンプル値を比較します。サンプル値が CPU 使用率のしきい値に到達した場合、装置はトラップを送信します。
- CPU 使用率の記録が有効である場合、設定した間隔で CPU 使用率を検出し、保存します。

以下に CPU 使用率のモニタリングの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． CPU 使用率のしきい値を設定する	**monitor cpu-usage threshold** *cpu-threshold* [**slot** *slot-number* [**cpu** *cpu-number*]]	デフォルト：99%
3． CPU 使用率のモニタリングを有効にする	**monitor cpu-usage enable** [**slot** *slot-number* [**cpu** *cpu-number*]]	デフォルト：有効
4． **display cpu-usage history** コマンドの情報取得間隔を設定する	**monitor cpu-usage interval interval** [**slot** *slot-number* [**cpu** *cpu-number*]]	デフォルト：1分
5． user view に戻る	**quit**	ー
6． CPU 使用率の統計情報を表示する	**display cpu-usage** [**slot** *slot-number* [**cpu** *cpu-number*]]	すべてのviewで実行可能です。
7． 表で CPU 使用率履歴の統計情報を表示する	**display cpu-usage history** [**slot** *slot-number* [**cpu** *cpu-number*]]	すべてのviewで実行可能です。

🕮 **メモ：**

monitor cpu-usage interval コマンドは **monitor cpu-usage threshold** コマンドの CPU 使用率を取得する間隔ではありません。**display cpu-usage history** コマンドの情報を取得する間隔です。

14.9 メモリ使用しきい値の設定

メモリ使用率をモニタするため、装置は以下の処理を行います。

- サンプリング間隔は 1 分です。メモリ容量がしきい値に達した場合、装置はトラップを送信します。
- 適切な動作とメモリ使用率を改善するため、装置はリアルタイムにおける空きメモリ容量をモニタリングします。空きメモリ容量がしきい値に達した場合、装置は alarm 通知あるいは alarm-removed 通知を生成し、関連するサービスモジュールあるいはプロセスに送信します。

(メモリ不足をサポートしていない装置上) **display memory** コマンドを使用して、メモリ使用量の情報を表示できます。

(メモリ不足をサポートする装置上) システムは、メモリ不足の空き容量のみを監視します。**display memory** コマンドを使用して、メモリ使用量の情報を表示できます。

(低メモリをサポートするスロットを備えた装置) 低メモリをサポートするスロットの場合、システムは空きメモリ容量のみを監視します。**display memory** コマンドを使用して、メモリ使用量の情報を表示できます。スロットの **LowMem** フィールドが表示される場合、そのスロットはメモリ不足をサポートしています

表 14-1に示すように装置は以下のレベルのしきい値をサポートしています。

表 14-1 Memory alarm 通知と memory alarm-removed 通知

通知	トリガー状況	補足
Early-warning notification	空きメモリ容量が early-warningしきい値以下に達した	early-warning通知を生成して送信した後、early-warningが削除されるまで、システムは追加の early-warning通知を生成して送信しません。
Minor alarm通知	空きメモリ容量がminor alarmしきい値以下に達した	minor alarm通知を作成、送信した後、装置はminor alarmがキャンセルされるまで追加でminor alarm通知を作成、送信しません。
Severe alarm通知	空きメモリ容量がsevere alarmしきい値以下に達した	severe alarm通知を作成、送信した後、装置はsevere alarmがキャンセルされるまで追加でsevere alarm通知を作成、送信しません。
Critical alarm通知	空きメモリ容量がcritical alarmしきい値以下に達した	critical alarm通知を作成、送信した後、装置はcritical alarmがキャンセルされるまで追加でcritical alarm通知を作成、送信しません。
Critical alarm-removed 通知	空きメモリ容量がsevere alarmしきい値以上に達した	ー
Severe alarm-removed 通知	空きメモリ容量がminor alarmしきい値以上に達した	ー
Minor alarm-removed 通知	空きメモリ容量が最初に normal alarmしきい値以上に達した	ー
Early-warning-removed notification	空きメモリ容量が sufficient-memoryしきい値以上に達した	ー

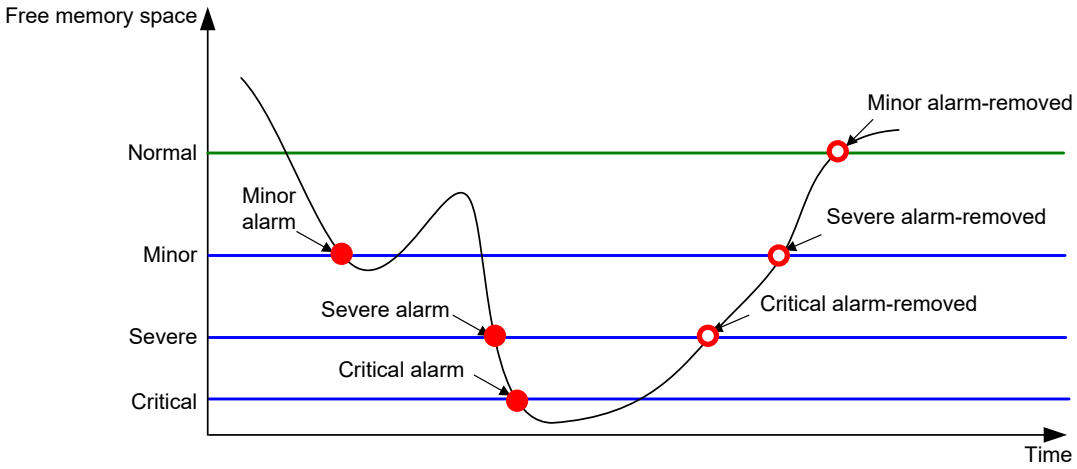


図 14-1 メモリ alarm 通知と alarm-removed 通知

メモリアラームが発生した場合は、未使用の設定アイテムを削除するか、一部の機能を無効にして空きメモリ領域を増やします。メモリ容量が不足しているため、一部の設定項目が削除できない場合があります。

以下にメモリ使用率のしきい値の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． メモリ使用率しきい値を設定する	**memory-threshold** [**slot** *slot-number* [**cpu** *cpu-number*]] **minor** *minor-value* **severe** *severe-value* **critical** *critical-value* **normal** *normal-value*	デフォルト： • **Minor alarm しきい値**– 96 MB • **Severe alarm しきい値**– 64 MB • **Critical alarm しきい値**– 48 MB • **Normal state しきい値**– 128 MB

14.10 装置の温度アラームのしきい値の設定

装置は以下のしきい値をもとに温度をモニタします。

- 下限温度しきい値
- 高温ワーニング温度しきい値
- 高温アラーム温度しきい値

温度が下限温度しきい値を下回った場合、以下の動作を行います。または高温ワーニング温度しきい値、高温アラーム温度しきい値に到達した場合、以下の動作を行います。

- ログメッセージを送信します。
- トラップを送信します。
- 装置の前面にある LED で通知します。

以下に温度アラームしきい値を設定する方法を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． 温度アラームしきい値を設定する	**temperature-limit slot** *slot-number* **hotspot** *sensor-number lowlimit warninglimit* [*alarmlimit*]	デフォルト：表 14-2を参照してください。 ワーニング温度しきい値とアラーム温度しきい値は下限温度しきい値よりも高い温度に設定してください。アラーム温度しきい値はワーニング温度しきい値よりも高い温度に設定してください。

表 14-2 温度アラームのしきい値のデフォルトと推奨値(QX-S1100G シリーズ)

装置	センサ	下限温度	ワーニング温度の推奨	ワーニング温度のデフォルト	アラーム温度の推奨	アラーム温度のデフォルト
QX-S1108GT-2G	Hotspot 1	0	87	84	92	98
	Hotspot 2	0	85	100	90	110
QX-S1116GT-4G	Hotspot 1	0	80	84	85	98
	Hotspot 2	0	88	100	93	110
	Hotspot 3	0	95	100	100	110
QX-S1124GT-4G	Hotspot 1	0	87	84	92	98
	Hotspot 2	0	99	100	104	110
	Hotspot 3	0	105	100	110	110
	Hotspot 4	0	104	100	109	110
QX-S1148GT-4G	Hotspot 1	0	88	84	93	98
	Hotspot 2	0	93	84	98	98
	Hotspot 3	0	108	100	113	110
	Hotspot 4	0	109	100	114	110
	Hotspot 5	0	80	100	85	110
	Hotspot 6	0	84	100	89	110

装置	センサ	下限温度	ワーニング温度の推奨	ワーニング温度のデフォルト	アラーム温度の推奨	アラーム温度のデフォルト
	Hotspot 7	0	83	100	88	110
	Hotspot 8	0	88	100	93	110
QX-S1108GT-2G-PW	Hotspot 1	0	77	84	82	98
	Hotspot 2	0	93	100	98	110
	Hotspot 3	0	87	110	92	130
QX-S1116GT-4G-PW	Hotspot 1	0	72	84	77	98
	Hotspot 2	0	69	100	74	110
	Hotspot 3	0	80	100	85	110
	Hotspot 4	0	78	110	83	130
QX-S1124GT-4G-PW	Hotspot 1	0	63	84	68	98
	Hotspot 2	0	77	100	82	110
	Hotspot 3	0	88	100	93	110
	Hotspot 4	0	87	100	92	110
	Hotspot 5	0	61	100	66	110
	Hotspot 6	0	63	100	68	110
	Hotspot 7	0	71	110	76	130

🕮 **メモ：**

設定温度をデフォルトのしきい値から推奨温度のしきい値に変更することを推奨します。

14.11 トランシーバの情報表示と診断

14.11.1 トランシーバの情報表示

搭載しているトランシーバ（SFP）のタイプ、コネクタの形状、送信するレーザーの中心波長、転送距離、ベンダ名などの情報を表示させることができます。

搭載しているトランシーバの情報表示を行うには、以下の手順に従ってください。

操作	コマンド	補足
トランシーバの情報を表示する	**display transceiver interface** [*interface-type interface-number*]	–

14.11.2 トランシーバの診断

装置はトランシーバモジュールのデジタル診断機能をサポートしていません。

14.12 装置管理の情報表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
システムクロック、日時、タイムゾーン、サマータイムを表示する	**display clock**
CPU使用率の統計情報を表示する	**display cpu-usage** [**slot** *slot-number* [**cpu** *cpu-number*]]
CPU使用率のヒストリ統計情報を図で表示する	**display cpu-usage history** [**slot** *slot-number* [**cpu** *cpu-number*]]
ハードウェアについての情報を表示する	**display device** [**slot** *slot-number* | **verbose**]
装置の製造情報を表示する	**display device manuinfo** [**slot** *slot-number*]
複数のモジュールの動作の統計情報を表示する	**display diagnostic-information** [**hardware** | **infrastructure** | **l2** | **l3** | **service**]
装置の温度情報を表示する	**display environment** [**slot** *slot-number*]
装置のファンの稼動情報を表示する	**display fan** [**slot** *slot-number* [*fan-id*]]
装置のメモリ使用率を表示する	**display memory** [**slot** *slot-number* [**cpu** *cpu-number*]]
装置のメモリ使用率のしきい値を表示する	**display memory-threshold** [**slot** *slot-number* [**cpu** *cpu-number*]]
電源ユニットの状態を表示する	**display power** [**slot** *slot-number* [*power-id*]]
システムバージョンを表示する	**display version**

目次

このセクションのページは **1-x-x** です。

15 章 Python 15-1
15.1 Python shell への移行 15-1
15.2 Python スクリプトの実行 15-1
15.3 Python shell の終了 15-1
15.4 Python 使用例 15-1
15.5 Comware 7 python 拡張 API 15-3
15.5.1 Comware 7 python 拡張 API のインポートと使用 15-3
15.5.2 Comware 7 python 拡張 API 機能 15-3

15章 Python

Python とは汎用プログラミング言語の 1 つで、分かりやすい文法が特徴です。

Python インタプリタは以下の機能をサポートします。

- Python 2.7 コマンド。
- Python 2.7 標準 API。
- Comware 7 拡張 API。詳細はオペレーションマニュアルのセクション 1 *はじめに*"*Python*"の"*Comware 7 python 拡張 API*"を参照してください。
- Python スクリプト。 Python スクリプトを使用して、システム制御が可能です。

15.1 Python shellへの移行

Python コマンドや API を使用するには、Python shell に移行する必要があります。以下に Python shell に移行する方法を示します。

操作	コマンド	補足
user viewからPython shellに移行する	**python**	―

15.2 Pythonスクリプトの実行

以下に user view で python スクリプトを実行する方法を示します。

操作	コマンド	補足
Pythonスクリプトを実行する	**python** *filename*	―

15.3 Python shellの終了

以下に python shell を終了する方法を示します。

操作	コマンド	補足
Python shellを終了する	**exit()**	―

15.4 Python使用例

I. ネットワーク要件

以下を行う Python スクリプトを使用します。

- コンフィグレーションファイル main.cfg と backup.cfg をダウンロードします。

- ダウンロードしたファイルを、次回起動時のメインとバックアップコンフィグレーションファイルに指定します。



図 15-1 ネットワーク図

II. 手順

PC 上でテキストエディタを使用し、以下の python スクリプト test.py を作成します。

```
#!usr/bin/python
import comware

comware.Transfer('tftp', '192.168.1.26', 'main.cfg', 'flash:/main.cfg')
comware.Transfer('tftp', '192.168.1.26', 'backup.cfg', 'flash:/backup.cfg')
comware.CLI('startup   saved-configuration   flash:/main.cfg   main   ;startup
saved-configuration flash:/backup.cfg backup')
```

TFTP を使用し、スクリプトをダウンロードします。

```
<Switch> tftp 192.168.1.26 get test.py
```

スクリプトを実行します。

```
<Switch> python flash:/test.py
<Switch>startup saved-configuration flash:/main.cfg main
Please wait...... Done.
<Switch>startup saved-configuration flash:/backup.cfg backup
Please wait...... Done.
```

III. 確認

スタートアップコンフィグレーションファイルを表示します。

```
<Switch> display startup
 Current startup saved-configuration file: flash:/startup.cfg
 Next main startup saved-configuration file: flash:/main.cfg
 Next backup startup saved-configuration file: flash:/backup.cfg


#!usr/bin/python
import comware

comware.Transfer('tftp', '192.168.1.26', 'main.cfg', 'flash:/main.cfg')
comware.Transfer('tftp', '192.168.1.26', 'backup.cfg', 'flash:/backup.cfg')
comware.CLI('startup   saved-configuration   flash:/main.cfg   main   ;startup
saved-configuration flash:/backup.cfg backup')
```

15.5 Comware 7 python 拡張 API

Comware 7 python 拡張 API は Python syntax と互換性があります。

15.5.1 Comware 7 python 拡張 API のインポートと使用

Comware 7 python 拡張 API を使用するには、python に API をインポートする必要があります。以下のいずれかの方法で、comware 7 拡張 API をインポートして使用する事ができます。

- import comware を使用し、全 API のインポートと comware API を使用する事ができます。例として、拡張 API を使用して、TFPT サーバ 192.168.1.26 から test.cfg をダウンロードします。

<Switch> python

```
Python 2.7.3 (default)
[GCC 4.4.1] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> import comware
>>>  comware.Transfer('tftp',  '192.168.1.26',  'test.cfg',  'flash:/test.cfg',
user='', password='')
<comware.Transfer object at 0xb7eab0e0>
```

- from comware import *API* を使用し、API のインポートと API を使用する事ができます。例として、拡張 API Transfer を使用して、TFTP サーバ 192.168.1.26 から test.cfg をダウンロードします。

<Switch> python

```
Python 2.7.3 (default)
[GCC 4.4.1] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> from comware import Transfer
>>>  Transfer('tftp', '192.168.1.26', 'test.cfg', 'flash:/test.cfg', user='',
password='')
<comware.Transfer object at 0xb7e5e0e0>
```

15.5.2 Comware 7 python 拡張 API 機能

I. CLI class

1) CLI

CLI を実行し、comware 7 CLI コマンドの実行と CLI オブジェクトを作成します。

Syntax

CLI(*command*='', *do_print*=True)

パラメータ

command: 実行するコマンドを指定します。複数のコマンドを実行するには、スペースとセミコロン(;)を区切り文字として使用します。User view 以外の view でコマンドを実行するは、コマンド実行前にその view へ移行する必要があります。たとえば、**local-user test class manage** コマンドを実行するには、'**system-view** ;**local-user test class manage**'を実行しておく必要があります。

do_print: コマンド実行時の出力を行うかどうかを指定します。

- **True**—実行結果を表示します。デフォルト動作です。
- **False**—実行結果を表示しません。

説明

この API は comware コマンドのみサポートします。Linux、Python や TCL コマンドではサポートしません。

返り値

CLI オブジェクト

例

ローカルユーザ test を作成します。

```
<Switch> python
Python 2.7.3 (default)
[GCC 4.4.1] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> import comware
>>> comware.CLI('system-view ;local-user test class manage')
```

出力例

```
<Switch> system-view
System View: return to User View with Ctrl+Z.
[Switch] local-user test class manage
New local user added.
<comware.CLI object at 0xb7f680a0>
```

2) get_output

get_output を使用して、コマンド実行時の出力を得ることができます。

Syntax

CLI.get_output()

返り値

コマンド実行時の出力が返ります。

例

#ローカルユーザを追加し、コマンド出力を得ます。

```
<Switch> python
Python 2.7.3 (default)
[GCC 4.4.1] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> import comware
>>> c = comware.CLI('system-view ;local-user test class manage', False)
>>> c.get_output()
```

出力例

```
['<Switch>system-view', 'System View: return to User View with Ctrl+Z.',
'[Switch]local-user test class manage', 'New local user added.']
```

II. Transfer class

1) Transfer

Transfer を使用して、サーバからファイルをダウンロードします。

Syntax

Transfer(*protocol*='', *host*='', *source*='', *dest*='',*login_timeout*=10, *user*='', *password*='')

パラメータ

protocol: ダウンロードで使用するプロトコルを指定します。

- **ftp**—FTP を使用します。
- **tftp**—TFTP を使用します。
- **http**—HTTP を使用します。

host: リモートサーバの IP アドレスを指定します。

source: リモートサーバからダウンロードするファイル名を指定します。

dest: ダウンロードしたファイルの名前を指定します。

login_timeout: タイムアウト値を秒で指定します。デフォルトは 10 秒です。

user: サーバログイン用のユーザ名を指定します。

password: ログインパスワードを指定します。

返り値

Transfer object

例

test.cfg を TFTP サーバ 192.168.1.26 からダウンロードします。

```
<Switch> python
Python 2.7.3 (default)
[GCC 4.4.1] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> import comware
>>> comware.Transfer('tftp', '192.168.1.26', 'test.cfg', 'flash:/test.cfg',
user='', password='')
```

出力例

```
<comware.Transfer object at 0xb7f700e0>
```

2) get_error

get_error を使用して、ダウンロード時のエラー情報を取得します。

Syntax

Transfer.get_error()

返り値

エラー情報(エラー情報が無ければ、None が返ります。)

例

test.cfg を TFTP サーバ 1.1.1.1 からダウンロードし、エラー情報を取得します。

```
<Switch> python
Python 2.7.3 (default)
[GCC 4.4.1] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> import comware
>>> c = comware.Transfer('tftp', '1.1.1.1', 'test.cfg', 'flash:/test.cfg',
user='', password='')
>>> c.get_error()
```

出力例

```
“Timeout was reached”
```

目次

このセクションのページは **1-x-x** です。

16 章 Auto Config..... 16-1
16.1 一般的なアプリケーションシナリオ 16-1
16.2 Auto Config の動作..... 16-2
16.2.1 DHCP による IP アドレスと設定パラメータの取得 16-2
16.2.2 TFTP サーバからのコンフィグレーションファイルの取得 16-3
16.2.3 コンフィグレーションファイルの適用..... 16-5

16章 Auto Config

Auto Config は、スタートアップコンフィグレーションファイルを設定されていない状態で装置が起動する場合、自動でコンフィグレーションファイルを取得し、適用することを可能にします。Auto Config はネットワークの設定を簡略化し、ネットワーク管理を容易にすることで、メンテナンスの作業負荷を削減することができます。

Auto Config を実装するために、ネットワーク管理者はサーバにコンフィグレーションファイルを保存しておく必要があります。装置は自動でコンフィグレーションファイルを取得し、その設定を適用します。

16.1 一般的なアプリケーションシナリオ

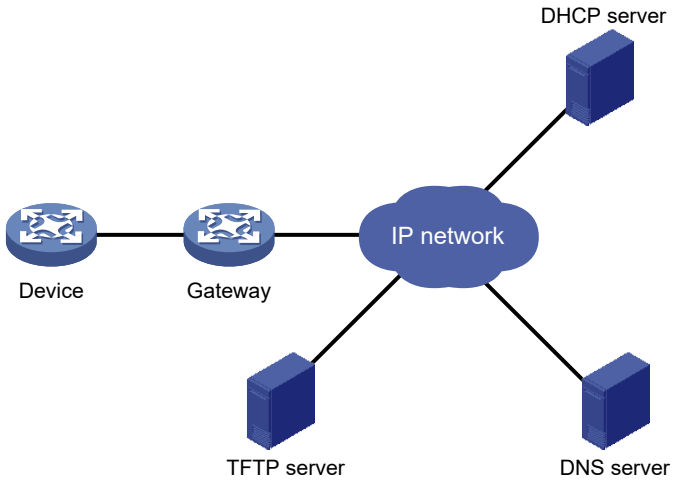


図 16-1 ネットワーク図

図 16-1に示すように、装置は以下のサーバによって Auto Config を実現します。

- **DHCP サーバ** – 装置は IP アドレスと、コンフィグレーションファイル名、TFTP サーバおよび DNS サーバの IP アドレスなどのパラメータを取得します。
- **DNS サーバ** – IP アドレスとホスト名を決定します。装置が DNS サーバを通して対応するホスト名の IP アドレスを解決した場合、TFTP サーバにホスト名と同じ名前を持つコンフィグレーションファイル（hostname.cfg)を要求します。装置が DHCP レスポンスによって TFTP サーバのドメイン名を取得するならば、DNS サーバを通して TFTP サーバのドメイン名から TFTP サーバの IP アドレスを導き出すことも可能です。
- **TFTP サーバ** – Auto Config に必要なファイルを保存しておきます。機器は、ホスト IP アドレスとホスト名のマッピングを含むホスト名ファイル（network.cfg)やコンフィグレーションファイルなど、必要なファイルを TFTP サーバから取得します。

16.2 Auto Configの動作

Auto Config は以下のように動作します。

1) スタートアップ時、装置は VLAN インタフェースを作成し、IP アドレスと TFTP サーバ名、DNS サーバ IP アドレス、およびコンフィグレーションファイル名などを DHCP サーバに要求するための DHCP クライアントにします。

   装置が、IP アドレスまたはコンフィグレーションファイル名を DHCP サーバから得ることに失敗した場合、1 つの IP アドレスと 1 つのコンフィグレーションファイル名を得るまで、機器は要求を繰り返します。

   処理を中断する場合、<CTRL+C>または<Ctrl+D>キーを押下します。

2) 関連するパラメータを取得したのち、装置は指定した TFTP サーバからコンフィグレーションファイルを取得するため、TFTP 要求を送信します。そして取得したコンフィグレーションファイルを適用します。クライアントがコンフィグレーションを取得できない場合、デフォルトコンフィグレーションで起動します。

Auto Config を実現するために、DHCP サーバ、DNS サーバ、TFTP サーバを設定する必要がありますが、Auto Config を行う装置に設定をする必要はありません。

Auto Config を使用する場合、装置を起動させる前に、Auto Config で必要なインタフェースのみをネットワークに接続してください。

16.2.1 DHCP による IP アドレスと設定パラメータの取得

I. アドレス取得プロセス

装置は起動時に DHCP クライアントのために VLAN インタフェースを作成します。

DHCP クライアントは、オプション 55 フィールドでコンフィグレーションファイル名、TFTP サーバのドメイン名と IP アドレス、DNS サーバの IP アドレスなどのクライアントが DHCP サーバから得たい情報を指定し、DHCP 要求をブロードキャストで送信します。

DHCP サーバから DHCP 応答を受信したのち、装置は IP アドレスを取得し、DHCP 応答の以下のフィールドを解決します。

- **オプション 67 あるいは file フィールド**－コンフィグレーションファイル名を取得します。装置は最初にオプション 67 を解決します。オプション 67 にコンフィグレーションファイル名が含まれる場合、装置はファイルフィールドを解決しません。オプション 67 にコンフィグレーションファイル名が含まれない場合、装置は file フィールドを解決します。
- **オプション 66**－TFTP サーバのドメイン名を取得します。
- **オプション 150**－TFTP サーバの IP アドレスを取得します。
- **オプション 6**－DNS サーバの IP アドレスを取得します。

DHCP サーバから DHCP 応答を受信しない場合、装置は一時的なコンフィグレーションを削除し、デフォルトコンフィグレーションで起動します。

一時的なコンフィグレーションは、下記の 2 つです。

- Auto Config を実行するために起動時に設定されたコンフィグレーション
- ホスト名ファイルを使用した際に設定された **ip host** コマンド

DHCP の詳細は、オペレーションマニュアルのセクション 3 *IP サービス*“*DHCP の概要*”を参照してください。**ip host** コマンドの詳細は、コマンドマニュアルのセクション 3 *IP サービス*“*DNS*”を参照してください。

II. DHCP サーバのアドレスプールの選択の基本

DHCP サーバは、クライアント用にアドレスプールから IP アドレスや、ほかのネットワークのコンフィグレーションパラメータを選択します。

DHCP は以下のタイプのアドレスプールをサポートします。

- **ダイナミックアドレスプール** − ダイナミックアドレスプールは、DHCP サーバがクライアントに動的に割り当てる IP アドレス範囲とほかのパラメータが含まれます。
- **スタティックアドレスプール** − スタティックアドレスプールには IP アドレスと MAC アドレス（またはクライアント ID)のバインディングが含まれます。DHCP サーバはバインディングされた IP アドレスと関連するコンフィグレーションパラメータを、MAC アドレスまたは ID がバインディングと一致する要求を持ったクライアントに割り当てます。これにより、クライアントは固定の IP アドレスを取得できます。

以下のいずれかの方法からアドレスプールの使用方法を選んでください。

- 複数の装置が同一のコンフィグレーションファイルを使う場合、同一のコンフィグレーションパラメータ（たとえばコンフィグレーションファイル名)と IP アドレスを装置に割り当てるために DHCP サーバ上のダイナミックアドレスプールを設定することができます。この場合に、コンフィグレーションファイルは装置共通のコンフィグレーションのみを含むことができ、各装置の具体的なコンフィグレーションは、ほかの方法で行う必要があります。たとえば、コンフィグレーションファイルは、管理者が装置で各装置に特定のコンフィグレーション（各インタフェースの IP アドレスを設定など)を実行できるようにするために、Telnet を有効にし、装置のローカルユーザを作成することができます。
- 複数の装置が異なるコンフィグレーションファイルを使用する場合、各装置で固定の IP アドレス、特定のコンフィグレーションファイルを取得できるようにするため、スタティックアドレスプールを設定する必要があります。この方法では装置に追加で設定をする必要はありません。

スタティックアドレスプールを設定するため、対応するクライアント ID を取得する必要があります。クライアント ID を取得する場合、装置が DHCP を通して IP アドレスを取得したのち、DHCP サーバのアドレスの割り当て情報を表示する **display dhcp server ip-in-use** コマンドを使用します。

16.2.2 TFTP サーバからのコンフィグレーションファイルの取得

Auto Config 中、装置は TFTP サーバから以下のファイルを取得することができます。

- DHCP 応答のオプション 67 あるいは file フィールドによって指定されたコンフィグレーションファイルを取得することができます。
- IP アドレスとホスト名のマッピングが記載されているホスト名ファイル network.cfg を取得することができます。

たとえば、ホスト名ファイルには以下が含まれます。

```
ip host host1 101.101.101.101
ip host host2 101.101.101.102
ip host client1 101.101.101.103
ip host client2 101.101.101.104
```

⚠ **重要：**

- ip host の文字列の行の先頭には半角スペースが必要です。
- ホスト名ファイルで定義するホスト名は、該当するホストで使用する予定のコンフィグレーションファイル名と同一にする必要があります。

- ホスト名ファイルで定義されたホスト名とファイル名が一致するコンフィグレーションファイル hostname.cfg を取得することができます。（たとえば、ホスト名が aaa である場合、コンフィグレーションファイル名は aaa.cfg です。）
- デフォルトのコンフィグレーションファイルを取得することができます。デフォルトのコンフィグレーションファイル名は device.cfg です。

I. コンフィグレーションファイルの取得手順

Auto Config は、以下の手順で動作します。

1) レイヤ 2 イーサネットインタフェースのステータスを識別します。1 つ以上のレイヤ 2 イーサネットインタフェースが UP 状態にあるならば、機器はデフォルト VLAN の VLAN インタフェース(vlan1)を使います。
2) すべてのレイヤ 2 イーサネットインタフェースが、Down 状態ならば、機器は 30 秒待った後、ステップ 1 に戻り、リトライします。

II. TFTP 要求の送信モード

装置は以下に示すように TFTP 要求をユニキャストとブロードキャストのどちらで送信するか選択します。

- DHCP 応答に適切な TFTP サーバの IP アドレスが含まれている場合、TFTP サーバに TFTP 要求をユニキャストで送信します。
- DHCP 応答に適切な TFTP サーバの IP アドレスが含まれていない場合、DHCP 応答に含まれる TFTP サーバのドメイン名を解決します。ドメイン名は DNS サーバを使用して IP アドレスにマッピングされます。TFTP サーバのドメイン名の解決が行われた場合、TFTP サーバに TFTP 要求をユニキャストで送信します。TFTP サーバのドメイン名の解決が行われなかった場合、TFTP サーバに TFTP 要求をブロードキャストで送信します。
- DHCP 応答に TFTP サーバの IP アドレス、およびドメイン名が含まれていない、あるいは TFTP サーバが不正である場合、TFTP 要求をブロードキャストで送信します。

TFTP 要求をブロードキャストで送信したのち、コンフィグレーションファイルを取得するため、TFTP 要求に最初に応答した TFTP サーバを選択します。要求したコンフィグレーションファイルが TFTP サーバに存在しない場合、TFTP 要求は失敗します。一時的なコンフィグレーションの設定を削除し、デフォルトコンフィグレーションで起動します。

装置と TFTP サーバが異なるサブネットにある場合、装置からの TFTP 要求をブロードキャストではなく、ユニキャストパケットに変更します。指定した TFTP サーバにユニキャストパケットを送信するため、ゲートウェイで UDP ヘルパーを設定する必要があります。

装置と TFTP サーバが異なるサブネットにある場合、装置からブロードキャストで送信された TFTP 要求をゲートウェイでユニキャストパケットに変更し、ユニキャストパケットを指定された TFTP サーバに転送するように UDP ヘルパー機能を設定する必要があります。

16.2.3 コンフィグレーションファイルの適用

コンフィグレーションファイルを取得したのち、装置は一時的なコンフィグレーションの設定を削除し、取得したコンフィグレーションファイルを適用します。コンフィグレーションファイルを取得していない場合、30 秒待った後、Auto Config を繰り返します。プロセスを止めるために、Ctrl+C または Ctrl+D キーを押してください。

基本的にコンフィグレーションファイルは適用した後に削除されます。**save** コマンドでコンフィグレーションの設定を保存してください。設定を保存せずに再起動をした場合、再起動後に Auto Config が再度実行されます。**save** コマンドの詳細は、コマンドマニュアルのセクション 1 *はじめに “コンフィグレーションファイル管理”* を参照してください。

🕮 **メモ：**

TFTP サーバに保存するコンフィグレーションファイルの末尾に **save force** コマンドを含めることで自動的に保存まで行うことが可能です。

⚠ **重要：**

auto-config 機能で未設定のコマンドは、デフォルト値となります。

QX-S1100G シリーズ Ethernet スイッチ

オペレーションマニュアル

2. アクセス

本マニュアルは以下に示す章で構成されています。

01-Ethernet インタフェース

02-ループバックインタフェースと Null インタフェース

03-Interface range

04-MAC アドレステーブル

05-MAC Information

06-リンクアグリゲーション

07-Port Isolation

08-STP

09-ループ検出

10-VLAN

11-Voice VLAN

12-LLDP

13-L2PT

14-Private VLAN

目次

このセクションのページは**2-x-x** です。

1 章 Ethernet インタフェース 1-1
1.1 Ethernet インタフェースの命名ルール 1-1
1.2 Ethernet インタフェースの共通設定 1-1
1.2.1 コンボインタフェースの設定(QX-S1124GT-4G-PW) 1-1
1.2.2 Ethernet インタフェースの基本設定 1-2
1.2.3 ジャンボフレームの設定 1-3
1.2.4 Ethernet インタフェースの抑制の設定 1-3
1.2.5 Ethernet インタフェースのループバックテストの実行 1-4
1.2.6 インタフェースの一般的なフロー制御の設定 1-5
1.2.7 Ethernet インタフェースの節電機能の有効化 1-5
1.2.8 統計情報のポーリング間隔の設定 1-6
1.2.9 ストーム制御機能の設定 1-6
1.3 Layer 2 Ethernet インタフェースの設定 1-7
1.3.1 Ethernet インタフェースのオートネゴシエーションの通信速度の設定 1-7
1.3.2 Ethernet インタフェースのストーム抑止の設定 1-9
1.3.3 Ethernet インタフェースの MDI モードの設定 1-10
1.3.4 Ethernet インタフェースのケーブル接続テスト 1-11
1.4 Ethernet インタフェースの表示と維持 1-12

1章 Ethernet インタフェース

装置は Ethernet インタフェース、コンソールインタフェースをサポートしています。サポートするインタフェースタイプと番号は、装置の種類により異なります。インタフェースタイプと番号については、*インスタレーションマニュアル*を参照してください。

この章では Ethernet インタフェースの設定方法について記載します。

1.1 Ethernetインタフェースの命名ルール

Ethernet インタフェースは *interface type A/B/C* のフォーマットで指定されます。文字は以下のインタフェースタイプを表します。

- **A**– A はデフォルトで 1 です。
- **B**– 装置のスロット番号です。固定インタフェースは 0 となります。
- **C**– インタフェース番号です。

1.2 Ethernetインタフェースの共通設定

この章は Ethernet インタフェースの共通設定について記載します。

1.2.1 コンボインタフェースの設定(QX-S1124GT-4G-PW)

コンボインタフェースは、論理的なインタフェースです。SFP ポートか RJ-45 ポートを選択します。SFP ポートと、RJ-45 ポートを同時に使用できません。一方を使用する場合、もう一方は自動的に使用不可になります。

I. 設定必要条件

コンボインタフェースを設定する前に以下の処理が完了していることを確認してください。

- **display interface** コマンドを使用して、コンボポートのどのポート（SFP ポートあるいは RJ-45 ポート）が有効かを確認します。
  - RJ-45 ポートが有効な場合、 "Media type is twisted pair, Port hardware type is 1000_BASE_T."と表示されます。
  - SFP ポートが有効な場合、上記の表示はありません。
- コンボインタフェースの設定を表示するため各コンボインタフェースの view で **display this** コマンドを使用してください。
  - SFP ポートが有効な場合、**combo enable fiber** コマンドがあります。
  - RJ-45 ポートが有効な場合、**combo enable copper** コマンドがあります。

II. コンボインタフェースのアクティブポートの変更

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． Ethernet interface view に移行する	**interface** *interface-type interface-number*	―
3． コンボポートを有効にする	**combo enable** { **copper** | **fiber** | **auto** }	デフォルト： auto

🕮 **メモ：**

- コンボポートは使用するポートのみケーブルまたは SFP モジュールを接続してください。
- SFP トランシーバモジュールが実装され、RJ-45 ケーブルが接続されていない場合、SFP トランシーバモジュールのコンボポートが有効になります。SFP トランシーバモジュールをコンボポートに実装してから、RJ-45 コンボポートに RJ-45 ケーブルを接続してもリンクアップしません。
- RJ-45 コンボポートに RJ-45 ケーブルが接続され、SFP トランシーバモジュールのコンボポートが実装されていない場合、RJ-45 コンボポートが有効になります。RJ-45 コンボポートが接続されリンクアップされていたのち、SFP トランシーバモジュールがコンボポートに実装されても、RJ-45 コンボポートがリンクアップのままとなります。

1.2.2 Ethernet インタフェースの基本設定

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． Ethernet interface view に移行する	**interface** *interface-type interface-number*	―
3． 説明を設定する	**description** *text*	デフォルト：*interface-name* **Interface** たとえば“GigabitEthernet 1/0/1 Interface”です。
4． 通信モードを設定する	**duplex** { **auto** | **full** | **half** }	デフォルト：auto 1000BASE-Tを含むSFPトランシーバモジュールで動作するポート、1000Mbpsで動作するRJ-45ポートは、halfパラメータが未サポートです。
5． 通信速度を設定する	**speed** { **10** | **100** | **1000** | **auto** }	デフォルト：auto インタフェースタイプによってサポート速度は異なります。
6． Ethernet インタフェースを有効にする	**undo shutdown**	デフォルト：up

1.2.3 ジャンボフレームの設定

Ethernet で起こる莫大な量のトラフィックにより、フレームが Ethernet フレームの標準サイズよりも大きくなることがあります。このようなフレーム（ジャンボフレームと呼ばれます） が Ethernet ポートを通過できるようにすることで、標準サイズより大きなフレーム（ただし指定したパラメータ範囲内のもの）を転送できます。

- Ethernet インタフェースでジャンボフレームの設定が無効（**undo jumboframe enable** コマンド）にされている場合、ジャンボフレームの処理を行わないで廃棄します。
- Ethernet インタフェースでジャンボフレームの設定が行われている場合、以下の処理を行います。
  - □ 指定したフレーム長でジャンボフレームを処理します。
  - □ 指定したフレーム長を超過したフレームは処理を行わないで廃棄します。

以下にジャンボフレームを設定する手順を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. Ethernet interface view に移行する	**interface** *interface-type interface-number*	—
3. ジャンボフレームを設定する	**jumboframe enable** [*value*]	デフォルト：10000バイトのジャンボフレームが可能です。

🕮 **メモ：**

ジャンボフレームの設定は、VLAN タグ(１つにつき 4 バイト)を含むパケットサイズで設定して下さい。

1.2.4 Ethernet インタフェースの抑制の設定

⚠ **重要：**

STP、Smart Link が有効な Ethernet インタフェースでは抑制の設定を行うことができません。

Ethernet インタフェースは、up あるいは down の物理的なリンク状態のいずれかで動作します。物理的なリンク状態が up あるいは down となる際、物理レイヤは CPU に変更を通知します。CPU は以下の処理を行います。

- パケット転送を処理する上位レイヤモジュール（ルーティングやフォワーディングモジュールのような）にパケット転送の変更を反映します。
- トラップ、ログを作成し、対応するアクションをユーザに通知します。

up、down を頻繁に繰り返すことによるシステムのパフォーマンスの低下を防ぐため、物理リンク状態の変更レポートを遅らせます。つまりリンクの変化を抑制する設定を行います。遅延時間が経過した後、インタフェースは変更を通知します。

リンクアップイベントとリンクダウンイベントに異なる抑制間隔を設定できます。

インタフェースで **link-delay** コマンドを複数回実行する場合、次のルールが適用されます。

- リンクアップイベントとリンクダウンイベントの抑制間隔を個別に設定できます。
- リンクアップまたはリンクダウンイベントの抑制間隔を複数回設定すると、最新の設定が有効になります。

link-delay コマンドは、Ethernet インタフェースで相互に排他的です。

以下に Ethernet インタフェースの抑制の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. Ethernet interface view に移行する	**interface** *interface-type interface-number*	—
3. Ethernet インタフェースの抑制を設定する	**link-delay { down | up } [msec]** *delay-time*	デフォルト : リンクの変化がある場合、すぐにCPUに通知します。

1.2.5 Ethernet インタフェースのループバックテストの実行

注意：

インタフェースでループバックテストを有効にした場合、インタフェースはトラフィックデータを転送しません。

ループバックテストは以下のタイプに分けられます。

- **内部ループバックテスト** – Ethernet インタフェースに関連したスイッチングチップ内にあるすべての機能のテストを実行します。
- **外部ループバックテスト** – Ethernet インタフェースのハードウェアのテストを行います。外部ループバックテストを行うため、インタフェースにループバックプラグを挿入します。外部ループバックテストを行っている間、インタフェースはテストパケットを送信します。そこでプラグで折り返してインタフェースにループします。インタフェースがテストパケットを受信しない場合、インタフェースのハードウェアが故障しています。

I. 設定の制限とガイドライン

- インタフェースがシャットダウンされている場合（インタフェースのステータスは **ADM** あるいは **Administratively DOWN** と表示されます）は、内部/外部ループバックテストともに利用できません。
- ループバックテストの間、**speed**、**duplex**、**mdix-mode**、**shutdown** コマンドは適用できません。
- ループバックテスト実行中、Ethernet インタフェースは全二重モードで動作します。テスト終了後はもとの設定で動作します。

II. 設定手順

以下に Ethernet インタフェースのループバックテストの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． Ethernet interface view に移行する	**interface** *interface-type interface-number*	―
3． ループバックテストを実行する	**loopback** { **external** | **internal** }	デフォルト：実行なし

1.2.6 インタフェースの一般的なフロー制御の設定

リンクのエンド間で一般的なフロー制御を有効にすることで、リンクでのパケット廃棄を防ぐことができます。受信エンドでフロー制御を有効にすると、フロー制御（Pause フレーム）を送信エンドに通知し、トラフィックが混雑した際に一時的にパケットの送信を停止することができます。

インタフェースは送受信の両方のフロー制御を有効にすることができます。インタフェースはピアからパケットの送信停止を要求するパラメータを持つフロー制御フレームを受信した場合、パケットの送信を停止します。

リンクのトラフィック混雑を制御する場合、**flow-control** コマンドを双方向に設定します。

以下に Ethernet インタフェースでフロー制御の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． Ethernet interface view に移行する	**interface** *interface-type interface-number*	―
3． フロー制御を設定する	**flow-control**	デフォルト：無効

1.2.7 Ethernet インタフェースの節電機能の有効化

I. Ethernet インタフェースの EEE 省電力機能の有効化

EEE（Energy Efficient Ethernet）省電力機能を有効にすることで、ポートで一定期間、パケットを受信しない場合、アップリンクポートを低電力状態に遷移します。この期間はチップの仕様に依存し、設定を変更することができません。パケットが到着した後、ポートは通常の状態に遷移します。

以下に EEE 省電力機能を有効にする設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． Ethernet interface view に移行する	**interface** *interface-type interface-number*	―
3． EEE 省電力機能を有効にする	**eee enable**	デフォルト：無効 この機能はRJ-45ポートでのみ有効です。

1.2.8 統計情報のポーリング間隔の設定

以下に Ethernet インタフェースで統計情報のポーリング間隔の設定を行う方法を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Ethernet interface view に移行する	**interface** *interface-type interface-number*	―
3. 統計情報のポーリング間隔を設定する	**flow-interval** *interval*	デフォルト：300秒

設定したポーリング間隔によって収集された統計情報を表示するには、**display interface** コマンドを使用します。

1.2.9 ストーム制御機能の設定

ストーム抑制により、インタフェースでブロードキャスト、マルチキャスト、不明なユニキャストトラフィックの制御ができます。ブロードキャスト、マルチキャスト、不明なユニキャストトラフィックがしきい値を超過している場合、装置はトラフィックがしきい値を下回るまでパケットを廃棄します。

I. 設定の制限とガイドライン

- トラフィックの同じタイプに **storm constrain** コマンドと、**broadcast-suppression** コマンド、**multicast-suppression** コマンド、**unicast-suppression** コマンドのいずれかの設定を一緒に設定しないでください。一緒に設定した場合、トラフィックの抑止は正しく動作しません。**storm-constrain** コマンドの詳細は、オペレーションマニュアルのセクション 2 *アクセス* "*Ethernet インタフェース*"の"*Ethernet インタフェースのストーム抑止の設定*"を参照してください。
- 抑制するしきい値を kbps で設定する場合、正確な抑制しきい値は、設定する値と異なります。
  - 設定された値が 64 よりも小さい場合、64 の値が適用されます。
  - 設定された値が 64 の整数倍より大きく、64 の整数倍でない場合、設定された 64 の整数倍にもっとも近い値が適用されます。

  適用される抑制しきい値は、装置のプロンプトを参照してください。

II. 設定手順

以下に Ethernet インタフェースでストーム抑制のしきい値を設定する方法を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Ethernet interface view に移行する	**interface** *interface-type interface-number*	―

操作	コマンド	補足
3. ブロードキャストパケット転送抑制を設定し、しきい値を設定する	**broadcast-suppression** { *ratio* | **pps** *max-pps* | **kbps** *max-kbps* }	デフォルト : すべてのブロードキャストを通過します。
4. マルチキャストパケット転送抑制を設定し、しきい値を設定する	**multicast-suppression** { *ratio* | **pps** *max-pps* | **kbps** *max-kbps* }	デフォルト : すべてのマルチキャストを通過します。
5. 不明なユニキャストパケット転送抑制を設定し、しきい値を設定する	**unicast-suppression** { *ratio* | **pps** *max-pps* | **kbps** *max-kbps* }	デフォルト : すべての不明なユニキャストを通過します。

注意：

suppression 機能を Ethernet インタフェースもしくはポートグループに複数設定した場合、設定値は以下の優先度で有効化されます。
ブロードキャスト＞不明なユニキャスト＞マルチキャスト
たとえば、**broadcast-suppression** コマンド、**multicast-suppression** コマンド、**unicast-suppression** コマンドをそれぞれ抑制比率 10/20/30 で設定した場合、ブロードキャストの値が反映され、ブロードキャスト、マルチキャスト、不明なユニキャストの合計が 10%まで疎通可能となります。
suppression 機能を **pps** で使用する場合、標準の 10/100/1000BASE-T ポートでは 65 の倍数、SFP ポートでは 650 の倍数で制御します。

1.3 Layer 2 Ethernetインタフェースの設定

1.3.1 Ethernet インタフェースのオートネゴシエーションの通信速度の設定

デフォルトでは通信速度のオートネゴシエーションは、接続する両方の装置がサポートする最高速度でネゴシエートされます。最高速度にしたくない場合、ネゴシエーション用に通信速度のパラメータで限定することができます。

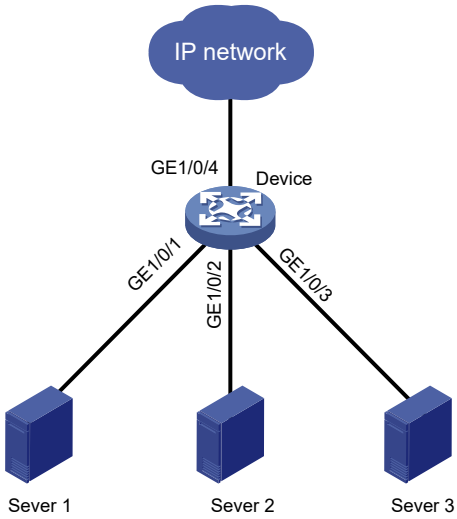


図 1-1 オートネゴシエーションの通信速度の設定

図 1-1に示すようなネットワーク構成があるとします。

- すべてのインタフェースは、最大速度が 1000Mbps の通信速度オートネゴシエーションモードに設定されています。
- GigabitEthernet 1/0/4 はサーバのためインタネットにアクセスを許可します。

サーバクラスタの各サーバの転送レートが 1000Mbps である場合、全転送レートは、インタネットにアクセスする GigabitEthernet 1/0/4 インタフェースの容量を超えてしまいます。

GigabitEthernet 1/0/4 の負荷を下げるため、GigabitEthernet 1/0/1、GigabitEthernet 1/0/2、GigabitEthernet 1/0/3 のオートネゴシエーションの通信速度のパラメータを **speed auto 100** コマンドにより 100Mbps に設定します。これによって各インタフェースの転送レートが 100Mbps に制限されます。**speed auto 100** コマンドを使用する場合は 10Mbps で接続することはありません。

以下に Ethernet インタフェースのオートネゴシエーションの通信速度の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. Ethernet interface view に移行する	**interface** *interface-type interface-number*	—
3. オートネゴシエーションの通信速度を設定する	**speed auto** { **10** | **100** | **1000** } *	デフォルト：設定なし **speed**コマンドと**speed auto**コマンドは一緒に設定することはできません。最初に設定したコマンドが廃棄され、後から設定された設定が有効となります。

1.3.2 Ethernet インタフェースのストーム抑止の設定

I. 概要

ストーム抑止は、ブロードキャスト、マルチキャスト、不明なユニキャストトラフィックを Ethernet インタフェースで受信した各トラフィックと比較します。ストーム抑止は、トラフィックの各タイプにしきい値の下限と上限があります。

インタフェースのトラフィックが上限のしきい値を超えた場合、インタフェースは設定によって以下のいずれかのアクションを行います。

- **トラフィックの特定のタイプをブロックし、他のタイプを転送** – インタフェースが転送されずにブロックされた場合でも、トラフィックはカウントされます。ブロックされたトラフィックがしきい値を下回ったと判断した場合、インタフェースはトラフィックの転送を開始します。
- **インタフェースの自動シャットダウン** – インタフェースが自動でシャットダウンされた場合、すべてのトラフィック転送を行いません。ブロックされたトラフィックがしきい値を下回ったと判断した場合でも、インタフェースはトラフィック転送を行いません。インタフェースをアップにする場合、**undo shutdown** コマンドを行うか、ストーム抑止を無効にする必要があります。

モニタしたトラフィックが以下の状況になった場合、管理用にトラップを送信する設定とログを記録するようにインタフェースに設定することができます。

- トラフィックがしきい値の上限を超過する
- トラフィックがしきい値の下限を下回る

broadcast-suppression コマンド、**multicast-suppression** コマンド、**unicast-suppression** コマンドはハードウェアのチップを使用するため、ソフトウェアでトラフィックを制御する **storm-constrain** コマンドに比べて装置の性能への影響は少なくなります。

ストーム抑止はトラフィックデータを収集するのにポーリングサイクルを使用し、次回のサイクルにデータの解析を行います。インタフェースで、2 つのポーリング間隔の設定を行ってください。

II. 設定の制限とガイドライン

トラフィックの同じタイプに **storm constrain** コマンドと、**broadcast-suppression** コマンド、**multicast-suppression** コマンド、**unicast-suppression** コマンドのいずれかの設定を一緒に設定しないでください。一緒に設定した場合、トラフィックの抑止は正しく動作しません。**broadcast-suppression** コマンド、**multicast-suppression** コマンド、**unicast-suppression** コマンドの詳細は、オペレーションマニュアルのセクション 2 *アクセス* "*Ethernet インタフェース*"の"*ストーム制御機能の設定*"を参照してください。

III. 設定手順

Ethernet インタフェースにストーム抑止を設定する方法を示します。

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

操作	コマンド	補足
2.　（オプション設定項目）ストーム抑止のポーリング間隔を設定する	**storm-constrain interval** *seconds*	デフォルト：10秒 ネットワークの信頼性のため、デフォルト値以上の値を使用してください。
3.　Ethernet interface view に移行する	**interface** *interface-type interface-number*	—
4.　（オプション設定項目）ストーム抑止の設定を有効にし、ブロードキャスト、マルチキャスト、不明なユニキャストトラフィックの上限/下限を設定する	**storm-constrain** { **broadcast** | **multicast** | **unicast** } { **pps** | **kbps** | **ratio** } *upperlimit lowerlimit*	デフォルト：無効
5.　トラフィックが上限を超過した場合のアクションを設定する	**storm-constrain control** { **block** | **shutdown** }	デフォルト：無効
6.　（オプション設定項目）ストーム抑止しきい値イベントのログの送信を有効にする	**storm-constrain enable log**	デフォルト：トラフィックが上限を上回るか、上限になった後に下限を下回った場合、インタフェースはログメッセージを送信します。
7.　（オプション設定項目）ストーム抑止しきい値イベントのトラップの送信を有効にする	**storm-constrain enable trap**	デフォルト：上限を超過した場合あるいは下回った場合トラップを送信します。

1.3.3 Ethernet インタフェースの MDI モードの設定

重要：

MDI モードの機能は、SFP ポートで未サポートです。

メタルの Ethernet インタフェースは、8 ピンのケーブルを使用します。各ピンはそれぞれ固有の役割があります。たとえば、ピン 1 とピン 2 は信号を送信し、ピン 3 とピン 6 は信号を受信します。Ethernet インタフェースに接続するためクロスオーバーケーブルとストレートケーブルの両方を使用することができます。Ethernet インタフェースが自動でケーブルタイプを適用させるため、以下の MDI（Medium Dependent Interface-Crossover）モードのいずれかで動作します。

- **MDIX モード**－ピン 1、ピン 2 は信号を受信し、ピン 3 とピン 6 は信号を送信します。
- **MDI モード**－ピン 1、ピン 2 は信号を送信し、ピン 3 とピン 6 は信号を受信します。
- **Auto MDIX モード**－ピア間でインタフェースのネゴシエーションが行われます。

🕮 **メモ：**

この機能は物理インタフェースのピン 4、5、7、8 に影響しません。

- 10Mbps あるいは 100Mbps で動作するインタフェースのピン 4、5、7、8 は信号の送受信を行いません。
- 1000Mbps で動作するインタフェースのピン 4、5、7、8 は信号の送受信を行います。

ピア間でインタフェースと通信できるように、以下のガイドラインに従ってインタフェースの MDIX モードを設定してください。

- 通常、インタフェースの MDIX モードを Auto MDIX モードに設定してください。装置がケーブルタイプを確定できない場合、インタフェースの MDIX モードを MDI あるいは MDIX モードに設定してください。
- ストレートケーブルを使用する場合、ローカル MDI モードとリモート MDI モードは異なる必要があります。
- クロスオーバーケーブルを使用する場合、以下のいずれかのモードに設定してください。
  - □ ローカル MDI モードとリモート MDI モードは同じにしてください。
  - □ どちらか一端を Auto MDIX モードに設定してください。

以下に Ethernet インタフェースに MDI モードを設定する手順を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. Ethernet interface view に移行する	**interface** *interface-type interface-number*	—
3. Ethernet インタフェースへの MDI モードを設定する	**mdix-mode** { **automdix** | **mdi** | **mdix** }	デフォルト：**automdix**

1.3.4 Ethernet インタフェースのケーブル接続テスト

⚠ **重要：**

- このコマンドは SFP ポート、10/100M で未サポートです。
- リンクアップしていないポートでは動作しません。
- Ethernet インタフェースのリンクがアップしている場合、そのケーブル接続をテストすると、リンクがダウンしてからアップになります。

以下に Ethernet インタフェースのケーブル接続テストを行う手順を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. Ethernet interface view に移行する	**interface** *interface-type interface-number*	—
3. Ethernet インタフェースに接続されたケーブルをテストする	**virtual-cable-test**	—

1.4 Ethernetインタフェースの表示と維持

すべての view で **display** コマンドを実行し、user view で **reset** コマンドを実行できます。

操作	コマンド
インタフェースのトラフィック統計情報を表示する	**display counters** { **inbound** | **outbound** } **interface** [*interface-type* [*interface-number*]]
最後のサンプリング間隔からのトラフィックレートの統計情報を表示する	**display counters rate** { **inbound** | **outbound** } **interface** [*interface-type* [*interface-number*]]
指定されたEthernetインタフェースあるいは全インタフェースの動作情報とステータス情報を表示する	**display interface** [*interface-type* [*interface-number*]]
指定されたEthernetインタフェースあるいは全インタフェースの概要情報を表示する	**display interface** [*interface-type* [*interface-number*]] [**brief** [**description** | **down**]]
指定されたEthernetインタフェースあるいは全インタフェースのストーム抑止を表示する	**display storm-constrain** [**broadcast** | **multicast** | **unicast**] [**interface** *interface-type interface-number*]
インタフェースの統計情報を削除する	**reset counters interface** [*interface-type* [*interface-number*]]

目次

このセクションのページは**2-x-x** です。

2 章 ループバックインタフェースと Null インタフェース..... 2-1
2.1 ループバックインタフェースの設定 2-1
2.2 Null インタフェースの設定 2-1
2.3 ループバックインタフェースと NULL インタフェースの表示と維持 2-2

2章 ループバックインタフェースと Null インタフェース

この章ではループバックインタフェースと Null インタフェースを設定する方法について記載します。

2.1 ループバックインタフェースの設定

ループバックインタフェースは、仮想的なインタフェースです。手動でコマンドによるシャットダウンをしない限り、ループバックインタフェースの物理層の状態は常に UP しています。この利点によって以下のように広く使用されます。

- **装置が作成したパケットの送信元 IP アドレスとしてループバックアドレスを設定**
  - ループバックインタフェースアドレスは安定したユニキャストアドレスであるため、装置を識別するのに使用されます。
    - 認証あるいはセキュリティサーバでルールを設定する場合、装置を識別するループバックインタフェースアドレスを送信元 IP アドレスとしたパケットを許可/禁止するようにルールを簡略化することができます。
    - ループバックインタフェースに IP アドレスを割り当て、送信元アドレスに使用した場合、ループバックインタフェースからピアまでのルートが届くことを確認してください。ループバックインタフェースに送信されるすべてのデータパケットは装置自体に送信されていると認識するため、装置はこのパケットを転送しません。
- **ダイナミックルーティングプロトコルのループバックインタフェースの使用** – ダイナミックルーティングプロトコル用にルータ ID を設定する際、ルータ ID として最も高いループバックインタフェースの IP アドレスを使用します。

以下にループバックインタフェースを設定する方法を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. ループバックインタフェースを作成し loopback interface view に移行する	**interface loopback** *interface-number*	—
3. ループバックインタフェースの説明を設定する	**description** *text*	デフォルト：*interface name* **Interface** (例 **LoopBack1 Interface**)
4. ループバックインタフェースを up にする	**undo shutdown**	デフォルト：up

2.2 Nullインタフェースの設定

NULL インタフェースは、仮想的なインタフェースで、常に UP しています。しかし、データパケットの転送、IP アドレスやリンク層プロトコルの設定をすることはできません。NULLインタフェースをネットワークセグメントのネクストホップとしてスタティックル

ートに指定した場合、ネットワークセグメントに送信されたパケットはすべて破棄されます。したがって、ACL を適用する代わりにパケットを NULL インタフェースに送信することで、不要なトラフィックをフィルタすることができます。

以下に NULL インタフェースを設定する方法を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． null interface view に移行する	**interface null 0**	NULL 0インタフェースはデフォルト固定です。 NULLインタフェースは装置に一つだけサポートしています。NULLインタフェースは削除、作成することはできません。
3． NULL インタフェースの説明を設定する	**description** *text*	デフォルト：NULL0 Interface

2.3 ループバックインタフェースとNULLインタフェースの表示と維持

すべての view で **display** コマンドを実行し、user view で **reset** コマンドを実行できます。

操作	コマンド
指定したあるいはすべてのループバックインタフェースの情報を表示する	**display interface** [**loopback** [*interface-number*]] [**brief** [**description** | **down**]]
NULLインタフェースを表示する	**display interface** [**null** [**0**]] [**brief** [**description** | **down**]]
指定したあるいはすべてのループバックインタフェースの情報を削除する	**reset counters interface** [**loopback** [*interface-number*]]
NULLインタフェースを削除する	**reset counters interface** [**null** [**0**]]

目次

このセクションのページは**2-x-x** です。

3 章 Interface range 3-1
3.1 設定ガイドライン 3-1
3.2 設定手順 3-2
3.3 表示と維持 3-2

3章 Interface range

interface range コマンドはインタフェースレンジを作成し、interface range view に移行します。同じ機能を 1 つずつインタフェースに設定する代わりに、interface range view に移行して、複数のインタフェースにまとめて設定することができます。たとえば、複数のインタフェースをまとめてシャットダウンする場合、interface range view で **shutdown** コマンドを実行します。

interface range でインタフェースを設定するとき、**interface range** コマンドあるいは **interface range name** コマンドを使用して interface range を設定し、その view に移行する必要があります。

interface range コマンドを使用して設定した場合、interface range で指定した各インタフェースに反映されます。**interface range** コマンドでは、繰り返し interface range を使用することはできません。繰り返し設定する場合は、**interface range name** コマンドを使用します。

3.1 設定ガイドライン

interface range view で interface range を設定する際は、以下の点に注意してください。

- interface range view では、**interface range** コマンドで最初に指定したインタフェースでサポートされるコマンドのみ有効です。
- **interface** *interface-type interface-number* コマンドで interface view に移行できない場合、interface range で最初に指定したインタフェースでインタフェース設定をしないでください。
- リンクアグリゲーションのアグリゲートインタフェースとメンバポートを同じ interface range に設定しないでください。設定した場合、あるコマンドによってリンクアグリゲーションが失敗することがあります。
- interface range のインタフェースの最大数に制限はありませんが、interface range でのインタフェースが多くなれば、実行時間も長くなります。
- 1000 個以上の interface range name を作成しないでください。

装置は、interface range 設定処理中にプロンプトまたはアラームメッセージを出力しません。interface range 設定の影響を十分に認識してください。

- interface range view でコマンドを実行した後、以下のいずれかの状況が発生する場合があります。
  - システムはエラーメッセージを表示し、interface range view にとどまります。これは 1 つ以上のメンバインタフェースで実行が失敗したことを示します。
    - インタフェースレンジの最初に指定したインタフェースでコマンドの実行に失敗した場合、他のメンバインタフェースで実行されません。
    - 最初に指定したインタフェースではないインタフェースで、コマンドの実行に失敗した場合、残りのメンバインタフェースでコマンドが適用されます。
  - システムは interface range view に移行します。以下のことを示します。
    - コマンドは system view と interface range view でサポートされます。
    - interface range view のメンバインタフェースでコマンドの実行に失敗した場合、システムは system view でコマンドを実行します。
    - システムは後続のメンバインタフェースでコマンドを実行しません。

各メンバインタフェースの interface view の設定を確認する場合、**display this** コマンドを使用することができます。また system view の設定が必要でない場合、**undo** コマンドで設定を削除することができます。

3.2 設定手順

Interface range の設定をするには以下の手順に従ってください。

操作	コマンド	補足
1． system view へ移行する	**system-view**	–
2． Interface range view へ移行する	● 名前設定なし： **interface range** { *interface-type interface-number* **to** *interface-type interface-number* }&<1-24> ● 名前設定あり： **interface range name** *name* [**interface** { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-24>]	**interface range name**コマンドを使用すると interface rangeに名前を割り当てることができます。そしてinterface range viewに移行するためにinterface rangeを入力する代わりに名前を指定することができます。
3． （オプション設定項目）最初に指定したインタフェースで有効なコマンドを表示する	Interface range viewで”?”を入力する	―
4． インタフェースに設定を行う	有効なコマンドはインタフェースによって異なる	―
5． （オプション設定項目）設定を確認する	**display this**	―

3.3 表示と維持

すべての view で **display** コマンドを実行します。

操作	コマンド
インタフェースレンジの情報を表示する	**display interface range** [**name** *name*]

目次

このセクションのページは**2-x-x** です。

4章 MACアドレステーブル 4-1
4.1 概要 4-1
4.1.1 MACアドレスエントリの作成方法 4-1
4.1.2 MACアドレスエントリのタイプ 4-2
4.2 MACアドレス設定作業リスト 4-2
4.3 MACアドレスエントリの設定 4-3
4.3.1 設定ガイドライン 4-3
4.3.2 グローバルでのスタティック/ダイナミックMACアドレスエントリの追加/修正 4-3
4.3.3 インタフェースでのスタティック/ダイナミックMACアドレスエントリの追加/修正 4-3
4.3.4 ブラックホールMACアドレスエントリの追加/修正 4-4
4.4 MACアドレス学習の無効化 4-4
4.4.1 グローバルでのMACアドレス学習の無効化 4-4
4.4.2 インタフェースでのMACアドレス学習の無効化 4-5
4.4.3 VLANでのMACアドレス学習の無効化 4-5
4.5 ダイナミックMACアドレスエントリのエージングタイマの設定 4-5
4.6 インタフェースで学習可能なMACアドレス数の設定 4-6
4.7 インタフェースで学習可能なMACアドレスの上限到達後での未知のフレームの転送の設定 4-6
4.8 MACアドレスの移動の通知と抑制機能の有効化 4-7
4.9 MACアドレスの移動によるARPクイックアップデートの有効化 4-8
4.10 MACアドレステーブルのSNMP通知の有効化 4-9
4.11 MACアドレステーブルのハッシュバケットサイズの設定 4-10
4.11.1 概要 4-10
4.11.2 制限とガイドライン 4-10
4.11.3 設定手順 4-10
4.11.4 MACアドレスの学習モードの設定 4-10
4.12 MACアドレステーブルの表示と維持 4-11
4.13 MACアドレステーブルの設定例 4-11
4.13.1 ネットワーク要件 4-11
4.13.2 設定手順 4-12
4.13.3 設定の確認 4-12

4章 MAC アドレステーブル

4.1 概要

Ethernet 装置は、フレームを転送するために MAC アドレステーブルを使用します。このテーブルは、宛先 MAC アドレス、出力インタフェース、VLAN ID を記載しています。フレームを転送した場合、装置は最初に MAC アドレステーブルにフレームの MAC アドレスと一致するか検索します。

- エントリがある場合、出力インタフェースへフレームを転送します。
- エントリがない場合、装置はフレームが所属する VLAN にフレームをブロードキャストします。

4.1.1 MAC アドレスエントリの作成方法

MAC アドレステーブルのエントリは 2 つのソースから成り立ちます。装置によって自動的に学習されたエントリと、管理者によって手動で追加されたエントリから構成されます。

I. MAC アドレスの学習

通常、MAC アドレステーブルは装置の各インタフェースの入力フレームの送信元 MAC アドレスを学習することによって自動的に MAC アドレステーブルを生成します。

装置は入力フレームの MAC アドレスを学習するため以下の処理を行います。

1) フレームの送信元 MAC アドレス（例：MAC-SOURCE）を確認します。
2) フレームの MAC アドレスに対応するエントリを MAC アドレステーブルから検索します。
   - □ 対応するエントリがある場合、そのエントリを更新します。
   - □ 対応するエントリがない場合、入力ポートのエントリに MAC-SOURCE を追加します。

装置は、不明な送信元 MAC アドレスのフレームを受信した場合、MAC アドレステーブルが完全に書き込まれるまで、毎回学習プロセスを行います。

II. MAC アドレスエントリの手動設定

装置が送信元 MAC アドレス学習を介して動的に MAC アドレスを学習する場合、装置は正規ユーザの正当なフレームかハッカーからの不正なフレームかを見分けることができません。これは潜在的にセキュリティに危険をもたらします。ホスト A がポート A に接続されている場合、MAC アドレスエントリはホスト A の MAC アドレス（たとえば、MAC A）を学習します。不正なユーザがポート B への送信元 MAC アドレスとして MAC A のフレームを送信する場合、装置は以下の処理を行います。

1) 出力インタフェースとしてポート B の新しい MAC アドレスエントリを学習し、MAC A の古いエントリに上書きします。

2)　ポート B から MAC A の宛先のフレームを不正ユーザに転送します。

その結果、不正なユーザはホスト A のデータを取得します。ポート A のセキュリティを強化するために、ホスト A をポート A と結合するためスタティックエントリを手動で設定します。ホスト A のフレームは常にポート A に向けて送信されます。ホスト A の偽造した MAC アドレスを使っている他のホストはホスト A の宛先フレームを取得することができません。

4.1.2 MAC アドレスエントリのタイプ

MAC アドレステーブルには以下のタイプのエントリがあります。

- **スタティックエントリ** – 関連したインタフェースから特定の宛先 MAC アドレスによってフレームを転送するため、手動で設定されます。エージアウトしません。スタティックエントリはダイナミックエントリよりも優先されます。
- **ダイナミックエントリ** – 手動で設定されたダイナミックエントリ、または動的に学習したエントリです。エージアウトします。手動で設定されたダイナミックエントリと動的に学習したエントリの優先度は同じです。
- **ブラックホールエントリ** – 手動で設定され、エージアウトしません。ブラックホールエントリは特定の宛先 MAC アドレスでフレームをフィルタするために設定されます。たとえば、セキュリティに問題のある指定したユーザへのすべてのフレームを、ブラックホール MAC アドレスエントリとしてユーザの MAC アドレスを設定することができます。

スタティック、ブラックホール MAC アドレスエントリはダイナミック MAC アドレスに上書きすることができます。逆にダイナミック MAC アドレスは上書きすることができません。

4.2 MACアドレス設定作業リスト

この項で記載される設定項目はすべてオプション設定であり、設定する順番は関係ありません。必要に応じて設定を行ってください。

作業リスト
（オプション設定項目）MACアドレステーブルの設定 • グローバルでのスタティック/ダイナミックMACアドレスエントリの追加/修正 • インタフェースでのスタティック/ダイナミックMACアドレスエントリの追加/修正 • ブラックホールMACアドレスエントリの設定
（オプション設定項目）MACアドレス学習の無効化
（オプション設定項目）ダイナミックMACアドレスエントリのエージングタイマの設定
（オプション設定項目）インタフェースで学習可能なMACアドレス数の設定
（オプション設定項目）インタフェースで学習可能なMACアドレスの上限到達後での未知のフレームの転送の設定
（オプション設定項目）MACアドレスの移動の通知と抑制機能の有効化
（オプション設定項目）MACアドレスの移動によるARPクイックアップデートの有効化
（オプション設定項目）MACアドレステーブルのSNMP通知の有効化
（オプション設定項目）MACアドレステーブルのハッシュバケットサイズの設定
（オプション設定項目）MACアドレスの学習モードの設定

4.3 MACアドレスエントリの設定

4.3.1 設定ガイドライン

- 自動学習した MAC アドレスと異なる出力インタフェースで同じ MAC アドレスが存在する場合、ダイナミックエントリは適用されません。
- 設定を保存していない場合、手動で設定されたスタティック、ブラックホール MAC アドレスエントリは、再起動が行われると削除されます。手動で設定されたダイナミック MAC アドレスは設定を保存するあるいはしないに関わらず、削除されます。

送信元 MAC アドレスのフレームが、異なるタイプの MAC アドレスエントリとマッチするフレームは、別に処理されます

タイプ	説明
スタティックMACアドレスエントリ	フレームの入力インタフェースがエントリのインタフェースと同一かどうかにかかわらず、宛先MACアドレスにフレームを転送します。
ブラックホールMACアドレスエントリ	フレームを廃棄します。
ダイナミックMACアドレスエントリ	• そのエントリと異なるインタフェースから入力したフレームのMACアドレスを学習し、元のエントリに上書きします。 • そのエントリと異なるインタフェースから入力したフレームを転送し、エージングタイマをアップデートします。

4.3.2 グローバルでのスタティック/ダイナミック MAC アドレスエントリの追加/修正

操作	コマンド	補足
1. system view に移行する	**system-view**	–
2. MAC アドレスエントリを追加/変更する	**mac-address** { **dynamic** | **static** } *mac-address* **interface** *interface-type interface-number* **vlan** *vlan-id*	デフォルト : グローバルで設定されたMACアドレスエントリはありません。 VLANが作成され、VLANにインタフェースが割り当てられていることを確認してください。

4.3.3 インタフェースでのスタティック/ダイナミック MAC アドレスエントリの追加/修正

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

操作	コマンド	補足
2. interface view に移行する	● interface viewに移行する：**interface** *interface-type interface-number* ● aggregate interface viewに移行する：**interface bridge-aggregation** *interface-number*	―
3. スタティック、ダイナミックMACアドレスエントリを追加/変更する	**mac-address** { **dynamic** | **static** } *mac-address* **vlan** *vlan-id*	デフォルト：インタフェースで設定されたMACアドレスエントリはありません。VLANが作成され、VLANにインタフェースが割り当てられていることを確認してください。

4.3.4 ブラックホール MAC アドレスエントリの追加/修正

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. ブラックホール MAC アドレスエントリを追加/変更する	**mac-address blackhole** *mac-address* **vlan** *vlan-id*	デフォルト：設定されたブラックホールMACアドレスエントリはありません。VLANが作成されていることを確認してください。

4.4 MACアドレス学習の無効化

MAC アドレス学習はデフォルトで有効です。MAC アドレス学習を無効にしたのち、装置はただちに既存のダイナミック MAC アドレスエントリを削除します。

4.4.1 グローバルでの MAC アドレス学習の無効化

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. グローバルでMACアドレス学習を無効にする	**undo mac-address mac-learning enable**	デフォルト：有効

4.4.2 インタフェースでの MAC アドレス学習の無効化

グローバルで MAC アドレス学習が有効である場合、インタフェースごとに MAC アドレス学習を無効にすることができます。

以下にインタフェースでの MAC アドレス学習を無効にする設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. interface view に移行する	● interface viewに移行する：**interface** *interface-type interface-number* ● aggregate interface viewに移行する：**interface** *bridge-aggregation interface-number*	―
3. インタフェースで MAC アドレス学習を無効にする	**undo mac-address mac-learning enable**	デフォルト：有効

4.4.3 VLAN での MAC アドレス学習の無効化

グローバルで MAC アドレス学習が有効である場合、VLAN ごとに MAC アドレス学習を無効にすることができます。

以下に VLAN での MAC アドレス学習を無効にする設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. グローバルで MAC アドレス学習を有効にする	**mac-address mac-learning enable**	デフォルト：有効
3. VLAN view に移行する	**vlan** *vlan-id*	―
4. VLAN で MAC アドレス学習を無効にする	**undo mac-address mac-learning enable**	デフォルト：有効

4.5 ダイナミックMACアドレスエントリのエージングタイマの設定

装置の MAC アドレステーブルには、セキュリティとダイナミックエントリのリソースの浪費を防ぐために、エージングタイマがあります。エージングタイマが満了する前にダイナミック MAC アドレスエントリのアップデートが行われないと、装置はエントリを削除します。エージング機能は、MAC アドレステーブルを、最新のネットワークトポロジの変化に対応して即座にアップデートするためのものです。

エージングタイマは適切な時間に設定してください。トポロジの変更が少ない安定したネットワークではエージングタイマを長い時間にする必要があり、トポロジの変更が多いネットワークではエージングタイマを短い時間にする必要があります。

エージング間隔が長いと、有効期限切れのエントリを MAC アドレステーブルに残す可能性があり、最新のネットワークの変化に対応できなくなる可能性があります。また、エージング間隔が短いと、有効なエントリを削除してしまい、装置のパフォーマンスに影響をおよぼす不要なブロードキャストを送信する結果になる可能性があります。

不必要なエージアウトからダイナミックエントリを防ぐために、エージングタイマの設定を長くするあるいはエージングタイマを無効にすることで安定したネットワークのブロードキャストを削減することができます。ネットワークのパフォーマンスを向上するだけでなく、思いがけない宛先にデータフレームを送信することを減らすことができるため、セキュリティも改善することができます。

以下に MAC アドレス学習のエージングタイマを設定する方法を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. ダイナミック MAC アドレスエントリのエージングタイマを設定する	**mac-address timer** { **aging** *seconds* | **no-aging** }	デフォルト：300秒 **no-aging**パラメータを使用した場合、エージングタイマを無効にします。

4.6 インタフェースで学習可能なMACアドレス数の設定

この機能は MAC アドレステーブルサイズを制限します。MAC アドレステーブルが大きくなって転送処理が低下することを防ぐためにポートまたはポートグループごとに学習可能な MAC アドレス数を制限することができます。

MAC 学習制限は、Voice VLAN で学習される MAC アドレスの数を制御しません。詳細はオペレーションマニュアルのセクション 2 *アクセス" Voice VLAN"* を参照してください。

以下にインタフェースで学習可能な MAC アドレス数の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. interface view に移行する	**interface** *interface-type interface-number*	—
3. インタフェースで学習可能なMACアドレス数を設定する	**mac-address max-mac-count** *count*	デフォルト：設定なし

4.7 インタフェースで学習可能なMACアドレスの上限到達後での未知のフレームの転送の設定

この章では、未知のフレームは、送信元 MAC アドレスが MAC アドレステーブルにないフレームのことを示します。

インタフェースで学習できる MAC アドレスの数が制限に到達したのち、インタフェースで受信された未知のフレームを装置が転送することを有効あるいは無効にすることができます。

以下にインタフェースで受信された未知のフレームの転送の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. interface view に移行する	**interface** *interface-type interface-number*	―
3. インタフェースで学習できるMACアドレスの数が制限に到達したのち、インタフェースで受信された未知のフレームを装置が転送することを有効にする	**mac-address max-mac-count enable-forwarding**	デフォルト：有効

4.8 MACアドレスの移動の通知と抑制機能の有効化

以下の状況である場合、インタフェース A で学習された MAC アドレスエントリの出力インタフェースがインタフェース B に変更します。

- インタフェース B が、送信元 MAC アドレスのフレームを受信します。
- インタフェース B がインタフェース A と同じ VLAN に所属しています。

この場合、MAC アドレスがインタフェース A からインタフェース B に移動し、MAC アドレスの移動が発生します。

MAC アドレスの移動の通知機能は、MAC アドレスの移動を検出した場合、MAC アドレスが移動したことのログを出力します。

2 つのインタフェース間で継続して MAC アドレスが移動した場合、レイヤ 2 のループが発生する可能性があります。ループを検出し、位置を特定するために **display mac-address mac-move** コマンドで MAC アドレスの移動情報を表示することができます。

MAC アドレスの移動がインタフェースで頻繁に発生することをシステムが検出した場合、インタフェースをダウンするように MAC アドレスの移動抑制を設定することができます。指定した抑制間隔の経過後、インタフェースは自動で UP 状態になります。あるいは手動でインタフェースを UP にすることができます。MAC アドレスの抑制を適用するため、ARP クイックアップデートの機能と一緒に設定する必要があります。ARP クイックアップデートの詳細は次項を参照してください。

以下に MAC アドレスの移動の通知を設定する手順を示します。

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

操作	コマンド	補足
2. MAC アドレスの移動を通知することを有効にし、MAC アドレスの検出間隔を指定します。	**mac-address notification mac-move** [**interval** *interval-value*]	デフォルト：無効 パラメータを指定しない場合、デフォルトで1分が指定されます。 このコマンドを実行した後、システムはInformation Centerにsyslogメッセージのみを送信します。**snmp-agent trap enable mac-address**コマンドが有効である場合、装置のSNMPモジュールにSNMP情報を送信します。
3. （オプション設定項目）検出間隔内に送信元インタフェースから移動する MAC アドレスのしきい値と検出間隔を設定する	**mac-address notification mac-move suppression** { **interval** *interval* | **threshold** *threshold* }	デフォルト : 検出間隔内に送信元インタフェースから移動するMACアドレスのしきい値は3です。MACアドレスの抑制間隔は30秒です。
4. interface view に移行する	• interface viewに移行する：**interface** *interface-type interface-number* • aggregate interface viewに移行する：**interface bridge-aggregation** *interface-number*	ー
5. MAC アドレスの移動の抑制機能を有効にする	**mac-address notification mac-move suppression**	デフォルト：無効
6. MAC アドレスの移動による ARP クイックアップデートを有効にする	**mac-address mac-move fast-update**	デフォルト：有効 MACアドレスの移動の抑制機能を有効にした場合、必要です。

4.9 MACアドレスの移動によるARPクイックアップデートの有効化

MAC アドレスの移動による ARP クイックアップデート機能は、MAC アドレスの出力インタフェースを変更したのち、ARPエントリをすぐにアップデートすることができます。この機能によってデータ通信を中断することなく行うことができます。

図 4-1に示すように、モバイルユーザ Laptop が AP1 あるいは AP2 に接続されているネットワークにアクセスします。ユーザが接続している AP が変更した場合、スイッチは MAC アドレスローミングを検出したのち、ユーザの ARP エントリをすぐにアップデートします。

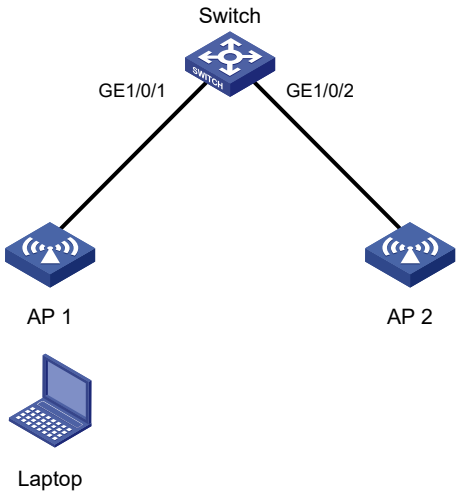


図 4-1 ARP クイックアップデートアプリケーションシナリオ

以下に MAC アドレスの移動による ARP クイックアップデートの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. MAC アドレスの移動による ARP クイックアップデートを有効にする	**mac-address mac-move fast-update**	デフォルト：有効

4.10 MACアドレステーブルのSNMP通知の有効化

MAC アドレステーブルの SNMP 通知を有効にしたのち、装置は NMS に重要なイベントを通知するため、SNMP モジュールに SNMP 通知を送信します。送信する通知の属性を決定するため、SNMP の送信パラメータを SNMP 通知に設定することができます。

MAC アドレステーブルの SNMP 通知を無効にした場合、装置は Information Center モジュールにログメッセージの送信を行います。MAC アドレステーブルモジュールのログメッセージを調査するため、出力ルールと宛先を設定することができます。

SNMP 通知と Information Center の詳細は、オペレーションマニュアルのセクション 9 *システム管理*”*SNMP*”、”*Information Center*”を参照してください。

以下に MAC アドレステーブルの SNMP 通知の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. MAC アドレステーブルの SNMP 通知を有効にする	**snmp-agent trap enable mac-address**	デフォルト：無効

4.11 MACアドレステーブルのハッシュバケットサイズの設定

4.11.1 概要

装置はハッシュチェーンを通じて MAC アドレステーブルを保存します。複数の MAC アドレスがハッシュによって同じハッシュキーを取得する場合、MAC アドレスハッシュの競合が発生し、装置はこれらの MAC アドレスの一部を学習できません。装置は、未知の MAC アドレス宛てにトラフィックをブロードキャストします。この MAC アドレスは、帯域幅とリソースを消費します。

MAC アドレステーブルのハッシュバケットサイズを大きくすると、MAC アドレスハッシュの競合を減らすことができます。ハッシュバケットサイズが大きいほど、より多くのシステムリソースが必要になります。システムリソースに応じて、ハッシュバケットのサイズを適切に設定してください。**display mac-address hash-bucket-size** コマンドを使用すると、現在のハッシュバケットサイズと、次の起動時に有効になるハッシュバケットサイズを表示できます。

4.11.2 制限とガイドライン

設定されたハッシュバケットサイズは、次回の起動時に有効になります。

4.11.3 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	–
2. MAC アドレステーブルのハッシュバケットサイズを設定する	**mac-address hash-bucket-size** *size*	デフォルト：4

4.11.4 MAC アドレスの学習モードの設定

装置のデフォルトは、MAC アドレスの学習をソフトウェア処理でおこなっています。そのため、wire rate で MAC アドレスを学習できません。 MAC アドレスの学習モードを変更するには、以下の手順に従ってください。

表7-1 MAC アドレスの学習モード変更の設定

操作	コマンド	補足
system viewに移行する	**system-view**	–
MACアドレスの学習モードを変更する	**mac-learn-mode** { **hardware** | **software** }	必須設定項目 デフォルト：ソフトウェア

注意:

- MAC アドレスの学習モードを"hardware"モードに設定した場合、すべてのインタフェースで MAC アドレスの学習モードが"hardware モードになります。
- MAC アドレスの学習モードを"hardware"モードに設定しても、dot1x 認証機能、または **mac-address max-mac-count** 設定を行ったポートでは、内部的に"software"モードでの動作となる為、wire rate での MAC アドレス学習はできません。

4.12 MACアドレステーブルの表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
MACアドレステーブル情報を表示する	**display mac-address** [*mac-address* [**vlan** *vlan-id*]	[[**dynamic**	**static**] [**interface** *interface-type interface-number*]	**blackhole**	**multiport**] [**vlan** *vlan-id*] [**count**]]
ダイナミックMACアドレスエントリのエージングタイマを表示する	**display mac-address aging-time**
グローバルMACアドレスの学習状態と指定された、あるいはすべてのインタフェースのMACアドレスの学習状態を表示する	**display mac-address mac-learning** [**interface** *interface-type interface-number*]
MACアドレスの統計情報を表示する	**display mac-address statistics**
MACアドレスの移動記録を表示する	**display mac-address mac-move** [**slot** *slot-number*]
MACアドレステーブルのハッシュバケットサイズを表示する	**display mac-address hash-bucket-size**

4.13 MACアドレステーブルの設定例

4.13.1 ネットワーク要件

図 4-2に示すように、以下の要件を設定します。

- Host A （000f-e235-dc71）は Device のインタフェース GigabitEthernet 1/0/1 に接続され、VLAN1 に属しています。
- ネットワークで一度疑わしいふるまいをした Host B （000f-e235-abcd）は VLAN1 に属しています。

MAC アドレスの設定を以下に示します。

- MAC アドレス spoofing を防ぐため、Device の MAC アドレステーブルに Host A のスタティック MAC アドレスエントリを追加します。
- Host B で定義されたすべてのフレームを廃棄するように、Device の MAC アドレステーブルに Host B のブラックホール MAC アドレスエントリを追加します。

- ダイナミック MAC アドレスエントリのエージングタイマを 500 秒に設定します。

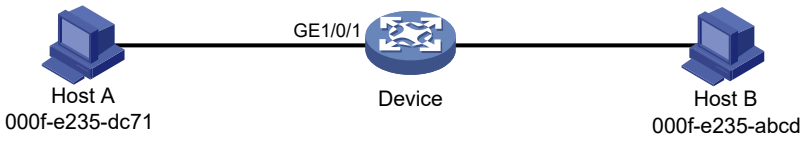


図 4-2 ネットワーク図

4.13.2 設定手順

VLAN1 に属している GigabitEthernet 1/0/1 に MAC アドレス 000f-e235-dc71 のスタティック MAC アドレスエントリを追加します。

```
<Device> system-view
[Device] mac-address static 000f-e235-dc71 interface gigabitethernet 1/0/1 vlan 1
```

VLAN1 に属している MAC アドレス 000f-e235-abcd にブラックホール MAC アドレスエントリを追加します。

```
[Device] mac-address blackhole 000f-e235-abcd vlan 1
```

ダイナミック MAC アドレスエントリのエージングタイマを 500 秒に設定します。

```
[Device] mac-address timer aging 500
```

4.13.3 設定の確認

GigabitEthernet 1/0/1 のスタティック MAC アドレスエントリを表示します。

```
[Device] display mac-address static interface gigabitethernet 1/0/1
MAC Address       VLAN ID    State           Port/NickName           Aging
000f-e235-dc71    1          Static          GE1/0/1                 N
```

ブラックホール MAC アドレスエントリを表示します。

```
[Device] display mac-address blackhole
MAC Address       VLAN ID    State           Port/NickName           Aging
000f-e235-abcd    1          Blackhole       N/A                     N
```

ダイナミック MAC アドレスエントリのエージングタイマを表示します。

```
[Device] display mac-address aging-time
MAC address aging time: 500s.
```

目次

このセクションのページは**2-x-x** です。

5 章 MAC Information 5-1
5.1 MAC Information の有効化 5-1
5.2 MAC Information モードの設定 5-1
5.3 Syslog メッセージあるいは SNMP トラップメッセージの送信間隔の設定 5-2
5.4 MAC Information のキュー長の設定 5-2
5.5 MAC Information 設定例 5-2
5.5.1 ネットワーク要件 5-2
5.5.2 設定の制限とガイドライン 5-3
5.5.3 設定手順 5-3

5章 MAC Information

MAC Information 機能は MAC アドレスエントリが学習あるいは削除された場合、Syslog メッセージあるいは SNMP トラップメッセージを作成します。これらのメッセージを解析することによって、監視端末はネットワークにアクセスしているユーザを監視することができます。

MAC Information 機能は、MAC アドレスの変更の Syslog メッセージあるいは SNMP トラップメッセージをキューに格納します。以下の場合、装置はキューの最後の MAC アドレス変更を最新の MAC アドレス変更に上書きします。

- MAC アドレス変更を通知するタイマが満了していない場合
- キューが使い果たされた場合

Syslog メッセージあるいは SNMP トラップメッセージが作成された後、すぐに送信するようにキューの長さを 0 に設定します。

5.1 MAC Informationの有効化

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. グローバルで MAC Information を有効にする	**mac-address information enable**	デフォルト：無効
3. Layer 2 Ethernet interface view に移行する	**interface** *interface-type interface-number*	―
4. インタフェースで MAC Information を有効にする	**mac-address information enable** { **added** | **deleted** }	デフォルト：無効 インタフェースでMAC Informationを有効にする前にグローバルで有効であることを確認してください。

5.2 MAC Informationモードの設定

MAC アドレスの変更を通知するため、MAC Information は以下のモードがあります。

- **Syslog**– 装置は MAC アドレスの変更を通知するため、Syslog メッセージを送信します。このモードでは Syslog メッセージを監視端末の Information Center に送信します。Information Center についての詳細は、オペレーションマニュアルのセクション 9 *システム管理* "*Information Center*"を参照してください。
- **Trap**– 装置は MAC アドレスの変更を通知するため、SNMP トラップメッセージを送信します。このモードでは SNMP トラップメッセージを NMS に送信します。SNMP についての詳細は、オペレーションマニュアルのセクション 9 *システム管理* "*SNMP*" を参照してください。

以下に MAC Information モードを設定する方法を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. (オプション設定項目)MAC Information モードを設定する	**mac-address information mode** { **syslog** | **trap** }	デフォルト：**trap**

5.3 Syslogメッセージあるいは SNMP トラップメッセージの送信間隔の設定

Syslog メッセージあるいは SNMP トラップメッセージを頻繁に送信することを防ぐため、送信間隔の設定を行うことができます。

以下に Syslog メッセージあるいは SNMP トラップメッセージの送信間隔を設定する方法を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. Syslog メッセージあるいは SNMP トラップメッセージの送信間隔を設定する	**mac-address information interval** *interval-time*	デフォルト：1秒

5.4 MAC Informationのキュー長の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. MAC Information のキュー長を設定する	**mac-address information queue-length** *value*	デフォルト：50

5.5 MAC Information設定例

5.5.1 ネットワーク要件

図 5-1に示すように、Host A に MAC アドレスの変更があった場合に Server に Syslog メッセージを送信するため、Device のインタフェース GigabitEthernet 1/0/1 に MAC Information を有効にします。

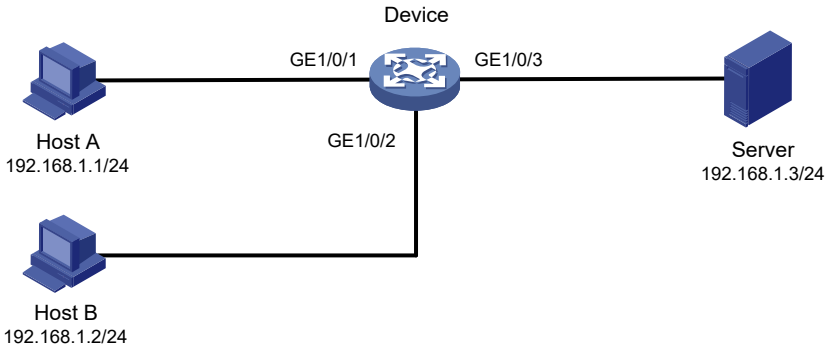


図 5-1 ネットワーク図

5.5.2 設定の制限とガイドライン

UNIX 系の Syslog サーバの設定ファイル（**/etc/syslog.conf**）を編集する場合のガイドラインを以下に示します。

- コメントは個別の行に記入し“#”記号で始めてください。
- 設定ファイル名に不要なスペース等をいれないでください。
- ロギングファシリティ名と設定ファイル**/etc/syslog.conf** が指定するログ情報の重要度は、QX-S1100G シリーズで **info-center loghost** コマンドと **info-center source** コマンドで設定したものと一致しなければなりません。一致しないと、ログ情報は正しく Syslog サーバ（ログホスト）に出力されないことがあります。

5.5.3 設定手順

1)　Device で Server（Syslog サーバ）に Syslog メッセージを送信する設定を行います。

information center を有効にします。

```
<Device> system-view
[Device] info-center enable
```

ログホスト 192.168.1.3/24 を指定し、ロギング facility として local4 を指定します。

```
[Device] info-center loghost 192.168.1.3 facility local4
```

ログホストへの出力を無効にします。

```
[Device] info-center source default loghost deny
```

出力ルールを設定する前に、不必要な情報の送信をしないように、出力するログから指定した宛先へのすべてモジュールを無効にします(この例では **loghost**)。

informational レベル以上の severity を持つ MAC アドレスのログをログホストに出力するルールを設定します。

```
[Device] info-center source mac loghost level informational
```

2)　Server を設定します。

以下のように Server の設定例を記載します。使用する Syslog サーバによって設定方法が異なる場合がありますので、設定する際は Syslog サーバのマニュアルもご確認ください。

a)　ルートユーザとしてログホストにログインします。

b)　ディレクトリ**/var/log/**にサブディレクトリ**Device**を作成します。

```
# mkdir /var/log/Device
```

c)　**Device**からのログを保存するため、**Device**ディレクトリに**info.log**を作成します。

```
# touch /var/log/Device/info.log
```

d)　ディレクトリ**/etc/**の**syslog.conf**を編集し、以下の内容を追加します。

メッセージを設定します。

```
local4.info /var/log/Device/info.log
```

この設定では、**local4** はログを受信するのに使用するログホストのロギング facility の名前です。info は informational レベルです。UNIX システムはファイル **/var/log/Device/info.log** に informational 以上の severity レベルのログ情報を記録します。

e)　**syslogd**のプロセスIDを表示します。**syslogd**のプロセスを削除し、新しい設定を適用するため、**-r**オプションを使用して**syslogd**を再起動します。

```
# ps -ae | grep syslogd
147
# kill -HUP 147
# syslogd -r &
```

Device は、ログホストに MAC アドレスのログを出力し、指定したファイルにログを記録することができます。

3)　Device で MAC Information を有効にします。

グローバルで MAC Information を有効にします。

```
[Device] mac-address information enable
```

MAC Information モードを Syslog に設定します。

```
[Device] mac-address information mode syslog
```

MAC アドレスの情報の変更を記録するため、GigabitEthernet 1/0/1 で MAC Information を有効にします。

- 新しい MAC アドレスを学習します。
- 既存の MAC アドレスを削除します。

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] mac-address information enable added
[Device-GigabitEthernet1/0/1] mac-address information enable deleted
[Device-GigabitEthernet1/0/1] quit
```

MAC Information のキュー長を 100 に設定します。

```
[Device] mac-address information queue-length 100
```

Syslog またはトラップメッセージの送信間隔を 20 秒に設定します。

```
[Device] mac-address information interval 20
```

目次

このセクションのページは**2-x-x** です。

6 章 リンクアグリゲーション 6-1
6.1 概要 6-1
6.1.1 アグリゲーショングループ、メンバポート、アグリゲートインタフェース 6-1
6.1.2 アグリゲーショングループのメンバポートのステート 6-1
6.1.3 オペレーショナルキー 6-2
6.1.4 コンフィグレーションタイプ 6-2
6.1.5 リンクアグリゲーションモード 6-3
6.1.6 スタティックモードのリンクアグリゲーションの動作 6-3
6.1.7 LACP 6-5
6.1.8 ダイナミックリンクアグリゲーションの動作 6-6
6.1.9 アグリゲーショングループの負荷分散 6-8
6.2 リンクアグリゲーション設定作業リスト 6-8
6.3 アグリゲーショングループの設定 6-8
6.3.1 設定の制限とガイドライン 6-9
6.3.2 アグリゲーショングループの設定 6-9
6.4 アグリゲートインタフェースの設定 6-11
6.4.1 アグリゲートインタフェースの説明の設定 6-11
6.4.2 アグリゲーショングループの Selected ポートの最小と最大数の設定 6-11
6.4.3 アグリゲートインタフェースのシャットダウン 6-13
6.5 グローバルでのリンクアグリゲーションのロードシェアリングモードの設定 6-13
6.5.1 リンクアグリゲーションの表示と維持 6-14
6.6 リンクアグリゲーションの設定例 6-14
6.6.1 スタティックアグリゲーション設定例 6-14
6.6.2 ダイナミックアグリゲーション設定例 6-16

6章 リンクアグリゲーション

6.1 概要

リンクアグリゲーションは、複数のイーサネットインタフェースを束ねて、一つの論理インタフェースとして扱う機能です。図 6-1は、3 つイーサネットインタフェースを束ねて、一つの論理インタフェース（リンクアグリゲーション 1）として接続している例です。

これにより、装置間の接続帯域幅を拡大することができます。また、1 つのイーサネットインタフェースが故障した場合に、残ったイーサネットインタフェースで通信を継続する冗長性を確保できます。



図 6-1 リンクアグリゲーション図

6.1.1 アグリゲーショングループ、メンバポート、アグリゲートインタフェース

アグリゲーショングループは、集約された Ethernet インタフェースのグループです。アグリゲーショングループには、アグリゲートインタフェースと呼ばれる論理的なインタフェースが作成されます。上位レイヤエンティティにリンクアグリゲーションを使用すると、以下のようになります。

アグリゲートインタフェースのレートは、Selected ステートのそのメンバポートのレートの合計と同一です。また通信モードは Selected ステートのメンバポートと同一です。アグリゲーショングループのメンバポートの状態についての詳細は、オペレーションマニュアルのセクション 2 *アクセス "リンクアグリゲーション"の"アグリゲーショングループのメンバポートのステート"*を参照してください。

6.1.2 アグリゲーショングループのメンバポートのステート

アグリゲーショングループのメンバポートは、以下のステートのいずれかとなります。

- **Selected**：ユーザにトラフィックを送受信できます。
- **Unselected**：ユーザにトラフィックを送受信できません。
- **Individual**：Individual ポートは通常の物理インタフェースとしてトラフィックを転送することができます。以下の状態の場合、ポートは Individual 状態となります。
  - 対応するアグリゲートインタフェースがエッジアグリゲートインタフェースとして設定された場合

□　ポートがピアポートから LACPDU（Link Aggregation Control Protocol Data Units）を受信していない場合

6.1.3 オペレーショナルキー

ポートを集約する際に、リンクアグリケーションは、通信速度、通信モードのような設定を含むポート属性にもとづいてオペレーショナルキーをそれぞれのポートに自動的に制御し割り当てます。

リンクアグリゲーショングループ内にある Selected ステートのすべてのメンバポートは、同じオペレーショナルキーを持っています。

6.1.4 コンフィグレーションタイプ

リンクアグリゲーショングループのメンバポートに設定するすべての設定は、グループのポートのアグリゲーションステートに影響を与える可能性があります。影響を与える設定は以下のコンフィグレーションタイプに分類されます。

- **属性コンフィグレーション**– Selected ポートになるためには、メンバポートはアグリゲートインタフェースとして同じ属性の設定を持つ必要があります。表 6-1に属性コンフィグレーションを示します。

  Selected ポートへの同期化に失敗した場合、ポートは Unselected ポートに移行します。ポートが再度 Selected ポートになるために、アグリゲートインタフェースあるいはメンバポートの属性コンフィグレーションを変更します。同期化が失敗しても、アグリゲートインタフェースで変更された属性コンフィグレーションの変更に影響しません。アグリゲートインタフェースが削除された後でも、これらのメンバポートの設定は保持されます。

  属性コンフィグレーションの変更は、リンクアグリゲーションメンバポートのアグリゲーションのステートと動作中のサービスに影響する可能性があります。この影響を確認するため、システムは、メンバポートの属性設定を変更するごとに警告メッセージを表示します。

表 6-1 属性コンフィグレーション

機能	考慮事項
Port Isolation	● ポートのメンバはアイソレーショングループ ● アイソレーショングループの番号 Port Isolationの詳細は、オペレーションマニュアルのセクション2 *アクセス* "*Port Isolation*"を参照してください。
VLAN	以下を含むVLAN属性コンフィグレーション。 ● 許可されたVLAN ID ● PVID ● リンクタイプ（trunk、hybrid、access） ● VLANタグモード VLANの詳細は、オペレーションマニュアルのセクション2 *アクセス* "*VLAN*"を参照してください。

- **プロトコルコンフィグレーション**– プロトコルコンフィグレーションは、アグリゲートインタフェースの変更があってもメンバポートのアグリゲートステートに影響しません。プロトコルコンフィグレーションの例として、MAC アドレス学習があります。

  アグリゲーションインタフェースのプロトコルコンフィグレーションのみ適用します。メンバポートのプロトコルコンフィグレーションは、ポートがアグリゲーショングループから削除されるまで適用されません。

6.1.5 リンクアグリゲーションモード

リンクアグリゲーションは、ダイナミックモードとスタティックモードがあります。

- **スタティックアグリゲーションモード** — 論理インタフェースグループに割り当てたポートがリンクアップした時点で運用を開始します。メンバポートのアグリゲーションステートは対向先の影響を受けません。
- **ダイナミックアグリゲーションモード** — IEEE802.3ad 準拠の LACP を利用したリンクアグリゲーションです。LACP によるネゴシエーションが成功した場合に論理インタフェースとしての運用を開始します。LACP によって、隣接装置との整合性確認やリンクの正常性確認ができます。

6.1.6 スタティックモードのリンクアグリゲーションの動作

I. リファレンスポートの選出

アグリゲーショングループでポートのアグリゲーションステートを設定する場合、システムはリファレンスポートとして自動でメンバポートを選出します。Selected ポートはリファレンスポートとして、同じオペレーショナルキーと属性コンフィグレーションを持つ必要があります。

メンバポートから、アグリゲートインタフェースとして同一の属性を持つ up 状態のリファレンスポートを選択します。

候補となるポートの優先順位は、以下の順番となります。

1) もっとも高いポート優先度
2) 全 2 重/高速
3) 全 2 重/低速
4) 半 2 重/高速
5) 半 2 重/低速

アグリゲートインタフェースと同じ属性コンフィグレーションを持つ候補のポートから、もっとも高い優先度レベルを持つポートがリファレンスポートとして選択されます。

- 同じ優先度を持つポートが複数あり、Selected ポートがある場合、Selected ポートが選ばれます。1 つ以上の最初の Selected ポートがある場合、ポート番号が一番小さい Selected ポートに選択されます。
- 複数のポートに同じ優先度があり、Selected ポートがない場合、ポート番号が一番小さい Selected ポートに選択されます。

II. 各メンバポートのアグリゲーションステートの設定

リファレンスポートを選択すると、システムはスタティックアグリゲーショングループ内の各メンバートの集約状態を設定します。

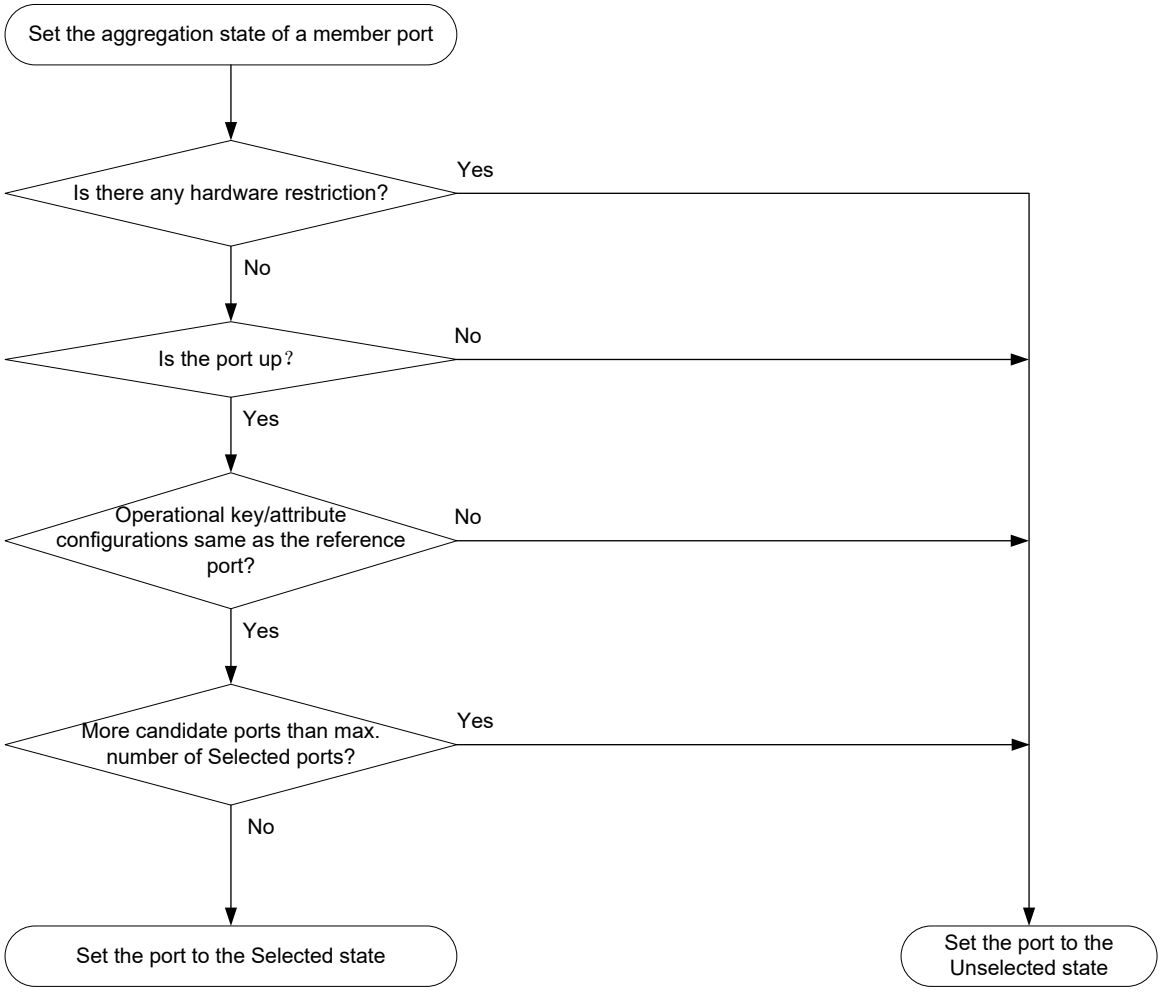


図 6-2 スタティックアグリゲーショングループのアグリゲーションステートの設定

Selected ポートの制限に到達したのち、新しいメンバポートのアグリゲーションの状態は以下の状態によって変わります。

- ポートと Selected ポートが同一の優先度を持つ場合、ポートは Unselected ステートに遷移します。このメカニズムによって既存の Selected ポートでトラフィックの中断を防ぎます。装置の再起動を行うとメンバポートのアグリゲーションステートの再計算が行われます。
- 以下の状態の場合、ポートは Selected ステートに遷移します。
  - □ ポートと Selected ポートが異なる優先度を持つ場合、ポートは少なくとも 1 つの Selected ポートの優先度よりも高い優先度を持ちます。
  - □ アグリゲートインタフェースとして同一の属性コンフィグレーションを持ちます。

オペレーショナルキーと属性コンフィグレーションを変更すると、リンクアグリゲーションメンバポートのアグリゲーションの状態に影響を及ぼす可能性があります。

6.1.7 LACP

ダイナミックアグリゲーションモードは、IEEE802.3ad Link Aggregation Control Protocol（LACP）で規定されています。

LACP は LACP 対応装置と LACPDU（Link Aggregation Control Protocol Data Units）を使用し、情報交換を行います。LACP が有効なアグリゲーショングループのメンバポートは、対向先と情報の交換を行います。メンバポートが LACPDU を受信すると、ほかのメンバポートで受信された情報と受信された情報を比較します。比較することで、2 つのシステム間で Selected ステートになるポートを選定します。

I. LACP 機能

表 6-2に示すように LACP は、基本 LACP 機能と拡張 LACP 機能に分類されます。

表 6-2 基本 LACP 機能と拡張 LACP 機能

カテゴリ	説明
基本LACP機能	LACPシステムプライオリティ、システムMACアドレス、ポートLACPプライオリティ、ポート番号、オペレーショナルキーを含む基本的なLACPDUフィールドから実装されます。
拡張LACP機能	新しいType/Length/Value（TLV）フィールドでLACPDUを拡張して実装されます。

II. LACP 動作モード

LACP はアクティブモードあるいはパッシブモードで動作することができます。

LACP がローカルメンバポートとピアのポート上でパッシブモードとして動作する場合、双方のポートは LACPDU を送信することができません。LACP がローカルメンバポートとピアのポート上でアクティブモードとして動作する場合、双方のポートは LACPDU を送信することができます。

QX-S1100G シリーズはアクティブモードのみをサポートしています。

III. LACP プライオリティ

表 6-3に示すように LACP プライオリティには、LACP システムプライオリティとポートプライオリティの 2 種類があります。値が大きいほどプライオリティは高くなります。

表 6-3 LACP プライオリティ

タイプ	説明
LACPシステムプライオリティ	リンクアグリゲーションで優勢な装置かを決定するために2つの対向装置（あるいはシステム）で使用します。 ダイナミックリンクアグリゲーションでより高いLACPシステムプライオリティを持つ2つの対向装置（あるいはシステム）がメンバポートのSelectedステートになるポートを最初に設定します。 低いプライオリティを持つシステムはそれぞれの対向先のポートと同様にローカルメンバポートのアグリゲーションステートを設定します。

タイプ	説明
ポートプライオリティ	システムで選択されるために、メンバポートのプライオリティが決められます。 より高いポートプライオリティを持つメンバポートが Selectedステートになります。

IV. LACP タイムアウト間隔

LACP タイムアウト間隔は、メンバポートが対向のポートから LACPDU を受信するための待ち時間です。ローカルメンバポートが、LACP タイムアウト間隔に 3 秒を加えた時間内に対向先から LACPDU を受信できない場合、メンバポートは対向先が故障していると認識します。

LACP タイムアウト間隔は、対向先の LACPDU 送信レートも決定します。LACP タイムアウト間隔は以下のタイプを含みます。

- **短いタイムアウト間隔**－タイムアウト間隔は 3 秒です。短いタイムアウト間隔を設定した場合、対向先は LACPDU をただちに送信します。1 秒ごとに 1 つの LACPDU を送信します。
- **長いタイムアウト間隔**－長いタイムアウト間隔は 90 秒です。長いタイムアウト間隔を設定した場合、対向先は LACPDU をロング間隔で送信します。30 秒ごとに 1 つの LACPDU を送信します。

6.1.8 ダイナミックリンクアグリゲーションの動作

I. リファレンスポートの選出

システムは up 状態のインタフェースにある、アグリゲートインタフェースと同じ属性コンフィグレーションを持つメンバポートからリファレンスポートを選出します。Selected ポートはリファレンスポートと同じオペレーショナルキーと属性コンフィグレーションを持つ必要があります。

ローカルシステムは、リファレンスポートを選出するために、リモートシステムと以下の手順が行われます。

1) ローカルシステムのシステム ID をリモートシステムのシステム ID と比較します。システム ID は LACP システムプライオリティと MAC アドレスが含まれます。
   a) LACPプライオリティの値を比較します。LACPプライオリティの値が低いとシステムIDが小さくなり、優位になります。LACPプライオリティの値が同一の場合、2つのシステムは次のb)に進みます。
   b) MACアドレスを比較します。MACアドレスが低いと、システムIDは小さくなり、優位になります。
2) ポート ID を比較します。ポート ID はポート LACP プライオリティとポート番号から構成されます。
   a) システムはポートLACPプライオリティを比較します。ポートLACPプライオリティが低いポートが優位になります。複数のポートが同じポートLACPプライオリティを持つ場合、次のb)に進みます。
   b) システムはポート番号を比較します。より小さいポート番号のポートが優位に

なります。もっとも低いポートIDと同一の属性コンフィグレーションを持つポートがリファレンスポートとして選出されます。

II. メンバポートのアグリゲーションステートの設定

リファレンスポートを選出した後、ダイナミックアグリゲーショングループは、個々のメンバポートのアグリゲーションステートを設定します。

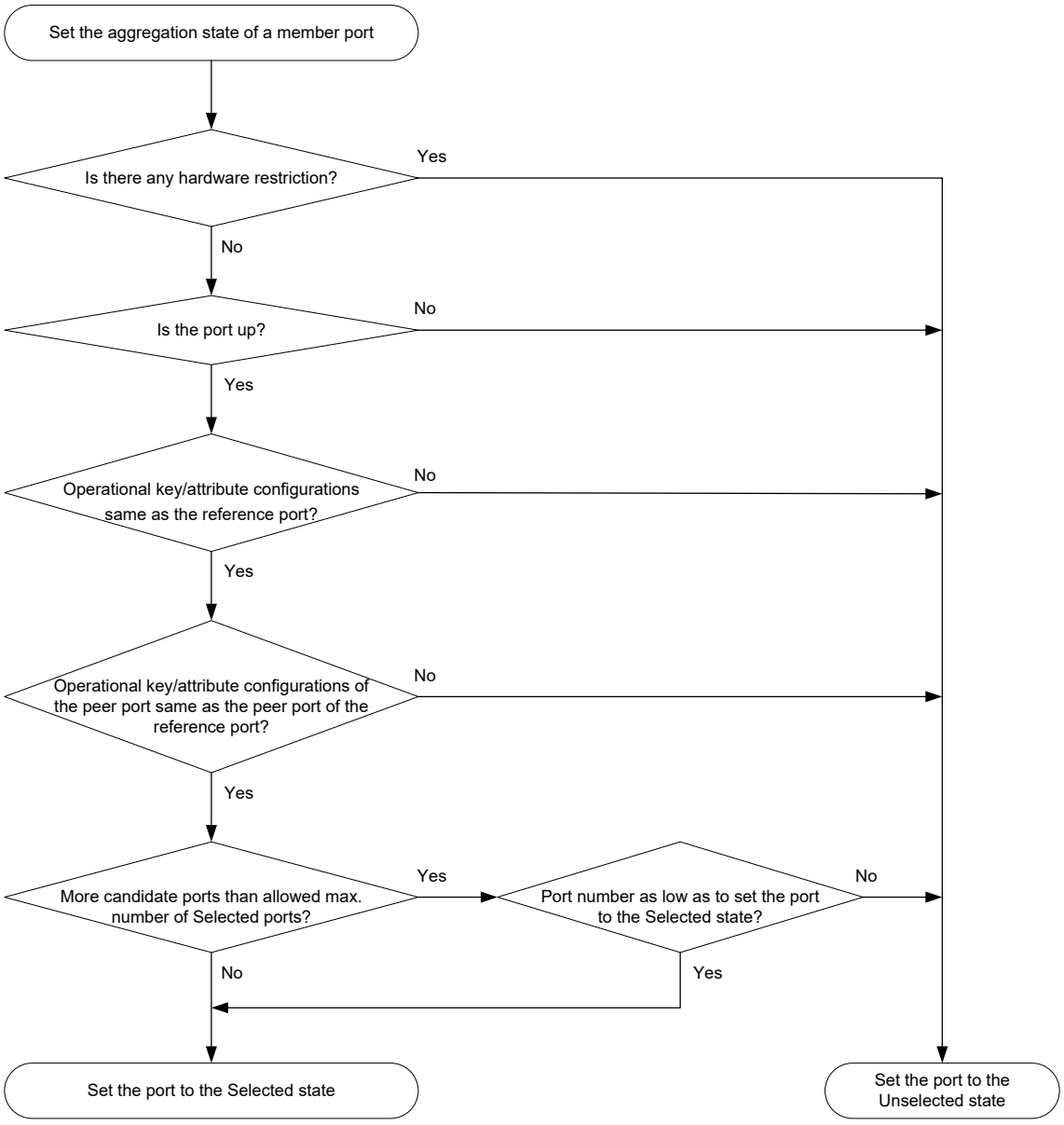


図 6-3 ダイナミックアグリゲーショングループのアグリゲーションステートの設定

高いシステム ID を持つシステムが、リモートシステムのステート状態を認識している間、対向先のポートと同じようにローカルメンバポートのアグリゲーションステートを設定します。

ダイナミックモードでアグリゲートインタフェースを設定する場合、以下のガイドラインに従ってください。

- ダイナミックリンクアグリゲーショングループは、Selected ポートとして全 2 重のみ選択します。
- 安定的なアグリゲーションステートやサービスを中断させないため、メンバポートのオペレーショナルキーや属性コンフィグレーションを変更しないでください。
- Selected ポートが制限に達した後、現在のメンバポートよりも適したポートである場合、ダイナミックアグリゲーショングループに追加されたポートは、Selected ポートになります。

6.1.9 アグリゲーショングループの負荷分散

リンクアグリゲーショングループにおいて、トラフィックは、Selected メンバポートを通り、以下のモードにもとづいて負荷分散が行われます。

- **フローベース負荷分散** —トラフィックはフローごとに負荷分散されます。負荷分散モードはパケットをフローで分類し、同じリンクの同一フローのパケットを転送します。このモードは以下の基準またはその組み合わせによってトラフィックフローを分類することができます。
  - 入力ポート
  - 送信に元あるいは宛先 IP アドレス
  - 送信元あるいは宛先 MAC アドレス
  - 送信元あるいは宛先ポート番号
- **パケットベース負荷分散** — 自動的にパケットタイプ（例 レイヤ 2、IPv4、IPv6）のリンクアグリゲーション負荷分散を選択します。

6.2 リンクアグリゲーション設定作業リスト

作業リスト
（必須設定項目）アグリゲーショングループの設定
（オプション設定項目）アグリゲートインタフェースの設定 • アグリゲートインタフェースの説明の設定 • アグリゲーショングループのSelectedポートの最小と最大数の設定 • アグリゲートインタフェースのシャットダウン
（オプション設定項目）グローバルでのリンクアグリゲーションのロードシェアリングモードの設定

6.3 アグリゲーショングループの設定

この章ではアグリゲーショングループの設定方法について説明します。

6.3.1 設定の制限とガイドライン

I. アグリゲーションメンバインタフェースの制限

インタフェースで表 6-4に示す機能が設定されている場合、アグリゲーショングループにインタフェースを割り当てることができません。

表 6-4 アグリゲーションメンバインタフェースで設定できない機能

インタフェースの機能	参照
MACアドレス認証	オペレーションマニュアルのセクション7 *セキュリティ* “*MACアドレス認証*”を参照してください。
ポートセキュリティ	オペレーションマニュアルのセクション7 *セキュリティ*“*ポートセキュリティ*”を参照してください。
802.1X	オペレーションマニュアルのセクション7 *セキュリティ* “*802.1X*”を参照してください。

アグリゲーションインタフェースとは異なる属性設定がある場合、インタフェースはアグリゲーショングループに参加できません。アグリゲーショングループに参加すると、インタフェースはアグリゲーションインタフェースの属性設定を継承します。属性設定は、アグリゲーションインタフェースでのみ変更できます。

ポートミラーリングのリフレクタポートとして使用されているポートはアグリゲーショングループに割り当てることはできません。リフレクタポートの詳細は、オペレーションマニュアルのセクション 9 *システム管理* "*ポートミラーリング*"を参照してください。

II. 設定の整合性の要件

- アグリゲーションリンクのエンド間に同じアグリゲーションモードを設定する必要があります。
- スタティックアグリゲーションを正常に動作させるには、各アグリゲーションリンクポートの両端に同じアグリゲーションステートを設定する必要があります。
- ダイナミックアグリゲーションを正常に動作させるには、装置と対向装置でポートがアグリゲートされていることを確認してください。2 つのエンド間で、各メンバポートのアグリゲーションステートを自動的に処理することができます。

III. その他

アグリゲートインタフェースを削除する場合、アグリゲーショングループを削除し、そのすべてのメンバポートを削除してください。

6.3.2 アグリゲーショングループの設定

I. スタティックアグリゲーショングループの設定

以下にスタティックアグリゲーショングループの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． アグリゲートインタフェースを作成し、aggregate interface view に移行する	**interface bridge-aggregation** *interface-number*	アグリゲートインタフェースを作成すると、スタティックアグリゲーショングループ番号が、自動的に同一番号で作成されます。
3． system view へ戻る	**quit**	ー
4． 指定されたアグリゲーショングループにインタフェースを割り当てる	1． Ethernet interface view に移行する：**interface** *interface-type interface-number* 2． 指定されたアグリゲーショングループにインタフェースを割り当てる：**port link-aggregation group** *group-id*	アグリゲーショングループに複数のインタフェースを割り当てる場合、このステップを繰り返してください。
5． （オプション設定項目）ポート LACP プライオリティを設定する	**link-aggregation port-priority** *priority*	デフォルト：32768

II. ダイナミックアグリゲーショングループの設定

以下にダイナミックアグリゲーショングループの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． LACP システムプライオリティを設定する	**lacp system-priority** *priority*	デフォルト：32768 LACPシステムプライオリティの値を変えるとポートの状態（selected/unselected）が変わる可能性があります。
3． アグリゲートインタフェースを作成し、aggregate interface view に移行する	**interface bridge-aggregation** *interface-number*	アグリゲートインタフェースを作成すると、スタティックアグリゲーショングループ番号は、自動的に同一番号で作成されます。
4． ダイナミックアグリゲーションモードで動作するように設定する	**link-aggregation mode dynamic**	デフォルト: スタティックアグリゲーションモード
5． system view へ戻る	**quit**	ー
6． 指定されたアグリゲーショングループにインタフェースを割り当てる	1． Ethernet interface view に移行する：**interface** *interface-type interface-number* 2． 指定されたアグリゲーショングループにインタフェースを割り当てる：**port link-aggregation group** *group-id*	アグリゲーショングループに複数のインタフェースを割り当てる場合、このステップを繰り返してください。
7． ポート LACP プライオリティを設定する	**link-aggregation port-priority** *priority*	デフォルト：32768

操作	コマンド	補足
8． short LACP タイムアウト間隔（3 秒）をインタフェースに設定する	**lacp period short**	デフォルト：90秒 ピアはLACPDUをロング間隔で送信します。

6.4 アグリゲートインタフェースの設定

インタフェースで実行できる設定のほとんどは、アグリゲートインタフェースでも実行できます。

6.4.1 アグリゲートインタフェースの説明の設定

インタフェースの目的などを記載するように、管理者用にアグリゲートインタフェースの説明を記載することができます。

以下にアグリゲートインタフェースの説明の設定する方法を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． aggregate interface view に移行する	**interface bridge-aggregation** *interface-number*	—
3． アグリゲートインタフェースの説明を設定する	**description** *text*	デフォルト：*interface-name* **Interface**

6.4.2 アグリゲーショングループの Selected ポートの最小と最大数の設定

重要：

スタティックアグリゲーショングループに Selected ポートの最小値と最大値を設定した場合、正しい接続を保証するために、対向先のアグリゲーショングループに同じ設定をしてください。

アグリゲートリンクの帯域幅は、Selected メンバポートを増やすことで増加させることができます。アグリゲートリンクの Selected ポートが不足することによる輻輳を防ぐため、アグリゲートインタフェースの Selected メンバポートの最小数を設定できます。

この最小数のしきい値はアグリゲーションメンバポートとアグリゲートインタフェースの両方の状態に影響します。

- 適切なメンバポートが最小数を下回った場合、以下の処理が行われます。
  - □ すべてのメンバポートが Unselected ポートに変更します。
  - □ アグリゲートインタフェースのリンクがダウンします。

- Selected ポートに適切なメンバポートの数が最小数以上になった場合、以下の処理が行われます。
  - □ 適切なメンバポートが Selected ポートに変更します。
  - □ アグリゲートインタフェースのリンクがアップします。

アグリゲートグループの Selected ポートの最大数は、設定された最大数あるいはハードウェア性能のいずれか小さいほうで制限されます。

以下の処理を行うことで 2 つのポート間でバックアップを設定することができます。

- アグリゲートグループに 2 つのポートを割り当てます。
- アグリゲートグループの Selected ポートの最大数を 1 に設定します。

このように設定すると、1 つのメンバポートが Selected ポートになります。もう一方のメンバポートが Unselected ポートとなり、バックアップポートとして動作します。

⚠ **重要**：

アグリゲーショングループの Selected ポートの最小パーセンテージを設定した後、ポートがアグリゲーショングループに参加または脱退すると、アグリゲートインタフェースのフラッピングが発生する場合があります。稼働中のネットワークで設定する場合は、この設定の影響を十分に理解してください。

アグリゲーショングループの Selected ポートの最小数または最小パーセンテージを設定できます。アグリゲーションインタフェースで両方の設定をする場合、より高い Selected ポート番号制限が有効になります。

Selected ポートの最小数と最大数は、アグリゲーションリンクの両端で同じでなければなりません。

Selected ポートの最小パーセンテージは、アグリゲーションリンクの両端で同じでなければなりません。

アグリゲーショングループの場合、Selected ポートの最大数は、Selected ポートの最小数以上である必要があります。

以下に Selected ポートの最小と最大数の設定方法を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. aggregate interface view に移行する	**interface bridge-aggregation** *interface-number*	—
3. アグリゲーショングループの Selected ポートの最小数あるいは最小パーセンテージを設定する	• Selectedポートの最小数を設定する **link-aggregation selected-port minimum** *min-number* • Selectedポートの最小パーセンテージを設定する **link-aggregation selected-port minimum percentage** *number*	デフォルト：設定なし

操作	コマンド	補足
4. アグリゲーショングループの Selected ポートの最大数を設定する	**link-aggregation selected-port maximum** *max-number*	デフォルト：8

6.4.3 アグリゲートインタフェースのシャットダウン

アグリゲートインタフェースをシャットダウンあるいはアップすると、対応するアグリゲーショングループのステートとリンク状態に以下のような影響があります。

- アグリゲートインタフェースがシャットダウンした場合、アグリゲーショングループのすべての Selected ポートは Unselected になります。
- アグリゲートインタフェースをアップさせると、対応するアグリゲーショングループのポートの Selected ステートを再計算します。

以下にアグリゲートインタフェースをシャットダウンする方法を示します。

操作	コマンド
1. system view に移行する	**system-view**
2. aggregate interface view に移行する	**interface bridge-aggregation** *interface-number*
3. アグリゲートインタフェースをシャットダウンする	**shutdown**

6.5 グローバルでのリンクアグリゲーションのロードシェアリングモードの設定

すべてのリンクアグリゲーショングループにグローバル負荷分散モードを設定できます。

リンクアグリゲーショングループに負荷分散モードを設定すると、ECMP ルート間でトラフィックが不均衡になる可能性があります。ライブネットワークでこの機能を設定するときは、この機能の影響を十分に理解していることを確認してください。

装置でサポートされているグローバルな負荷分散モードは次のとおりです。

- パケットタイプに基づいて自動的に決定されるロードシェアリングモード
- 送信元 IP
- 宛先 IP
- 送信元 MAC
- 宛先 MAC
- 入力ポート
- 送信元 IP および宛先 IP
- 送信元 IP および送信元ポート
- 宛先 IP および宛先ポート
- 送信元 IP、送信元ポート、宛先 IP、および宛先ポート
- 入力ポート、送信元 MAC、および宛先 MAC の任意の組み合わせ

以下にグローバルでのリンクアグリゲーションモードの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． グローバルでのロードシェアリングモードを設定する	**link-aggregation global load-sharing mode** { **destination-ip** | **destination-mac** | **destination-port** | **ingress-port** | **source-ip** | **source-mac** | **source-port** } *	デフォルト : パケットは次の情報に基づいて負荷分散されます。 ● 送信元および宛先IPアドレス ● 送信元および宛先MACアドレス

6.5.1 リンクアグリゲーションの表示と維持

すべての view で **display** コマンドを実行し、user view で **reset** コマンドを実行できます。

操作	コマンド
1つ以上のアグリゲーションインタフェースを表示する	**display interface** [**bridge-aggregation** [*interface-number*]] [**brief** [**description** | **down**]]
ローカルシステムIDを表示する	**display lacp system-id**
グローバルあるいはグループのロードシェアリングモードを表示する	**display link-aggregation load-sharing mode** [**interface** [**bridge-aggregation** *interface-number*]]
アグリゲーションメンバポートのリンクアグリゲーションの詳細情報を表示する	**display link-aggregation member-port** [*interface-list*]
すべてのアグリゲーショングループの概要を表示する	**display link-aggregation summary**
アグリゲーショングループの詳細情報を表示する	**display link-aggregation verbose** [**bridge-aggregation** [*interface-number*]]
ポートのLACP統計情報をクリアする	**reset lacp statistics** [**interface** *interface-list*]
アグリゲートインタフェース統計情報を削除する	**reset counters interface** [**bridge-aggregation** [*interface-number*]]

6.6 リンクアグリゲーションの設定例

6.6.1 スタティックアグリゲーション設定例

I. ネットワーク要件

図 6-4に示すように以下の要件を設定します。

- Device A と Device B の両方で、スタティックアグリゲーショングループを設定します。
- 片端で VLAN10 を有効にし、VLAN10 でアグリゲートリンクの対向先と通信します。
- 片端で VLAN20 を有効にし、VLAN20 でアグリゲートリンクの対向先と通信します。

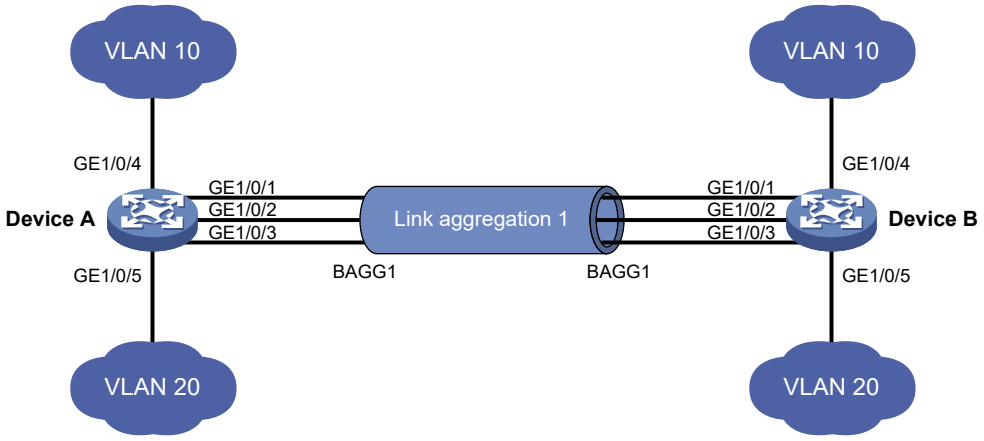


図 6-4 ネットワーク図

II. 設定手順

1)　Device A を設定します。

VLAN 10 を作成し、GigabitEthernet 1/0/4 に割り当てます。

```
<DeviceA> system-view
[DeviceA] vlan 10
[DeviceA-vlan10] port gigabitethernet 1/0/4
[DeviceA-vlan10] quit
```

VLAN 20 を作成し、GigabitEthernet 1/0/5 に割り当てます。

```
[DeviceA] vlan 20
[DeviceA-vlan20] port gigabitethernet 1/0/5
[DeviceA-vlan20] quit
```

アグリゲートインタフェース Bridge-Aggregation 1 を作成します。

```
[DeviceA] interface bridge-aggregation 1
[DeviceA-Bridge-Aggregation1] quit
```

GigabitEthernet 1/0/1～GigabitEthernet 1/0/3 にリングアグリゲーショングループ 1 を割り当てます。

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-aggregation group 1
[DeviceA-GigabitEthernet1/0/1] quit
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port link-aggregation group 1
[DeviceA-GigabitEthernet1/0/2] quit
[DeviceA] interface gigabitethernet 1/0/3
```

```
[DeviceA-GigabitEthernet1/0/3] port link-aggregation group 1
[DeviceA-GigabitEthernet1/0/3] quit
```

アグリゲートインタフェース Bridge-Aggregation 1 をトランクポートとして作成し、VLAN10、VLAN20 を割り当てます。

```
[DeviceA] interface bridge-aggregation 1
[DeviceA-Bridge-Aggregation1] port link-type trunk
[DeviceA-Bridge-Aggregation1] port trunk permit vlan 10 20
[DeviceA-Bridge-Aggregation1] quit
```

2)　Device A の設定と同様に Device B を設定します。（詳細は省略します。）

III. 設定の確認

Device A ですべてのアグリゲーショングループの詳細情報を表示します。

```
[DeviceA] display link-aggregation verbose
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected, I -- Individual
Port: A -- Auto port, M -- Management port, R -- Reference port
Flags:  A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
        D -- Synchronization, E -- Collecting, F -- Distributing,
        G -- Defaulted, H -- Expired

Aggregate Interface: Bridge-Aggregation1
Aggregation Mode: Static
Loadsharing Type: NonS
Management VLANs: None
  Port             Status  Priority Oper-Key
  GE1/0/1          S       32768    1
  GE1/0/2          S       32768    1
  GE1/0/3          S       32768    1
```

出力では、リンクアグリゲーション 1 がスタティックアグリゲーショングループで、3 つの Selected ポートがあることを示しています。

6.6.2 ダイナミックアグリゲーション設定例

I. ネットワーク要件

図 6-5に示すように以下の要件を設定します。

- Device A と Device B の両方で、ダイナミックアグリゲーショングループを設定します。
- 片端で VLAN10 を有効にし、VLAN10 でアグリゲートリンクの対向先と通信します。
- 片端で VLAN20 を有効にし、VLAN20 でアグリゲートリンクの対向先と通信します。

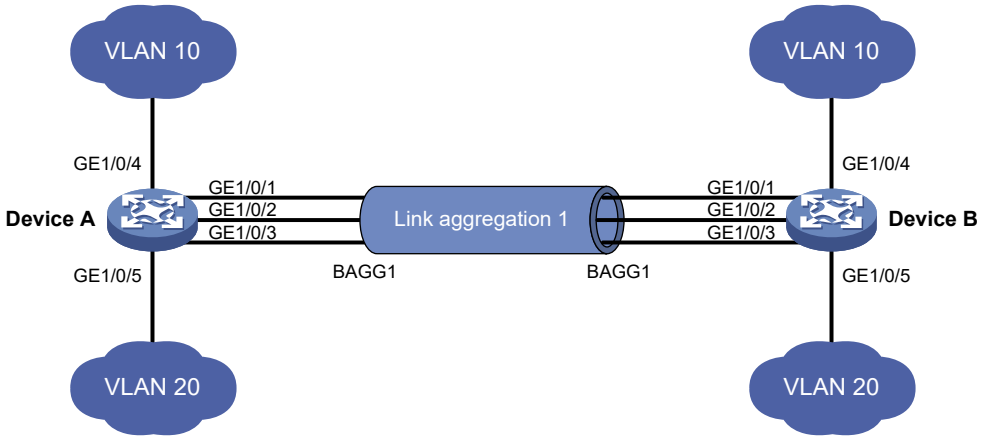


図 6-5 ネットワーク図

II. 設定手順

1)　Device A を設定します。

VLAN 10 を作成し、GigabitEthernet 1/0/4 に割り当てます。

```
<DeviceA> system-view
[DeviceA] vlan 10
[DeviceA-vlan10] port gigabitethernet 1/0/4
[DeviceA-vlan10] quit
```

VLAN 20 を作成し、GigabitEthernet 1/0/5 に割り当てます。

```
[DeviceA] vlan 20
[DeviceA-vlan20] port gigabitethernet 1/0/5
[DeviceA-vlan20] quit
```

アグリゲートインタフェース Bridge-Aggregation 1 を作成し、ダイナミックリンクアグリゲーションモードを設定します。

```
[DeviceA] interface bridge-aggregation 1
[DeviceA-Bridge-Aggregation1] link-aggregation mode dynamic
[DeviceA-Bridge-Aggregation1] quit
```

GigabitEthernet 1/0/1～GigabitEthernet 1/0/3 にリングアグリゲーショングループ 1 を割り当てます。

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-aggregation group 1
[DeviceA-GigabitEthernet1/0/1] quit
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port link-aggregation group 1
```

```
[DeviceA-GigabitEthernet1/0/2] quit
[DeviceA] interface gigabitethernet 1/0/3
[DeviceA-GigabitEthernet1/0/3] port link-aggregation group 1
[DeviceA-GigabitEthernet1/0/3] quit
```

アグリゲートインタフェース Bridge-Aggregation 1 をトランクポートとして作成し、VLAN10、VLAN20 を割り当てます。

```
[DeviceA] interface bridge-aggregation 1
[DeviceA-Bridge-Aggregation1] port link-type trunk
[DeviceA-Bridge-Aggregation1] port trunk permit vlan 10 20
[DeviceA-Bridge-Aggregation1] quit
```

2)　Device A の設定と同様に Device B を設定します。（詳細は省略します。）

III. 設定の確認

Device A ですべてのアグリゲーショングループの詳細情報を表示します。

```
[DeviceA] display link-aggregation verbose
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected, I -- Individual
Port: A -- Auto port, M -- Management port, R -- Reference port
Flags:  A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
        D -- Synchronization, E -- Collecting, F -- Distributing,
        G -- Defaulted, H -- Expired

Aggregate Interface: Bridge-Aggregation1
Creation Mode: Manual
Aggregation Mode: Dynamic
Loadsharing Type: NonS
Management VLANs: None
System ID: 0x8000, 000f-e267-6c6a
Local:
  Port                Status   Priority Index    Oper-Key               Flag
  GE1/0/1(R)          S        32768    11       1                      {ACDEF}
  GE1/0/2             S        32768    12       1                      {ACDEF}
  GE1/0/3             S        32768    13       1                      {ACDEF}
Remote:
  Actor               Priority Index    Oper-Key SystemID               Flag
  GE1/0/1             32768    81       1        0x8000, 000f-e267-57ad {ACDEF}
  GE1/0/2             32768    82       1        0x8000, 000f-e267-57ad {ACDEF}
  GE1/0/3             32768    83       1        0x8000, 000f-e267-57ad {ACDEF}
```

出力では、リンクアグリゲーション 1 がダイナミックアグリゲーショングループで、3 つの Selected ポートがあることを示しています。

目次

このセクションのページは**2-x-x** です。

7 章 Port Isolation 7-1
7.1 アイソレーショングループへのポートの追加 7-1
7.2 ポートアイソレーションの表示と維持 7-2
7.3 ポートアイソレーションの設定例 7-2
7.3.1 ネットワーク要件 7-2
7.3.2 設定手順 7-3
7.3.3 設定の確認 7-3

7章 Port Isolation

🕮 **メモ：**

QX-S1100G シリーズは、ポートアイソレーションと、MLD スヌーピングを同時に使用することができません。

ポートアイソレーション(Port Isolation)機能はデータのプライバシーやセキュリティのために、VLAN を使用することなくレイヤ 2 トラフィックを分離します。

アイソレーショングループのポートは互いに通信することができませんが、外部のアイソレーショングループのポートと通信することができます。

7.1 アイソレーショングループへのポートの追加

装置は手動で設定することで複数のアイソレーショングループをサポートしています。ポートの追加数に制限はありません。

以下にアイソレーショングループにポートを割り当てる設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． アイソレーショングループを作成する	**port-isolate group** *group-id*	デフォルト：設定なし
3． interface view に移行する	● Layer 2 Ethernet interface view に移行する： **interface** *interface-type interface-number* ● aggregate interface viewに移行する： **interface bridge-aggregation** *interface-number*	● Layer 2 Ethernet interface view に設定すると設定されたインタフェースで適用されます。 ● aggregate interface viewに設定するとアグリゲートインタフェースとアグリゲーションメンバポートに適用されます。アグリゲートインタフェースの設定を適用できない場合、アイソレーショングループにメンバポートが割り当てられません。アグリゲーションメンバポートで故障が発生すると、装置はポートをスキップし、他のアイソレーショングループにメンバポートを割り当てることができます。

操作	コマンド	補足
4. アイソレーショングループにポートを追加する	**port-isolate enable group** *group-id*	デフォルト：設定なし ポートは1つのアイソレーショングループに割り当てることができます。**port-isolate enable group**コマンドを複数行った場合、最後に行った設定が適用されます。

7.2 ポートアイソレーションの表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
アイソレーショングループ情報を表示する	**display port-isolate group** [*group-id*]

7.3 ポートアイソレーションの設定例

7.3.1 ネットワーク要件

図 7-1に示すように以下の要件を設定します。

- Host A は GigabitEthernet 1/0/1 に接続されています。Host B は GigabitEthernet 1/0/2 に接続されています。Host C は GigabitEthernet 1/0/3 に接続されています。
- Device(装置)は GigabitEthernet 1/0/4 を通してインタネットに通信できます。

各 Host はインタネットには通信可能であるが、レイヤ 2 で互いに通信できないように設定します。

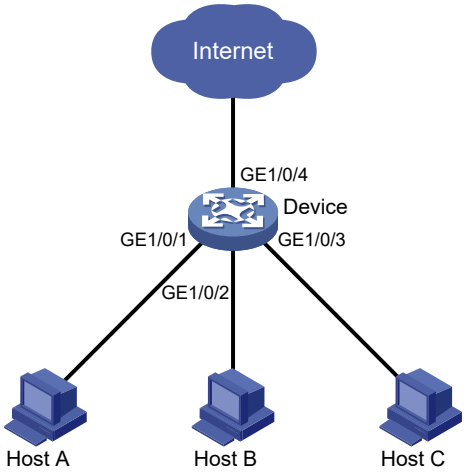


図 7-1 ネットワーク図

7.3.2 設定手順

アイソレーショングループ 1 を作成します。

```
<Device> system-view
[Device] port-isolate group 1
```

GigabitEthernet 1/0/1、GigabitEthernet 1/0/2、GigabitEthernet 1/0/3 をアイソレーショングループ 1 に割り当てます。

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] port-isolate enable group 1
[Device-GigabitEthernet1/0/1] quit
[Device] interface gigabitethernet 1/0/2
[Device-GigabitEthernet1/0/2] port-isolate enable group 1
[Device-GigabitEthernet1/0/2] quit
[Device] interface gigabitethernet 1/0/3
[Device-GigabitEthernet1/0/3] port-isolate enable group 1
[Device-GigabitEthernet1/0/3] quit
```

7.3.3 設定の確認

アイソレーショングループ 1 の情報を表示します。

```
[Device] display port-isolate group 1
 Port isolation group information:
 Group ID: 1
 Group members:
   GigabitEthernet1/0/1     GigabitEthernet1/0/2     GigabitEthernet1/0/3
```

出力は、GigabitEthernet 1/0/1、GigabitEthernet 1/0/2、GigabitEthernet 1/0/3 がアイソレーショングループ 1 に割り当てられていることを示します。その結果、Host A、Host B、Host C はレイヤ 2 で互いの通信は遮断されています。

目次

このセクションのページは**2-x-x** です。

8章 STP 8-1
8.1 STP 8-1
8.1.1 STPのプロトコルフレーム 8-1
8.1.2 STPの基本概念 8-3
8.1.3 STPアルゴリズムの計算プロセス 8-5
8.2 RSTP 8-12
8.2.1 RSTPの基本概念 8-12
8.2.2 RSTPの動作 8-13
8.2.3 RSTPのBPDU処理 8-13
8.3 PVST 8-14
8.3.1 PVSTのプロトコルフレーム 8-14
8.3.2 PVSTの基本概念 8-15
8.3.3 PVSTの動作 8-15
8.4 MSTP 8-15
8.4.1 MSTPの特徴 8-16
8.4.2 MSTPのプロトコルフレーム 8-16
8.4.3 MSTPの基本概念 8-18
8.4.4 MSTPの動作 8-22
8.4.5 装置でのMSTPの実行 8-23
8.4.6 高速収束メカニズム 8-23
8.5 プロトコルと規格 8-26
8.6 スパニングツリー設定作業リスト 8-26
8.6.1 STP設定作業リスト 8-27
8.6.2 RSTP設定作業リスト 8-28
8.6.3 PVST設定作業リスト 8-29
8.6.4 MSTP設定作業リスト 8-30
8.7 動作モードの設定 8-30
8.8 MST regionの設定 8-31
8.9 RootブリッジとSecondary Rootブリッジの設定 8-32
8.9.1 Rootブリッジの設定 8-33
8.9.2 Secondary Rootブリッジの設定 8-33
8.10 ブリッジプライオリティの設定 8-33
8.11 MST regionの最大ホップ数の設定 8-34
8.12 ネットワークダイアメータの設定 8-34
8.13 スパニングツリータイマの設定 8-35
8.13.1 設定の制限とガイドライン 8-35
8.13.2 設定手順 8-36
8.14 タイムアウトファクタの設定 8-36
8.15 BPDU最大送出レートの設定 8-37
8.16 Edgeポートの設定 8-37
8.16.1 設定の制限とガイドライン 8-38
8.16.2 設定手順 8-38
8.17 ポートパスコストの設定 8-38
8.17.1 デフォルトパスコストの計算時の基準指定 8-38
8.17.2 ポートのパスコストの設定 8-40

8.17.3 設定例 ... 8-40
8.18 ポートプライオリティの設定 ... 8-41
8.19 Point-to-Pointリンクの設定 ... 8-41
8.19.1 設定の制限とガイドライン ... 8-42
8.19.2 設定手順 ... 8-42
8.20 MSTPパケットのフォーマット設定 ... 8-42
8.21 ポート遷移状態情報の出力の有効化 ... 8-43
8.22 スパニングツリー機能の有効化 ... 8-43
8.22.1 STP/RSTP/MSTPモードでのスパニングツリー機能の有効化 ... 8-43
8.22.2 PVSTモードでのスパニングツリー機能の有効化 ... 8-44
8.23 mCheck機能の設定 ... 8-44
8.23.1 設定の制限とガイドライン ... 8-44
8.23.2 グローバルでのmCheckの設定手順 ... 8-45
8.23.3 interface viewでのmCheckの実行 ... 8-45
8.24 Digest Snoopingの設定 ... 8-45
8.24.1 設定の制限とガイドライン ... 8-46
8.24.2 設定手順 ... 8-46
8.24.3 Digest Snooping設定例 ... 8-46
8.25 No Agreement Checkの設定 ... 8-47
8.25.1 設定要件 ... 8-49
8.25.2 設定手順 ... 8-49
8.25.3 No Agreement Check設定例 ... 8-49
8.26 TC snoopingの設定 ... 8-50
8.26.1 設定の制限とガイドライン ... 8-50
8.26.2 設定手順 ... 8-50
8.27 保護機能の設定 ... 8-50
8.27.1 保護機能の設定作業リスト ... 8-50
8.27.2 BPDUガードの設定 ... 8-51
8.27.3 Rootガードの有効化 ... 8-52
8.27.4 Loopガードの有効化 ... 8-52
8.27.5 ポート役割の制限機能の設定 ... 8-53
8.27.6 TC-BPDUガードの有効化 ... 8-54
8.27.7 BPDUドロップ機能の有効化 ... 8-54
8.27.8 PVST BPDUガードの有効化 ... 8-55
8.28 TC BPDUの検出、受信イベントのログ作成の有効化 ... 8-55
8.29 BPDUガードによりシャットダウンされたエッジポートの再アクティブ化の無効化 ... 8-56
8.30 新規ルートブリッジの選択、トポロジ変更イベントによるSNMP notificationの有効化 ... 8-56
8.31 スパニングツリーの表示と維持 ... 8-57
8.32 スパニングツリー設定例 ... 8-57
8.32.1 MSTP設定例 ... 8-57
8.32.2 PVST設定例 ... 8-62

8章 STP

スパニングツリーは、ループ検出時に物理的に通信しないインタフェースを設定することによりループを防止します。

STP は、狭義では、IEEE802.1d STP を意味しており、広義では IEEE802.1d STP と拡張されたスパニングツリープロトコル（RSTP（Rapid Spanning Tree Protocol）、MSTP（Multiple Spanning Tree Protocol）、PVST（Per-VLAN Spanning Tree）など）を含めたものを意味します。

8.1 STP

STP（Spanning Tree Protocol）は、IEEE の 802.1d で規定されている、LAN（local area network）の円環上（ループ状）に形成されたレイヤ 2 プロトコルにおいてデータトラフィックが永続的に流れ続けることを防止するプロトコルです。

STP が動作している装置は、ネットワークでループを検出します。ほかの装置と情報を交換し、ループがないツリー構成にループの構成を設定させ、特定のポートをブロックすることで、ループを防ぎます。

8.1.1 STP のプロトコルフレーム

スパニングツリープロトコルでは、リンクレイヤパケットの BPDU（Bridge Protocol Data Units）を使用して、情報交換、状態の維持管理を行います。この章ではスパニングツリーのすべてのタイプを代表して BPDU を使用します。

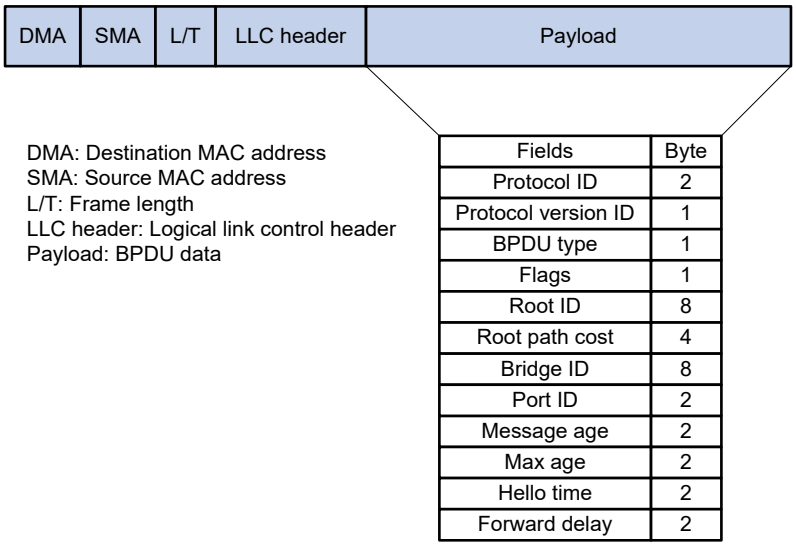
STP が有効なネットワークの装置は BPDU を交換してスパニングツリーを確立します。BPDU はスパニングツリーの計算を行うために十分な情報を含みます。

STP では、以下の 2 種類の BPDU を使用します。

- **Configuration BPDU** — スパニングツリーを構成し、ツリートポロジを維持するために使います。
- **TCN（Topology change notification） BPDU** — ネットワークトポロジの変更を通知するために使います。

I. Configuration BPDU

装置は Root ブリッジを選択し Root ポートを決定するために、ネットワーク内の装置間で Configuration BPDU の交換を行います。図 8-1に Configuration BPDU のフォーマットを示します。



Fields	Byte
Protocol ID	2
Protocol version ID	1
BPDU type	1
Flags	1
Root ID	8
Root path cost	4
Bridge ID	8
Port ID	2
Message age	2
Max age	2
Hello time	2
Forward delay	2

図 8-1 Configuration BPDU のフォーマット

Configuration BPDU には、ネットワークトポロジを構築するための以下のデータが書き込まれています。

- **Protocol ID**– IEEE802.1d を示します。0x0000 で固定です。
- **Protocol version ID**– スパニングツリープロトコルバージョンの ID です。STP は 0x00 です。
- **BPDU type**– BPDU のタイプです。Configuration BPDU は 0x00 です。
- **Flags**– 8 ビットフィールドは BPDU の目的を示します。最下位ビットは TC（Topology Change）フラグです。最上位ビットは TCA（Topology Change Acknowledge）フラグです。ほかのビットは予約済みビットです。
- **Root ID**– Root ブリッジの ID です。Root ブリッジのプライオリティと MAC アドレスで構成されます。
- **Root path cost**– Root ブリッジまでの最短ルートのコストです。
- **Bridge ID**– Designated ブリッジの ID です。Designated ブリッジのプライオリティと MAC アドレスで構成されます。
- **Port ID**– Designated ブリッジのポート ID です。Designated ブリッジのプライオリティとグローバルポート番号で構成されます。
- **Message age**– ネットワーク内で転送された Configuration BPDU の経過時間です。
- **Max age**– 装置に記録された Configuration BPDU の有効時間です。
- **Hello time**– Configuration BPDU の転送間隔です。
- **Forward delay**– 装置の状態が遷移する場合の遅延時間です。

装置はスパニングツリーの計算を行うため、Root ブリッジ ID（Root ID）、Root パスコスト(Root path cost)、Designated ブリッジ ID（Bridge ID）、Designated ポート ID（Port ID）、Message age、Max age、Hello 時間（Hello time）、Forward delay を使用します。

II. TCN BPDU

TCN BPDU には、ネットワークトポロジの変更を通知します。図 8-2に TCN BPDU のフォーマットを示します。

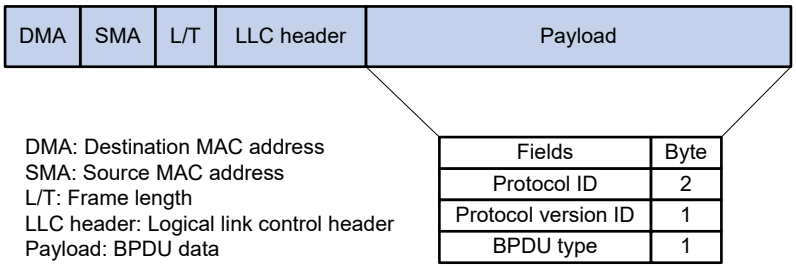


図 8-2 TCN BPDU のフォーマット

TCN BPDU には以下のデータが書き込まれています。

- **Protocol ID**– IEEE802.1d を示します。0x0000 で固定です。
- **Protocol version ID**– スパニングツリーの Version ID です。STP のプロトコルバージョン ID は 0x00 です。
- **BPDU type**– BPDU のタイプです。TCN BPDU の値は 0x80 です。

ブリッジで以下のいずれかのイベントが発生した場合、Root ブリッジ以外のブリッジが TCN BPDU を送信します。

- ポートが Forwarding 状態に遷移し、ブリッジに少なくとも 1 つの Designated ポートがあります。
- ポートが Forwarding 状態あるいは Learning 状態から、Blocking 状態に遷移します。

Root ブリッジ以外のブリッジはネットワークトポロジの変更を通知するため、TCN BPDU を使用します。そして Root ブリッジは Configuration BPDU の TC フラグを設定し、ほかのブリッジに転送します。

8.1.2 STP の基本概念

I. Root ブリッジ

STP のツリーは、1 つの Root ブリッジと複数のほかのブリッジで構成されます。ほかのブリッジは“Leaf ノード”と呼ばれます。Root ブリッジはトポロジの変化に応じて変更することができます。

ネットワークの初期設定において、各装置は Root ブリッジとして Configuration BPDU を生成し、定期的に送信します。ネットワークの収束後、Root ブリッジのみが定期的に Configuration BPDU を送信します。ほかの装置は、BPDU を転送するのみとなります。

II. Root ポート

Root ブリッジ以外の装置において、Root ブリッジへのパスコストがもっとも低い 1 つのポートが Root ポートとなります。Root ポートは、Root ブリッジの装置と通信を行うポートになります。なお、Root ブリッジの装置には、Root ポートはありません。

III. Designated ブリッジと Designated ポート

分類	Designated ブリッジ	Designated ポート
装置	ローカル装置に直接、接続されている装置でローカルの装置にBPDUの転送を行います。	Designatedブリッジがこのポートにbpduを転送します。
LAN	LANセグメントにBPDUを転送します。	Designatedブリッジが、このLANセグメントにBPDUを転送します。

図 8-3に示すように、Device B と Device C は LAN に直接接続されています。

Device A がポート A1 を経由して Device B に BPDU を転送する場合、Designated ブリッジと Designated ポートは以下のようになります。

- Device B の Designated ブリッジは Device A です。
- Device B の Designated ポートは Device A のポート A1 です。

Device B が LAN に BPDU を転送する場合、Designated ブリッジと Designated ポートは以下のようになります。

- LAN の Designated ブリッジは Device B です。
- LAN の Designated ポートは Device B のポート B2 です。

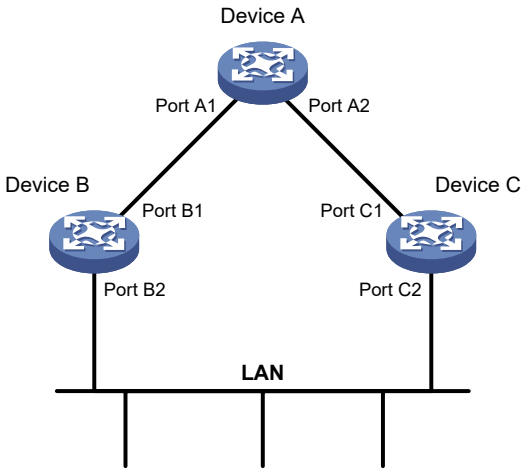


図 8-3 Designated ブリッジと Designated ポート

IV. ポート状態

STP のポート状態を表 8-1に示します。

表 8-1 STP のポート状態

状態	BPDU の送受信	MAC アドレスの学習	データの転送
Disabled	No	No	No
Listening	Yes	No	No
Learning	Yes	Yes	No
Forwarding	Yes	Yes	Yes
Blocking	受信のみ	No	No

V. パスコスト

パスコストは、STP でリンクを選択するのに使用される値です。STP はリンク間のパスコストを比較し、もっともパスコストの小さいリンクを使ったトポロジを構成します。STP はループがないようにネットワークを構成させるため、冗長な STP のリンクをブロックします。

8.1.3 STP アルゴリズムの計算プロセス

スパニングツリーのアルゴリズムは以下の計算プロセスを使用しています。動作をわかりやすくするため、簡単な例をもとに説明します。

I. ネットワークの初期化

STP アルゴリズムは以下のプロセスを使用します。

1)　ネットワークの初期化

装置の初期化として、各ポートは以下の内容で BPDU を作成します。

- □　ポートを Designated ポートとします。
- □　装置自身を Root ブリッジとします。
- □　Root パスコストを 0 とします。
- □　Designated ブリッジ ID を自身の Device ID とします。

2)　Root ブリッジの選択

最初にネットワーク上の STP が有効な各装置は、自身が Root ブリッジとして仮定し、Root ブリッジを自身の Device ID とします。BPDU の交換を行うことによって、装置は自身の Root ブリッジ ID と、Root ブリッジとなるもっとも小さい Root ブリッジ ID の装置を選択するため、Root ブリッジ ID を比較します。

3)　Root ブリッジでない Root ポートと Designated ポートを選択します。

操作	説明
1	Rootブリッジ以外の装置は、もっとも優先度の高いConfiguration BPDUを受信したポートをRootポートと認識します。表 8-2にConfiguration BPDUを選択する方法を記載します。
2	Configuration BPDUとRootポートのパスコストをもとにして、装置はほかのポートのDesignatedポートのConfiguration BPDUを計算します。 ● RootブリッジIDをRootポートで受信したConfiguration BPDUのRootブリッジIDに書き換えます。 ● RootポートコストをRootポートで受信するConfiguration BPDUのRootポートコストにRootポートのパスコストを加算した値に書き換えます。 ● DesignatedブリッジIDをその装置のブリッジIDに書き換えます。 ● DesignatedポートIDを出力ポートのIDに書き換えます。

操作	説明
3	書き換えたConfiguration BPDUとそのポートで受信するConfiguration BPDUを比較することで、そのポートの役割が決定します。 ● 書き換えたConfiguration BPDUの優先度が高い場合、装置は以下の処理を行います。 　• ポートはDesignatedポートと認識します。 　• ポートのConfiguration BPDUを計算したConfiguration BPDUに書き換えます。 　• Configuration BPDUを定期的に送信します。 ● そのポートで受信するConfiguration BPDUの優先度が高い場合、そのポートからConfiguration BPDUを送信することを止め、対向装置からのConfiguration BPDUの受信だけを行います。

ネットワークのトポロジが安定している場合、Root ポートと Designated ポートはユーザのトラフィックのみを転送します。ほかのブロックされたポートは BPDU の受信のみを行い、BPDU やトラフィックの転送を行いません。

表 8-2 もっとも優先度の高い Configuration BPDU の選出

操作	アクション
1	ポートでConfiguration BPDUを受信し、装置はポートによって作成されたConfiguration BPDUと受信したConfiguration BPDUの優先度を比較します。 ● 受信したConfiguration BPDUの優先度が低い場合、装置は受信したConfiguration BPDUを廃棄し、ポートで作成されたConfiguration BPDUを保存します。 ● 受信したConfiguration BPDUの優先度が高い場合、受信したConfiguration BPDUの内容にもとづいてポートで作成したConfiguration BPDUの内容を書き換えます。
2	装置はすべてのConfiguration BPDUを比較し、もっとも優先度の高いConfiguration BPDUを選出します。

以下に Configuration BPDU の比較順序を示します。

a) RootブリッジIDがもっとも小さいConfiguration BPDUの優先度がもっとも高くなります。

b) すべてのConfiguration BPDUのRootブリッジIDが同じ場合には、次にRootパスコストを比較します。Configuration BPDUのRootパスコストとその受信ポートのパスコストの加算値のもっとも小さいConfiguration BPDUの優先度が高くなります。たとえばConfiguration BPDUのRootパスコストと受信したポートのパスコストがSとします。もっとも小さいSのConfiguration BPDUがもっとも高い優先度となります。

c) すべてのConfiguration BPDUのRootブリッジIDとSが同じ場合、以下の領域を順に比較します。

- □ Designated ブリッジ ID
- □ Designated ポート ID
- □ 受信したポートの ID

Designated ブリッジ ID、Designated ポート ID あるいは受信したポートの ID の小さい Configuration BPDU が選択されます。

Root ブリッジの場合、ツリー構造のトポロジは、Root ポート、Designated ポートが選択されます。

II. STP アルゴリズム計算の例

図 8-4に STP アルゴリズムの計算例を示します。

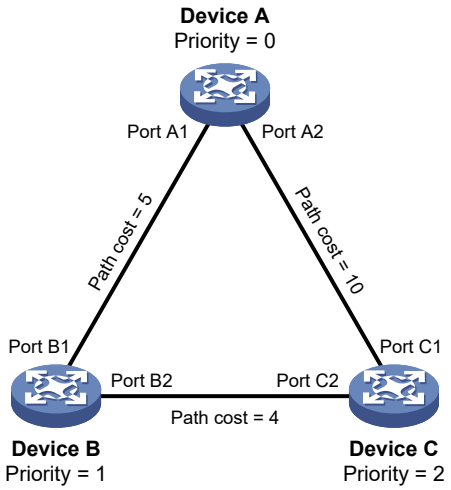


図 8-4 STP アルゴリズム

図 8-4に示すように、Device A、Device B、Device C の優先度の値は、それぞれ 0、1、2 で、3 つの装置間のリンクパスコストは、それぞれ 5、10、4 です。

1)　装置の初期状態

表 8-3に示すように各 Configuration BPDU は Root ブリッジ ID、Root パスコスト、Designated ブリッジ ID、Designated ポート ID を含みます。

表 8-3 各装置の初期状態

装置	ポート名	ポートの Configuration BPDU
Device A	ポートA1	{0, 0, 0, ポートA1}
	ポートA2	{0, 0, 0, ポートA2}
Device B	ポートB1	{1, 0, 1, ポートB1}
	ポートB2	{1, 0, 1, ポートB2}
Device C	ポートC1	{2, 0, 2, ポートC1}
	ポートC2	{2, 0, 2, ポートC2}

2)　各装置の Configuration BPDU を比較します。

表 8-4において、各 Configuration BPDU は Root ブリッジ ID、Root パスコスト、Designated ブリッジ ID、Designated ポート ID を含みます。

表 8-4 各装置の比較プロセスと結果

装置	比較プロセス	比較後のポートの Configuration BPDU
Device A	ポートA1は以下の操作をします。 1． Device B の Configuration BPDU {1,0,1,ポートB1}を受信します。 2． ローカルポートの Configuration BPDU{0,0,0, ポート A1}が受信した Configuration BPDU より優位であることを検出します。 3． 受信した Configuration BPDU を破棄します。 ポートA2は以下の操作をします。 1． Device C の Configuration BPDU {2,0,2, ポートC1}を受信します。 2． ローカルポートの Configuration BPDU {0,0,0, ポート A2}が受信した Configuration BPDU より優位であることを検出します。 3． 受信した Configuration BPDU を破棄します。 Device Aは、Device Aの全ポートのConfiguration BPDUのRootブリッジおよびDesignatedブリッジがDevice Aであることを検出するとそれ自体をRootブリッジとみなします。この場合、Device Aは各ポートのConfiguration BPDUに対して何の変更も行わず、定期的にConfiguration BPDUの送信を開始します。	• ポートA1：{0, 0, 0,ポートA1} • ポートA2：{0, 0, 0,ポートA2}
Device B	ポートB1は以下の操作をします。 1． Device A の Configuration BPDU {0,0,0, ポートA1}を受信します。 2． 受信した Configuration BPDUがローカルポートの Configuration BPDU {1, 0, 1,ポートB1}より優位であることを検出します。 3． ポート B1 の Configuration BPDU を更新します。 ポートB2は以下の操作をします。 1． Device C の Configuration BPDU {2,0,2, ポートC2}を受信します。 2． ローカルポートの Configuration BPDU {1,0,1, ポート B2}が受信した Configuration BPDU より優位であることを検出します。 3． 受信した Configuration BPDU を破棄します。	• ポートB1：{0, 0, 0, ポートA1} • ポートB2：{1, 0, 1, ポートB2}

装置	比較プロセス	比較後のポートの Configuration BPDU
	Device Bは以下の操作をします。 1． すべてのポートの Configuration BPDU を比較します。 2． ポート B1 の Configuration BPDU が最適な Configuration BPDU であると判断します。 3． ポート B1 を Root ポートとして使い、その Configuration BPDU は変更しません。 ポートB1のConfiguration BPDUおよびRootポートのパスコストにもとづき、ポートB2のConfiguration BPDUのDesignated {0,5,1, ポートB2}を計算します。Device Bは計算したConfiguration BPDU {0,5,1, ポートB2}とポートB2のConfiguration BPDUを比較します。計算したConfiguration BPDUが優位であればポートB2はDesignatedポートとなります。このポートのConfiguration BPDUは計算したConfiguration BPDUに置き換えられ、定期的に送信されます。	• Rootポート（ポートB1）: {0, 0, 0, ポートA1} • Designatedポート（ポートB2）: {0, 5, 1, ポートB2}
Device C	ポートC1は以下の操作をします。 1． Device A の Configuration BPDU{0,0,0, ポート A2}を受信します。 2． 受信した Configuration BPDU がローカルポートの Configuration BPDU{2,0,2, ポート C1}より優位であることを検出します。 3． ポート C1 の Configuration BPDU を更新します。 ポートC2は以下の操作をします。 1． メッセージが更新される前に、Device B のポート B2 の Configuration BPDU{1,0,1, ポート B2}を受信します。 2． 受信した Configuration BPDU がローカルポートの Configuration BPDU{2,0,2, ポート C2}より優位であることを検出します。 3． ポート C2 の Configuration BPDU を更新します。	• ポートC1：{0, 0, 0, ポートA2} • ポートC2：{1, 0, 1, ポートB2}
	Device Cは以下の操作をします。 1． すべてのポートの Configuration BPDU を比較します。 2． ポート C1 の Configuration BPDU が最適な Configuration BPDU であると判断します。 3． ポート C1 を Root ポートとして使い、その Configuration BPDU は変更しません。 ポートC1のConfiguration BPDUおよびRootポートのパスコストにもとづき、ポートC2のConfiguration BPDUのDesignated {0,10,2, ポートC2}を計算します。Device Cは計算したConfiguration BPDU {1,0,1, ポートB2}とポートC2のConfiguration BPDUを比較します。計算したConfiguration BPDUが優位であればポートC2はDesignatedポートとなります。このポートのConfiguration BPDUは計算したConfiguration BPDUに置き換えられます。	• Rootポート（ポートC1）: {0, 0, 0, ポートA2} • Designatedポート（ポートC2）: {0, 10, 2, ポートC2}

装置	比較プロセス	比較後のポートの Configuration BPDU
	ポートC2は以下の操作をします。 1． 更新された Device B の Configuration BPDU{0,5,1, ポート B2}を受信します。 2． 受信した Configuration BPDU がローカルポートの Configuration BPDU{0,10,2, ポート C2}より優位であることを検出します。 3． ポート C1 の Configuration BPDU を更新します。 ポートC1は以下の操作をします。 1． Device A から定期的に Configuration BPDU {0,0,0, ポート A2}を受信します。 2． ローカルポートの Configuration BPDU と同じであることを検出します。 3． Configuration BPDU を更新します。	● ポートC1：{0, 0, 0, ポート A2} ● ポートC2：{0, 5, 1, ポート B2}
	Device Cは、ポートC1のルートパスコスト（10）（受信したConfiguration BPDU（0）のルートパスコスト＋ポートC1のパスコスト（10））は、ポートC2のパスコスト（9）よりも大きいと判断し、ポートC2のBPDUが最適なConfiguration BPDUと判断します。ポートC2がルートポートとなり、そのメッセージは変更されません。 Configuration BPDUとルートポートのパスコストにもとづき、Device Cは以下の操作をします。 1． ポート C1 の Designated ポートの Configuration BPDU {0,9,2, ポート C1}を計算します。 2． それをポート C1 の Configuration BPDU {0,0,0, ポート A2}と比較します。 3． 計算された Configuration BPDU よりもローカルポートの Configuration BPDU が優位であることを検出します。ポート C1 はブロックされ、Configuration BPDU はそのまま変更しません。 ポートC1は、たとえば、Device BとDevice Cの間のリンクが切断されるなど、STPの計算プロセスのあらたな契機があるまで、データを転送しません。	● Blockedポート（ポート C1）：{0, 0, 0, ポートA2} ● Rootポート（ポートC2）：{0, 5, 1, ポートB2}

表 8-4に記述した比較プロセス後は、Device A を Root ブリッジとするスパニングツリーが図 8-5のように確立されます。

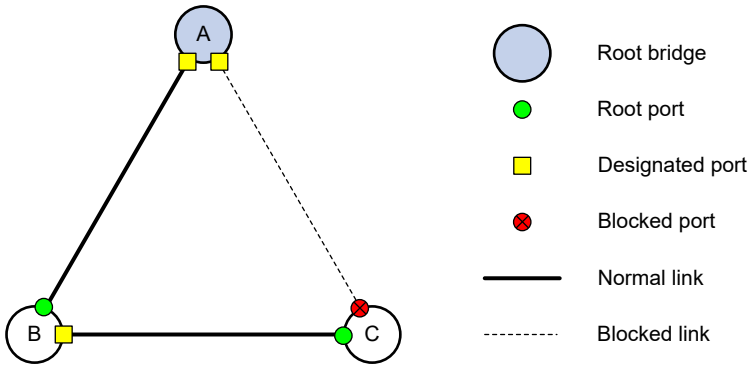


図 8-5 比較プロセス後のスパニングツリー

III. STP の Configuration BPDU 転送メカニズム

STP の Configuration BPDU は以下のガイドラインに従って転送されます。

- ネットワークの初期化をした際、各装置は自身を Root ブリッジとみなします。Configuration BPDU を生成し、Hello 時間の間隔で Configuration BPDU を送信します。
- Configuration BPDU を受信した Root ポートのプライオリティがポートの Configuration BPDU より高い場合、装置は以下の操作をします。
  - Configuration BPDU の有効時間を延ばします。
  - Configuration BPDU の時間を計るタイマをスタートさせます。
  - Designated ポートから Configuration BPDU を送信します。
- Designated ポートがローカルポートの Configuration BPDU と比較してプライオリティの低い Configuration BPDU を受信した場合、ローカルポートの Configuration BPDU を返信します。
- 通信ができなくなると、Root ポートは新しい Configuration BPDU を受信せず、古い Configuration BPDU はタイムアウトして破棄されます。この場合、装置は装置自体をルートとする Configuration BPDU を生成し、その BPDU を送信します。これが新しいスパニングツリーを計算する契機になり、ネットワークの接続を回復させます。

新しく計算された Configuration BPDU は、すぐにネットワーク内に広まらないため、トポロジの変更を検出していない古い Root ポートや Designated ポートは古い通信経路でデータの転送を継続します。新しい Root ポートや Designated ポートが選出されてから、すぐにデータの転送を開始すると、ループが発生する可能性があります。

IV. STP タイマ

STP には 3 つの重要なパラメータがあります。

- Forward delay

装置の状態が遷移する場合の遅延時間です。

リンク障害等が発生すると、STP トポロジは再構築されます。再構築後の Configuration BPDU は、ネットワーク内にすぐには広まらないため、新しく選出された Root ポートや Designated ポートがすぐにデータの転送をはじめてしまうと、ループが発生する可能性があります。

このため、新しく選出された Root ポートまたは Designated ポートは、Forwarding 状態に遷移する前に Forward delay タイマの 2 倍の時間を必要とします。これにより、新しい Configuration BPDU をネットワークに広げることができます。

- Hello 時間

装置が周辺の装置に Hello パケットを送信する間隔です。通信が正常であることを確認するものです。デフォルトは 2 秒です。装置がタイムアウト時間以内に Configuration BPDU を受信しない場合、装置はスパニングツリーの再計算を行います。タイムアウト時間を計算する式を以下に示します。

タイムアウト時間 ＝ タイムアウトファクタ × 3 × Hello 時間

- Max age

装置の Configuration BPDU が時間切れになっていないかどうかを判断するのに使うパラメータです。最大有効時間を越えた Configuration BPDU は破棄されます。デフォルトは 20 秒です。MSTP ネットワークの CIST では、装置は、Configuration BPDU 内に記載されている Max age を経過した BPDU メッセージを廃棄します。最大エージング時間は CIST を除いて MSTI に影響がありません。

ポートがタイムアウト時間以内に Configuration BPDU を受信しない場合、ポートは Listening 状態に遷移します。装置はスパニングツリーを再計算します。ポートが Forwarding 状態に遷移するまで約 50 秒かかります。この値は Max age が 20 秒、Listening 状態が 15 秒、Learning 状態が 15 秒です。

スパニングツリーの状態変更が頻繁に発生するのを回避するには、Hello 時間、Forward delay、最大エージング時間の設定を次式に満足するよう設定してください。

- 2 ×（Forward delay － 1 秒）≧ Max age
- Max age ≧ 2 ×（Hello 時間 ＋ 1 秒）

8.2 RSTP

RSTP は、新しく選出された Root ポートあるいは Designated ポートを Forwarding 状態にするため、STP よりもネットワークの高速な収束を行います。

- **Protocol version ID**– スパニングツリーの Version ID です。RSTP のプロトコルバージョン ID は 0x02 です。
- **BPDU type**– BPDU のタイプです。RSTP BPDU の値は 0x02 です。
- **Flags**– BPDU の目的を示します。8 ビットフィールドです。
- **Version1 length**– Version 1 のプロトコル情報が存在しないことを示します。値は 0x00 です。

RSTP はトポロジの変更を通知する際に TCN BPDU を使用しません。トポロジの変更を通知する場合、RSTP は TC フラグを設定し、BPDU をフラッディングします。

8.2.1 RSTP の基本概念

I. ポートの役割

- **Alternate ポート**（代替ポート）– Root ポートのバックアップとして動作します。Root ポートがブロックされた場合、Alternate ポートが引き継ぎます。

- **Backup ポート**– Designated ポートのバックアップとして動作します。Designated ポートが無効である場合、backup ポートは新しい Designated ポートになります。同一のスパニングツリーの 2 つのポートが接続された場合、ループが発生します。そのため装置はポートの 1 つをブロックします。ブロックされたポートは backup ポートです。
- **Edge ポート**– ネットワークの装置あるいはネットワークセグメントに接続されておらず、ユーザホストに直接接続しているポートです。

II. ポート状態

RSTP は、STP の Disabled 状態、Blocking 状態、Listening 状態が discarding 状態に変わります。表 8-5に RSTP と STP のポート状態の違いを示します。

表 8-5 STP のポート状態

STP ポート状態	RSTP ポート状態	BPDU の送信	MAC アドレスの学習	データの転送
Disabled	Discarding	No	No	No
Blocking	Discarding	No	No	No
Listening	Discarding	Yes	No	No
Learning	Learning	Yes	Yes	No
Forwarding	Forwarding	Yes	Yes	Yes

8.2.2 RSTP の動作

RSTP の計算中、以下のイベントが発生します。

- discarding 状態のポートが Alternate ポートになる場合、状態を保持します。
- discarding 状態のポートが Root ポートあるいは Designated ポートとして選出された場合、Forward delay 後、Learning 状態に遷移します。ポートは MAC アドレスを学習し、別の Forward delay 後に Forwarding 状態に遷移します。
  - □ 以下の要件に一致した場合、新しく選出された RSTP の Root ポートは即座に Forwarding 状態になります。
    - 装置の古い Root ポートが転送データを止めた場合
    - 上り方向の Designated ポートが転送をはじめた場合
  - □ 以下の要件のいずれかに一致した場合、新しく選出された RSTP の Designed ポートは即座に Forwarding 状態になります。
    - Designed ポートがユーザ端末に直接接続された Edge ポートとして設定された場合
    - Designated ポートが point-to-point リンクに接続し、直接接続された装置からハンドシェイクの応答を受信した場合

8.2.3 RSTP の BPDU 処理

Root ブリッジ以外のアクティブな装置は Root ブリッジが RSTP BPDU を送信するのを待たずに、Designated ポートを経由して Hello 時間の間隔で RSTP BPDU を送信します。これにより RSTP はリンク障害をすぐに検出することができます。装置が Hello 時間の 3 倍以内にポートで RSTP BPDU を受信しない場合、装置はリンク障害が発生したと認識します。記録された Configuration BPDU の有効期限が終了したのち、装置は RSTP の計算を行うため、TC フラグを設定し、RSTP BPDU をフラッディングします。

RSTP では、Blocking 状態のポートは自身の BPDU よりも低いプライオリティで即座に RSTP BPDU に応答することができます。

図 8-6に示すように、Device A は Root ブリッジです。Device B のプライオリティは Device C のプライオリティよりも高く、Device C のポート C2 はブロックされます。

Device A と Device B 間のリンクに障害が発生した場合、以下のイベントが発生します。

1) Device B は Root ブリッジとして RSTP BPDU を Device C に送信します。
2) Device C は RSTP BPDU を自身の BPDU と比較します。
3) Device B からの RSTP BPDU のプライオリティが低いため、Device C は自身の BPDU を Device B に送信します。
4) Device B はポート B2 が Root ポートと認識し、Device C への RSTP BPDU の送信を停止します。

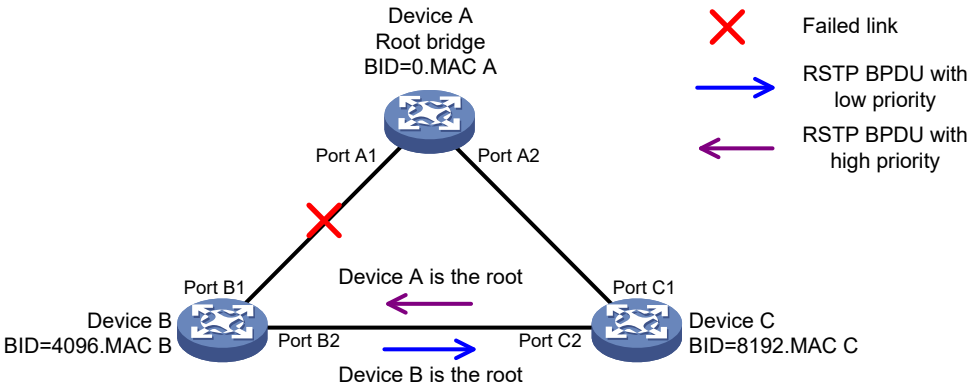


図 8-6 RSTP の BPDU 処理

8.3 PVST

STP あるいは RSTP 対応 LAN では、すべてのブリッジが 1 つのスパニングツリーで共有されます。すべての VLAN からのトラフィックはスパニングツリーを経由して転送されます。ループがあった場合、ポートは、VLAN でループをブロックすることができません。

PVST では、すべての VLAN が独自のスパニングツリーを使用できるようになり、リンクと帯域幅を増大することができます。各 VLAN は独立して RSTP を実行するため、スパニングツリーはその VLAN のみをサポートします。

PVST 対応の NEC の装置は、Rapid PVST または PVST を実行しているサードパーティ製の装置と通信することができます。PVST 対応の NEC の装置は、PVST 対応の NEC の装置または Rapid PVST 対応のサードパーティ製の装置に接続した場合、RSTP のような高速ネットワークの収束をサポートします。

8.3.1 PVST のプロトコルフレーム

図 8-7に示すように PVST BPDU は以下の相違点を除いて RSTP BPDU と同一のフォーマットを使用します。

- PVST BPDU の宛先 MAC アドレスは 01-00-0c-cc-cc-cd です。これはプライベート MAC アドレスです。
- 各 PVST BPDU は VLAN タグを転送します。VLAN タグは PVST BPDU が所属する VLAN を識別します。
- 組織コード、PID フィールドは PVST BPDU の LLC ヘッダに追加されています。

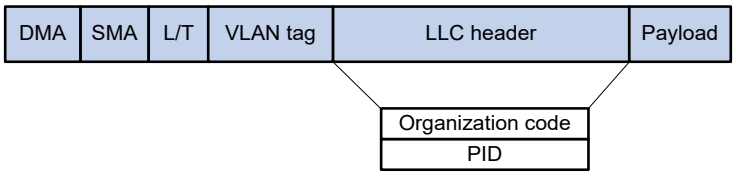


図 8-7 PVST BPDU フォーマット

ポートのリンクタイプは、ポートが送信する BPDU タイプを決定します。

- アクセスポートは RSTP BPDU を送信します。
- トランクあるいはハイブリッドポートはデフォルト VLAN で RSTP BPDU を送信し、ほかの VLAN で PVST BPDU を送信します。

8.3.2 PVST の基本概念

PVST は高速収束を行うため、RSTP と同一のポートの役割とポート状態を使用します。詳細はオペレーションマニュアルのセクション 2 *アクセス*“*STP*”の“*RSTP*”の“*RSTP の基本概念*”を参照してください。

8.3.3 PVST の動作

PVST は、各 VLAN を MSTI にマッピングすることで VLAN ごとのスパニングツリーの計算を行います。PVST では各 VLAN は独立して RSTP を実行して、ほかのスパニングツリーに影響せずに、自身のスパニングツリーを維持します。これにより各 VLAN のループは除去され、異なる VLAN のトラフィックがリンクを超えて共有されます。PVST はスパニングツリーの計算を行うため、デフォルト VLAN では RSTP BPDU を使用し、ほかの VLAN では PVST BPDU を使用します。

8.4 MSTP

MSTP は以下の STP、RSTP、PVST の制限を克服したものです。

- **STP の制限**– STP は、ポートの高速な状態遷移には対応できません。新しく選出されたポートは、Forwarding 状態に遷移する前に 2 倍の Forward delay を待たなければなりません。
- **RSTP の制限**– RSTP（rapid spanning tree protocol）は、STP よりも収束時間を早くしたにもかかわらず、STP 同様 VLAN 上の全ネットワークブリッジがスパニング

ツリーを共有するため、冗長リンクを VLAN ごとにブロックできない欠点があります。

- **PVST の制限**– 各 VLAN はスパニングツリーを持つため、PVST BPDU の量は、トランクあるいはハイブリッドポートの VLAN の数に比例して増加します。トランクあるいはハイブリッドポートが多くの VLAN を許可している場合、VLAN スパニングツリーを維持するリソースと計算を行うリソースの両方が劇的に増加します。複数の VLAN があるトランクあるいはハイブリッドポートでステータスの変更がある場合、装置の CPU は影響するスパニングツリーを再計算するために負担がかかります。その結果、ネットワークの性能が低下します。

8.4.1 MSTP の特徴

IEEE802.1s をもとに発展させた MSTP（multiple spanning tree protocol）は、STP、RSTP、PVST の制限を克服します。ネットワークを高速に収束させるだけでなく、VLAN ごとにデータフローがそれぞれのパスに転送されるので、冗長リンクの負荷分散ができます。

MSTP には以下のような特徴があります。

- MSTP によりスイッチネットワークは複数の領域に分けられ、それぞれの領域が独立した複数のスパニングツリーで構成されます。
- MSTP は、マッピングテーブルを使用し、MST インスタンスへの VLAN のマッピングを行います。MSTP は、複数の VLAN を 1 つの MST インスタンスにマッピングすることで、通信帯域やリソースの使用を節約できます。
- MSTP はループのあるネットワークをループのないツリー構造に変え、ループネットワーク内でのループを回避します。さらに、MSTP はデータ転送用の冗長パスを複数提供し、データ転送プロセスにおける VLAN データの負荷分散を行います。
- MSTP は STP、RSTP と一部の PVST に互換性があります。

8.4.2 MSTP のプロトコルフレーム

図 8-8に MSTP BPDU のフォーマットを示します。

Fields	Byte
Protocol ID	2
Protocol version ID	1
BPDU type	1
Flags	1
Root ID	8
Root path cost	4
Bridge ID	8
Port ID	2
Message age	2
Max age	2
Hello time	2
Forward delay	2
Version1 length=0	1
Version3 length	2
MST configuration ID	51
CIST IRPC	4
CIST bridge ID	8
CIST remaining ID	1
MSTI configuration messages	LEN

MSTP-specific fields

図 8-8 MSTP BPDU のフォーマット

MSTP BPDU の最初の 13 フィールドは RSTP BPDU と同一です。ほかの 6 つのフィールドは MSTP で固有です。

- **Protocol version ID**– MSTP の値は 0x03 です。
- **BPDU type**– RSTP BPDU、MSTP BPDU の値は 0x02 です。
- **Root ID**– 共通 Root ブリッジの ID です。
- **Root path cost**– CIST 外部パスコストです。
- **Bridge ID**– IST あるいは MSTI の regional Root の ID です。
- **Port ID**– CIST の Designated ポートの ID です
- **Version3 length**– MSTP 固有のフィールドの長さです。装置は MSTP BPDU の受信を確認するために、このフィールドを使用します。
- **MST Configuration ID**– フォーマットセレクタ、Configuration 名、revision レベル、Configuration ダイジェストが含まれます。フォーマットセレクタは 0x00 に固定されています。ほかのパラメータは、発信ブリッジの MST region を識別するために使用されます。
- **CIST IRPC**– もとのブリッジから MST region のルートへの内部ルートパスコスト（IRPC）です。
- **CIST bridge ID**– MSTP BPDU を送信するブリッジの ID です。
- **CIST remaining ID**– 残りホップ数です。このフィールドは MST region の規模を制限します。regional Root は残りホップ数を最大値に設定し、BPDU を送信します。BPDU を受信する各装置はホップ数を 1 つずつ削除します。ホップ数が 0 になった場合、BPDU を廃棄します。MST region の最大ホップ数を超える装置はスパニングツリーの計算に参加することができません。デフォルトの残りホップ数は 20 です。
- **MSTI Configuration messages**– MSTI の Configuration メッセージが含まれます。各 MSTI Configuration メッセージは 16 バイトです。このフィールドは 0～64 まで含むことができます。MSTI Configuration メッセージの数は MST region の MSTI の数によって決定します。

8.4.3 MSTP の基本概念

図 8-9は 4 つの MST region から構成され、各 MST region は 4 つの MSTP 装置から構成されます。図 8-10は MST region3 のネットワークトポロジを示します。

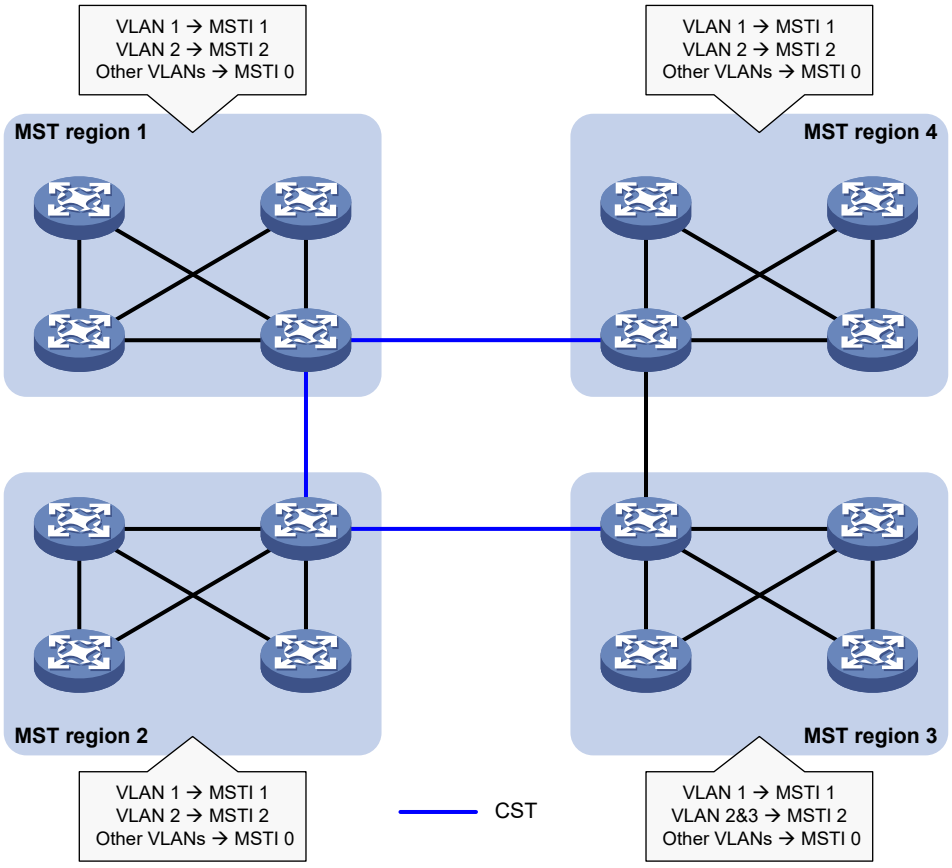


図 8-9 MSTP の基本概念

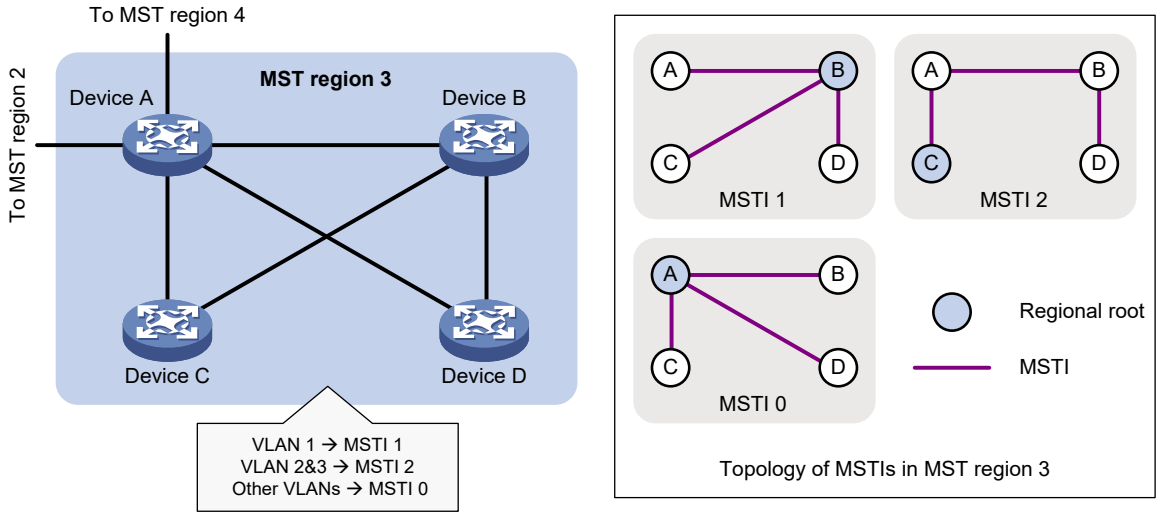


図 8-10 MST region 3 のネットワーク図とトポロジ

I. MST region

複数のスパニングツリーregion（MST region）は、スイッチネットワークの複数の装置と装置間のネットワークセグメントで構成されています。これらの装置には、以下のような特性があります。

- すべて MSTP を有効にしています。
- 同じ region 名を持っています。
- VLAN インスタンスマッピングの設定が同じです。
- MSTP リビジョンレベルの設定が同じです。
- 物理的に相互にリンクしています。

複数の MST region はスイッチネットワークで使用され、同じ MST region に装置を割り当てることができます。図 8-9は以下のようになっています。

- スイッチネットワークは MST region1～4 の 4 つの MST region から構成されます。
- 各 MST region のすべての装置は同じ MST region 設定を持ちます。

II. MSTI

MSTP により、複数のスパニングツリーをほかから独立したスパニングツリーとして、1 つの MST region で生成でき、VLAN を指定するために各スパニングツリーでマッピングされます。それぞれのスパニングツリーは 1 つの MST インスタンス（MSTI（Multiple Spanning Tree Instance））とみなされます。

図 8-10では、MSTI1、MSTI2、MSTI0 の 3 つの MSTI があります。

III. VLAN インスタンスマッピングテーブル

VLAN インスタンスマッピングテーブルは VLAN と MST インスタンス間のマッピングの関係ついて、MST region ごとに記載されています。

図 8-10では、MST region 3 の VLAN インスタンスマッピングテーブルは以下のようになっています。

- VLAN 1 は MSTI 1 にマッピングされています。
- VLAN 2 は MSTI 2 にマッピングされています。
- 残りは MSTI0 にマッピングされています。

MSTP は、VLAN インスタンスマッピングテーブルを使って負荷分散を行います。

IV. CST

CST は、スイッチネットワークのすべての MST region に接続する 1 つのスパニングツリーです。MST region をそれぞれ装置とみなすと、CST はこれらの装置が STP または RSTP で計算したスパニングツリーです。図 8-9の青い線は CST を示しています。

V. IST

IST（Internal spanning tree）は、MST region で動作するスパニングツリーです。特別な MSTI で MSTI0 と呼ばれます。デフォルトではすべての VLAN は MSTI0 にマッピングされています。図 8-9では、MSTI 0 は MST region3 の IST です。

VI. CIST

CIST（common and internal spanning tree）はスイッチネットワークですべての装置に接続する 1 つのスパニングツリーです。CIST は、すべての MST region にある IST と CST で構成されます。図 8-9では、すべての MST region と inter-region CST を加えた IST（MSTI 0）は、全体の CIST を構成します。

VII. Regional Root

MST region 内の IST または MSTI の Root ブリッジは、MST またはその MSTI の regional Root ブリッジです。トポロジをベースに、MST region のそれぞれのスパニングツリーが異なる region ルートを持つ場合があります。

図 8-10の MST region3 では、以下のようになっています。

- MSTI1 の regional ルートは Device B です。
- MSTI2 の regional ルートは Device C です。
- MSTI0（IST）の regional ルートは Device A です。

VIII. 共通 Root ブリッジ

共通 Root ブリッジは、CIST の Root ブリッジです。

図 8-9では、MST Region 1 のスイッチが共通 Root ブリッジです。

IX. ポートの役割

異なる MSTI で、ポートは異なる役割を行います。図 8-11に示すように MST region は Device A、Device B、Device C、Device D があります。Device A のポート A1 とポート A2 は共通 Root ブリッジに接続されています。Device B のポート B2、ポート B3 はループしています。Device C のポート C3、ポート C4 はほかの MST region に接続されています。Device D のポート D3 はホストに接続されています。

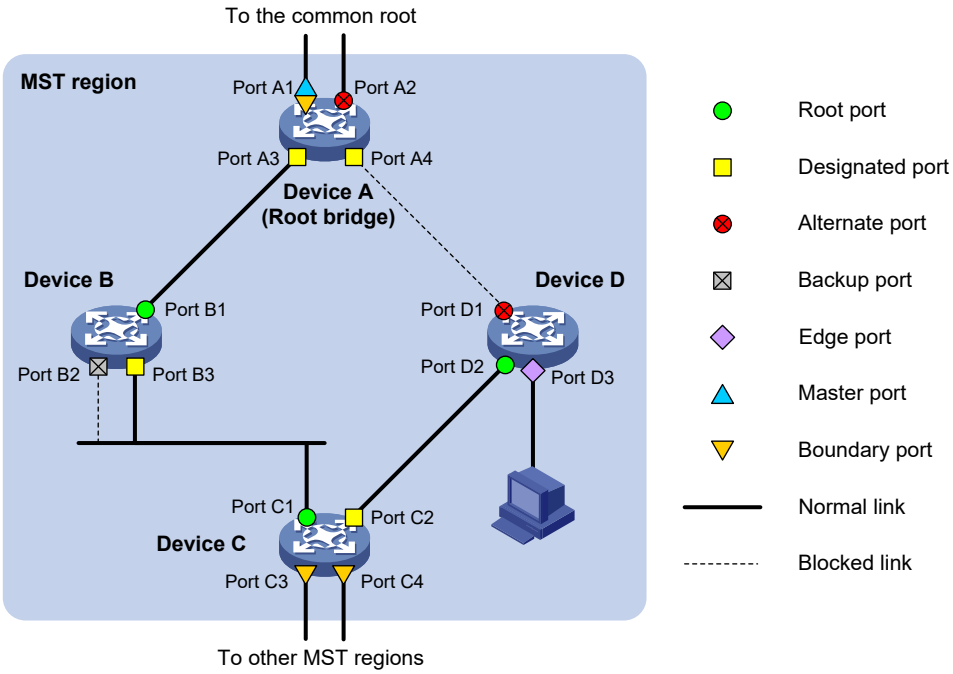


図 8-11 ポートの役割

MSTP では、以下のポートの計算を行っています。

- **Root ポート**– 非 Root ブリッジ用にデータを Root ブリッジに転送します。Root ブリッジは Root ポートを持っていません。
- **Designated ポート**– データを下流方向のネットワークセグメントや装置に転送するポートです。
- **Alternate ポート**– Root ポートもしくは Master ポートの代替ポートです。Root ポートもしくは Master ポートがブロッキング状態になると、その代わりに Root ポートもしくは Master ポートになるポートです。
- **Backup ポート**– Designated ポートの代替ポートで、高速な切り替えのために使われます。Designated ポートがブロッキング状態になると、即座に Designated ポートとなり、データの転送を開始できます。
- **Edge ポート**– ネットワーク装置あるいはネットワークセグメントに接続されていないポートで、ユーザホストに直接接続されています。
- **Master ポート**– MST Region を共通 Root ブリッジに接続するポートで、その MST Region における Root ポートでもあります。Master ポートから共通 Root ブリッジへのパスは、最短パスとなります。Master ポートはいつも regional Root にあるわけではありません。IST や CIST の Root ポートであり、ほかの MSTI の Master ポートです。
- **Boundary ポート**– MST Region の端点のポートで、ほかの MST Region や STP/RSTP で制御される装置と接続します。MSTP の計算を行う場合、MSTI の boundary ポートの役割は CIST の役割と同一です。Master ポートになるわけではありません。MSTI の Master ポートは CIST の Root ポートです。

X. ポートの状態

MSTP では、ポートは以下のいずれかの状態になっています。

- **Forwarding**ーポートは BPDU の送受信が可能で、MAC アドレスを学習し、ユーザトラフィックを転送できます。
- **Learning**ーポートは BPDU の送受信が可能で、MAC アドレスを学習しますが、ユーザトラフィックを転送できません。
- **Discarding**ーポートは BPDU の受信のみ可能です。MAC アドレスの学習やユーザトラフィックを転送できません。

🕮 **メモ：**

MSTI が異なると、ポートの状態も異なります。

ポートの状態はポートの役割と排他的ではありません。表 8-6にポートの役割と、ポート状態の関係を示します。“〇”はポートがこの状態に対応することを示し、“×”はポートがこの状態に対応しないことを示します。

表 8-6 ポートの役割とポート状態の関係

ポートの役割（右） ポートの状態（下）	Root ポート /master ポート	Designated ポート	Alternate ポート	Backup ポート
Forwarding	〇	〇	×	×
Learning	〇	〇	×	×
Discarding	〇	〇	〇	〇

8.4.4 MSTP の動作

MSTP はレイヤ 2 ネットワーク全体を複数の MST Region に分割します。MST Region 間で CST を生成し、各 MST Region 内に MSTI と呼ばれる複数のスパニングツリーを生成します。MSTI が 0 の MSTI は IST です。

MSTP では、STP と同様に、スパニングツリーを構成するための情報転送に BPDU を使用します。MSTP 用の BPDU との違いは、MSTP の BPDU に加えて、MSTI 用のパラメータを付加します。

I. CIST の構築

CIST の構築では、以下の処理が行われます

- もっとも優先度の高い装置を、CIST の Root として選出します。
- 各 MST Region では IST が構築されます。
- MSTP はそれぞれの MST Region を 1 つの装置とみなして、ネットワークの CST を構築します。

構築された IST と CST で CIST が構成されます。

II. MSTI の構築

MST Region 内では、VLAN とインスタンスのマッピング情報によって VLAN グループごとの MSTI を構築します。それぞれの MSTI では、STP と同様にスパニングツリーを構成します。詳細はオペレーションマニュアルのセクション 2 *アクセス "STP"*の"*STP アルゴリズムの計算プロセス*"を参照してください。

MSTP では、VLAN パケットは以下のパスに沿って転送されます。

- MST region 内ではパケットは対応する MSTI に沿って転送されます。
- MST region 間ではパケットは CST に沿って転送されます。

8.4.5 装置での MSTP の実行

MSTP は STP および RSTP と互換性があります。STP および RSTP プロトコルパケットは、MSTP を実行している装置に認識され、スパニングツリーの計算に使用されます。

基本的な MSTP 機能に加え、以下のような特別な機能を提供することで、管理を容易にします。

- Root ブリッジの保持
- Root ブリッジのバックアップ
- Root ガード
- BPDU ガード
- Loop ガード
- TC-BPDU ガード
- ポート役割制限
- TC-BPDU 転送制限機能

8.4.6 高速収束メカニズム

STP ではポートは Blocking 状態から Forwarding 状態に遷移する前、Forward delay（デフォルトで 30 秒）の 2 倍待機する必要があります。Forward delay は Hello 時間とネットワークダイアメータに関連します。Forward delay が短すぎる場合、ループが発生する可能性があります。これはネットワークの安定性に影響します。

RSTP、PVST、MSTP は Edge ポート、Root ポート、Designated ポートのポート状態の遷移を早く行う高速収束メカニズムを使用します。Designated ポートの高速収束メカニズムは P/A transition（proposal/agreement_transition）として知られます。

I. Edge ポートの高速収束

図 8-12に示すようにポート C3 はホストに接続された Edge ポートです。ネットワークトポロジの変更が発生した場合、ループが発生しないためにポートはに Blocking 状態から Forwarding 状態に遷移します。

装置はポートが端末に直接接続されているかどうかを判別できないため、Edge ポートとしてポートを手動で設定する必要があります。

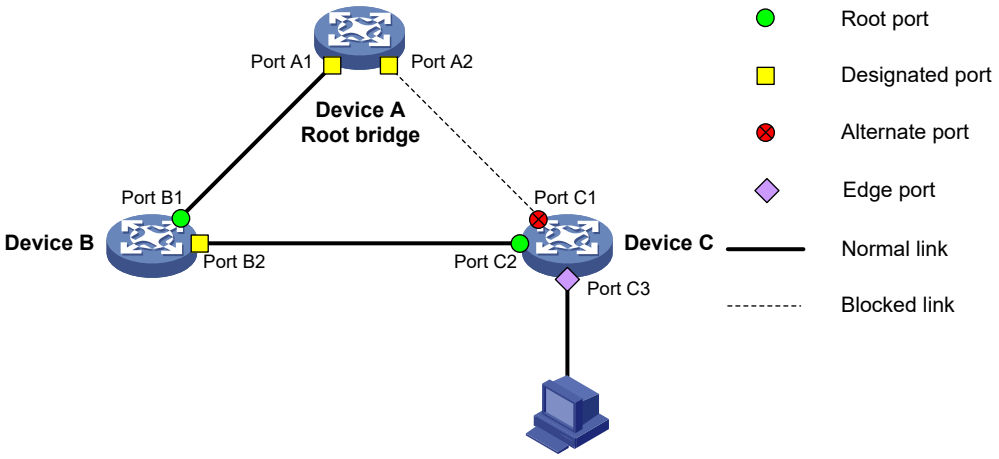


図 8-12 Edge ポートの高速収束

II. Root ポートの高速収束

Root ポートがブロックされた場合、ブリッジは新しい Root ポートとしてもっともプライオリティが高い Alternate ポートを選出します。新しい Root ポートの対向先が Forwarding 状態である場合、新しい Root ポートは即座に Forwarding 状態に遷移します。

図 8-13に示すように Device C のポート C2 は Root ポートで、ポート C1 は Alternate ポートです。ポート C2 が Blocking 状態に遷移した場合、ポート C1 は Root ポートとして選出され、即座に Forwarding 状態に遷移します。

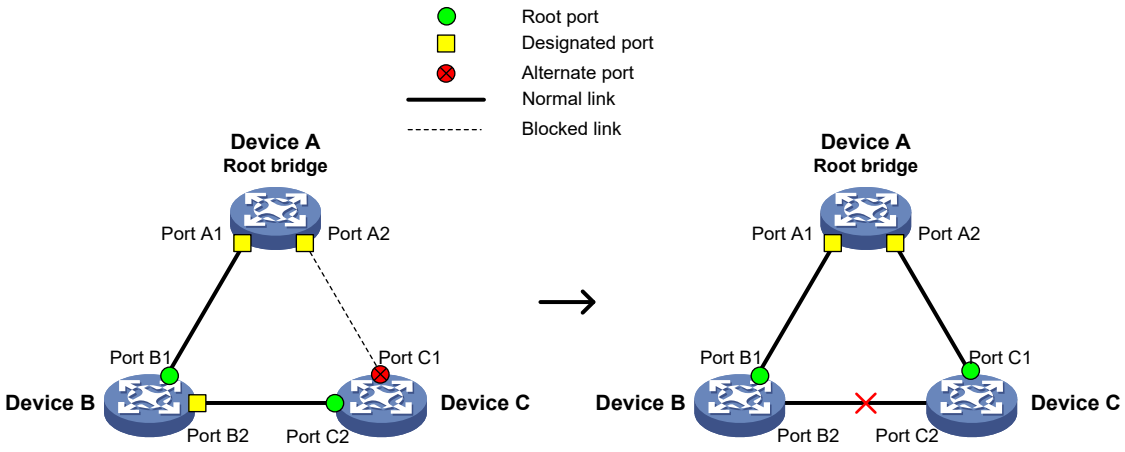


図 8-13 Root ポートの高速収束

III. P/A transition

P/A transition は対向先とハンドシェイクを行った後、Designated ポートが高速に Forwarding 状態に遷移することを可能にします。P/A transition は Point-to-Point リンクにのみ適用されます。

- RSTP と PVST の P/A transition

RSTP あるいは PVST では、新しいリンクあるいは回復したリンクのポートは Blocking 状態の Designated ポートです。

Designated ポートの 1 つが discarding 状態あるいは Learning 状態に遷移した場合、BPDU の proposal フラグが設定されます。対向先の装置は BPDU を受信し、受信ポートが Root ポートであるかどうかを決定します。そしてブリッジは Designated ポートに agreement BPDU を返信します。agreement BPDU を受信すると、Designated ポートは即座に Forwarding 状態に遷移します。Designated ポートが agreement BPDU を受信しない場合、Forwarding 状態に遷移するために Forward delay の 2 倍を待機します。

図 8-14に示すように、P/A transition の動作を示します。

1) Device A はポート A1 を通して Device B に proposal BPDU を送信します。
2) Device B はポート B2 で proposal BPDU を受信します。ポート 2 は Root ポートとして選出されます。
3) Device B はループを取り除くため Designated ポート B2 と Alternate ポート B3 をブロックします。
4) Root ポート B2 は Forwarding 状態に遷移し、Device A に agreement BPDU を送信します。
5) agreement BPDU を受信したのち、Device A の Designated ポート A1 は即座に Forwarding 状態に遷移します。

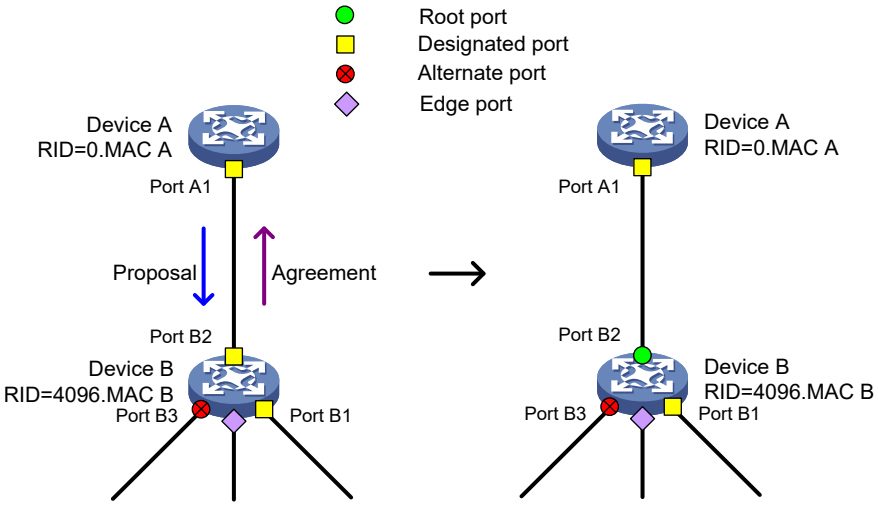


図 8-14 RSTP と PVST の P/A transition

- MSTP の P/A transition

MSTP では上流ブリッジは BPDU の proposal フラグと agreement フラグの両方を設定します。下流ブリッジが BPDU を受信し、その受信ポートが Root ポートとして選出された場合、ブリッジは Edge ポートを除くほかのすべてのポートをブロックします。下流ブリッジは上流ブリッジに agreement BPDU を返信します。agreement BPDU を受信すると、上流ポートは即座に Forwarding 状態に遷移します。上流ポートが agreement BPDU を受信しない場合、Forwarding 状態に遷移するために Forward delay の 2 倍を待機します。

図 8-15に示すように、P/A transition の動作を示します。

1) Device A は BPDU の proposal フラグと agreement フラグの両方を設定し、ポート A1 を通して Device B に BPDU を送信します。

2) Device B は BPDU を受信します。Device B のポート B1 は Root ポートとして選出されます。
3) Device B は Edge ポートを除くほかのすべてのポートをブロックします。
4) Device B の Root ポート B1 は Forwarding 状態に遷移し、Device A に agreement BPDU を送信します。
5) agreement BPDU を受信すると、Device A のポート A1 は即座に Forwarding 状態に遷移します。

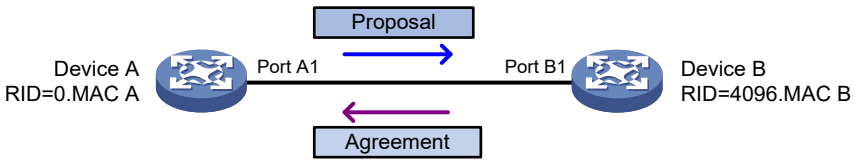


図 8-15 MSTP の P/A transition

8.5 プロトコルと規格

MSTP は以下に示すプロトコルと規格に記載されています。

- IEEE 802.1d, *Media Access Control (MAC) Bridges*
- IEEE 802.1w, *Part 3: Media Access Control (MAC) Bridges− Amendment 2: Rapid Reconfiguration*
- IEEE 802.1s, *Virtual Bridged Local Area Networks− Amendment 3: Multiple Spanning Trees*
- IEEE 802.1Q-REV/D1.3, *Media Access Control (MAC) Bridges and Virtual Bridged Local Area Networks − Clause 13: Spanning tree Protocols*

8.6 スパニングツリー設定作業リスト

スパニングツリーを設定する前に、以下の作業を完了してください。

- 各 MST インスタンス内のそれぞれの装置で使用するプロトコル（STP、RSTP、MSTP、PVST）を定義してください。
- 装置の役割（Root ブリッジまたは Leaf ノード）を定義してください。

スパニングツリーを設定する場合、以下の制限とガイドラインに従ってください。

- スパニングツリーの設定は、Smart Link と一緒に設定できません。
- system view で行った設定は全体に適用されます。Ethernet interface view で行った設定は、インタフェースでのみ適用されます。aggregate interface view で行った設定は、アグリゲートインタフェースでのみ適用されます。アグリゲーションメンバポートで行った設定は、アグリゲーショングループから取り除かれた後に有効になります。
- アグリゲートインタフェースでスパニングツリーを有効にした後、アグリゲートインタフェースでアルゴリズムの計算が行われます。アグリゲーションメンバポートでは行われません。スパニングツリーは、状態を有効にすることに加えて、対応するアグリゲートインタフェースに一致する各選択されたメンバポートの Forwarding 状態を有効にします。

- アグリゲーショングループのメンバポートはスパニングツリーの計算に関与しませんが、ポートは、アグリゲーショングループから取り除かれた後に、MSTP 計算に参加するために、その MSTP 設定を確保しています。

8.6.1 STP 設定作業リスト

作業リスト
Rootブリッジの設定： ● （必須設定項目）動作モードの設定 ● （オプション設定項目）RootブリッジとSecondary Rootブリッジの設定 ● （オプション設定項目）ブリッジプライオリティの設定 ● （オプション設定項目）ネットワークダイアメータの設定 ● （オプション設定項目）スパニングツリータイマの設定 ● （オプション設定項目）タイムアウトファクタの設定 ● （オプション設定項目）BPDU最大送出レートの設定 ● （オプション設定項目）ポート遷移状態情報の出力の有効化 ● （必須設定項目）スパニングツリー機能の有効化
Leafノードの設定： ● （必須設定項目）動作モードの設定 ● （オプション設定項目）ブリッジプライオリティの設定 ● （オプション設定項目）タイムアウトファクタの設定 ● （オプション設定項目）BPDU最大送出レートの設定 ● （オプション設定項目）ポートパスコストの設定 ● （オプション設定項目）ポートプライオリティの設定 ● （オプション設定項目）ポート遷移状態情報の出力の有効化 ● （必須設定項目）スパニングツリー機能の有効化
（オプション設定項目）TC snoopingの設定
（オプション設定項目）保護機能の設定
（オプション設定項目）新しいRootの選出とトポロジ変更によるSNMP notificationの有効化

8.6.2 RSTP 設定作業リスト

作業リスト
Rootブリッジの設定： ● （必須設定項目）動作モードの設定 ● （オプション設定項目）RootブリッジとSecondary Rootブリッジの設定 ● （オプション設定項目）ブリッジプライオリティの設定 ● （オプション設定項目）ネットワークダイアメータの設定 ● （オプション設定項目）スパニングツリータイマの設定 ● （オプション設定項目）タイムアウトファクタの設定 ● （オプション設定項目）BPDU最大送出レートの設定 ● （オプション設定項目）Edgeポートの設定 ● （オプション設定項目）Point-to-Pointリンクの設定 ● （オプション設定項目）ポート遷移状態情報の出力の有効化 ● （必須設定項目）スパニングツリー機能の有効化
Leafノードの設定： ● （必須設定項目）動作モードの設定 ● （オプション設定項目）ブリッジプライオリティの設定 ● （オプション設定項目）タイムアウトファクタの設定 ● （オプション設定項目）BPDU最大送出レートの設定 ● （オプション設定項目）Edgeポートの設定 ● （オプション設定項目）ポートパスコストの設定 ● （オプション設定項目）ポートプライオリティの設定 ● （オプション設定項目）Point-to-Pointリンクの設定 ● （オプション設定項目）ポート遷移状態情報の出力の有効化 ● （必須設定項目）スパニングツリー機能の有効化
（オプション設定項目）mCheck機能の設定
（オプション設定項目）TC snoopingの設定
（オプション設定項目）保護機能の設定
（オプション設定項目）新しいRootの選出とトポロジ変更によるSNMP notificationの有効化

8.6.3 PVST 設定作業リスト

作業リスト
Rootブリッジの設定： ● （必須設定項目）動作モードの設定 ● （オプション設定項目）RootブリッジとSecondary Rootブリッジの設定 ● （オプション設定項目）ブリッジプライオリティの設定 ● （オプション設定項目）ネットワークダイアメータの設定 ● （オプション設定項目）スパニングツリータイマの設定 ● （オプション設定項目）タイムアウトファクタの設定 ● （オプション設定項目）BPDU最大送出レートの設定 ● （オプション設定項目）Edgeポートの設定 ● （オプション設定項目）Point-to-Pointリンクの設定 ● （オプション設定項目）ポート遷移状態情報の出力の有効化 ● （必須設定項目）スパニングツリー機能の有効化
Leafノードの設定： ● （必須設定項目）動作モードの設定 ● （オプション設定項目）ブリッジプライオリティの設定 ● （オプション設定項目）タイムアウトファクタの設定 ● （オプション設定項目）BPDU最大送出レートの設定 ● （オプション設定項目）Edgeポートの設定 ● （オプション設定項目）ポートパスコストの設定 ● （オプション設定項目）ポートプライオリティの設定 ● （オプション設定項目）Point-to-Pointリンクの設定 ● （オプション設定項目）ポート遷移状態情報の出力の有効化 ● （必須設定項目）スパニングツリー機能の有効化
（オプション設定項目）mCheck機能の設定
（オプション設定項目）保護機能の設定
（オプション設定項目）TC BPDUの検出、受信イベントのログ作成の有効化
（オプション設定項目）新しいRootの選出とトポロジ変更によるSNMP notificationの有効化

8.6.4 MSTP 設定作業リスト

作業リスト
Rootブリッジの設定： • （必須設定項目）動作モードの設定 • （必須設定項目）MST regionの設定 • （オプション設定項目）RootブリッジとSecondary Rootブリッジの設定 • （オプション設定項目）ブリッジプライオリティの設定 • （オプション設定項目）MST regionの最大ホップ数の設定 • （オプション設定項目）ネットワークダイアメータの設定 • （オプション設定項目）スパニングツリータイマの設定 • （オプション設定項目）タイムアウトファクタの設定 • （オプション設定項目）BPDU最大送出レートの設定 • （オプション設定項目）Edgeポートの設定 • （オプション設定項目）Point-to-Pointリンクの設定 • （オプション設定項目）MSTPパケットのフォーマット設定 • （オプション設定項目）ポート遷移状態情報の出力の有効化 • （必須設定項目）スパニングツリー機能の有効化
Leafノードの設定： • （必須設定項目）動作モードの設定 • （必須設定項目）MST regionの設定 • （オプション設定項目）ブリッジプライオリティの設定 • （オプション設定項目）タイムアウトファクタの設定 • （オプション設定項目）BPDU最大送出レートの設定 • （オプション設定項目）Edgeポートの設定 • （オプション設定項目）ポートパスコストの設定 • （オプション設定項目）ポートプライオリティの設定 • （オプション設定項目）Point-to-Pointリンクの設定 • （オプション設定項目）MSTPパケットのフォーマット設定 • （オプション設定項目）ポート遷移状態情報の出力の有効化 • （必須設定項目）スパニングツリー機能の有効化
（オプション設定項目）mCheck機能の設定
（オプション設定項目）Digest Snoopingの設定
（オプション設定項目）No AgreementCheckの設定
（オプション設定項目）TC snoopingの設定
（オプション設定項目）保護機能の設定
（オプション設定項目）新しいRootの選出とトポロジ変更によるSNMP notificationの有効化

8.7 動作モードの設定

スパニングツリーの動作モードは以下があります。

- **STP モード**– 装置のすべてのポートは STP BPDU を送信します。ポートの対向装置が STP のみをサポートしている場合、このモードを選択します。

- **RSTP モード**– 装置のすべてのポートは RSTP BPDU を送信します。対向装置から STP BPDU を受信した場合、ポートは自動で STP モードに遷移します。対向装置から MSTP BPDU を受信した場合、ポートは MSTP モードに遷移しません。
- **PVST モード**－装置のすべてのポートは PVST BPDU を送信します。各 VLAN はスパニングツリーを維持します。スパニングツリーの容量は PVST 対応ポートと、PVST 対応 VLAN を掛け合わせた数になります。ネットワークの容量がスパニングツリーの容量を超える場合、装置の CPU に負荷がかかります。パケット転送が中断され、ネットワークが不安定になります。スパニングツリーの数は最大 128 にしてください。
- **MSTP モード**– 装置のすべてのポートは MSTP BPDU を送信します。対向装置から STP BPDU を受信した場合、ポートは自動で STP モードに遷移します。対向装置から RSTP BPDU を受信した場合、ポートは RSTP モードに遷移しません。

MSTP モードは、RSTP モードと互換性があり、RSTP モードは STP モードと互換性があります。

PVST モードの互換性はポートのリンクタイプに依存します。

- アクセスポートでは、PVST モードはすべての VLAN でほかのスパニングツリーと互換性があります。
- トランクポートあるいはハイブリッドポートでは、PVST モードは、VLAN1 でほかのスパニングツリーと互換性があります。

以下に動作モードの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	－
2． 動作モードを設定する	**stp mode** { **mstp** | **pvst** | **rstp** | **stp** }	デフォルト：MSTP

8.8 MST regionの設定

2 つのスパニングツリー装置が物理的に接続され、以下が同じ設定の場合、スパニングツリー装置は同じ MST region に属します。

- フォーマットセレクタ（デフォルトは 0 で設定不可）
- MST region 名
- MST region revision レベル
- MST region の同一 VLAN インスタンスマッピングエントリ

MST region に関連したパラメータ（特に VLAN インスタンスマッピングテーブル）の設定は、MSTI に新しいスパニングツリーの計算の原因になり、ネットワークトポロジが不安定になる可能性があります。ネットワークトポロジが不安定になる可能性を減らすために、以下のいずれかの設定をしてから MST region の設定を適用してください。

- **active region-configuration** コマンドで MST region 関連のパラメータをアクティブにします。
- スパニングツリーが無効な状態では、**stp global enable** コマンドで MSTP を有効にします。

STP、RSTP、PVST モードでは MST region の設定は適用されません。

以下に MST region の設定を示します。

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

操作	コマンド	補足
2． MST region view に移行する	**stp region-configuration**	―
3． MST region 名を設定する	**region-name** *name*	デフォルト：装置のMACアドレス
4． VLAN インスタンスマッピングテーブルを作成する	• **instance** *instance-id* **vlan** *vlan-id-list* • **vlan-mapping modulo** *modulo*	どちらかの設定を使用します。 デフォルト：全VLANがCIST（あるいはMSTI 0）にマッピングされています。
5． MST region の MSTP Revision レベルを設定する	**revision-level** *level*	デフォルト：0
6． （オプション設定項目）MST Region の設定がアクティブ化されていないことを表示する	**check region-configuration**	―
7． 手動で MST Region の設定を有効にする	**active region-configuration**	―

8.9 RootブリッジとSecondary Rootブリッジの設定

MSTP は、MSTP 計算でスパニングツリーの Root ブリッジを指定できます。あるいは、Root ブリッジあるいは Secondary Root ブリッジとして装置を指定することができます。

装置は、異なるスパニングツリーと独立しています。あるスパニングツリーの Root ブリッジや Secondary Root ブリッジは、別のスパニングツリーの Root ブリッジや Secondary Root ブリッジにすることができます。しかし 1 つの装置を同じスパニングツリーの Root ブリッジや Secondary Root ブリッジにすることはできません。

スパニングツリーは 1 つの Root ブリッジのみ持ちます。同一時間に、スパニングツリーで複数の Root ブリッジが選択された場合、もっとも小さい MAC アドレスの装置が選択されます。

インスタンスの Root ブリッジが故障あるいはシャットダウンした場合、以下のようになります。

- 1 つの Secondary Root ブリッジのみが指定されている場合、Root ブリッジになります。
- インスタンスに複数の Secondary Root ブリッジを指定していた場合、MSTP が MAC アドレスのもっとも小さい Secondary Root ブリッジを新しい Root ブリッジに指定します。
- Secondary Root ブリッジが指定されていない場合、新しい Root ブリッジを選出します。

装置のプライオリティの設定に関係なく、各スパニングツリーに 1 つの Root ブリッジを指定することができます。装置を Root ブリッジあるいは Secondary Root ブリッジに指定した後は、装置のプライオリティを変更することはできません。

装置のプライオリティを 0 に設定し、Root ブリッジに指定することもできます。装置のプライオリティの設定については、オペレーションマニュアルのセクション 2 *アクセス "STP"の" ブリッジプライオリティの設定"*を参照してください。

8.9.1 Root ブリッジの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． Root ブリッジを設定する	• STP/RSTPモード： **stp root primary** • PVSTモード： **stp vlan** *vlan-id-list* **root primary** • MSTPモード： **stp** [**instance** *instance-list*] **root primary**	デフォルト：Rootブリッジとして機能しません。

8.9.2 Secondary Root ブリッジの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． Secondary Root ブリッジを設定する	• STP/RSTPモード： **stp root secondary** • PVSTモード： **stp vlan** *vlan-id-list* **root secondary** • MSTPモード： **stp** [**instance** *instance-list*] **root secondary**	デフォルト：Secondary Root ブリッジとして機能しません。

8.10 ブリッジプライオリティの設定

スパニングツリーでは、ブリッジプライオリティのパラメータを用いて、Root ブリッジを決定します。この際に使用するブリッジプライオリティの値を、以下のコマンドを使用して設定します。もっとも小さい値のブリッジプライオリティを設定することで、その装置を Root ブリッジにすることができます。異なるスパニングツリーには異なるブリッジプライオリティを設定することができます。

Root ブリッジの選出中に、スパニングツリーのすべての装置が同じプライオリティの値である場合、もっとも小さい MAC アドレスの装置が Root ブリッジとして選択されます。Root ブリッジもしくは Secondary Root ブリッジを指定した後に、装置のブリッジプライオリティを変更することはできません。

以下に指定された MSTI のブリッジプライオリティの設定を示します。

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

操作	コマンド	補足
2． ブリッジプライオリティを設定する	● STP/RSTPモード： **stp priority** *priority* ● PVSTモード： **stp vlan** *vlan-id-list* **priority** *priority* ● MSTPモード： **stp** [**instance** *instance-list*] **priority** *priority*	デフォルト：32768

8.11 MST regionの最大ホップ数の設定

MST Region における最大ホップ数は、MST Region の最大範囲を制限するために使用します。

regional Root ブリッジによって送信された Configuration BPDU は最大値に設定されたホップカウントがあります。装置が Configuration BPDU を受信した場合、ホップカウントを 1 ずつマイナスします。転送される BPDU に新しいホップカウントを使用します。装置が BPDU のホップカウントが 0 の Configuration BPDU を受信した場合、装置は Configuration BPDU 廃棄します。最大ホップを超過する装置はスパニングツリーの計算を行うことができないため、MST region のサイズは制限されます。

この設定は Root ブリッジのみ設定できます。MST region 内にあるほかのすべての装置は、Root ブリッジで設定された値を使用します。

STP ネットワークサイズにもとづいて、MST Region の最大ホップ数を設定することができます。ルートブリッジの最大ホップ数の設定は、Edge ポートの最大ホップ数よりも大きい値にすることを推奨します。

以下に MST region の最大ホップ数の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． MST Region の最大ホップ数を設定する	**stp max-hops** *hops*	デフォルト：20

8.12 ネットワークダイアメータの設定

ネットワークにおける任意の 2 台の装置を結ぶもっとも遠いパス上にある装置の数を、ネットワークの大きさを示す 1 つの指標として設定します。ネットワークダイアメータが大きいと、ネットワークが大きいことを示します。

ネットワークダイアメータの設定に従って、装置は MSTP の Hello 時間、Forward delay、最大エージング時間を適切な値に自動的に設定します。

STP、RSTP、MSTP モードでは、以下のようになります。

- 各 MST region は装置とみなされます。
- 設定したネットワークダイアメータは、CIST（あるいは Root ブリッジ）でのみ有効で、MSTI では無効です。

PVST モードでは、設定されたネットワークダイアメータは指定された VLAN の Root ブリッジでのみ有効です。

以下にネットワークダイアメータの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． ネットワークダイアメータを設定する	● STP/RSTP/MSTPモード： **stp bridge-diameter** *diameter* ● PVSTモード： **stp vlan** *vlan-id-list* **bridge-diameter** *diameter*	デフォルト：7

8.13 スパニングツリータイマの設定

設定可能なスパニングツリー関連タイマには、以下のタイマがあります。

- **Forward delay**– ポートが状態遷移に要する時間です。ネットワークで一時的なループの発生を防ぐため、スパニングツリーは discarding 状態から Forwarding 状態に遷移する前に、中間状態（Learning 状態）に設定します。また Forward delay が終了したのち、ポートが Forwarding 状態に遷移するように要求します。これにより対向先とローカルポートの状態が同期化されることを保証します。
- **Hello 時間**– リンク障害等を検出するために、Hello 時間に設定された間隔で Configuration BPDU（Hello パケット）を定期的に送信します。タイムアウト時間内に Configuration BPDU を受信しない場合、スパニングツリーを再計算します。タイムアウト時間の式は以下となります。

  タイムアウト時間＝タイムアウトファクタ × 3 × Hello 時間
- **Max age**– MSTP ネットワークの CIST で、装置の Configuration BPDU が時間切れになっていないかどうかを判断するのに使うパラメータです。最大有効時間を越えた Configuration BPDU は破棄されます。時間切れになった場合、新しくスパニングツリーの計算を行います。最大エージング時間は MSTI に影響しません。

スパニングツリーの状態変更が頻繁に発生するのを回避するには、Hello 時間、Forward delay、最大エージング時間の設定を次式に満たすよう設定してください。

- 2 ×（Forward delay － 1 秒）≧ Max age
- Max age ≧ 2 ×（Hello 時間 ＋ 1 秒）

スパニングツリーのタイマは手動ではなく自動で設定することを推奨します。ネットワークダイアメータの設定にもとづいて、自動的に計算します。ネットワークダイアメータがデフォルトである場合、スパニングツリーのタイマはデフォルト値となります。

Root ブリッジに設定されるタイマは、ネットワーク全体のすべての装置で適用されます。

8.13.1 設定の制限とガイドライン

- ネットワークのダイアメータに応じて、Forward delay の設定値は変更します。一般的に、ネットワークのダイアメータが大きい程、Forward delay は長く設定してください。Forward delay を極端に短く設定すると一時的に冗長パスが発生してしまい、Forward delay を極端に長くするとネットワーク接続が再開するまでの時間が長くな

ります。よって、一般的なネットワークにおいては、デフォルト値で使用することを推奨します。

- Hello 時間を適切に設定することで、リンク障害等を適切に検出しリンクの切り替えを行えます。Hello 時間を極端に短く設定すると、消費されるネットワークリソースが増えると共に装置での処理も大きくなります。また Hello 時間を極端に長く設定すると、リンク上でパケットロスが発生すると、装置はそれをリンク障害と認識するためスパニングツリーの再構築が発生してしまいます。よって、一般的なネットワークにおいては、デフォルト値で使用することを推奨します。
- スパニングツリーの段数および構成する装置での処理能力に応じて、最大エージング時間の設定値は変更します。極端に小さい設定を行うと、ネットワークの輻輳発生によってスパニングツリーの再構築が発生する可能性があります。また、極端に大きい設定を行うと、リンク障害を所定の時間内に検出し、スパニングツリーを再構築できなくなります。よって、一般的なネットワークにおいては、デフォルト値で使用することを推奨します。

8.13.2 設定手順

以下にスパニングツリータイマの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． Forward delay タイマを設定する	● STP/RSTP/MSTPモード： **stp timer forward-delay** *time* ● PVSTモード： **stp vlan** *vlan-id-list* **timer forward-delay** *time*	デフォルト：15秒
3． Hello 時間を設定する	● STP/RSTP/MSTPモード： **stp timer hello** *time* ● PVSTモード： **stp vlan** *vlan-id-list* **timer hello** *time*	デフォルト：2秒
4． Max age タイマを設定する	● STP/RSTP/MSTPモード： **stp timer max-age** *time* ● PVSTモード： **stp vlan** *vlan-id-list* **timer max-age** *time*	デフォルト：20秒

8.14 タイムアウトファクタの設定

タイムアウトファクタは、以下の式で表されるタイムアウト時間を決めるために使用されるパラメータです。

タイムアウト時間 ＝ タイムアウトファクタ × 3 × Hello 時間

スパニングツリーの状態が安定している場合、Root ブリッジでない装置は Hello パケット（Configuration BPDU）を Hello 間隔で下流の装置にリンクの故障を検知するため転送します。通常、Hello タイマの 9 倍の時間、上流の装置から Hello パケットを受信しないと、上流の装置が故障しているとみなし、ネットワークのトポロジの再構築を開始します。

ネットワークの安定性を保つために、タイムアウトファクタを 5、6、7 に設定することを推奨します。

- 予期しないスパニングツリーの再構築を防ぎます。安定したネットワークにおいても、上流の装置の処理能力がビジー状態の場合に、ネットワークのトポロジの再構築が行われる可能性があります。たとえば、多くのレイヤ 2 インタフェースが上流の装置で設定されているとします。下流の装置がタイムアウト時間内に BPDU の受信に失敗し、予期せずスパニングツリーの再構築が行われます。
- 安定したネットワークでネットワークリソースを削減します。

以下にタイムアウトファクタの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. タイムアウトファクタを設定する	**stp timer-factor** *factor*	デフォルト：3

8.15 BPDU最大送出レートの設定

各 Hello 時間内にポートが送信できる BPDU の最大数は、BPDU 転送レートと Hello 時間の合計に等しいです。ポートの物理状態とネットワークの構成にもとづいて適切な BPDU 転送レートを設定してください。

BPDU 転送レートが高いほど、各 Hello 時間内で BPDU が送信され、システムリソースが多く使用されます。適切な BPDU 転送レートを設定することで、ポートが BPDU を送信するレートを制限できます。適切なレートを設定すると、ネットワークトポロジが変更した際に、スパニングツリープロトコルが過剰なネットワークリソースを使用するのを防ぐことができます。デフォルト値を使うことを推奨します。

以下に BPDU 最大送出レートの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Ethernet interface view あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	―
3. BPDU 最大送出レートを設定する	**stp transmit-limit** *limit*	デフォルト：10

8.16 Edgeポートの設定

Edge ポートとは、ほかの Ethernet スイッチや共有ネットワークセグメントに接続されず、ユーザ端末等に直接接続しているポートを示します。ネットワークトポロジが変化した場合、Edge ポートは一時的なループを起こしません。装置はポートが端末に直接接続されているかどうかを認識しないため、Edge ポートを手動で設定する必要があります。Edge ポートと設定することによって、接続装置が STP をサポートしていない場合には、ポートがリンクアップすると即座に Forwarding 状態に遷移させることができます。

8.16.1 設定の制限とガイドライン

- BPDU ガード機能が無効である場合、Edge ポートが別のポートから BPDU を受信すると、Edge ポートは非 Edge ポートになります。Edge ポートに戻す場合、再度有効化を行う必要があります。
- ポートがユーザ端末に接続されている場合、Edge ポートとして設定し、BPDU ガードを有効にします。この機能によってネットワークのセキュリティを保持しながら Forwarding 状態をすぐに収束させることができます。
- ループガード、Edge ポートの機能を、ポートに同時に設定することはできません。

8.16.2 設定手順

以下に Edge ポートの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Ethernet あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	―
3. Edge ポートを設定する	**stp edged-port**	デフォルト : すべてのポートは非エッジポートです。

8.17 ポートパスコストの設定

パスコストは、ポートに接続するリンクの速度に関係するパラメータです。MSTP 対応の装置では、ポートは MSTI ごとに異なるパスコストを持つことができます。パスコストを適切に設定することで、VLAN トラフィックフローが別々の物理リンクで転送されるため、VLAN ごとの負荷分散が可能です。

装置は自動的にデフォルトのパスコストを計算でき、一方でユーザはポートのパスコストを設定できます。

8.17.1 デフォルトパスコストの計算時の基準指定

⚠ **注意**：
装置がデフォルトパスコストを計算する際に使用する基準を変更した際は、デフォルトにパスコストを戻してください。

ポートパスコストのデフォルト値には以下のモードがあります。設定の標準から選択できます。

- **dot1d-1998**– IEEE 802.1d-1998 で規定されているポートパスコストの対応値を使用します。
- **dot1t**– IEEE 802.1t で規定されているポートパスコストの対応値を使用します。

- **legacy**– QX シリーズ独自のポートパスコストの対応値を使用します。

デフォルトのパスコストを計算する際に基準を設定する場合、以下のガイドラインに従ってください。

- アグリゲーションリンクのパスコストの計算は、IEEE 802.1d-1998 の場合、アグリゲーションリンクのポートの数を考慮しません。IEEE 802.1t は、アグリゲーションリンクのポートの数を考慮にします。計算式は、パスコスト＝ 200,000,000/リンク速度（100kbps 単位）で、リンク速度はアグリゲーションリンクがブロックされていないポートのリンク速度の合計です。
- IEEE 802.1d-1998 あるいは QX シリーズ独自の基準は、ポートあるいはインタフェースのリンク速度が 10Gbps を超えた場合、単一ポートあるいはアグリゲートインタフェースに設定可能なもっとも小さい値を指定してください。この基準にもとづいて転送するパスは、最適なパスにならない可能性があります。この問題に対応するため、以下のいずれかを行ってください。
  - □ デフォルトパスコスト計算の基準として、**dot1t** を使用します。
  - □ ポートのパスコストを手動で設定します。（オペレーションマニュアルのセクション 2 *アクセス "STP"の"パスコストの設定"*を参照してください。）

以下にデフォルトパスコストを計算する場合に装置に使用する基準を指定する方法を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． パスコストの計算基準を設定する	**stp pathcost-standard** { **dot1d-1998** | **dot1t** | **legacy** }	デフォルト：**legacy**

表 8-7 リンク速度とパスコスト間のマッピング

リンク速度	ポートタイプ	パスコスト		
		IEEE 802.1d-1998	IEEE 802.1t	QX シリーズ独自
0	―	65535	200000000	200000
10 Mbps	単一ポート	100	2000000	2000
	集約リンク2ポート		1000000	1800
	集約リンク3ポート		666666	1600
	集約リンク4ポート		500000	1400
100 Mbps	単一ポート	19	200000	200
	集約リンク2ポート		100000	180
	集約リンク3ポート		66666	160
	集約リンク4ポート		50000	140
1000 Mbps	単一ポート	4	20000	20
	集約リンク2ポート		10000	18
	集約リンク3ポート		6666	16
	集約リンク4ポート		5000	14
10 Gbps	単一ポート	2	2000	2
	集約リンク2ポート		1000	1
	集約リンク3ポート		666	1
	集約リンク4ポート		500	1
20 Gbps	単一ポート	1	1000	1
	集約リンク2ポート		500	1
	集約リンク3ポート		333	1
	集約リンク4ポート		250	1
40 Gbps	単一ポート	1	500	1

リンク速度	ポートタイプ	パスコスト		
		IEEE 802.1d-1998	IEEE 802.1t	QX シリーズ独自
	集約リンク2ポート		250	1
	集約リンク3ポート		166	1
	集約リンク4ポート		125	1
100 Gbps	単一ポート	1	200	1
	集約リンク2ポート		100	1
	集約リンク3ポート		66	1
	集約リンク4ポート		50	1

8.17.2 ポートのパスコストの設定

ポートのパスコストを変更した場合、ポートの役割を再計算し、状態遷移を初期化します。

以下にポートのパスコストの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Ethernet あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	―
3. パスコストを設定する	• STP/RSTPモード： **stp cost** *cost* • PVSTモード： **stp vlan** *vlan-id-list* **cost** *cost* • MSTPモード： **stp** [**instance** *instance-list*] **cost** *cost*	デフォルト：システムがパスコストを自動計算します。

8.17.3 設定例

MSTP モードで、以下の設定をします。

- IEEE 802.1d-1998 の計算基準を使用します。
- MSTI 2 の GigabitEthernet 1/0/3 のパスコストを 200 に設定します。

```
<Switch> system-view
[Switch] stp pathcost-standard dot1d-1998
Cost of every port will be reset and automatically re-calculated after you change
the current pathcost standard. Continue?[Y/N]:y
Cost of every port has been re-calculated.
[Switch] interface gigabitethernet 1/0/3
[Switch-GigabitEthernet1/0/3] stp instance 2 cost 200
```

PVST モードで以下を設定します。

- IEEE 802.1d-1998 の計算基準を使用します。
- VLAN20～VLAN30 の GigabitEthernet 1/0/3 のパスコストを 2000 に設定します。

```
<Switch> system-view
[Switch] stp pathcost-standard dot1d-1998
Cost of every port will be reset and automatically re-calculated after you change
the current pathcost standard. Continue?[Y/N]:y
Cost of every port has been re-calculated
[Switch] interface gigabitethernet 1/0/3
[Switch-GigabitEthernet1/0/3] stp vlan 20 to 30 cost 2000
```

8.18 ポートプライオリティの設定

Root ポートを選出する際、ポートのポートプライオリティが重要な役割を果たします。ほかのパラメータが同じ場合、ポートプライオリティの高いポート（ポートプライオリティ値が小さいポート）が Root ポートに選出されます。

スパニングツリーでは異なるパスごとに異なるポートプライオリティを設定でき、スパニングツリーごとに役割を指定できます。そのため、VLAN 単位で異なる物理ポートを介してデータを流すことができるため、VLAN ベースで負荷分散が可能となります。正確なネットワーク要件にもとづいてポートプライオリティを設定することができます。

ポートのプライオリティを変更した場合、システムはポートの役割を再計算し、状態遷移を開始します。

以下にポートプライオリティの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. Ethernet interface view あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	—
3. ポート priority を設定する	• STP/RSTPモード： **stp port priority** *priority* • PVSTモード： **stp vlan** *vlan-id-list* **port priority** *priority* • MSTPモード： **stp** [**instance** *instance-list*] **port priority** *priority*	デフォルト：128

8.19 Point-to-Pointリンクの設定

Point-to-Point リンクは、2 台の装置を直結するリンクです。2 つの Root ポートや Designated ポートが Point-to-Point リンクである場合、そのリンクの両端に Point-to-Point リンクと設定することで、ポート間で同期のためのパケットを使用して、即座に Forwarding 状態に遷移させることができます。

8.19.1 設定の制限とガイドライン

- リンクアグリゲーションを設定している場合や全 2 重モードを設定している場合、Point-to-Point リンクとして設定することができます。NEC ではデフォルトの設定を使用し、リンクタイプを自動的に設定した値とすることを推奨します。
- MSTP あるいは PVST モードのポートに **stp point-to-point force-false** コマンドあるいは **stp point-to-point force-true** コマンドを設定した場合、設定はすべての VLAN あるいは MSTI に適用されます。
- 実際には Point-to-Point でないポートに対して、Point-to-Point の設定を行うと、一時的にループが発生する可能性がありますので、注意してください。

8.19.2 設定手順

以下に Point-to-Point リンクの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Ethernet あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	―
3. Point-to-Point リンクを設定する	**stp point-to-point** { **auto** | **force-false** | **force-true** }	デフォルト：**auto** autoではポートが自動的にリンクタイプを決定します。

8.20 MSTPパケットのフォーマット設定

ポートは以下のフォーマットで MSTP パケットの送受信を行うことができます。

- **dot1s** – IEEE802.1s で規定された形式です。
- **legacy** – QX シリーズ独自形式（IEEE802.1s ドラフト版で規定された形式）です。対向装置は、QX シリーズの製品のみです。

デフォルトの MSTP のパケットフォーマットは **auto** です。ポートは自動で 2 つの MSTP パケットのフォーマットを区別します。対向装置からの BPDU に合わせて、自動でフォーマットを選択し、送信します

MSTP パケットフォーマットをポートに設定できます。設定後、MSTP モードで動作している場合は、ポートは設定しているフォーマットのパケットのみ送受信し、同じフォーマットのパケットを送信する装置と通信します。

auto モードのポートはデフォルトで IEEE 802.1s MSTP パケットのみ送信します。ポートが legacy フォーマットの MSTP パケットを受信した場合、ポートは **legacy** フォーマットのパケットのみ送信を行います。これは、ポートがパケットのフォーマットを頻繁に変更することを防ぎます。IEEE 802.1s MSTP パケットを送信するように設定するために、ポートをシャットダウンし、その後ポートをアップ状態にします。

MSTI 数が 48 を超えた場合、ポートは IEEE 802.1s のみ送信することができます。

以下にポートでサポートされる MSTP パケットフォーマットの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． Ethernet あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	―
3． MSTP パケットフォーマットを設定する	**stp compliance** { **auto** | **dot1s** | **legacy** }	デフォルト：**auto**

8.21 ポート遷移状態情報の出力の有効化

大規模なスパニングツリーネットワークでは、MSTI のポート状態の遷移に関する情報を出力できるように設定し、リアルタイムでポート状態をモニタリングできます。

以下にポート状態の遷移に関する情報を出力する設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． ポート遷移状態の情報を出力するように設定を有効にする	• STP/RSTPモード：**stp port-log instance 0** • PVSTモード：**stp port-log vlan** *vlan-id-list* • MSTPモード：**stp port-log** { **all** | **instance** *instance-list* }	デフォルト：無効

8.22 スパニングツリー機能の有効化

ほかのスパニングツリー機能に関連した設定を有効にする前に、装置でスパニングツリー機能を有効化する必要があります。STP、RSTP、MSTP モードではスパニングツリー機能がグローバルと設定したポートで有効化されることを確認してください。PVST モードではスパニングツリー機能がグローバル、指定した VLAN および設定したポートで有効化されることを確認してください。

ポートでのスパニングツリーの計算と装置の CPU のリソースを節約するため、**undo stp enable** コマンドを使用して、ポートでスパニングツリー機能を無効にすることができます。スパニングツリー機能を無効にしたら、ループが発生していないことを確認してください。

8.22.1 STP/RSTP/MSTP モードでのスパニングツリー機能の有効化

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． スパニングツリー機能を有効にする	**stp global enable**	デフォルト：無効

操作	コマンド	補足
3． Ethernet interface view あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	―
4． （オプション設定項目）ポートでスパニングツリー機能を有効にする	**stp enable**	デフォルト : すべてのポートで有効

8.22.2 PVST モードでのスパニングツリー機能の有効化

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． スパニングツリー機能を有効にする	**stp global enable**	デフォルト：無効
3． VLAN でスパニングツリー機能を有効にする	**stp vlan** *vlan-id-list* **enable**	デフォルト：すべてのVLANで有効
4． Ethernet interface view あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	―
5． ポートでスパニングツリー機能を有効にする	**stp enable**	デフォルト : すべてのポートで有効

8.23 mCheck機能の設定

mCheck 機能はポート状態転送プロセスをユーザが設定できるようにする機能です。

MSTP、MSTP あるいは PVST が動作している装置のポートが STP で動作する装置に接続し STP BPDU を受信した場合、ポートは STP モードに自動的に変更します。しかし以下の場合は、ポートは自動的にもとのモードに戻ることができません。

- 対向の STP 装置がシャットダウンあるいは取り外された場合
- ローカルの装置が変更を検出できない場合

もとのモードで動作するようにポートの設定を強制的に変更するために、mCheck 機能の設定を行うことができます。

たとえば Device A、Device B、Device C が順に接続されています。Device A は STP が動作し、Device B はスパニングツリーが動作しておらず、Device C は RSTP、MSTP あるいは PVST で動作しています。この場合、Device C は、Device B によって透過的に転送された STP BPDU を受信すると、受信したポートは STP モードに変更します。Device B が Device C と RSTP、MSTP あるいは PVST で動作するように設定された場合、Device B と Device C で相互に接続されているポートは mCheck を動作させる必要があります。

8.23.1 設定の制限とガイドライン

mCheck 機能は MSTP、RSTP あるいは PVST モードで動作する装置で適用されます。

8.23.2 グローバルでの mCheck の設定手順

操作	コマンド
1． system view に移行する	**system-view**
2． mCheck を実行する	**stp global mcheck**

8.23.3 interface view での mCheck の実行

操作	コマンド
1． system view に移行する	**system-view**
2． Ethernet あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*
3． mCheck を実行する	**stp mcheck**

8.24 Digest Snoopingの設定

⚠ **注意：**

以下に示す状況において、グローバルで Digest Snooping を設定する場合、注意してください。

- VLAN インスタンスマッピングを変更する場合
- デフォルトの MST region の設定を復元する場合

VLAN インスタンスマッピングが隣り合う装置と異なる場合、ループあるいは通信断が発生します。

IEEE 802.1s で定義されているように、同じ region で接続された装置は、MST region 関連の設定が一致します。MST region 関連の設定は以下が含まれます。

- region 名
- リビジョンレベル
- VLAN インスタンスマッピング

MSTP 対応の装置は、BPDU パケットの Configuration ID をチェックすることで、同じ MST region の装置かを識別します。Configuration ID は、region 名、リビジョンレベル、設定ダイジェスト（16 バイト長、VLAN インスタンスマッピングにもとづく HMAC-MD5 アルゴリズムによる計算結果）で構成されています。

MSTP の実装はベンダによって異なり、プライベートキーを使用して計算する設定ダイジェストも異なります。同じ MST region でも装置を提供するベンダが異なると、互いに通信することができません。

NEC の装置とほかのベンダの装置間で通信を行う場合、同じ MST region で接続するポートで Digest snooping 機能を有効にします。

8.24.1 設定の制限とガイドライン

Digest snooping の設定を行う場合以下のガイドラインに従ってください。

- Digest snooping を有効にする前に、別のベンダの装置がスパニングツリーに接続され、動作していることを確認してください。
- Digest Snooping 機能が有効になっている場合、同じ region（in-the-same-region）チェックに設定ダイジェストの比較は行われないため、関連するポートでは VLAN インスタンスマッピングを同じにしなければなりません。
- Digest snooping 機能を適用するためには、グローバルと設定ポートの両方で Digest snooping 機能を有効にしてください。まず、関連するすべてのポートで Digest snooping 機能を有効にし、それからグローバルでも有効にすることを推奨します。これにより設定がすべてのポートに適用され、ネットワークへの影響を減らすことができます。
- ループを防ぐため、MST region の Edge ポートで Digest snooping を有効にしないでください。
- Digest snooping を有効にした後、スパニングツリー機能を有効にしてください。ネットワークの動作が安定している場合は、トラフィックの中断を避けるため、Digest snooping を有効にしないでください。

8.24.2 設定手順

設定 Digest を計算するために秘密鍵を使用している他ベンダの装置が、NEC の装置に接続されている場合、NEC の装置でのみ Digest snooping の設定を有効にすることができます。

以下に Digest snooping の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Ethernet あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	―
3. インタフェースで Digest Snooping を有効にする	**stp config-digest-snooping**	デフォルト：無効
4. system view から戻る	**quit**	―
5. グローバルで Digest Snooping を有効にする	**stp global config-digest-snooping**	デフォルト：無効

8.24.3 Digest Snooping 設定例

I. ネットワーク要件

図 8-16に示すように、Device A、Device B が Device C に接続されています。Device C はほかベンダの装置で、すべての装置は同じ region を使用しています。

3 つの装置が互いに通信できるように、Device C に接続されている Device A、Device B のポートで Digest snooping を有効にします。

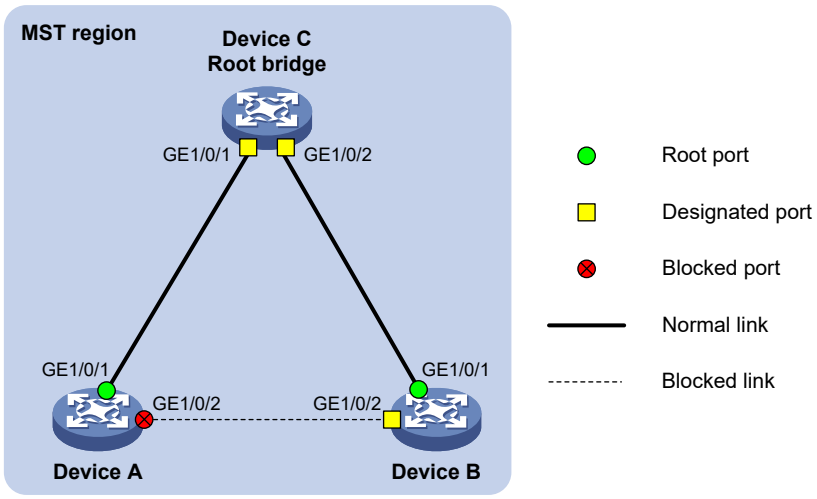


図 8-16 ネットワーク図

II. 設定手順

Device A の GigabitEthernet 1/0/1 で Digest snooping を有効にし、Device A のグローバルで Digest snooping を有効にします。

```
<DeviceA> system-view
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] stp config-digest-snooping
[DeviceA-GigabitEthernet1/0/1] quit
[DeviceA] stp global config-digest-snooping
```

Device B の GigabitEthernet 1/0/1 で Digest snooping を有効にし、Device B のグローバルで Digest snooping を有効にします。

```
<DeviceB> system-view
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] stp config-digest-snooping
[DeviceB-GigabitEthernet1/0/1] quit
[DeviceB] stp global config-digest-snooping
```

8.25 No Agreement Checkの設定

RSTP と MSTP の Designated ポートの高速な状態遷移には、2 つのタイプのメッセージが使用されています。

- **Proposal** – Designated ポートから送信される高速遷移リクエスト
- **Agreement** – 高速遷移リクエストの応答（acknowledge）パケット

RSTP、MSTP が動作している装置のポートが下流装置から、agreement パケットを受信した場合にのみ、Designated ポートで高速遷移を実行できます。RSTP 装置と MSTP 装置の相違点は以下のとおりです。

- MSTP 装置は、下流装置の Root ポートが上流装置から agreement パケットを受信した後にのみ、agreement パケットを送信します。
- RSTP 装置は、下流装置の Root ポートが上流装置から agreement パケットを受信したかに関わらず、agreement パケットを送信します。

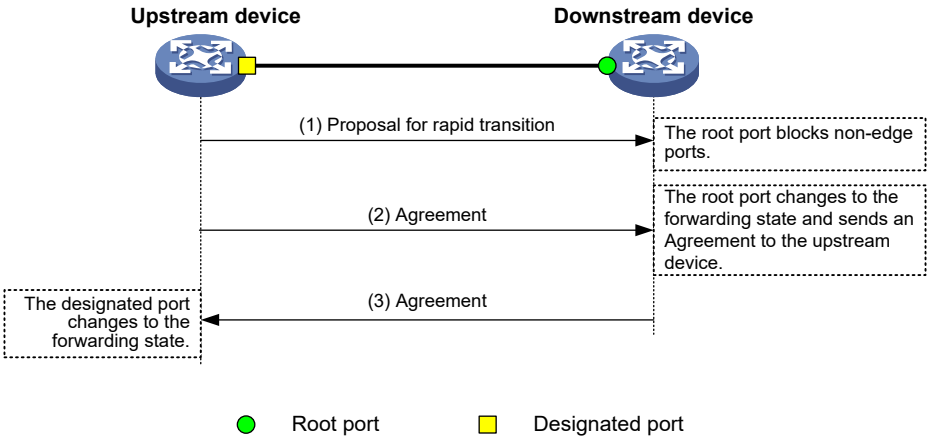


図 8-17 MSTP の Designated ポートの高速状態遷移のメカニズム

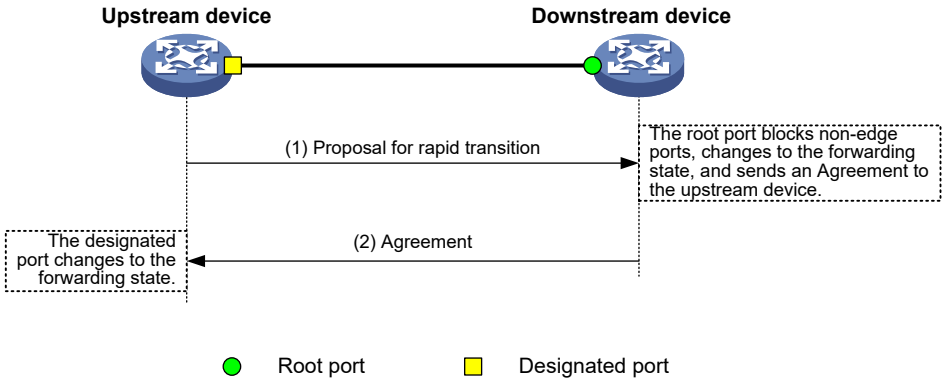


図 8-18 RSTP の Designated ポートの高速状態遷移のメカニズム

上流装置がほかベンダの装置である場合、高速状態遷移の実行が以下のように制限される可能性があります。

- 上流装置が RSTP と類似の高速遷移メカニズムを使用します。
- 下流装置が MSTP を使用し、RSTP モードをサポートしません。

この場合、以下の事象が発生します。

1)　下流装置の Root ポートは上流装置から agreement パケットを受信しません。
2)　上流装置に no agreement パケットを送信します。

その結果、上流装置の Designated ポートは 2 倍の Forward delay の後、Forwarding 状態に遷移します。

このような場合に下流装置のポートで No Agreement Check 機能を有効にすることで、高速状態遷移を実行できます。

8.25.1 設定要件

No Agreement Check 機能を設定する前に、以下の作業を行う必要があります。

- 装置は、スパニングツリーに対応している他ベンダの装置と point-to-point リンクによって接続しています。
- 2 台の装置に同じ region 名、リビジョンレベル、VLAN インスタンスマッピングを設定し、同じ region に所属させます。

8.25.2 設定手順

Root ポートで No Agreement Check 機能を有効にすることができます。

以下に No Agreement Check の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. Ethernet interface view あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	—
3. No Agreement Check 機能を有効にする	**stp no-agreement-check**	デフォルト：無効

8.25.3 No Agreement Check 設定例

I. ネットワーク要件

図 8-19に示すように、以下の要件に従います。

- Device A は、同じ region に属し、異なる MSTP を実装した他ベンダの装置に接続しています。
- ほかのベンダの装置（Device B）は Regional Root ブリッジで、Device A は下流装置です。

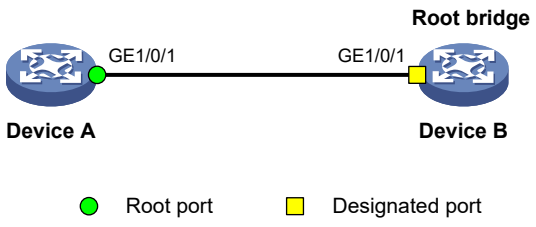


図 8-19 ネットワーク図

II. 設定手順

Device A の GigabitEthernet 1/0/1 で、No Agreement Check 機能を有効にします。

```
<DeviceA> system-view
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] stp no-agreement-check
```

8.26 TC snoopingの設定

8.26.1 設定の制限とガイドライン

TC snooping の設定を行う場合、以下のガイドラインに従ってください。

- TC snooping とスパニングツリー機能を同時に設定できません。TC snooping 機能を有効化する前に、グローバルでスパニングツリー機能を無効にしてください。
- TC snooping は PVST モードではサポートしておりません。

8.26.2 設定手順

以下に TC snooping の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. スパニングツリー機能を無効にする	**undo stp global enable**	デフォルト：無効
3. TC snooping 機能を有効にする	**stp tc-snooping**	デフォルト：無効

8.27 保護機能の設定

8.27.1 保護機能の設定作業リスト

すべてのスパニングツリー保護機能はオプション設定項目です。

作業リスト
BPDUガードの設定
Rootガードの有効化
Loopガードの有効化
ポート役割の制限機能の設定
TC-BPDUガードの有効化
BPDUドロップ機能の有効化
PVST BPDUガードの有効化

8.27.2 BPDU ガードの設定

アクセスポートは通常、ユーザ端末（PC など）やファイルサーバに直接接続されており、高速な遷移を実現するために、Edge ポートに設定されています。こうしたポートで BPDU パケットを受信すると、装置はそのポートを自動的に非 Edge ポートに設定し、スパニングツリーの再計算を開始します。その結果、ネットワーク全体でトポロジ変更が発生する可能性があります。通常の状況下ではこれらのポートは Configuration BPDU を受信すべできではありません。しかし不正な装置への攻撃によって Configuration BPDU を偽造した場合、ネットワークは不安定となります。

スパニングツリープロトコルは、このような攻撃に対してシステムを保護する BPDU ガード機能を提供します。BPDU ガードが有効になっている装置で、Edge ポートが configuration BPDU を受信すると、装置は以下の操作を実行します。

- Edge ポートに設定しているポートを shutdown 状態にします。
- NMS に shutdown 状態であることを通知します。

装置は検出の間隔後に、shutdown 状態のポートの解除を行います。検出の間隔は shutdown-interval コマンドを使用して設定することができます。検出の間隔についての詳細は、オペレーションマニュアルのセクション 1 *はじめに* "*装置管理*"を参照してください。

BPDU ガードは、グローバルあるいは Edge ポートで設定します。

loopback test が設定されたポートでは、BPDU ガードを有効にすることができません。loopback test についての詳細は、オペレーションマニュアルのセクション 2 *アクセス* "*Ethernet インタフェース*"を参照してください。

I. グローバルでの BPDU ガードの有効化

グローバルでの BPDU ガードの設定はすべての Edge ポートで適用されます。

以下に BPDU ガードの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. BPDU ガードを有効にする	**stp bpdu-protection**	デフォルト：無効

II. インタフェースでの BPDU ガードの有効化

Edge ポートはインタフェースで設定された BPDU ガードを優先します。インタフェースで BPDU ガードの設定が行われていない場合、グローバルでの BPDU ガードの設定が適用されます。

以下にインタフェースでの BPDU ガードの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Ethernet interface view あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	―

操作	コマンド	補足
3. BPDU ガードを有効にする	**stp port bpdu-protection** { **enable** | **disable** }	edgeポートに設定されていません。インタフェースのBPDUガード機能の状態はグローバルでのBPDUガード機能と同一です。

8.27.3 Root ガードの有効化

スパニングツリーの Root ブリッジと Secondary Root ブリッジは、同一 MST region に割り当てられることを推奨します。特に CIST では、Root ブリッジと Secondary Root ブリッジは、ネットワーク設計で、高帯域幅を持つ領域に配置されます。しかし設定ミスや攻撃により、不正な装置がより高い優先度を持った Configuration BPDU を配信すると、本来意図されるスパニングツリーのトポロジが構成されないだけでなく、ネットワークトポロジの変更が多発します。トラフィックが高帯域幅のリンクから低帯域幅のリンクに切り替えられてしまい、ネットワークを安定して使用できなくなります。

この状況を防止するための機能として、Root ガードをサポートします。Root ガードが Root ブリッジのポートで有効である場合、ポートはすべてのポートの Designated ポートの役割を実行します。MSTI から高い優先度の Configuration BPDU を受信した後、以下の操作を行います。

- すぐに MSTI の Listening 状態にポートを切り替えます。
- 受信した Configuration BPDU を転送しません。

ポートが 2 倍の Forward delay 内に高い優先度の BPDU を受信しない場合、もとの状態に戻ります。

ポートで Loop ガード、Root ガードの設定を同時に設定することができません。

Root ガードは、Designated ポートで設定します。

以下に Root ガードの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Ethernet interface view あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	―
3. Root ガードを有効にする	**stp root-protection**	デフォルト：無効

8.27.4 Loop ガードの有効化

上流装置から BPDU を受信し続けることによって、Root ポートと Blocking ポートの状態を維持することができます。しかしリンクの衝突あるいは片方向リンクの障害が発生すると、ポートは上流装置から BPDU を受信できなくなる可能性があります。この場合、装置は以下のポートの役割を再選択します。

- 上流の BPDU の受信に失敗した Forwarding 状態のポートは Designated ポートになります。
- Blocked ポートは Forwarding 状態に遷移します。

この結果、スイッチネットワークでリンクループが発生します。Loop ガード機能はこのループを防止します。

Loop ガード対応ポートの初期状態は、各 MSTI で Discard 状態です。ポートが BPDU を受信し、正常状態になっても、そのポートを Designated ポートとして Forwarding 状態に遷移しません。Blocking 状態でパケットを転送しないため、一時的なリンクのループを回避できます。

ユーザの端末を接続したポートで Loop ガードを有効にしないでください。BPDU を受信できないため、すべての MSTI で discard 状態になったままとなります。

ポートの Loop ガード機能は Root ガード機能あるいは Edge ポートの設定を同時に設定することはできません。

装置の Root ポートと、Alternate ポートで Loop ガードを設定します。

以下に Loop ガードの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Ethernet interface view あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	―
3. Loop ガードを有効にする	**stp loop-protection**	デフォルト：無効

8.27.5 ポート役割の制限機能の設定

注意：
この機能を使用することで、スパニングツリーのトポロジの接続に影響する可能性がありますので、注意して設定してください。

ユーザアクセスネットワークの装置のブリッジ ID を変更すると、コアネットワークのスパニングツリーのトポロジが変更する可能性があります。この問題を回避するため、ポート役割の制限機能を有効にすることができます。この機能を有効にすることで、ポートが上位の BPDU を受信した場合、ルートポートではなく Alternate ポートになります。

この機能はユーザアクセスネットワークに接続するポートに設定してください。

以下にポート役割の制限機能の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Ethernet interface view あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	―
3. ポート役割の制限機能を有効にする	**stp role-restriction**	デフォルト：無効

8.27.6 TC-BPDU ガードの有効化

装置はトポロジ変更（TC）の BPDU（BPDU はトポロジ変更を装置に通知します）パケットを受信すると、転送アドレスエントリを削除します。しかし、悪意のユーザから偽装した TC-BPDU パケットの攻撃を受けた場合、装置は非常に短い時間内に大量の TC-BPDU パケットを受信することになります。頻繁に削除オペレーション（MAC アドレステーブルの更新）を実行すると、装置のリソースを浪費し、ネットワークの安定性に大きな被害をもたらす可能性があります。

TC-BPDU ガードを有効にすると、最初に TC-BPDU を受信した後、指定時間内（10 秒）の間に、転送アドレスエントリを即座に削除する最大数を設定することができます。TC-BPDU を制限以上受信した場合、装置は一定の期間の満了後に、転送アドレスエントリを削除します。これにより、頻繁に転送アドレスエントリの削除オペレーションを行うことを防ぐことができます。NEC は TC-BPDU ガードを有効にすることを推奨します。

以下に TC-BPDU ガードの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. TC-BPDU ガードを有効にする	**stp tc-protection**	デフォルト：有効 無効にすることを推奨しません。
3. （オプション設定項目）10 秒ごとに、装置が即座に転送アドレスエントリを削除する最大の回数を設定する	**stp tc-protection threshold** *number*	デフォルト：6

8.27.7 BPDU ドロップ機能の有効化

I. BPDU ドロップ機能

スパニングツリーネットワークにおいて、装置に到着した各 BPDU は、STP 計算プロセスを行い、ネットワークのほかの装置に転送を行います。悪意のある攻撃者はこの脆弱性を使用して、BPDU を偽造してネットワークを攻撃する可能性があります。偽造された BPDU を継続的に送信することにより、ネットワークのすべての装置が STP の計算を計算し続けることになり、結果として CPU が過負荷になるような問題によって、BPDU プロトコルの状態エラーが発生します。

この問題を回避するため、ポートで BPDU ドロップ機能を有効にします。BPDU ドロップ機能が有効になったポートでは、BPDU の受信を行わず、BPDU 攻撃による影響を受けません。

II. 制限とガイドライン

この機能を使用することで、装置は以下の BPDU パケットをドロップします。

- EOAM
- GVRP
- LACP
- LLDP

- PVST
- STP（STP、RSTP、MSTP を含みます）

III. 設定手順

以下に BPDU ドロップ機能の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． Ethernet interface view に移行する	**interface** *interface-type interface-number*	―
3． BPDU ドロップ機能を設定する	**bpdu-drop any**	デフォルト：無効

8.27.8 PVST BPDU ガードの有効化

MSTP 対応装置は PVST BPDU を認識できないため、データトラフィックとして PVST BPDU を転送します。別の独立したネットワークにある PVST 対応装置で PVST BPDU を受信した場合、PVST の計算に失敗する可能性があります。PVST の計算を失敗させないため、MSTP 対応装置で PVST BPDU ガード機能を有効にします。ポートで PVST BPDU を受信した場合、装置はポートをシャットダウンします。

以下に PVST BPDU ガード機能の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． PVST BPDU ガード機能を有効にする	**stp pvst-bpdu-protection**	デフォルト：無効

8.28 TC BPDUの検出、受信イベントのログ作成の有効化

TC BPDU を検出、あるいは受信した場合、装置でログを作成します。この機能は PVST モードでのみ有効です。

以下に TC BPDU の検出、受信イベントの作成の有効化の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． TC BPDU を検出、あるいは受信した場合、装置でログを作成する	**stp log enable tc**	デフォルト：無効

8.29 BPDUガードによりシャットダウンされたエッジポートの再アクティブ化の無効化

BPDU ガードは、BPDU を受信したエッジポートをシャットダウンし、NMS にシャットダウンを通知します。

装置はポートステータス検出タイマが期限切れになった場合に、シャットダウンされたポートを再アクティブ化します。このタイマは **shutdown-interval** コマンドを使用して設定することができます。

この機能は、この機能が設定された後、BPDU ガードによってシャットダウンされたエッジポートを再アクティブ化することを防ぎます。**undo stp port shutdown permanent** コマンドを実行すると、装置はシャットダウンポートを起動しません。これらのポートを起動するには、**undo shutdown** コマンドを使用します。

以下に BPDU ガードによりシャットダウンしたエッジポートの再アクティブ化を無効化する設定手順を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． T BPDU ガードによりシャットダウンしたエッジポートの再アクティブ化を無効にする	**stp port shutdown permanent**	デフォルト：無効

8.30 新規ルートブリッジの選択、トポロジ変更イベントによるSNMP notificationの有効化

この機能を有効にすると、新規ルートブリッジの選択、あるいはスパニングツリーのトポロジ変更イベントが発生した場合、装置はログを作成し、SNMP に通知します。正常にイベントの notification を送信するため、装置で SNMP を設定する必要があります。SNMP の設定の詳細は、オペレーションマニュアルのセクション 9 *システム管理 ”SNMP”* を参照してください。

snmp-agent trap enable stp [**new-root** | **tc**]コマンドを使用する場合、以下のガイドラインに従ってください。

- **new-root** パラメータは STP、MSTP、RSTP モードでのみ適用します。
- **tc** パラメータは PVST モードでのみ適用します。
- STP、MSTP、RSTP モードでは、**snmp-agent trap enable stp** コマンドは、新規ルートブリッジの選択イベントが発生した場合、SNMP notification の送信を有効にします。
- PVST モードでは、**snmp-agent trap enable stp** コマンドは、スパニングツリーのトポロジ変更が発生した場合、SNMP notification の送信を有効にします。

以下に新規ルートブリッジの選択イベント、スパニングツリーのトポロジ変更イベントによる SNMP notification の送信の有効化の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． 新規ルートブリッジの	STP、MSTP、RSTPモード：	デフォルト：

操作	コマンド	補足
選択イベントによる SNMP notification の送信を有効にする	• **snmp-agent trap enable stp new-root** • **snmp-agent trap enable stp**	• 新規ルートブリッジの選択イベントによるSNMP notificationの送信は無効です。 • MSTPモードではスパニングツリーのトポロジの変更が発生した場合、MSTI 0のSNMP notificationの送信は有効です。ほかのMSTIのSNMP notificationの送信は無効です。 • PVSTモードではすべてのVLANのスパニングツリーのトポロジの変更が発生した場合、SNMP notificationの送信は無効です。
3. スパニングツリーのトポロジ変更イベントによる SNMP notification の送信を有効にする	PVSTモード： **snmp-agent trap enable stp tc**	

8.31 スパニングツリーの表示と維持

すべての view で **display** コマンドを実行し、user view で **reset** コマンドを実行できます。

操作	コマンド
STPのガード機能によってブロッキング状態にあるポートの表示する	**display stp abnormal-port**
ポートのBPDU統計情報を表示する	**display stp bpdu-statistics** [**interface** *interface-type interface-number* [**instance** *instance-list*]]
STPの保護機能によってダウンしているポートを表示する	**display stp down-port**
MSTIポートの役割計算の履歴を表示する	**display stp** [**instance** *instance-list* | **vlan** *vlan-id-list*] **history** [**slot** *slot-number*]
MSTIの全ポートで送受信されたTC/TCN BPDUの統計情報を表示する	**display stp** [**instance** *instance-list* | **vlan** *vlan-id-list*] **tc** [**slot** *slot-number*]
スパニングツリーの状態および統計情報を表示する	**display stp** [**instance** *instance-list* | **vlan** *vlan-id-list*] [**interface** *interface-list* | **slot** *slot-number*] [**brief**]
有効なMST regionの設定情報を表示する	**display stp region-configuration**
MSTIのRootブリッジの情報を表示する	**display stp root**
スパニングツリーの統計情報を削除する	**reset stp** [**interface** *interface-list*]

8.32 スパニングツリー設定例

8.32.1 MSTP 設定例

I. ネットワーク要件

図 8-20に示すようにすべての装置は同じ MST region にあります。Device A、Device B はディストリビューション層にあり、Device C、Device D はアクセス層にあります。

異なる VLAN のパケットが異なるスパニングツリーに転送されるように MSTP を設定します。

- VLAN 10 のパケットは MSTI1 で転送されます。
- VLAN 30 のパケットは MSTI3 で転送されます。
- VLAN 40 のパケットは MSTI4 で転送されます。
- VLAN 20 のパケットは MSTI0 で転送されます。

VLAN 10 と VLAN 30 はディストリビューション層の装置のみ、VLAN 40 はアクセス層の装置のみで通信します。MSTI1 と MSTI3 の Root ブリッジは Device A、Device B となり、MSTI4 の Root ブリッジは Device C となります

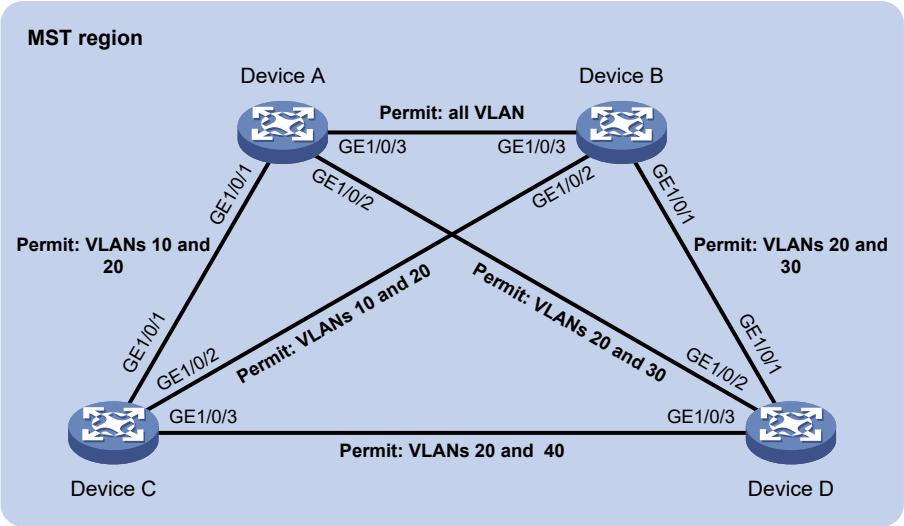


図 8-20 ネットワーク図

II. 設定手順

1)　VLAN を作成し、VLAN メンバポートを設定します。（詳細は省略します）
   - □　Device A、Device B の両方で VLAN 10、VLAN 20、VLAN 30 を作成します。
   - □　Device C で VLAN 10、VLAN 20、VLAN 40 を作成します。
   - □　Device D で VLAN 20、VLAN 30、VLAN 40 を作成します。
   - □　装置のポートをトランクポートに設定し、関連する VLAN を割り当てます。

2)　Device A を設定します。

MST region view に移行し、MST region 名 **example** を設定します。

```
<DeviceA> system-view
[DeviceA] stp region-configuration
[DeviceA-mst-region] region-name example
```

VLAN 10、VLAN 30、VLAN 40 をそれぞれ MSTI1、MSTI3、MSTI4 に割り当てます。

```
[DeviceA-mst-region] instance 1 vlan 10
[DeviceA-mst-region] instance 3 vlan 30
[DeviceA-mst-region] instance 4 vlan 40
```

MST region レベルを 0 とします。

```
[DeviceA-mst-region] revision-level 0
```

MST region の設定をアクティブにします。

```
[DeviceA-mst-region] active region-configuration
[DeviceA-mst-region] quit
```

MSTI1 の Root ブリッジとして Device A を設定します。

```
[DeviceA] stp instance 1 root primary
```

グローバルにスパニングツリーを有効にします。

```
[DeviceA] stp global enable
```

3) Device B を設定します。

MST region view に移行し、MST region 名 **example** を設定します。

```
<DeviceB> system-view
[DeviceB] stp region-configuration
[DeviceB-mst-region] region-name example
```

VLAN 10、VLAN 30、VLAN 40 をそれぞれ MSTI1、MSTI3、MSTI4 に割り当てます。

```
[DeviceB-mst-region] instance 1 vlan 10
[DeviceB-mst-region] instance 3 vlan 30
[DeviceB-mst-region] instance 4 vlan 40
```

MST region レベルを 0 とします。

```
[DeviceB-mst-region] revision-level 0
```

MST region の設定をアクティブにします。

```
[DeviceB-mst-region] active region-configuration
[DeviceB-mst-region] quit
```

MSTI3 の Root ブリッジとして Device B を設定します。

```
[DeviceB] stp instance 3 root primary
```

グローバルにスパニングツリーを有効にします。

```
[DeviceB] stp global enable
```

4) Device C を設定します。

MST region view に移行し、MST region 名 **example** を設定します。

```
<DeviceC> system-view
[DeviceC] stp region-configuration
[DeviceC-mst-region] region-name example
```

VLAN 10、VLAN 30、VLAN 40 をそれぞれ MSTI1、MSTI3、MSTI4 に割り当てます。

```
[DeviceC-mst-region] instance 1 vlan 10
[DeviceC-mst-region] instance 3 vlan 30
[DeviceC-mst-region] instance 4 vlan 40
```

MST region レベルを 0 とします。

```
[DeviceC-mst-region] revision-level 0
```

MST region の設定をアクティブにします。

```
[DeviceC-mst-region] active region-configuration
[DeviceC-mst-region] quit
```

MSTI4 の Root ブリッジとして Device C を設定します。

```
[DeviceC] stp instance 4 root primary
```

グローバルにスパニングツリーを有効にします。

```
[DeviceC] stp global enable
```

5) Device D を設定します。

MST region view に移行し、MST region 名 **example** を設定します。

```
<DeviceD> system-view
[DeviceD] stp region-configuration
[DeviceD-mst-region] region-name example
```

VLAN 10、VLAN 30、VLAN 40 をそれぞれ MSTI1、MSTI3、MSTI4 に割り当てます。

```
[DeviceD-mst-region] instance 1 vlan 10
[DeviceD-mst-region] instance 3 vlan 30
[DeviceD-mst-region] instance 4 vlan 40
```

MST region レベルを 0 とします。

```
[DeviceD-mst-region] revision-level 0
```

MST region の設定をアクティブにします。

```
[DeviceD-mst-region] active region-configuration
[DeviceD-mst-region] quit
```

グローバルにスパニングツリーを有効にします。

```
[DeviceD] stp global enable
```

III. 設定の確認

この例では Device B がもっとも小さい Root ブリッジ ID を持っています。結果として、Device B が MSTI 0 の Root ブリッジとなります。

ネットワークが安定したのち、**display stp brief** コマンドで、各装置で STP の概要情報を表示し、設定の確認を行います。

Device A のスパニングツリーの概要情報を表示します。

```
[DeviceA] display stp brief
 MST ID      Port                        Role  STP State     Protection
 0           GigabitEthernet1/0/1        ALTE  DISCARDING    NONE
 0           GigabitEthernet1/0/2        DESI  FORWARDING    NONE
 0           GigabitEthernet1/0/3        ROOT  FORWARDING    NONE
 1           GigabitEthernet1/0/1        DESI  FORWARDING    NONE
 1           GigabitEthernet1/0/3        DESI  FORWARDING    NONE
 3           GigabitEthernet1/0/2        DESI  FORWARDING    NONE
 3           GigabitEthernet1/0/3        ROOT  FORWARDING    NONE
```

Device B のスパニングツリーの概要情報を表示します。

```
[DeviceB] display stp brief
 MST ID      Port                        Role  STP State     Protection
 0           GigabitEthernet1/0/1        DESI  FORWARDING    NONE
 0           GigabitEthernet1/0/2        DESI  FORWARDING    NONE
 0           GigabitEthernet1/0/3        DESI  FORWARDING    NONE
 1           GigabitEthernet1/0/2        DESI  FORWARDING    NONE
 1           GigabitEthernet1/0/3        ROOT  FORWARDING    NONE
 3           GigabitEthernet1/0/1        DESI  FORWARDING    NONE
 3           GigabitEthernet1/0/3        DESI  FORWARDING    NONE
```

Device C のスパニングツリーの概要情報を表示します。

```
[DeviceC] display stp brief
 MST ID      Port                        Role  STP State     Protection
 0           GigabitEthernet1/0/1        DESI  FORWARDING    NONE
 0           GigabitEthernet1/0/2        ROOT  FORWARDING    NONE
 0           GigabitEthernet1/0/3        DESI  FORWARDING    NONE
 1           GigabitEthernet1/0/1        ROOT  FORWARDING    NONE
 1           GigabitEthernet1/0/2        ALTE  DISCARDING    NONE
 4           GigabitEthernet1/0/3        DESI  FORWARDING    NONE
```

Device D のスパニングツリーの概要情報を表示します。

```
[DeviceD] display stp brief
 MST ID      Port                        Role  STP State     Protection
 0           GigabitEthernet1/0/1        ROOT  FORWARDING    NONE
 0           GigabitEthernet1/0/2        ALTE  DISCARDING    NONE
 0           GigabitEthernet1/0/3        ALTE  DISCARDING    NONE
 3           GigabitEthernet1/0/1        ROOT  FORWARDING    NONE
 3           GigabitEthernet1/0/2        ALTE  DISCARDING    NONE
 4           GigabitEthernet1/0/3        ROOT  FORWARDING    NONE
```

出力情報から、図 8-21のように VLAN の MSTI マッピングの設定を行っていることがわかります。

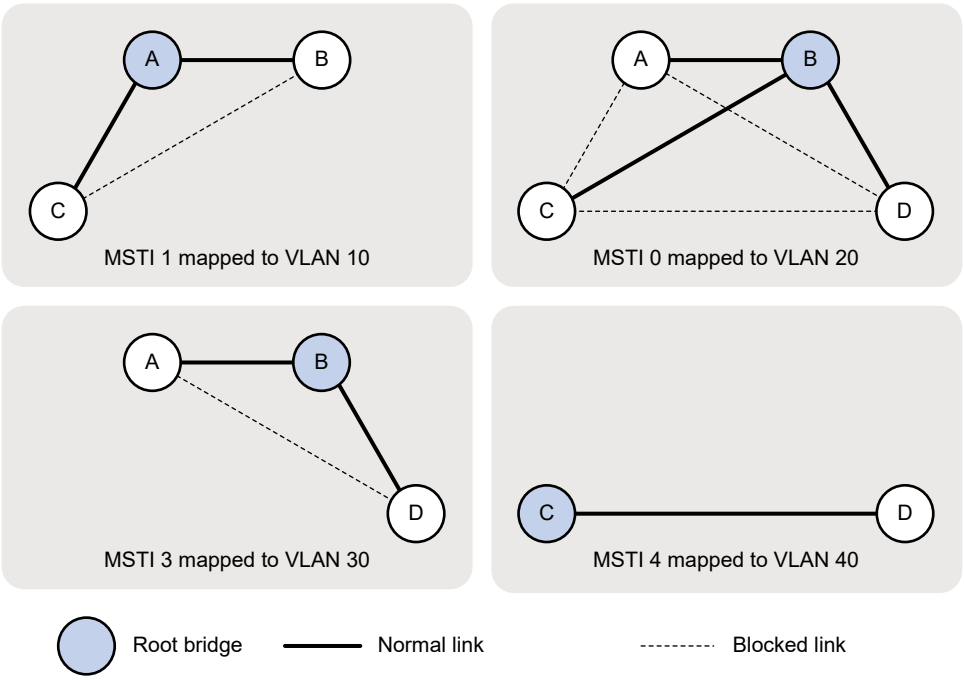


図 8-21 異なる VLAN への MSTI のマッピングの設定

8.32.2 PVST 設定例

I. ネットワーク要件

図 8-22に示すように、Device A、Device B はディストリビューション層にあり、Device C、Device D はアクセス層にあります。

以下の要件を満たすように PVST を設定します。

- VLAN のスパニングツリー間で VLAN パケットを転送します。
- VLAN 10、VLAN 20、VLA N30 はディストリビューション層の装置で終端し、VLAN 40 はアクセス層で終端します。
- VLAN 10、VLAN 20 の Root ブリッジは Device A です。
- VLAN 30 の Root ブリッジは Device B です。
- VLAN 40 の Root ブリッジは Device C です。

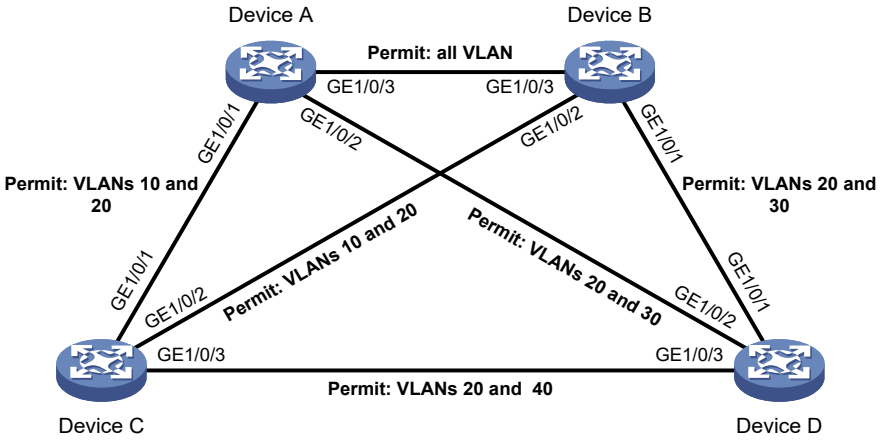


図 8-22 ネットワーク図

II. 設定手順

1)　VLAN、VLAN メンバポートを設定します。（詳細は省略します）
- □　Device A、Device B の両方で VLAN 10、VLAN 20、VLAN 30 を作成します。
- □　Device C で VLAN 10、VLAN 20、VLAN 40 を作成します。
- □　Device D で VLAN 20、VLAN 30、VLAN 40 を作成します。
- □　トランクポートとして Device のポートを設定し、関連する VLAN に割り当てます。

2)　Device A を設定します。

動作モードを PVST に設定します。

```
<DeviceA> system-view
[DeviceA] stp mode pvst
```

VLAN 10、VLAN 20 の Root ブリッジとして Device を設定します。

```
[DeviceA] stp vlan 10 20 root primary
```

グローバル、VLAN 10、VLAN 20、VLAN 30 でスパニングツリーを有効にします。

```
[DeviceA] stp global enable
[DeviceA] stp vlan 10 20 30 enable
```

3)　Device B を設定します。

動作モードを PVST に設定します。

```
<DeviceB> system-view
[DeviceB] stp mode pvst
```

VLAN 30 の Root ブリッジとして Device を設定します。

```
[DeviceB] stp vlan 30 root primary
```

グローバル、VLAN 10、VLAN 20、VLAN 30 でスパニングツリーを有効にします。

```
[DeviceB] stp global enable
[DeviceB] stp vlan 10 20 30 enable
```

4) Device C を設定します。

動作モードを PVST に設定します。

```
<DeviceC> system-view
[DeviceC] stp mode pvst
```

VLAN 40 の Root ブリッジとして Device を設定します。

```
[DeviceC] stp vlan 40 root primary
```

グローバル、VLAN 10、VLAN 20、VLAN 40 でスパニングツリーを有効にします。

```
[DeviceC] stp global enable
[DeviceC] stp vlan 10 20 40 enable
```

5) Device D を設定します。

動作モードを PVST に設定します。

```
<DeviceD> system-view
[DeviceD] stp mode pvst
```

グローバル、VLAN 20、VLAN 30、VLAN 40 でスパニングツリーを有効にします。

```
[DeviceD] stp global enable
[DeviceD] stp vlan 20 30 40 enable
```

III. 設定の確認

ネットワークが安定したのち、**display stp brief** コマンドで、各装置の STP の概要情報を表示し、設定の確認を行います。

Device A のスパニングツリーの概要情報を表示します。

```
[DeviceA] display stp brief
 VLAN ID     Port                      Role  STP State     Protection
 10          GigabitEthernet1/0/1      DESI  FORWARDING    NONE
 10          GigabitEthernet1/0/3      DESI  FORWARDING    NONE
 20          GigabitEthernet1/0/1      DESI  FORWARDING    NONE
 20          GigabitEthernet1/0/2      DESI  FORWARDING    NONE
 20          GigabitEthernet1/0/3      DESI  FORWARDING    NONE
 30          GigabitEthernet1/0/2      DESI  FORWARDING    NONE
 30          GigabitEthernet1/0/3      ROOT  FORWARDING    NONE
```

Device B のスパニングツリーの概要情報を表示します。

```
[DeviceB] display stp brief
 VLAN ID     Port                          Role  STP State     Protection
 10          GigabitEthernet1/0/2          DESI  FORWARDING    NONE
 10          GigabitEthernet1/0/3          ROOT  FORWARDING    NONE
 20          GigabitEthernet1/0/1          DESI  FORWARDING    NONE
 20          GigabitEthernet1/0/2          DESI  FORWARDING    NONE
 20          GigabitEthernet1/0/3          ROOT  FORWARDING    NONE
 30          GigabitEthernet1/0/1          DESI  FORWARDING    NONE
 30          GigabitEthernet1/0/3          DESI  FORWARDING    NONE
```

Device C のスパニングツリーの概要情報を表示します。

```
[DeviceC] display stp brief
 VLAN ID     Port                          Role  STP State     Protection
 10          GigabitEthernet1/0/1          ROOT  FORWARDING    NONE
 10          GigabitEthernet1/0/2          ALTE  DISCARDING    NONE
 20          GigabitEthernet1/0/1          ROOT  FORWARDING    NONE
 20          GigabitEthernet1/0/2          ALTE  DISCARDING    NONE
 20          GigabitEthernet1/0/3          DESI  FORWARDING    NONE
 40          GigabitEthernet1/0/3          DESI  FORWARDING    NONE
```

Device D のスパニングツリーの概要情報を表示します。

```
[DeviceD] display stp brief
 VLAN ID     Port                          Role  STP State     Protection
 20          GigabitEthernet1/0/1          ALTE  DISCARDING    NONE
 20          GigabitEthernet1/0/2          ROOT  FORWARDING    NONE
 20          GigabitEthernet1/0/3          ALTE  DISCARDING    NONE
 30          GigabitEthernet1/0/1          ROOT  FORWARDING    NONE
 30          GigabitEthernet1/0/2          ALTE  DISCARDING    NONE
 40          GigabitEthernet1/0/3          ROOT  FORWARDING    NONE
```

出力情報から、図 8-23のように各 VLAN のスパニングツリーのトポロジの設定を行っていることがわかります。

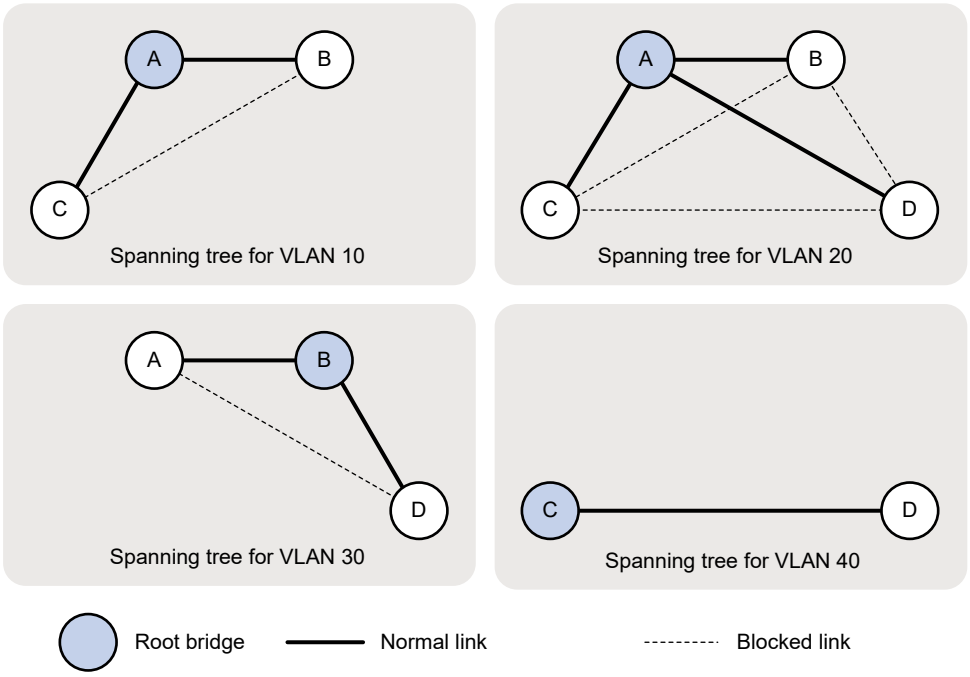


図 8-23 VLAN のスパニングツリーのトポロジ

目次

このセクションのページは**2-x-x** です。

9章 ループ検出 9-1
9.1 概要 9-1
9.1.1 ループ検出メカニズム 9-1
9.1.2 ループ検出間隔 9-2
9.1.3 ループ保護アクション 9-2
9.1.4 ポート状態自動回復 9-3
9.2 ループ検出設定作業リスト 9-3
9.3 ループ検出の有効化 9-3
9.3.1 制限とガイドライン 9-3
9.3.2 グローバルでのループ検出の有効化 9-4
9.3.3 ポートでのループ検出の有効化 9-4
9.4 ループ保護アクションの設定 9-4
9.4.1 グローバルでのループ保護アクションの設定 9-4
9.4.2 Ethernetインタフェースでのループ保護アクションの設定 9-5
9.4.3 アグリゲートインタフェースでのループ保護アクションの設定 9-5
9.5 ループ検出間隔の設定 9-5
9.6 ループ検出の表示と維持 9-5
9.7 ループ検出設定例 9-6
9.7.1 ネットワーク要件 9-6
9.7.2 設定手順 9-6
9.7.3 設定の確認 9-8

9章 ループ検出

9.1 概要

不正なネットワークの接続あるいは設定は、レイヤ 2 のループを発生させます。ループができると送信されたデータがループ内を無限に巡り続け、回線が圧迫されて通信ができなくなり、ネットワーク機器が過負荷になって性能が低下するなどの、ネットワーク障害を引き起こす原因となります。

ループ検出機能は、ループが発生した場合、ネットワークの接続と設定に対応するように通知させるため、すぐさまログを作成します。ループ検出はネットワークの接続と設定をシャットダウンすることができます。ログは Information center で維持されます。詳細はオペレーションマニュアルのセクション 9 *システム管理* "*Information Center*"を参照してください。

9.1.1 ループ検出メカニズム

装置は検出フレームを送信し、装置のポートからフレームが戻るかどうかを確認することでループを検出します。検出した場合、装置はループされたリンクに接続されていると認識します。

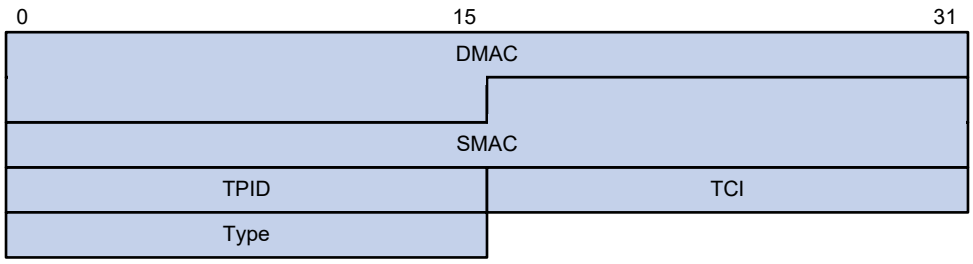


図 9-1 ループ検出のイーサネットフレームヘッダ

ループ検出のイーサネットフレームヘッダは以下のフィールドがあります。

- **DMAC** – フレームの宛先 MAC アドレスです。MAC アドレスは、マルチキャスト MAC アドレス 010F-E200-0007 です。ループ検出機能が有効で、この宛先 MAC アドレスのフレームを受信した場合、以下の処理を行います。
  - □ CPU にフレームを送信します。
  - □ フレームを最初に受信した VLAN にフラッドします。
- **SMAC** – フレームの送信元 MAC アドレスで、送信している装置の MAC アドレスです。
- **TPID** – VLAN タグのタイプで、0x8100 です。
- **TCI** – VLAN タグの情報で優先度と VLAN ID が含まれます。
- **Type** – プロトコルタイプで、0x8918 です。

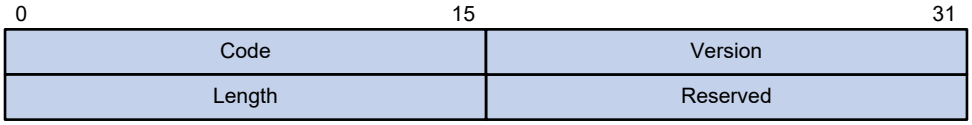


図 9-2 ループ検出の内部フレームヘッダ

ループ検出の内部フレームヘッダは以下のフィールドがあります。

- **Code** – プロトコルサブタイプで、0x0001 です。ループ検出プロトコルを含みます。
- **Version** – プロトコルバージョンで、0x0000 です。
- **Length** – フレーム長です。値は内部ヘッダを含みますが、イーサネットヘッダは含みません。
- **Reserved** – 予約されたフィールドです。

ループ検出のフレームは TLV（タイプ、長さ、値）としてカプセル化されます。

表 9-1 ループ検出でサポートされる TLV

TLV	説明	補足
End of PDU	PDUの最後	オプション
Device ID	送信装置のBridge MACアドレス	必須
Port ID	ポートを送信するPDUのID	オプション
Port Name	ポートを送信するPDU名	オプション
System Name	装置名	オプション
Chassis ID	ポートを送信するシャーシID	オプション
Slot ID	ポートを送信するスロットID	オプション
Sub Slot ID	ポートを送信するサブスロットID	オプション

9.1.2 ループ検出間隔

ループ検出は、ネットワークの変化に対して連続して対応します。ループ検出フレームは、指定された間隔（ループ検出間隔と呼ばれます）で、ポートにループが発生したかどうか、ループが取り除かれたかどうかを確認するために送信されます。

9.1.3 ループ保護アクション

装置がポートを検出した場合、ログを作成しますが、デフォルト設定ではアクションは実行しません。以下のアクションのうちの 1 つを実行するように設定することができます。

- **Block** – ポートが MAC アドレスを学習することを無効にし、ポートに受信されるトラフィックをブロックします。
- **No-learning** – ポートが MAC アドレスを学習することを無効にします。
- **Shutdown** – すべてのフレームの送受信を無効にするため、ポートをシャットダウンします。

9.1.4 ポート状態自動回復

block、**no-learning** ポートを設定した装置がポートでループを検出すると、アクションを開始しループ検出間隔の 3 倍の時間待ちます。ポートでループを検出してからループ検出間隔の 3 倍の期間内にループ検出フレームを受信しない場合、以下の動作をします。

- 装置は自動的にポートを転送状態に設定します。
- ユーザにイベントを通知します。

loopback-detection action shutdown コマンドが使用されたとき、装置は以下の動作をします。

1) 装置は自動的にポートをシャットダウンします。
2) **shutdown-interval** コマンドで設定された検出タイマが満了したのち、装置は自動的にポートを転送状態に設定します。
3) 検出タイマが満了時にループが検出されると、装置は再びポートをシャットダウンします。

この処理はループが削除されるまで繰り返されます。

🕮 **メモ：**

ループ検出フレームが負荷抑制機能などで削除されることによって、ループが継続していても誤って回復する場合があります。この現象を避けるためには、**shutdown** アクションを使用するか、手動でループを取り除いてください。

9.2 ループ検出設定作業リスト

作業リスト
（必須設定項目）ループ検出の有効化
（オプション設定項目）ループ保護アクションの設定
（オプション設定項目）ループ検出間隔の設定

9.3 ループ検出の有効化

9.3.1 制限とガイドライン

ループ検出を有効にするときは、次の制限事項とガイドラインに従ってください。

- ループ検出はグローバルあるいはポート単位で有効にすることができます。指定のポートのみループ検出を有効化する場合は、グローバルの設定を無効に設定してください。
- ループ検出はポートで有効化されている VLAN の検出フレームを受信すると、受信したポートのループ検出が有効かどうかに関係なく、そのポートで指定したループ保護アクションが動作します。
- リンクアグリゲーションポート単位にループ検出を有効化する場合は、リンクアグリゲーショングループの論理ポート（aggregate interface view）にループ検出の設定をする必要があります。メンバポートに設定しても動作しません。

9.3.2 グローバルでのループ検出の有効化

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. グローバルでループ検出を有効にする	**loopback-detection global enable vlan** { *vlan-id-list* | **all** }	デフォルト：有効 すべてのVLANで有効です。

9.3.3 ポートでのループ検出の有効化

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. Ethernet interface view あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	ー
3. ポートでループ検出を有効にする	**loopback-detection enable vlan** { *vlan-id-list* | **all** }	デフォルト：無効

9.4 ループ保護アクションの設定

ループ保護アクションはグローバルあるいは指定されたポートで有効にすることができます。グローバルアクションは、指定された VLAN のすべてのポートに適用されます。ポート毎のアクションは、グローバルアクションよりも優先されます。

🕮 **メモ：**

- **shutdown** アクションを設定し、ポートでループが検出された場合、ポートをシャットダウンする際、ループ状態を解除するため、RECOVERED のログも出力します。
- **shutdown** アクションによるポートのシャットダウンが行われると、**display interface** コマンドの Current state フィールドが DOWN（Loopback detection down）と表示されます。

9.4.1 グローバルでのループ保護アクションの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. グローバルでループ保護アクションを設定する	**loopback-detection global action shutdown**	デフォルト：ループを検出してもアクションは実行しませんがログを出力します。

9.4.2 Ethernet インタフェースでのループ保護アクションの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. Ethernet interface view に移行する	**interface** *interface-type interface-number*	ー
3. インタフェースでループ保護アクションを設定する	**loopback-detection action** { **block** | **no-learning** | **shutdown** }	デフォルト : ループを検出してもアクションは実行しませんがログを出力します。

9.4.3 アグリゲートインタフェースでのループ保護アクションの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. aggregate interface view に移行する	**interface bridge-aggregation** *interface-number*	ー
3. アグリゲートインタフェースでループ保護アクションを設定する.	**loopback-detection action shutdown**	デフォルト : ループを検出してもアクションは実行しませんがログを出力します。

9.5 ループ検出間隔の設定

ループ検出が有効である場合、装置は、指定された間隔でループ検出フレームを送信します。短い間隔では検出感度が上がりますが、より多くのリソースが消費されます。ループ検出間隔の設定を行う場合には、システムのパフォーマンスとループ検出速度を考慮してください。

以下にループ検出間隔の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. ループ検出間隔を設定する	**loopback-detection interval-time** *interval*	デフォルト：5秒

9.6 ループ検出の表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
ループ検出の設定と状態を表示する	**display loopback-detection**

9.7 ループ検出設定例

> 🕮 メモ：
> STP 機能によってブロッキング状態のポートでは、ループ検出パケットの送受信はできません。

9.7.1 ネットワーク要件

図 9-3に示すように、ループを検出したとき、Device A がログを作成し、自動的にポートのシャットダウンを行うようにループ検出の設定を行います。

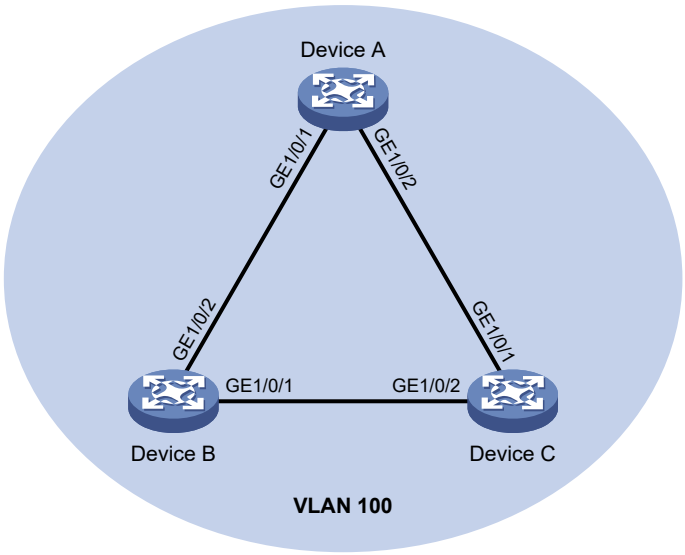


図 9-3 ネットワーク図

9.7.2 設定手順

1)　Device A を設定します。

VLAN 100 を作成し、グローバルにループ検出を設定します。

```
<DeviceA> system-view
[DeviceA] vlan 100
[DeviceA-vlan100] quit
[DeviceA] loopback-detection global enable vlan 100
```

GigabitEthernet 1/0/1、GigabitEthernet 1/0/2 をトランクポートとして設定し、VLAN 100 を割り当てます。

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-type trunk
[DeviceA-GigabitEthernet1/0/1] port trunk permit vlan 100
[DeviceA-GigabitEthernet1/0/1] quit
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port link-type trunk
[DeviceA-GigabitEthernet1/0/2] port trunk permit vlan 100
[DeviceA-GigabitEthernet1/0/2] quit
```

シャットダウンを行うループ保護アクションをグローバルで設定します。

```
[DeviceA] loopback-detection global action shutdown
```

ループ検出間隔を 35 秒に設定します。

```
[DeviceA] loopback-detection interval-time 35
```

2)　Device B を設定します。

VLAN 100 を作成します。

```
<DeviceB> system-view
[DeviceB] vlan 100
[DeviceB–vlan100] quit
```

GigabitEthernet 1/0/1、GigabitEthernet 1/0/2 をトランクポートとして設定し、VLAN 100 を割り当てます。

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port link-type trunk
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 100
[DeviceB-GigabitEthernet1/0/1] quit
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] port link-type trunk
[DeviceB-GigabitEthernet1/0/2] port trunk permit vlan 100
[DeviceB-GigabitEthernet1/0/2] quit
```

3)　Device C を設定します。

VLAN 100 を作成します。

```
<DeviceC> system-view
[DeviceC] vlan 100
[DeviceC–vlan100] quit
```

GigabitEthernet 1/0/1、GigabitEthernet 1/0/2 をトランクポートとして設定し、VLAN 100 を割り当てます。

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] port link-type trunk
[DeviceC-GigabitEthernet1/0/1] port trunk permit vlan 100
[DeviceC-GigabitEthernet1/0/1] quit
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] port link-type trunk
[DeviceC-GigabitEthernet1/0/2] port trunk permit vlan 100
[DeviceC-GigabitEthernet1/0/2] quit
```

9.7.3 設定の確認

Device A のログを確認します。

```
[DeviceA]
%Feb 24 15:04:29:663 2013 DeviceA LPDT/4/LPDT_LOOPED:  A loop was detected on
GigabitEthernet1/0/1.
%Feb 24 15:04:29:664 2013 DeviceA LPDT/4/LPDT_VLAN_LOOPED: A loop was detected
on GigabitEthernet1/0/1 in VLAN 100.
%Feb 24 15:04:29:667 2013 DeviceA LPDT/4/LPDT_LOOPED: A loop was detected on
GigabitEthernet1/0/2.
%Feb 24 15:04:29:668 2013 DeviceA LPDT/4/LPDT_VLAN_LOOPED: A loop was detected
on GigabitEthernet1/0/2 in VLAN 100.
%Feb 24 15:04:44:243 2013 DeviceA LPDT/5/LPDT_VLAN_RECOVERED: A loop was removed
on GigabitEthernet1/0/1 in VLAN 100.
%Feb 24 15:04:44:243 2013 DeviceA LPDT/5/LPDT_RECOVERED: All loops were removed
on GigabitEthernet1/0/1.
%Feb 24 15:04:44:248 2013 DeviceA LPDT/5/LPDT_VLAN_RECOVERED: A loop was removed
on GigabitEthernet1/0/2 in VLAN 100.
%Feb 24 15:04:44:248 2013 DeviceA LPDT/5/LPDT_RECOVERED: All loops were removed
on GigabitEthernet1/0/2.
```

出力内容は、以下のことを示します。

- Device A はループ検出間隔内に GigabitEthernet 1/0/1、GigabitEthernet 1/0/2 のポートでループを検出しました。
- Device A は自動的に GigabitEthernet 1/0/1、GigabitEthernet 1/0/2 をシャットダウンしました。

display loopback-detection コマンドを使用して Device A のループ検出の設定と情報を表示します。

```
[DeviceA] display loopback-detection
Loop detection is enabled.
Loop detection interval is 35 second(s).
Loop is detected on following interfaces:
 Interface                     Action mode     VLANs
 GigabitEthernet1/0/1          Shutdown        100
 GigabitEthernet1/0/2          Shutdown        100
```

出力は shutdown アクションに従って、GigabitEthernet 1/0/1、GigabitEthernet 1/0/2 ポートがループから開放されたことを示しています。

Device A の GigabitEthernet 1/0/1 の状態を表示します。

```
[DeviceA] display interface gigabitethernet 1/0/1
GigabitEthernet1/0/1 current state: DOWN (Loop detection down)
...
```

出力は、GigabitEthernet 1/0/1 がループ検出アクションによってシャットダウンしていることを示しています。

Device A の GigabitEthernet 1/0/2 の状態を表示します。

```
[DeviceA] display interface gigabitethernet 1/0/2
GigabitEthernet1/0/2 current state: DOWN (Loop detection down)
...
```

出力は、GigabitEthernet 1/0/2 がループ検出アクションによってシャットダウンしていることを示しています。

目次

このセクションのページは**2-x-x** です。

10 章 VLAN 10-1
10.1 概要 10-1
10.1.1 VLAN フレームのカプセル化 10-1
10.1.2 プロトコルと標準 10-2
10.2 VLAN の設定 10-2
10.2.1 制限とガイドライン 10-2
10.3 VLAN インタフェースの設定 10-3
10.3.1 制限とガイドライン 10-3
10.3.2 VLAN インタフェースの基本設定 10-3
10.4 ポートベース VLAN の設定 10-4
10.4.1 概要 10-4
10.4.2 アクセスポート VLAN の設定 10-5
10.4.3 トランクポート VLAN の設定 10-6
10.4.4 ハイブリッドポート VLAN の設定 10-7
10.5 MAC ベース VLAN 10-7
10.5.1 概要 10-7
10.5.2 設定の一般的な制限とガイドライン 10-10
10.5.3 スタティック MAC ベース VLAN の設定 10-10
10.5.4 ダイナミック MAC ベース VLAN の設定 10-11
10.5.5 サーバ割り当て MAC ベース VLAN 10-12
10.5.6 VLAN の表示と維持 10-12
10.6 VLAN 設定例 10-13
10.6.1 ポートベース VLAN の設定例 10-13
10.6.2 MAC ベース VLAN 設定例 10-15

10章 VLAN

10.1 概要

VLAN（Virtual Local Area Network）テクノロジは、物理 LAN を複数の論理 LAN に分割することで、スイッチ内を仮想的なグループに分けます。次の利点があります。

- **セキュリティ**－同じ VLAN 内のホストはレイヤ 2 で相互に通信できますが、レイヤ 2 の他の VLAN のホストから隔離され、直接通信できる範囲を限定します。
- **ブロードキャストトラフィックの分離**－グループの範囲内でのみ直接通信するため、ブロードキャストフレームによる回線の混雑を緩和します。
- **柔軟性**－VLAN は、ワークグループごとに論理的に分割できます。同じワークグループ内のホストは、物理的な場所に関係なく、ネットワーク構成を決めることができます。

図 10-1 のように VLAN を使用して、LAN を小さく分割することで、ブロードキャストドメインの影響を少なくすることができます。

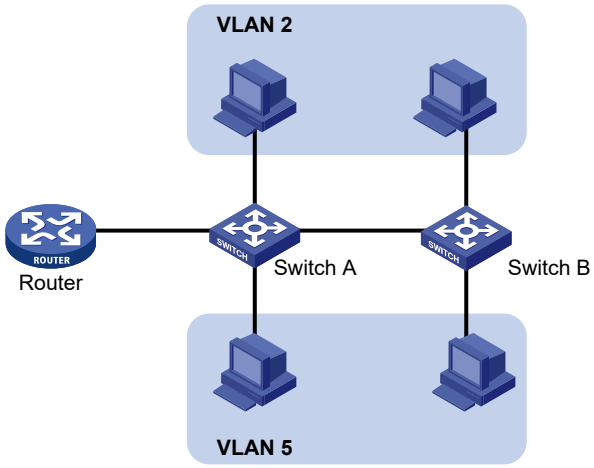


図 10-1 VLAN ネットワーク図

VLAN は物理的な要素からは制限を受けません。たとえば、特定のワークグループによって使用されるすべてのワークステーションとサーバは物理的な位置に関係なく、同じ LAN に接続することができます。異なる VLAN 間と通信するためにはルータやレイヤ 3 スイッチが必要となります。

10.1.1 VLAN フレームのカプセル化

異なる VLAN からイーサネットフレームを認識するため、図 10-2 に示すように宛先/送信元 MAC アドレス（DA&SA）フィールドと上位プロトコルタイプフィールドの間に 4byte の VLAN タグを追加しました。フレームに追加されたタグの既述は、「IEEE802.1Q」で標準化されています。

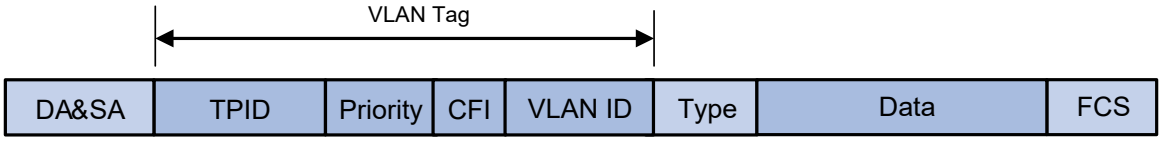


図 10-2 VLAN タグの位置とフォーマット

VLAN タグは以下のフィールドが含まれます。

- **TPID**–フレームに VLAN タグが付いているかどうかを識別するためのプロトコル識別子です。このフィールドは 16 ビット長です。デフォルトで TPID は 0x8100 で VLAN タグが付いています。
- **Priority**–フレームの 802.1p 優先度を示します。このフィールドは 3 ビット長です。詳細はオペレーションマニュアルのセクション 6 *ACL and QoS "プライオリティマッピング"*を参照してください。
- **CFI**–標準フォーマットを示すフィールドです。このフィールドは 1 ビット長です。パケットが異なるメディアを跨いで転送される場合、MAC アドレスは標準フォーマットでカプセル化されます。以下の値が設定できます。
  - **0（デフォルト）**–MAC アドレスは標準フォーマットでカプセル化されます。
  - **1**–MAC アドレスは非標準フォーマットでカプセル化されます。
- **VLAN ID**–フレームが所属する VLAN を示します。このフィールドは 12 ビット長です。VLAN-ID の範囲は 0～4095 です。0 と 4095 はプロトコルによって予約されているので、実際に使える値は 1～4094 となります。

フレームを受信した場合、ネットワーク装置はフレームに VLAN タグが付いているか、そして VLAN タグの値を確認して処理を決定します。詳細はオペレーションマニュアルのセクション 2 *アクセス "VLAN"の"ポートベース VLAN の設定"*を参照してください。

イーサネットは Ethernet II、802.3/802.2 LLC、802.3/802.2 SNAP、802.3 raw などのカプセル化フォーマットをサポートしています。ここでは Ethernet II カプセル化フォーマットを使用しています。VLAN タグフィールドは VLAN を識別するために、これらのカプセル化フォーマットにも付与されます。詳細は関連するプロトコルと標準を参照してください。

複数のタグ付きフレームのために、装置はもっとも外側の VLAN タグに従って処理し、ペイロードとしてその内部の VLAN タグを送信します。

10.1.2 プロトコルと標準

IEEE 802.1Q, *IEEE Standard for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks*

10.2 VLANの設定

10.2.1 制限とガイドライン

VLAN を設定する場合、以下の制限とガイドラインに従ってください。

- デフォルト VLAN である VLAN1 は作成または削除できません。
- ダイナミック VLAN、あるいはアプリケーションによってロックされている VLAN は **undo vlan** コマンドで削除することはできません。最初に各設定から VLAN の設定を削除してください。

以下に VLAN の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． （オプション設定項目）VLAN を作成し、view へ移行あるいは VLAN リストを作成する	**vlan** { *vlan-id1* [**to** *vlan-id2*] | **all** }	デフォルト： デフォルト VLAN（VLAN1）のみ
3． VLAN view に移行する	**vlan** *vlan-id*	VLANリストを作成した後、指定したVLANを設定するには、この操作を実行してください。
4． VLAN の名前を設定する	**name** *text*	デフォルト：**VLAN** *vlan-id* たとえばVLAN 100のVLAN名は**VLAN 0100**です。
5． VLAN の説明を設定する	**description** *text*	デフォルト：**VLAN** *vlan-id* *vlan-id*はVLANのIDです。 たとえばVLAN 100の説明は**VLAN 0100**です。

10.3 VLANインタフェースの設定

VLAN の異なるホスト間で通信を行うには、ルータまたはレイヤ 3 スイッチでレイヤ 3 転送を行う必要があります。VLAN インタフェースはこれを実現するために使用される仮想インタフェースです。装置上の VLAN インタフェースは物理的には存在しませんが、各 VLAN は 1 つの VLAN インタフェースを作成することができます。VLAN インタフェースには IP アドレスを割り当てることができ、そしてそれをゲートウェイとすることで、異なる IP ネットワークセグメントへのトラフィックを転送することが可能となります。

10.3.1 制限とガイドライン

VLAN インタフェースを設定する場合、以下の制限とガイドラインに従ってください。

以下に記載するセカンダリ VLAN には VLAN インタフェースを作成できません。

- 同じプライマリ VLAN に関連付けられている。
- プライマリ VLAN インタフェースの VLAN interface view でレイヤ 3 通信が有効になっている。

セカンダリ VLAN の詳細は、オペレーションマニュアルのセクション 2 *アクセス”Private VLAN*”を参照してください。

10.3.2 VLAN インタフェースの基本設定

VLAN インタフェースを作成する前に、対応する VLAN が作成されている必要があります。

以下に VLAN インタフェースの基本設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． VLAN インタフェースを作成し、VLAN interface view に移行する	**interface vlan-interface** *vlan-interface-id*	デフォルト：設定なし VLANが存在する場合、直接そのviewに移行します。

操作	コマンド	補足
3． VLAN インタフェースに IP アドレスを割り当てる	**ip address** *ip-address* { *mask* | *mask-length* } [**sub**]	デフォルト：設定なし
4． VLAN インタフェースの説明を設定する	**description** *text*	デフォルト : VLANインタフェース名 たとえば**Vlan-interface1 Interface**です。
5． （オプション設定項目）VLAN インタフェースをアップ状態にする	**undo shutdown**	デフォルト : 手動でシャットダウン状態になっていません。 ● VLANのすべてのポートがdownしている場合、VLANインタフェースもdownになります。 ● 1つ以上のVLANがupである場合、VLANインタフェースはupになります。

10.4 ポートベースVLANの設定

10.4.1 概要

ポートベース VLAN はポートに VLAN を割り当て、その VLAN のトラフィックだけを転送します。

I. ポートリンクタイプ

ポートリンクタイプはアクセス、トランク、ハイブリッドに設定することができます。3 つのリンクタイプは、異なる VLAN タグの処理方法を使用します。

- **アクセス**－アクセスポートは 1 つの VLAN にのみ所属することができます。タグが付与されずにパケットを送信します。通常、PC が直接接続されるポートはアクセスポートに設定します。アクセスポートは、以下の場合に使用されます。
  - □ VLAN パケットをサポートしない端末に接続します。
  - □ VLAN を区別できない装置に接続します。
- **トランク**－トランクポートは複数の VLAN に所属することができ、複数の VLAN のトラフィックを送受信可能です。デフォルト VLAN（PVID）以外のトラフィックがトランクポートを通過する場合、そのトラフィックには VLAN タグが付与されます。トランクポートは通常、同じ VLAN を持つネットワーク装置と接続するのに使用されます。
- **ハイブリッド**－ハイブリッドポートは複数の VLAN からパケットを転送することができます。ハイブリッドポートに転送されたパケットのタグの状態はポートの設定に依存します。

II. PVID

PVID は、ポートのデフォルト VLAN です。ポートで受信されたタグなしパケットは PVID のポートから受信されたパケットとして認識されます。

ポートに PVID を設定する際は、以下の制限とガイドラインに従ってください。

- アクセスポートは 1 つの VLAN にのみ属しているため、その VLAN 以外へ PVID を変更することはできません。
- トランクまたはハイブリッドポートは複数の VLAN と PVID 設定をサポートします。
- アクセスポートで **undo vlan** コマンドで PVID を削除すると、ポートのタイプによって以下のいずれかの動作をします。
  - □ アクセスポートでは、PVID は VLAN1 になります。
  - □ トランクまたはハイブリッドポートでは、PVID の設定に影響はありません。

  トランクまたはハイブリッドポートでは存在しない VLAN を PVID として設定することができますが、アクセスポートではできません。
- ローカルとリモートで同じ PVID を設定することを推奨します。
- ポートで PVID からのパケットとタグなしパケットを廃棄しないように、ポートを PVID に割り当ててください。

III. 異なるリンクタイプの処理方法

アクション	アクセス	トランク	ハイブリッド
VLANタグなしフレームの入力フレーム処理	PVIDのタグを各フレームに付与します。	• PVIDがポートで許可されている場合、PVIDのタグを各フレームに付与します。 • PVIDがポートで許可されていない場合、フレームを廃棄します。	
VLANタグ付きフレームの入力フレーム処理	• PVIDのタグが付いたフレームのみ受信します。 • PVID以外のタグ付きフレームは破棄します。	• VLANがポートで許可されている場合、フレームを受信します。 • VLANがポートで許可されていない場合、フレームを廃棄します。	
出力フレーム処理	VLANのタグを外して送信します。	• PVIDのタグが付いたフレームはタグを外して送信します。 • PVID以外の許可されているVLANの場合、タグを付けたまま送信します。	PVIDを含めた**port hybrid vlan**コマンドの設定に従います。タグを付けたまま送信するか、タグを外して送信します。

VLAN ネットワークでは、タグなしパケットが処理される順番は以下の通りです。

- MAC ベース VLAN
- ポートベース VLAN

10.4.2 アクセスポート VLAN の設定

VLAN view あるいは interface view でアクセスポートを VLAN に割り当てることができますが、その前に対応する VLAN が作成されている必要があります。

I. VLAN view でのアクセス VLAN の設定方法

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

操作	コマンド	補足
2． VLAN view 移行する	**vlan** *vlan-id*	―
3． アクセスポートを VLAN に割り当てる	**port** *interface-list*	デフォルト：VLAN 1

II. interface view でのアクセス VLAN の設定方法

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． interface view に移行する	● Ethernet interface viewに移行する： **interface** *interface-type interface-number* ● aggregate interface viewに移行する： **interface bridge-aggregation** *interface-number*	―
3． リンクタイプをアクセスに設定する	**port link-type access**	デフォルト：アクセス
4． （オプション設定項目）アクセスポートを VLAN に割り当てる	**port access vlan** *vlan-id*	デフォルト：VLAN1に属します。

10.4.3 トランクポート VLAN の設定

トランクポートは複数の VLAN に所属すことができます。トランクポート VLAN の設定は、interface view で VLAN に割り当てることができます。

VLAN にトランクポートを割り当てる場合、以下の制限とガイドラインに従ってください。

- ポートリンクタイプをトランクからハイブリッド（またはその逆）に直接変更することはできません。最初にリンクタイプをアクセスにしてから目的のタイプへ変更してください。
- PVID からのパケットを転送するために、**port trunk permit vlan** コマンドでトランクポートを PVID に割り当てる必要があります。

以下にトランクポートを VLAN に割り当てる設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． interface view に移行する	● interface viewに移行する： **interface** *interface-type interface-number* ● aggregate interface viewに移行する： **interface bridge-aggregation** *interface-number*	―
3． リンクタイプをトランクに設定する	**port link-type trunk**	デフォルト：アクセス
4． トランクポートで許可する VLAN を設定する	**port trunk permit vlan** { *vlan-id-list* | **all** }	デフォルト：vlan1のみ許可

操作	コマンド	補足
5.　（オプション設定項目）トランクポートの PVID を設定する	**port trunk pvid vlan** *vlan-id*	デフォルト： VLAN 1

10.4.4 ハイブリッドポート VLAN の設定

ハイブリッドポートは複数の VLAN に所属することができます。ハイブリッドポート VLAN の設定は interface view で VLAN に割り当てることができますが、その前に対応する VLAN が作成されている必要があります。

VLAN にハイブリッドポートを割り当てる場合、以下のガイドラインに従ってください。

- ポートリンクタイプをトランクからハイブリッド（またはその逆）に直接変更することはできません。最初にリンクタイプをアクセスにしてから目的のタイプへ変更してください。
- PVID からのパケットを転送するために、**port hybrid vlan** コマンドでハイブリッドポートを PVID に割り当てる必要があります。

以下にハイブリッドポートを VLAN に割り当てる設定を示します。

操作	コマンド	補足
1.　system view に移行する	**system-view**	ー
2.　interface view に移行する	• interface viewに移行する：**interface** *interface-type interface-number* • aggregate interface viewに移行する：**interface bridge-aggregation** *interface-number*	ー
3.　リンクタイプをハイブリッドに設定する	**port link-type hybrid**	デフォルト：アクセス
4.　ハイブリッドポートで許可する VLAN を設定する	**port hybrid vlan** *vlan-id-list* { **tagged** | **untagged** }	デフォルト：リンクタイプがアクセスである場合、ハイブリッドポートのPVIDはポートが所属しているVLANのIDです。
5.　（オプション設定項目）ハイブリッドポートの PVID を設定する	**port hybrid pvid vlan** *vlan-id*	デフォルト：リンクタイプがアクセスである場合、ハイブリッドポートはポートが所属しているVLANのタグなしメンバです。

10.5 MACベースVLAN

10.5.1 概要

この機能はハイブリッドポートでのみ有効です。

MAC ベース VLAN はフレームの送信元 MAC アドレスに基づいて割り当てられます。この機能は VLAN の設定がユーザの位置情報にかかわらず同一であるため、ユーザベース VLAN とも呼ばれます。

I. スタティック MAC ベース VLAN の割り当て

VLANユーザが少ないネットワークでは、スタティック MAC ベース VLAN を使用します。ポートでスタティック MAC ベース VLAN を設定するため、以下の作業を行う必要があります。

1) MAC-VLAN エントリを作成します。
2) ポートで MAC ベース VLAN を有効にします。
3) MAC ベース VLAN にポートを割り当てます。

スタティック MAC ベース VLAN の割り当てが完了したのち、ポートは受信したフレームを以下のように処理します。

- タグなしフレームの場合、ポートは以下の作業で VLAN ID を決定します。

a) 最初にポートは完全一致を実行します。マスクをすべてFに設定し、MAC-VLANエントリを検索します。フレームの送信元MACアドレスがMAC-VLANエントリのMACアドレスと完全に一致する場合、ポートはエントリに特定なVLAN IDのタグをフレームに付与します。

b) フレームの送信元MACアドレスがMAC-VLANエントリのMACアドレスと完全に一致しない場合、ポートはあいまい一致を実行します。
   - □ ALL-F ではないマスクで MAC-VLAN マッピングリストを検索します。
   - □ 検索キーワードと各マスクの上の論理積演算を実行します。論理積演算の結果がMACアドレスと完全に一致している場合、装置は検索を終了して、対応するVLANタグをパケットに追加します。

c) VLAN IDが一致しない場合、ポートはポートベースVLANを使用してパケットのVLANを決定します。

   一致している場合、ポートは対応する VLAN タグをフレームに付与します。

- タグ付けフレームを受信した場合、フレームの VLAN ID がポートで許可されているか確認します。
  - □ 許可されている場合、ポートはフレームを転送します。
  - □ 許可されていない場合、ポートはフレームを廃棄します。

II. ダイナミック MAC ベース VLAN の割り当て

対象のポートの MAC ベース VLAN を決定することができない場合、ダイナミック MAC ベース VLAN を割り当てることができます。ダイナミック MAC ベース VLAN の割り当てを行う場合、以下の作業を行う必要があります。

1) MAC-VLAN エントリを作成します。
2) ポートで MAC ベース VLAN を有効にします。
3) ポートでダイナミック MAC ベース VLAN を有効にします。

図 10-3 に示すように、ダイナミック MAC ベース VLAN の割り当てを以下のように処理します。

1) ポートでフレームを受信した場合、ポートはフレームがタグ付けされているか確認します。
   - □ タグ付けされている場合、ポートはフレームの送信元 MAC アドレスを取得します。
   - □ タグ付けされていない場合、ポートは以下の順番でフレームの VLAN を選択します。
     - □ MAC ベース VLAN（あいまい一致、完全一致）
     - □ ポートベース VLAN

選択した VLAN をフレームにタグ付けしたのち、ポートはフレームの送信元 MAC アドレスを取得します。

2) ポートは MAC-VLAN エントリに一致するフレームの送信元アドレスと VLAN ID を確認します。
   - □ フレームの送信元 MAC アドレスが MAC-VLAN エントリの MAC アドレスに一致している場合、ポートはフレームの VLAN ID がエントリの VLAN に一致するか確認します。
     - □ 2 つの VLAN ID が一致している場合、ポートは VLAN に加入し、フレームを転送します。
     - □ 2 つの VLAN ID が一致していない場合、ポートはフレームを廃棄します。
   - □ フレームの送信元 MAC アドレスが MAC-VLAN エントリの MAC アドレスに一致していない場合、ポートはフレームの VLAN ID が PVID かどうか確認します。
     - □ フレームの VLAN ID がポートの PVID である場合、ポートは PVID を許可するか確認します。ポートは PVID でフレームを転送します。PVID が許可されていない場合、ポートはフレームを廃棄します。
     - □ フレームの VLAN ID がポートの PVID でない場合、ポートはフレームの VLAN ID が、IP サブネット、プロトコルなどの他の基準に一致するか確認します。VLAN が有効でない場合、ポートはフレームを廃棄します。

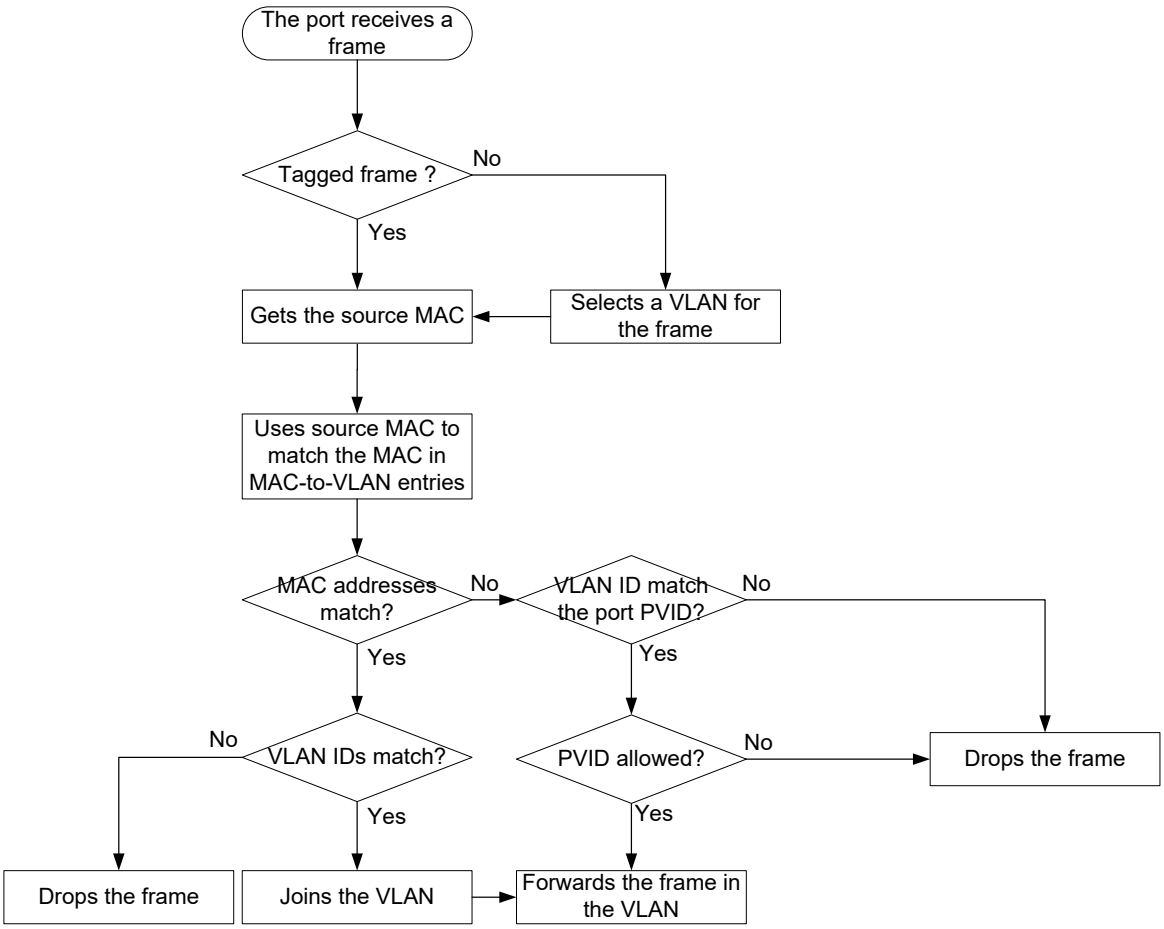


図 10-3 ダイナミック MAC ベース VLAN 割り当てでのフレーム処理のフローチャート

ダイナミック MAC ベース VLAN 割り当てを設定する場合、以下のガイドラインに従ってください。

- MAC-VLAN エントリで指定された VLAN に加入する場合、ポートの設定に依存して以下のいずれかの動作をします。
  - □ ポートが VLAN からのパケットを通過するように設定していない場合、ポートはタグなしメンバとして MAC-VLAN エントリの VLAN に加入します。
  - □ ポートが VLAN からのパケットを通過するように設定している場合、ポートの設定は変更されません。
- ポートでスタティック MAC ベース VLAN とダイナミック MAC ベース VLAN の両方が設定された場合、ダイナミック MAC ベース VLAN が適用されます。
- パケットが MAC-VLAN エントリに一致する場合、装置は MAC-VLAN エントリの VLAN の 802.1p 優先度に従い、パケットを転送します。

III. サーバ割り当て MAC ベース VLAN

端末が安全で柔軟にアクセスできるように MAC ベース 802.1X 認証のようなアクセス認証を使用して、サーバによる MAC ベース VLAN を使用します。

1) アクセス装置にアクセスするため、装置でサーバに割り当てられる MAC ベース VLAN を設定します。
2) アクセス認証サーバでユーザ名から VLAN エントリを設定します。

ユーザがアクセス認証サーバの認証にパスした場合、サーバは装置にユーザの VLAN ID を送信します。装置は以下の作業を行います。

1) ユーザパケットの送信元 MAC アドレスと受信した VLAN ID を使用して MAC-VLAN エントリを作成します。VLAN は MAC ベース VLAN です。

   作成された MAC－VLAN エントリは既存のスタティック MAC-VLAN エントリと競合することができません。競合する場合、ダイナミック MAC-VLAN エントリは生成されません。

2) MAC ベース VLAN にユーザに接続するポートを割り当てます。

ユーザがオフラインの場合、装置は自動的に MAC-VLAN エントリを削除し、MAC ベース VLAN からポートを削除します。802.1X、MAC アドレス認証の詳細は、オペレーションマニュアルのセクション 7 *セキュリティ*“*802.1X*”、“*MAC アドレス認証*”を参照してください。

10.5.2 設定の一般的な制限とガイドライン

MAC ベース VLAN を設定する場合、以下の制限とガイドラインに従ってください。

- MAC ベース VLAN 機能は主にユーザアクセス装置の下流ポートで設定されます。リンクアグリゲーションで、MAC ベース VLAN 機能を有効にしないでください。

10.5.3 スタティック MAC ベース VLAN の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	－
2. MAC-VLAN エントリを作成する	**mac-vlan mac-address** *mac-address* [**mask** *mac-mask*] **vlan** *vlan-id* [**dot1p** *priority*]	デフォルト：設定なし
3. interface view に移行する	**interface** *interface-type interface-number*	－

操作	コマンド	補足
4． リンクタイプをハイブリッドに設定する	**port link-type hybrid**	デフォルト：アクセス
5． MAC ベース VLAN でパケットを転送するためハイブリッドポートで許可する VLAN を設定する	**port hybrid vlan** *vlan-id-list* { **tagged** | **untagged** }	デフォルト : ポートのリンクタイプがアクセスである場合に所属しているVLANのタグなしメンバです。
6． MAC ベース VLAN を有効にする	**mac-vlan enable**	デフォルト：無効

10.5.4 ダイナミック MAC ベース VLAN の設定

I. 設定の制限とガイドライン

MAC ベース VLAN を設定する場合、以下の制限とガイドラインに従ってください。

- 802.1X 認証や MAC アドレス認証とダイナミック MAC ベース VLAN の割り当てを同時に設定しないでください。
- ダイナミック MAC ベース VLAN 割り当てがポートで有効である場合、MAC 学習を制限する、あるいは MAC 学習を無効にする設定は適用されません。
- ダイナミック MAC ベース VLAN の割り当てを行うため、MAC－VLAN エントリを作成する場合スタティック VLAN を使用してください。
- MSTP とダイナミック MAC ベース VLAN の割り当てを同時に設定しないことを推奨します。MSTP が有効になっており、対応する VLAN のインスタンスがブロックされている場合、装置が学習していない送信元 MAC アドレスのパケットは、CPU に送信されません。そのため、対応する VLAN をダイナミックに割り当てられることができません。
- PVST とダイナミック MAC ベース VLAN の割り当てを同時に設定しないことを推奨します。PVST が有効になっており、対応する VLAN がポートで許可されていない場合、ポートはブロック状態になります。受信パケットは CPU に送信されず、廃棄されます。そのため、対応する VLAN をダイナミックに割り当てられることができません。
- ダイナミック MAC ベース VLAN と自動 Voice VLAN の割り当てを同時に設定しないことを推奨します。ポートでダイナミック MAC ベース VLAN と自動 Voice VLAN の割り当ての両方を設定する場合、最初にダイナミック MAC ベース VLAN を設定してください。最初に自動 Voice VLAN の割り当てを設定した場合、衝突が発生します。設定の 1 つを削除する場合、もう一方の動作に影響します。

II. 設定手順

以下にダイナミック MAC ベース VLAN の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． MAC-VLAN エントリを作成する	**mac-vlan mac-address** *mac-address* [**mask** *mac-mask*] **vlan** *vlan-id* [**dot1p** *priority*]	デフォルト：設定なし
3． interface view に移行する	**interface** *interface-type interface-number*	―
4． リンクタイプをハイブリッドに設定する	**port link-type hybrid**	デフォルト：アクセス

操作	コマンド	補足
5． MAC ベース VLAN を有効にする	**mac-vlan enable**	デフォルト：無効
6． ダイナミック MAC ベース VLAN を有効にする	**mac-vlan trigger enable**	デフォルト：無効 ポートのVLAN割り当ては受信したパケットのMACアドレスがMAC-VLANエントリのMACアドレスと完全に一致した場合のみ発生します。
7． （オプション設定項目）PVID で MAC アドレスに一致しないパケットの転送を無効する	**port pvid forbidden**	デフォルト : 受信したパケットの送信元MACアドレスが一致しない場合、PVIDに転送します。

10.5.5 サーバ割り当て MAC ベース VLAN

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． interface view に移行する	**interface** *interface-type interface-number*	―
3． リンクタイプをハイブリッドに設定する	**port link-type hybrid**	デフォルト：アクセス
4． MAC ベース VLAN でパケットを転送するためハイブリッドポートで許可する VLAN を設定する	**port hybrid vlan** *vlan-id-list* { **tagged** | **untagged** }	デフォルト : ポートのリンクタイプがアクセスである場合に所属しているVLANのタグなしメンバです。
5． MAC ベース VLAN を有効にする	**mac-vlan enable**	デフォルト：無効
6． 802.1X あるいは MAC アドレス認証を設定する	コマンドマニュアルのセクション*7 セキュリティ*“*802.1X*”、“*MAC アドレス認証*”を参照してください。	―

🕮 **メモ：**

Radius サーバに Tunnel-Private-Group-ID 属性を設定して VLAN アサインする場合は、string で属性値を設定してください。integer で設定した属性値では VLAN のアサインはできません。

10.5.6 VLAN の表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
VLANインタフェース情報を表示する	**display interface** [**vlan-interface** [*interface-number*]] [**brief** [**description** | **down**]]
MACからVLANへのエントリを表示する	**display mac-vlan** { **all** | **dynamic** | **mac-address** *mac-address* [**mask** *mac-mask*] | **static** | **vlan** *vlan-id* }

操作	コマンド
MACベースのVLAN機能が有効になっているすべてのポートを表示する	**display mac-vlan interface**
VLAN情報を表示する	**display vlan** [*vlan-id1* [**to** *vlan-id2*] | **all** | **dynamic** | **reserved** | **static**]
VLANの概要情報を表示する	**display vlan brief**
装置のハイブリッドあるいはトランクポートを表示する	**display port** { **hybrid** | **trunk** }
VLANインタフェースの統計情報を削除する	**reset counters interface** [**vlan-interface** [*interface-number*]]

10.6 VLAN設定例

10.6.1 ポートベース VLAN の設定例

I. ネットワーク要件

図 10-4 に示すように設定します。

- Host A と Host C は部門 A に属します。VLAN100 は Department A に割り当てられます。
- Host B と Host D は部門 B に属します。VLAN200 は Department B に割り当てられます。

Host A が Host C と通信し、Host B が Host D に通信できるように、同一 VLAN のホストのみが互いに通信できることを確認します。

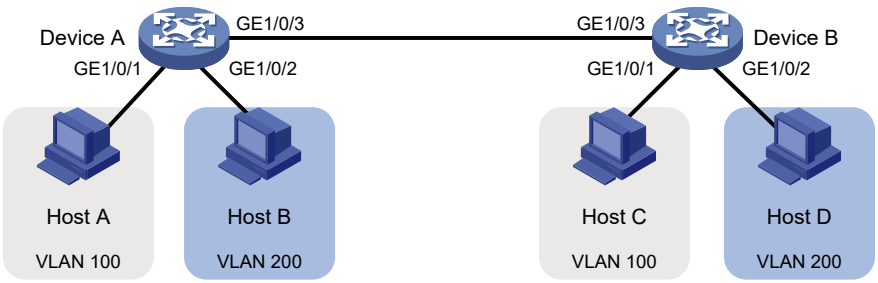


図 10-4 ネットワーク図

II. 設定手順

1) Device A を設定します。

VLAN 100 を作成し、GigabitEthernet 1/0/1 に割り当てます。

```
<DeviceA> system-view
[DeviceA] vlan 100
[DeviceA-vlan100] port gigabitethernet 1/0/1
[DeviceA-vlan100] quit
```

VLAN 200 を作成し、GigabitEthernet 1/0/2 に割り当てます。

```
[DeviceA] vlan 200
[DeviceA-vlan200] port gigabitethernet 1/0/2
[DeviceA-vlan200] quit
```

GigabitEthernet 1/0/3 をトランクポートとして VLAN 100、VLAN 200 からのパケットを Device B に転送するよう設定します。

```
[DeviceA] interface gigabitethernet 1/0/3
[DeviceA-GigabitEthernet1/0/3] port link-type trunk
[DeviceA-GigabitEthernet1/0/3] port trunk permit vlan 100 200
Please wait... Done.
```

2) Device A と同様に Device B の設定を行います。
3) host を設定します。
   - □ Host A と Host C を同じ IP サブネットに設定します。たとえば 192.168.100.0/24 です。
   - □ Host B と Host D を同じ IP サブネットに設定します。たとえば 192.168.200.0/24 です。

III. 設定の確認

Host A と Host C がお互いに **ping** ができることを確認し、Host B に **ping** が失敗することを確認します。（詳細は省略します。）

Host B と Host D がお互いに **ping** ができることを確認し、Host A に **ping** が失敗することを確認します。（詳細は省略します。）

VLAN100 と VLAN200 が Device A で正しく設定されていることを確認します。

```
[DeviceA-GigabitEthernet1/0/3] display vlan 100
VLAN ID: 100
VLAN type: Static
Route interface: Not configured
Description: VLAN 0100
Name: VLAN 0100
Tagged ports:
   GigabitEthernet1/0/3
Untagged ports:
   GigabitEthernet1/0/1


[DeviceA-GigabitEthernet1/0/3] display vlan 200
VLAN ID: 200
VLAN type: Static
Route interface: Not configured
Description: VLAN 0200
Name: VLAN 0200
Tagged ports:
   GigabitEthernet1/0/3
Untagged ports:
   GigabitEthernet1/0/2
```

10.6.2 MAC ベース VLAN 設定例

I. ネットワーク要件

図 10-5 に示すように設定します。

- Device A と Device C 上の GigabitEthernet 1/0/1 インタフェースはそれぞれ 2 つのミーティングルームに接続せれています。
- Laptop 1 と Laptop 2 は、2 つのミーティングルームのどちらかで使用されるポータルコンピュータです。Laptop 1 と Laptop 2 は、それぞれ VLAN 100 と VLAN 200 に属する 2 つの部門に所属しています。

Laptop 1 と Laptop 2 が、使用されているミーティングルームに関係なく、Laptop 1 と Laptop 2 は、それぞれの所属する部門のサーバー（Server 1 と Server 2）のみにアクセスできるように MAC ベース VLAN を設定します。

Laptop 1 と Laptop 2 の MAC アドレスは、それぞれ 000d-88f8-4e71 と 0014-222c-aa69 です。

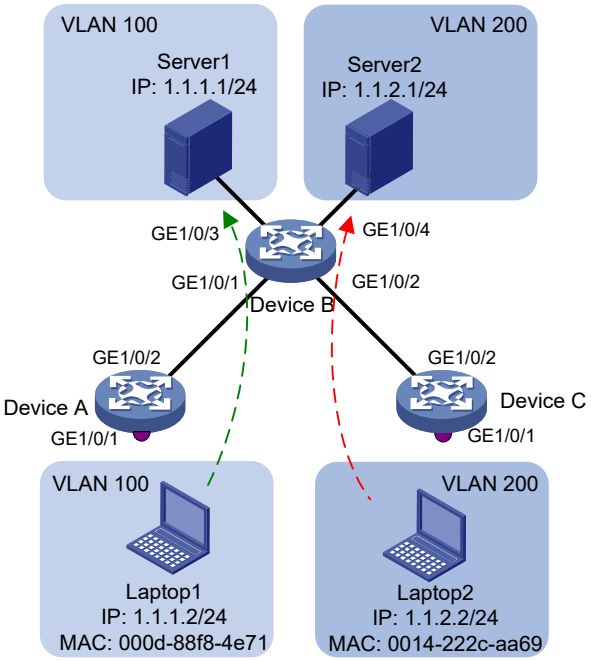


図 10-5 ネットワーク図

II. 設定手順

1) Device A を設定します。

VLAN100、VLAN200 を作成します。

```
<DeviceA> system-view
[DeviceA] vlan 100
[DeviceA-vlan100] quit
[DeviceA] vlan 200
[DeviceA-vlan200] quit
```

Laptop1 と Laptop2 の MAC アドレスをそれぞれ VLAN 100、VLAN 200 に関連づけます。

```
[DeviceA] mac-vlan mac-address 000d-88f8-4e71 vlan 100
[DeviceA] mac-vlan mac-address 0014-222c-aa69 vlan 200
```

VLAN100 と VLAN200 からのパケットを VLAN タグなしで転送するため、GigabitEthernet 1/0/1 をハイブリッドポートとして設定します。

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-type hybrid
[DeviceA-GigabitEthernet1/0/1] port hybrid vlan 100 200 untagged
```

GigabitEthernet 1/0/1 で MAC ベース VLAN を有効にします。

```
[DeviceA-GigabitEthernet1/0/1] mac-vlan enable
[DeviceA-GigabitEthernet1/0/1] quit
```

アップリンクポート GigabitEthernet 1/0/2 をトランクポートとして設定し、VLAN 100、VLAN 200 を割り当てます。

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port link-type trunk
[DeviceA-GigabitEthernet1/0/2] port trunk permit vlan 100 200
[DeviceA-GigabitEthernet1/0/2] quit
```

2) Device B を設定します。

VLAN 100 を作成し、GigabitEthernet 1/0/13 を VLAN100 に割り当てます。

```
<DeviceB> system-view
[DeviceB] vlan 100
[DeviceB-vlan100] port gigabitethernet 1/0/3
[DeviceB-vlan100] quit
```

VLAN 200 を作成し、GigabitEthernet 1/0/14 を VLAN 200 に割り当てます。

```
[DeviceB] vlan 200
[DeviceB-vlan200] port gigabitethernet 1/0/4
[DeviceB-vlan200] quit
```

GigabitEthernet 1/0/3 をトランクポートとして設定し、VLAN 100、VLAN 200 を割り当てます。

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port link-type trunk
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[DeviceB-GigabitEthernet1/0/1] quit
```

GigabitEthernet 1/0/4 をトランクポートとして設定し、VLAN 100、VLAN 200 を割り当てます。

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] port link-type trunk
[DeviceB-GigabitEthernet1/0/2] port trunk permit vlan 100 200
[DeviceB-GigabitEthernet1/0/2] quit
```

3) Device A の設定と同様に、Device C を設定します。（詳細は省略します）

III. 設定の確認

Laptop1 が Server 1 のみアクセスでき、Laptop2 が Server 2 のみアクセスできることを確認します。（詳細は省略します）

Device A と Device C の MAC-VLAN エントリを確認します。たとえば、Device A を確認します。

[DeviceA] display mac-vlan all

```
  The following MAC VLAN addresses exist:
  S:Static  D:Dynamic
  MAC address      Mask             VLAN ID  Priority    State
  000d-88f8-4e71   ffff-ffff-ffff   100       0          S
  0014-222c-aa69   ffff-ffff-ffff   200       0          S

  Total MAC VLAN address count: 2
```

目次

このセクションのページは**2-x-x** です。

11章 Voice VLAN 11-1
11.1 概要 11-1
11.2 IP電話の識別方法 11-1
11.2.1 OUIアドレスを使用したIP電話の識別方法 11-1
11.3 IP電話へのVoice VLANの配信 11-2
11.4 IP電話のアクセス方式 11-2
11.4.1 ホストとIP電話の直列接続 11-2
11.4.2 IP電話の装置への接続 11-3
11.5 Voice VLANのアサインモードの設定 11-3
11.5.1 自動モード 11-3
11.5.2 手動モード 11-4
11.5.3 Voice VLANのアサインモードとIP電話の協力 11-4
11.6 Voice VLANのセキュリティモードとノーマルモード 11-5
11.7 制限とガイドライン 11-6
11.8 Voice VLAN設定作業リスト 11-6
11.9 自動Voice VLANアサインモードの設定 11-7
11.9.1 設定の制限とガイドライン 11-7
11.9.2 設定手順 11-7
11.10 手動Voice VLANアサインモードの設定 11-8
11.10.1 設定の制限とガイドライン 11-8
11.10.2 設定手順 11-8
11.11 Voice VLANを配信するLLDPの設定 11-9
11.12 Voice VLANの表示と維持 11-10
11.13 Voice VLANの設定例 11-10
11.13.1 自動Voice VLANモードの設定例 11-10
11.13.2 手動Voice VLANアサインモードの設定例 11-12

11章 Voice VLAN

11.1 概要

Voice VLAN は音声トラフィックのために特別に設定されます。音声装置が接続されるポートを Voice VLAN に設定すると、音声トラフィックのために QoS（Quality Of Service）パラメータを設定し、転送プライオリティを改善することで音声品質を確保します。

音声装置とは、IP 電話 IAD（統合アクセス装置）がありますが、本章では IP 電話（IP Phone）を用いて説明します。

音声通信を転送するためには、装置は以下の操作をします。

- ネットワーク中の IP 電話を識別し、その MAC アドレスを取得します。
- IP 電話に VLAN 情報を通知します。

VLAN 情報を受け取ると、IP 電話は自動設定を実行し、IP 電話の音声パケットを Voice VLAN に送信します。

11.2 IP電話の識別方法

装置は、IP 電話を識別するために OUI アドレスを使用します。

11.2.1 OUI アドレスを使用した IP 電話の識別方法

装置は受信パケットの送信元 MAC アドレスを確認することで音声パケットかどうかを判断します。送信元 MAC アドレスが音声装置の OUI（Organizationally Unique Identifier）アドレスに対応するパケットは、音声トラフィックと見なされ、Voice VLAN に設定されます。

Voice VLAN には、事前に設定した OUI アドレスか、デフォルトで設定されている OUI アドレスを使用することができ手動でデフォルト OUI アドレスを削除することも、新しく追加することもできます。

表 11-1のリストは、装置にデフォルトで設定されている各ベンダの OUI アドレスです。

表 11-1 デフォルトで設定されている OUI アドレス

番号	OUI アドレス	ベンダ
1	0001-e300-0000	Siemens phone
2	0003-6b00-0000	Cisco phone
3	0004-0d00-0000	Avaya phone
4	00d0-1e00-0000	Pingtel phone
5	0060-b900-0000	Philips/NEC phone
6	00e0-7500-0000	Polycom phone
7	00e0-bb00-0000	3Com phone

通常、OUI アドレスは、バイナリフォーマットで MAC アドレスの最初の 24 ビットにアサインされ、IEEE が各ベンダに割り当てるグローバルに固有な識別子です。しかし、本マニュアルの OUI アドレスは、システムが受信パケットを音声パケットどうか判断するために使用されます。これらは、**voice vlan mac-address** コマンドで設定された MAC アドレスと OUI マスクの 2 つの AND 演算の結果で求められます。

11.3 IP電話へのVoice VLANの配信

図 11-1に、IP 電話に Voice VLAN 情報を配信するフローを示します。

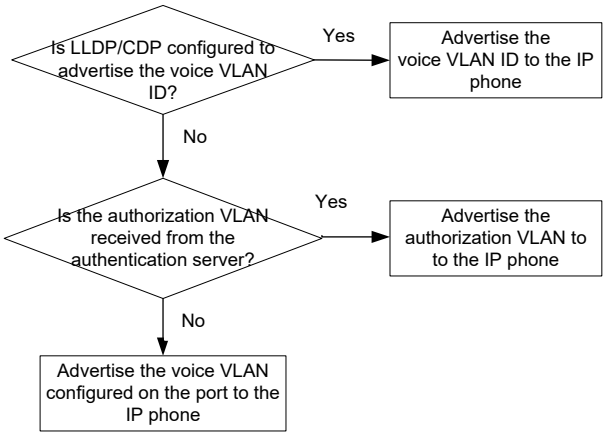


図 11-1 IP 電話への Voice VLAN の配信フロー

11.4 IP電話のアクセス方式

11.4.1 ホストと IP 電話の直列接続

図 11-2に示すように、ホストは IP 電話に接続され、IP 電話は装置に接続されています。この場合、以下の要件が満たされていなければなりません。

- ホストと IP 電話は異なる VLAN を使用してください。
- 装置がホストと IP 電話のトラフィックを区別できるように、IP 電話は、タグ付けした VLAN パケットを送ることができます。
- IP 電話に接続したポートは Voice VLAN と PVID からのパケットを転送します。

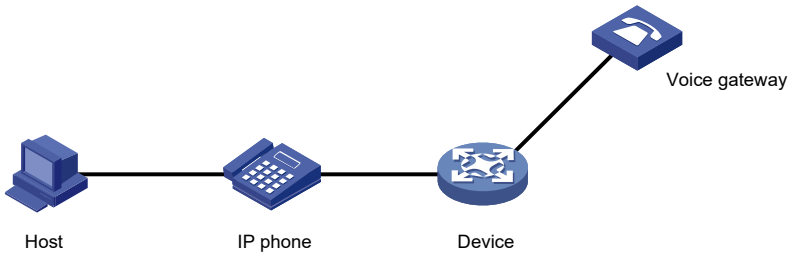


図 11-2 ホストと IP 電話が直列接続されたネットワーク

11.4.2 IP 電話の装置への接続

図 11-3に示すように、IP 電話はホストを使用せずに装置に接続されています。IP 電話がタグ無し音声パケットを送信する場合、この接続方法を使用してください。この場合、ポートの PVID として Voice VLAN を設定し、PVID からパケットを転送するためにポート設定をしなければなりません。

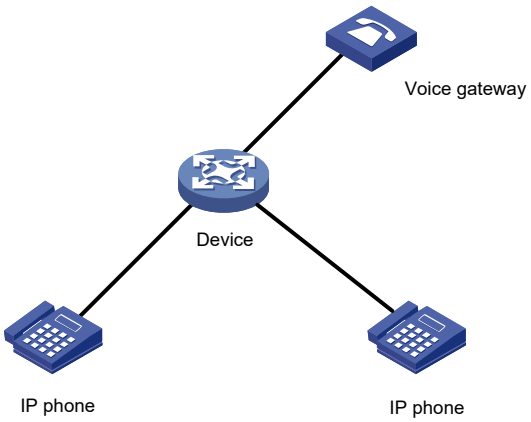


図 11-3 IP 電話が装置に接続されたネットワーク

11.5 Voice VLANのアサインモードの設定

ポートは、自動あるいは手動で Voice VLAN を割り当てることができます。

11.5.1 自動モード

図 11-2に示すように、PC と IP 電話が直列に接続されて装置を介してネットワークにアクセスする場合、自動モードを使用してください。装置のポートは、音声とデータのトラフィックの両方を送信します。

IP 電話は起動すると、プロトコルパケットを送信します。プロトコルパケットを受信した後、システムは装置の OUI アドレスとプロトコルパケットの送信元 MAC アドレスを照合します。照合が一致すれば、システムは以下の操作をします。

- 装置はプロトコルパケットの受信ポートに Voice VLAN を割り当てます。
- パケット優先順位を設定するために ACL ルールを適用します。
- Voice VLAN のエージングタイムを開始します。

エージングタイムが超過するまでにポートでパケットを受信しない場合、装置は Voice VLAN からポートを削除します。エージングタイムは設定可能です。

IP 電話が再起動すると、既存の音声接続が正しく動作するように、ポートが Voice VLAN に再割り当てされます。この再割り当ては、Voice VLAN が正常に動作している限り、音声トラフィックによって開始されることなく自動的に行われます。

11.5.2 手動モード

図 11-3に示すように、装置を介して IP 電話だけがネットワークに接続している場合、手動モードを使用してください。このモードでは、Voice VLAN に割り当てられたポートは音声トラフィックのみが送信されます。データトラフィックが音声トラフィックの送信に与える影響を防止します。

手動で Voice VLAN に装置の受信ポートを割り当ててください。装置は OUI アドレスと受信した音声パケットの送信元 MAC アドレスを照合します。照合が一致すれば、パケット優先順位を設定するために ACL ルールを適用します。

Voice VLAN からポートを削除する場合、手動で削除してください。

11.5.3 Voice VLAN のアサインモードと IP 電話の協力

IP 電話は VLAN タグ付きパケットを送信するものと、タグなしパケットのみを送信するものがあります。正しくパケット処理をするために、さまざまなリンクタイプのポートは違う Voice VLAN アサインモードの中で特定の設定要件を満たさなければなりません。

表 11-2 IP 電話のタグ付き音声トラフィックの送信

ポートリンクタイプ	Voice VLAN アサインモード	設定要件
Trunk	自動モード	ポートのデフォルトVLANはVoice VLANにできません。
	手動モード	ポートのデフォルトVLANはVoice VLANにできません。Voice VLANのパケットを転送できるように設定する必要があります。
Hybrid	自動モード	ポートのデフォルトVLANはVoice VLANにできません。
	手動モード	ポートのデフォルトVLANはVoice VLANにできません。Voice VLANのタグ付きパケットを転送できるように設定する必要があります。

IP 電話がタグなしパケットを送信する場合、手動で Voice VLAN を割り当てる必要があります。

表 11-3 IP 電話のタグなし音声トラフィックの送信

ポートリンクタイプ	設定要件
Access	Voice VLANはポートのPVIDを設定する必要があります。
Trunk	Voice VLANはポートのPVIDを設定する必要があります。 ポートはVoice VLANのパケットを転送する必要があります。
Hybrid	Voice VLANはポートのPVIDを設定する必要があります。 ポートはVoice VLANのタグなしパケットを転送する必要があります。

IP 電話が VLAN タグ付きの音声トラフィックを送信し、アクセスポートに 802.1X 認証、Guest VLAN、または Auth-Fail VLAN が設定されている場合、VLAN ID を以下と異なるように割り当てる必要があります。

- Voice VLAN
- アクセスポートの PVID
- 802.1X Guest VLAN、Auth-Fail VLAN

IP 電話がタグなしの音声トラフィックを送信する場合、アクセスポートの PVID は Voice VLAN にする必要があります。このため、802.1X 認証はサポートしません。

11.6 Voice VLANのセキュリティモードとノーマルモード

Voice VLAN が有効なポートは入力パケットのフィルタリングメカニズムにもとづいて、以下の 1 つのモードで運用することができます。

- **ノーマルモード**– ポートは Voice VLAN でタグ付きパケットを受信し、MAC アドレスを確認せずに Voice VLAN に転送します。ポートの PVID が Voice VLAN でポートが手動の VLAN アサインモードで動作する場合、ポートは Voice VLAN のすべての受信したタグなしパケットを転送します。

  このモードでは Voice VLAN は通信攻撃に対して脆弱です。悪意のあるユーザは、音声帯域を消費させ音声通信に影響するように大量のタグ付きあるいはタグなしの偽のパケットを送信する可能性があります。
- **セキュリティモード**– ポートは送信元MACアドレスが装置のOUIアドレスと一致する音声パケットのみを受信します。ほかのすべてのパケットは廃棄します。

安全なネットワークでは、Voice VLAN を通常モードで動作するように設定でき送信元 MAC アドレスのチェックを行うリソースの消費を削減することができます。

装置は OUI アドレスに一致する送信元 MAC アドレスの Voice VLAN パケットの転送プライオリティのみを変更することができます。

Voice VLAN で音声パケットと非音声パケットの両方を転送することは推奨しません。転送する必要がある場合は、Voice VLAN のセキュリティモードが無効であることを確認してください。

表 11-4 Voice VLAN 有効ポートのパケット処理方法

動作モード	パケットタイプ	パケット処理
ノーマルモード	• タグなしパケット • Voice VLANタグのパケット	MACアドレスをチェックしないため、音声トラフィックと非音声トラフィックの両方をVoice VLANで通過することができます。

動作モード	パケットタイプ	パケット処理
	ほかのVLANタグのパケット	ポートが、そのVLANのパケットが通過するのを許可するか許可しないかにより、パケットを通過させるか、廃棄させます。
セキュリティモード	• タグなしパケット • Voice VLANタグのパケット	• パケットの送信元MACアドレスが装置に設定されているOUIアドレスと一致する場合は、Voice VLANで通過します。 • パケットの送信元MACアドレスが装置に設定されているOUIアドレスと一致しない場合、パケットを廃棄します。
	ほかのVLANタグのパケット	ポートが、そのVLANのパケットが通過するのを許可するか許可しないかにより、パケットを通過させるか、廃棄させます。

11.7 制限とガイドライン

Voice VLAN のエージングタイマは、Voice VLAN のダイナミック MAC アドレスエントリが期限切れになった時にのみ開始されます。Voice VLAN のエージング期間は、Voice VLAN エージングタイマとそのダイナミック MAC アドレスエントリのエージングタイマの合計に等しくなります。ダイナミック MAC アドレスエントリのエージングタイマの詳細は、オペレーションマニュアルのセクション 2 *アクセス”MAC アドレステーブル”*を参照してください。

ベストプラクティスとして、ポートで Voice VLAN を設定し、MAC アドレス学習を無効にしないでください。2 つの機能がポートで一緒に設定されている場合、ポートは OUI アドレスと完全に一致するパケットのみを転送し、不正確に一致するパケットを廃棄します。

ベストプラクティスとして、ポートで Voice VLAN と MAC 学習制限の両方を設定しないでください。2 つの機能がポートで一緒に設定され、ポートが設定された MAC アドレスエントリの最大数を学習する場合、ポートは次のようにパケットを処理します。

- ポートおよびOUIアドレスによって学習されたMACアドレスエントリに一致するパケットのみを転送します。
- 一致しないパケットを廃棄します。

11.8 Voice VLAN設定作業リスト

作業リスト
（必須設定項目）以下のどちらか1つを設定します。 • 自動Voice VLANアサインモードの設定 • 手動Voice VLANアサインモードの設定
（オプション設定項目）Voice VLANを配信するLLDPの設定

11.9 自動Voice VLANアサインモードの設定

11.9.1 設定の制限とガイドライン

ポートに自動 Voice VLAN アサインモードを設定する場合、以下の制限とガイドラインに従ってください。

- 自動 Voice VLAN アサインモードと MSTP は同時に使用しないことを推奨します。MSTP モードでは、ポートがターゲット Voice VLAN の MSTI でブロックされている場合、ポートは受信パケットを CPU に送信せず廃棄します。結果として、受信ポートは Voice VLAN に動的に割り当てられません。
- 自動 Voice VLAN アサインモードと PVST は同時に使用しないことを推奨します。PVST モードでは、ポートでターゲット Voice VLAN の MSTI を許可されていない場合、ポートはブロック状態になり、受信パケットを CPU に送信せず廃棄します。結果として、受信ポートは Voice VLAN に動的に割り当てられません。
- ポートにダイナミック MAC ベース VLAN と自動 Voice VLAN アサインモードの両方を設定しないことを推奨します。ポートでダイナミック MAC ベース VLAN と自動 Voice VLAN の割り当ての両方を設定する場合、最初にダイナミック MAC ベース VLAN を設定してください。最初に自動 Voice VLAN の割り当てを設定した場合、衝突が発生します。設定の 1 つを削除するとき、もう一方の動作に影響します。

11.9.2 設定手順

以下にポートに自動 Voice VLAN アサインモードの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	-
2. （オプション設定項目）Voice VLAN のエージングタイムを設定する	**voice vlan aging** *minutes*	デフォルト：1440分 Voice VLANエージングタイムの設定は、自動Voice VLANアサインモードのポートでのみ適用されます。
3. （オプション設定項目）Voice VLAN セキュリティモードを有効にする	**voice vlan security enable**	デフォルト：有効
4. （オプション設定項目）登録 OUI アドレスを追加する	**voice vlan mac-address** *oui* **mask** *oui-mask* [**description** *text*]	デフォルト：表 11-1に示すアドレスが登録されています。
5. interface view に移行する	• Ethernet interface viewに移行する： **interface** *interface-type interface-number* • aggregate interface viewに移行する： **interface bridge-aggregation** *interface-number*	—
6. ポートのリンクタイプを設定する	• **port link-type trunk** • **port link-type hybrid**	—

操作	コマンド	補足
7．（オプション設定項目）自動 Voice VLAN アサインモードで動作するように設定する	**voice vlan mode auto**	デフォルト：有効
8．Voice VLAN を有効にする	**voice vlan** *vlan-id* **enable**	デフォルト：無効 VLANがすでに作成されていることを確認してください。

11.10 手動Voice VLANアサインモードの設定

11.10.1 設定の制限とガイドライン

ポートに自動 Voice VLAN アサインモードを設定する場合、以下の制限とガイドラインに従ってください。

- 同一装置の異なるポートに、同時に異なる Voice VLAN を設定することができます。以下の要件に従う必要があります。
  - □ 1 つのポートは 1 つの Voice VLAN のみ設定することができます。
  - □ Voice VLAN は装置で、すでにスタティック VLAN として設定されている必要があります。
- リンクアグリゲーショングループのメンバポートで Voice VLAN を有効にしないでください。リンクアグリゲーショングループの詳細は、オペレーションマニュアルのセクション 2 *アクセス”リンクアグリゲーション”*を参照してください。
- ポートで Voice VLAN を実行するには、Voice VLAN を有効にして、手動 Voice VLAN アサインモードを設定し、Voice VALN を手動でポートに割り当てる必要があります。

11.10.2 設定手順

以下にポートに手動 Voice VLAN アサインモードの設定を示します。

操作	コマンド	補足
1．system view に移行する	**system-view**	―
2．（オプション設定項目）Voice VLAN セキュリティモードを有効にする	**voice vlan security enable**	デフォルト：有効
3．（オプション設定項目）登録 OUI アドレスを追加する	**voice vlan mac-address** *oui* **mask** *oui-mask* [**description** *text*]	デフォルト：表 11-1に示すアドレスが登録されています。
4．interface view に移行する	● Ethernet interface viewに移行する： **interface** *interface-type interface-number* ● aggregate interface viewに移行する： **interface bridge-aggregation** *interface-number*	―

操作	コマンド	補足
5．（必須設定項目）手動 Voice VLAN アサインモードで動作するように設定する	**undo voice vlan mode auto**	デフォルト：無効
6．手動モードで Voice VLAN をポートにアサインする	アクセスポートに設定する場合、オペレーションマニュアルのセクション2 *アクセス”VLAN”の”アクセスポートVLANの設定”*を参照してください。	3つから1つを選択します。 Voice VLANにAccess port をアサインすると、自動的にポートのPVIDになります。
	トランクポートに設定する場合、オペレーションマニュアルのセクション2 *アクセス”VLAN”の”トランクポートVLANの設定”*を参照してください。	
	ハイブリッドポートに設定する場合、オペレーションマニュアルのセクション2 *アクセス”VLAN”の”ハイブリッドポートVLANの設定”*を参照してください。	
7．（オプション設定項目）ポートのデフォルト VLAN として Voice VLAN を設定する	トランクポートに設定する場合、オペレーションマニュアルのセクション2 *アクセス”VLAN”の”トランクポートVLANの設定”*を参照してください。	この設定は受信音声トラフィックがタグなしの場合に必要です。タグ付きの場合は設定することができません。
	ハイブリッドポートに設定する場合、オペレーションマニュアルのセクション2 *アクセス”VLAN”の”アクセスポートVLANの設定”*を参照してください。	
8．Voice VLAN を有効にする	**voice vlan** *vlan-id* **enable**	デフォルト：無効 VLANがすでに作成されていることを確認してください。

11.11 Voice VLANを配信するLLDPの設定

IP 電話が LLDP をサポートしている場合、装置は LLDP-MED TLV を用いて IP 電話に Voice VLAN 情報を配信します。

この機能を設定する前に、グローバルとアクセスポートの両方で LLDP を有効にしてください。

以下に Voice VLAN を配信する LLDP の設定を示します。

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

操作	コマンド	補足
3． LLDP を設定する	**lldp tlv-enable med-tlv network-policy** *vlan-id*	デフォルト：設定なし 詳細はコマンドマニュアルのセクション2 *アクセス”LLDP”*を参照してください。
4． （オプション設定項目）LLDP によって配信されあれた Voice VLAN を表示する	**display lldp local-information**	詳細はコマンドマニュアルのセクション2 *アクセス”LLDP”*を参照してください。

11.12 Voice VLANの表示と維持

すべての view で **display** コマンドを実行し、user view で **reset** コマンドを実行できます。

操作	コマンド
Voice VLANの状態を表示する	**display voice vlan state**
装置でサポートされているOUIアドレスを表示する	**display voice-vlan mac-address**

11.13 Voice VLANの設定例

11.13.1 自動 Voice VLAN モードの設定例

I. ネットワーク要件

図 11-4に示すように、Device A は IP 電話とホストからの通信トラフィックを転送します。

正しく音声トラフィックを転送するには、以下の操作を行ってください。

- IP 電話 A と IP 電話 B からの音声パケットを転送するように、それぞれ Voice VLAN 2 と Voice VLAN 3 を設定します。
- 自動 Voice VLAN アサインモードを動作させるために、GigabitEthernet 1/0/1 と GigabitEthernet 1/0/2 に設定をします。
- 音声パケットの認証のために IP 電話 A と IP 電話 B の MAC アドレスを追加します。2 つの MAC アドレスのマスクは FFFF-FF00-0000 です。

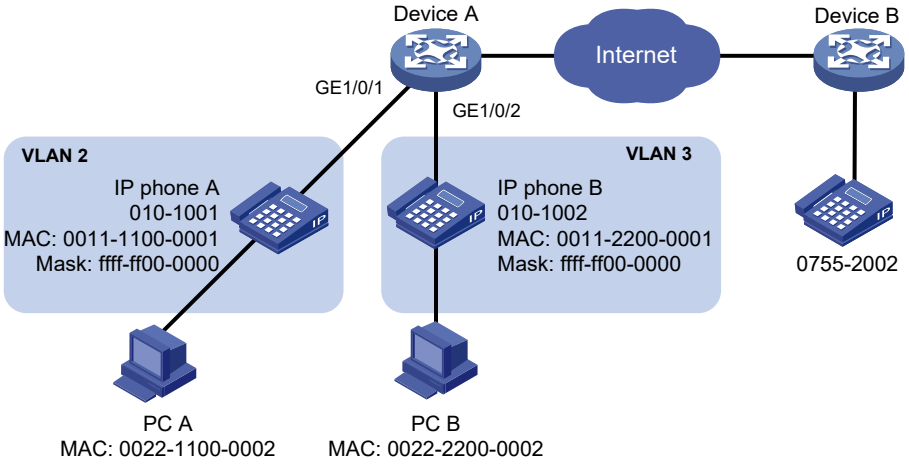


図 11-4 ネットワーク図

II. 設定手順

1)　VLAN を設定します

VLAN 2 と VLAN 3 を作成します。

```
<DeviceA> system-view
[DeviceA] vlan 2 to 3
```

Voice VLAN のエージングタイムを 30 分に設定します。

```
[DeviceA] voice-vlan aging 30
```

Voice VLAN が音声パケットのみ転送するようにセキュリティモードでの動作を設定します。

```
[DeviceA] voice-vlan security enable
```

IP 電話 A と IP 電話 B にマスク値 FFFF-FF00-0000 と MAC アドレスを追加します。

```
[DeviceA] voice-vlan mac-address 0011-1100-0001 mask ffff-ff00-0000 description IP phone A
[DeviceA] voice-vlan mac-address 0011-2200-0001 mask ffff-ff00-0000 description IP phone B
```

2)　GigabitEthernet 1/0/1 ポートを設定します。

GigabitEthernet 1/0/1 をハイブリッドポートに設定します。

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-type hybrid
```

GigabitEthernet 1/0/1 を自動 Voice VLAN アサインモードとして動作するように設定します。

```
[DeviceA-GigabitEthernet1/0/1] voice-vlan mode auto
```

GigabitEthernet 1/0/1 の Voice VLAN として VLAN 2 を設定します。

```
[DeviceA-GigabitEthernet1/0/1] voice-vlan 2 enable
[DeviceA-GigabitEthernet1/0/1] quit
```

3) GigabitEthernet 1/0/2 ポートを設定します。

```
# GigabitEthernet 1/0/2 をハイブリッドポートに設定します。
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port link-type hybrid
```

GigabitEthernet 1/0/2 を自動 Voice VLAN アサインモードとして動作するように設定します。

```
[DeviceA-GigabitEthernet1/0/2] voice-vlan mode auto
```

GigabitEthernet 1/0/2 の Voice VLAN として VLAN 3 を設定します。

```
[DeviceA-GigabitEthernet1/0/2] voice-vlan 3 enable
[DeviceA-GigabitEthernet1/0/2] quit
```

III. 設定の確認

Device A でサポートされている OUI アドレスを表示します。

```
[DeviceA] display voice-vlan mac-address
OUI Address      Mask            Description
0001-e300-0000   ffff-ff00-0000  Siemens phone
0003-6b00-0000   ffff-ff00-0000  Cisco phone
0004-0d00-0000   ffff-ff00-0000  Avaya phone
000f-e200-0000   ffff-ff00-0000  H3C Aolynk phone
0011-1100-0000   ffff-ff00-0000  IP phone A
0011-2200-0000   ffff-ff00-0000  IP phone B
0060-b900-0000   ffff-ff00-0000  Philips/NEC phone
00d0-1e00-0000   ffff-ff00-0000  Pingtel phone
00e0-7500-0000   ffff-ff00-0000  Polycom phone
00e0-bb00-0000   ffff-ff00-0000  3Com phone
```

現在の Voice VLAN の状態を表示します。

```
[DeviceA] display voice-vlan state
 Current voice VLANs: 2
 Voice VLAN security mode: Security
 Voice VLAN aging time: 30 minutes
 Voice VLAN enabled ports and their modes:
 Port                        VLAN        Mode        CoS         DSCP
 GE1/0/1                     2           Auto        6           46
 GE1/0/2                     3           Auto        6           46
```

11.13.2 手動 Voice VLAN アサインモードの設定例

I. ネットワーク要件

図 11-5に示すように設定します。

GigabitEthernet 1/0/1 で音声トラフィックのみ転送するため、以下の設定を行います。

- VLAN 2 を作成し Voice VLAN として使用します。

- 手動 Voice VLAN アサインモードを動作させるために、GigabitEthernet 1/0/1 を設定します。VLAN 2 に追加します。
- Device A の OUI リストに IP 電話 A の OUI アドレスを追加します。

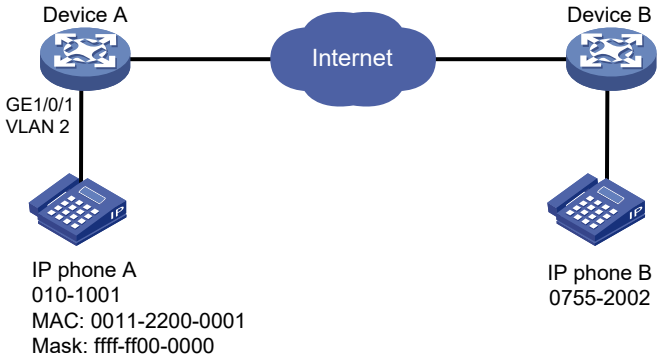


図 11-5 ネットワーク図

II. 設定手順

Voice VLAN がセキュリティモードで動作するように設定します。

```
<DeviceA> system-view
[DeviceA] voice-vlan security enable
```

マスク FFFF-FF00-0000 で MAC アドレス 0011-2200-0001 を追加します。

```
[DeviceA] voice-vlan mac-address 0011-2200-0001 mask ffff-ff00-0000 description test
```

VLAN 2 を作成します。

```
[DeviceA] vlan 2
[DeviceA-vlan2] quit
```

GigabitEthernet 1/0/1 を手動 Voice VLAN アサインモードで動作するように設定します。

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] undo voice-vlan mode auto
```

GigabitEthernet 1/0/1 をハイブリッドポートに設定します。

```
[DeviceA-GigabitEthernet1/0/1] port link-type hybrid
```

GigabitEthernet 1/0/1 の PVID を VLAN 2 に設定します。

```
[DeviceA-GigabitEthernet1/0/1] port hybrid pvid vlan 2
```

#タグなし VLAN メンバとして GigabitEthernet 1/0/1 を VLAN 2 に割り当てます。

```
[DeviceA-GigabitEthernet1/0/1] port hybrid vlan 2 untagged
```

Voice VLAN を有効にし、GigabitEthernet 1/0/1 の Voice VLAN として VLAN 2 を設定します。

```
[DeviceA-GigabitEthernet1/0/1] voice-vlan 2 enable
[DeviceA-GigabitEthernet1/0/1] quit
```

III. 設定の確認

Device A でサポートされている OUI アドレスを表示します。

```
[DeviceA] display voice-vlan mac-address
OUI Address     Mask            Description
0001-e300-0000  ffff-ff00-0000  Siemens phone
0003-6b00-0000  ffff-ff00-0000  Cisco phone
0004-0d00-0000  ffff-ff00-0000  Avaya phone
000f-e200-0000  ffff-ff00-0000  H3C Aolynk phone
0011-2200-0000  ffff-ff00-0000  test
0060-b900-0000  ffff-ff00-0000  Philips/NEC phone
00d0-1e00-0000  ffff-ff00-0000  Pingtel phone
00e0-7500-0000  ffff-ff00-0000  Polycom phone
00e0-bb00-0000  ffff-ff00-0000  3Com phone
```

現在の Voice VLAN の状態を表示します。

```
[DeviceA] display voice-vlan state
 Current voice VLANs: 1
 Voice VLAN security mode: Security
 Voice VLAN aging time: 1440 minutes
 Voice VLAN enabled ports and their modes:
 Port                        VLAN        Mode        CoS         DSCP
 GE1/0/1                     2           Manual      6           46
```

目次

このセクションのページは**2-x-x** です。

12 章 LLDP 12-1
12.1 概要 12-1
12.1.1 基本コンセプト 12-1
12.1.2 動作メカニズム 12-7
12.1.3 プロトコルと標準 12-8
12.2 LLDP 設定作業リスト 12-8
12.3 LLDP の基本設定 12-8
12.3.1 LLDP の有効化 12-8
12.3.2 LLDP 動作モードの設定 12-8
12.3.3 再初期化遅延時間の設定 12-9
12.3.4 LLDP ポーリングの有効化 12-9
12.3.5 アドバタイズ可能な TLV の設定 12-10
12.3.6 管理アドレスの設定とカプセル化フォーマットの設定 12-11
12.3.7 LLDP に関する他のパラメータの設定 12-12
12.3.8 LLDP フレームのカプセル化フォーマットの設定 12-12
12.4 CDP 互換モードの設定 12-13
12.4.1 設定要件 12-13
12.4.2 設定手順 12-14
12.5 LLDP トラップの設定 12-14
12.6 LLDP の表示と維持 12-15
12.7 LLDP の設定例 12-15
12.7.1 LLDP の基本的な設定例 12-15
12.7.2 CDP 互換モードの設定例 12-19

12章 LLDP

12.1 概要

異なるベンダが存在するネットワークのとき、標準の設定情報を交換するプラットフォームは、異なるベンダからの異なるタイプのネットワーク装置を相互に検出します。これにより設定を交換できることを保証します。

LLDP（Link Layer Discovery Protocol）は、IEEE802.1AB で規定されています。データリンクレイヤで直接装置に接続された装置間の装置情報を交換するプロトコルです。LLDP では、装置は LLDPDU（LLDP データユニット）にある TLV と呼ばれるタイプ（Type）長さ（Length）値（Value）の形式を利用して、ローカル装置情報を直接接続された装置に送信します。ローカル装置情報はシステム機能、管理 IP アドレス、装置 ID、ポート ID を含みます。装置は LLDP 隣接装置から受信した LLDPDU の装置情報を標準 MIB に格納します。MIB についての詳細は、オペレーションマニュアルのセクション 9 *システム管理”SNMP*”を参照してください。LLDP はレイヤ 2 のネットワークトポロジの変化をただちに検出し、識別するためにネットワーク管理システムを有効にします。

12.1.1 基本コンセプト

I. LLDP エージェント

LLDP が動作するところで LLDP エージェントはエンティティをマッピングします。複数の LLDP エージェントは同じインタフェースで動作することができます。

LLDP エージェントは以下のタイプに分類されます。

- Nearest bridge エージェント
- Nearest customer bridge エージェント
- Nearest non-TPMR bridge エージェント

Two-port MAC Relay （TPMR）は 2 つの外部アクセスブリッジポートのブリッジタイプで、MAC ブリッジの機能をサポートします。TPMR は以下を除いて、すべてのフレームベースのメディアに独立したプロトコルに透過的です。

- 独立したプロトコル行き
- TPMR のリレー機能が転送しないように予約された MAC アドレス行き

LLDP は隣接エージェント間でパケットを交換し、隣接情報を作成、維持します。図 12-1 に LLDP エージェントの隣接関係を示します。LLDP はカスタマブリッジ（CB）とサービスブリッジ（SB）の 2 つのブリッジモードをもちます。

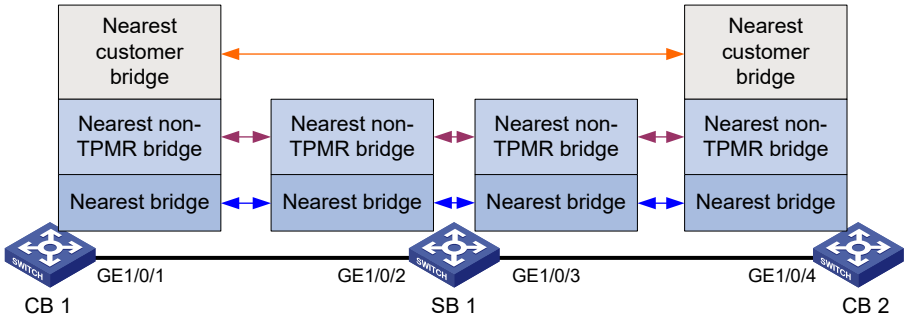


図 12-1 LLDP 隣接関係

II. LLDP フレームフォーマット

LLDP は LLDP フレームの装置情報を送信します。LLDP フレームは Ethernet II あるいは SNAP フレームでカプセル化されています。

- Ethernet II にカプセル化した LLDP フレーム

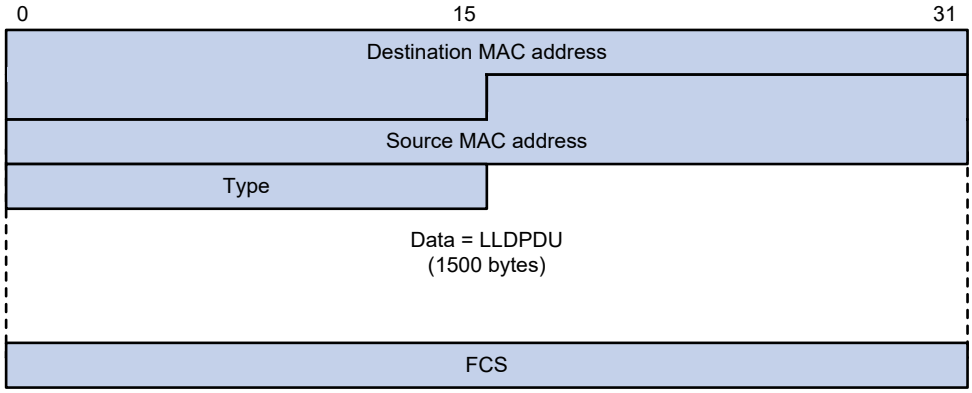


図 12-2 Ethernet II にカプセル化した LLDP フレーム

表 12-1 Ethernet II にカプセル化した LLDP フレームフィールド

フィールド	説明
Destination MAC address	LLDPフレームがアドバタイズしたMACアドレスです。 LLDPは異なるエージェントタイプ向けのLLDPフレームの宛先MACアドレスとして異なるマルチキャストアドレスを指定します。同一インタフェース上で異なるエージェントタイプで送受信したLLDPフレームを区別します。 • LLDPフレーム0x0180-C200-000Eはnearest bridge向けです。 • LLDPフレーム0x0180-C200-000はnearest customer bridge向けです。 • LLDPフレーム0x0180-C200-0003はnearest TPMR bridge向けです。
Source MAC address	送信ポートのMACアドレスです。
Type	上位レイヤプロトコルのEthernetタイプです。LLDPは0x88CCです。
Data	LLDPDUです。

フィールド	説明
FCS	フレームチェックシーケンスで、32ビットCRCの値が受信したEthernetフレームを確認するために使われます。

- SNAP にカプセル化した LLDP フレーム

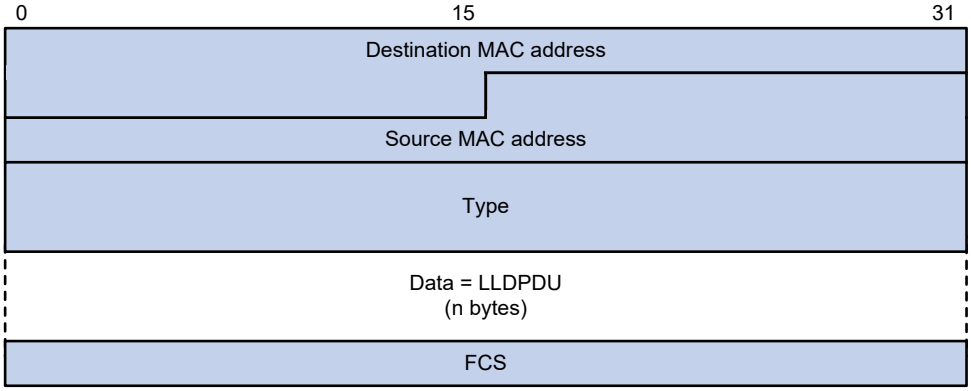


図 12-3 SNAP にカプセル化したフレーム

表 12-2 SNAP にカプセル化したフレームフィールド

フィールド	説明
Destination MAC address	LLDPフレームがアドバタイズしたマルチキャストのMACアドレスです。Ethernet2でカプセル化したLLDPフレームのMACアドレスと同一です。
Source MAC address	送信ポートのMACアドレスです。
Type	上位レイヤプロトコルのSNAPタイプです。LLDPは0xAAAA-0300-0000-88CCです。
Data	LLDPDUです。
FCS	フレームチェックシーケンスで、32ビットCRCの値が受信したEthernetフレームを確認するために使われます。

III. LLDPDU

LLDP は情報を交換するために LLDPDU を使用します。LLDPDU は複数の TLV（タイプ, 長さ,値）から構成されています。図 12-4 で示すように、装置上の各 TLV をアドバタイズします。

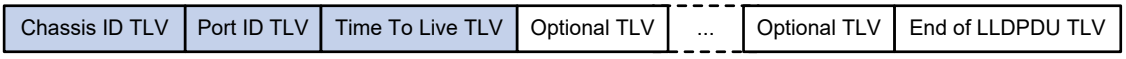


図 12-4 LLDPDU カプセルフォーマット

各 LLDPDU は、Chassis ID TLV、Port ID TLV、Time to Live TLV の必須 TLV から開始します。必須 TLV の後に、最大 29 種類のオプション TLV が続きます。

IV. TLV

TLV はタイプ、長さ、値のフィールドが含まれる情報の要素です。

LLDPDU TLV は以下のカテゴリに分類されます。

- 基本的な管理 TLV
- 組織規定された TLV （IEEE 802.1、IEEE 802.3）
- LLDP-MED（media endpoint discovery）関連の TLV

基本的な TLV は装置を管理するのに必要不可欠なカテゴリです。組織規定された TLV と LLDP-MED 関連の TLV は拡張された装置管理のために使用されます。標準あるいは他の組織によって定義され、LLDPDU のオプションです。

- 基本的な管理 TLV

表 12-3 に基本的な管理 TLV タイプを示します。基本的な管理 TLV のいくつかは、各 LLDPDU に必須です。

表 12-3 基本的な管理 TLV

タイプ	説明	補足
Chassis ID	送信する装置のBridge MACアドレスを指定します。	必須
Port ID	送信ポートのIDを指定します。 ● LLDPDUがLLDP-MEDを含んでいる場合、Port ID TLVは送信ポートのMACアドレスです。 ● LLDPDUがLLDP-MEDを含んでいない場合、Port ID TLVはポート名です。	
Time to Live	受信する装置のTTLを指定します。	
End of LLDPDU	LLDPDUのTLVシーケンスの終端をマーキングします。	
Port Description	送信するポートの説明を指定します。	オプション
System Name	送信する装置の装置名を指定します。	
System Description	送信する装置の説明を指定します。	
System Capabilities	送信する装置の主な機能や有効な機能を識別します。	
Management Address	以下の要素を指定します。 ● ローカル装置の管理アドレスです。 ● インタフェース番号、アドレスに関連したOIDです。	

- IEEE 802.1 組織指定 TLV

表 12-4 IEEE 802.1 組織指定 TLV

タイプ	説明
Port VLAN ID	ポートのVLAN識別子（PVID） を指定します。
VLAN Name	ポートが属しているVLANの名前を示します。
Protocol Identity	ポートでサポートされるプロトコルを示します。
DCBX	Data center bridging exchangeプロトコルです。 🕮 **メモ：** QX-S1100GシリーズはDCBX TLVをサポートしていません。
EVB module	Edge Virtual Bridgingモジュールです。EVB TLV、CDCP TLVが含まれます。 🕮 **メモ：** QX-S1100GシリーズはEVB TLVをサポートしていません。

タイプ	説明
Link Aggregation	リンクアグリゲーションをサポートするポートかどうかを示します。サポートしている場合、リンクアグリゲーションが有効です。
Management VID	Management VLAN IDです。
VID Usage Digest	VLAN ID usage digestです。
ETS Configuration	Enhanced Transmission Selection configurationです。
ETS Recommendation	ETS recommendationです。
PFC	Priority-based Flow Controlです。
APP	Application protocolです。
QCN	Quantized Congestion Notificationです。 🕮 **メモ：** QX-S1100GシリーズはQCN TLVをサポートしていません。

🕮 **メモ：**

QX-S1100G シリーズは Protocol identity TLV と VLAN ID usage digest TLV を受信することができますが、TLV を送信することはできません。

- IEEE 802.3 組織指定 TLV

表 12-5 IEEE 802.3 組織指定 TLV

タイプ	説明
MAC/PHY Configuration/Status	送信するポートの通信速度、通信モード、オートネゴシエーションのサポート状況、オートネゴシエーションの状態、現在の通信速度、現在の通信モードの状態を示します。
Power Via MDI	ポートの電源供給状態を示します。 ● PoEタイプ（PSEあるいはPD） ● PoEモード ● PSE電源供給のサポート状況 ● PSE電源供給の有効/無効状態 ● PoEモードの管理可能/不可状態 ● 電力供給タイプ ● 電力ソース ● 電力優先度 ● PDが要求した電力 ● PSEが割り当てた電力
Maximum Frame Size	ポートでサポートされる最大フレームサイズ（MTU）を示します。
Power Stateful Control	送信ポートで管理される電源状態制御を示します。 ● PSE/PDの電源 ● PSE/PDの優先度 ● PSE/PDの電力
Energy-Efficient Ethernet	EEE（Energy Efficient Ethernet）を示します。

🕮 **メモ：**

Power Stateful Control TLV は IEEE802.3at Draft1.0 で定義されています。最近のバージョンでは Power Stateful Control TLV をサポートしていません。QX シリーズは Power Stateful Control TLV を受信した場合のみ送信を行います。

LLDP-MED TLV は複数のアプリケーションを VoIP（voice over IP）の拡張されたアプリケーションに提供します。たとえば基本設定、ネットワークポリシー設定、アドレス、ディレクトリ管理などのアプリケーションです。LLDP-MED TLV は Ethernet で音声装置の費用効果、使用しやすさのソリューションを提供します。表 12-6 に LLDP-MED TLV を示します。

表 12-6 LLDP-MED TLV

タイプ	説明
LLDP-MED Capabilities	LLDP-MED LEDをサポートするネットワークの装置がLLDP-MED LEDをアドバタイズすることを可能にします。
Network Policy	ポートのVLAN ID、VLANタイプ、指定アプリケーションのレイヤ2/レイヤ3の優先度を、ネットワーク装置あるいは端末装置がアドバタイズすることを可能にします。
Extended Power-via-MDI	ネットワーク装置あるいは端末装置が電源供給能力をアドバタイズすることを可能にします。TLVはPower Via MDI TLVの拡張です。
Hardware Revision	端末装置がハードウェアバージョンをアドバタイズすることを可能にします。
Firmware Revision	端末装置がファームウェアバージョンをアドバタイズすることを可能にします。
Software Revision	端末装置がソフトウェアバージョンをアドバタイズすることを可能にします。
Serial Number	端末装置がシリアル番号をアドバタイズすることを可能にします。
Manufacturer Name	端末装置がベンダ名をアドバタイズすることを可能にします。
Model Name	端末装置がモデル名をアドバタイズすることを可能にします。
Asset ID	端末装置がasset IDをアドバタイズすることを可能にします。一般的な使用方法として、ディレクトリ管理、価値のトラッキングを補助するためのエンドポイント用に指定されます。
Location Identification	位置をもとにしたアプリケーションの内容を使用するため、ネットワーク装置が端末装置の位置識別情報をアドバタイズすることを可能にします。

🕮 **メモ：**

- MAC/PHY configuration/status TLV がアドバタイズされない場合、LLDP-MED TLV をアドバタイズ可能でも LLDP-MED TLV はアドバタイズされません。
- LLDP-MED Capabilities TLV がアドバタイズできない場合、他の LLDP-MED TLV がアドバタイズ可能でもアドバタイズされません。

V. 管理アドレス

装置の管理アドレスは、ネットワークマネジメントシステムで使われ、トポロジ維持やネットワーク管理で装置を認識するために使われます。管理アドレスは、management address TLV にカプセル化されています。

12.1.2 動作メカニズム

I. LLDP 動作モード

LLDP エージェントは以下のモードを動作させることができます。

- **TxRx モード** – LLDP フレームの送信、受信を行うことができます。
- **Tx モード** – LLDP フレームの送信のみを行うことができます。
- **Rx モード** – LLDP フレームの受信のみを行うことができます。
- **Disable モード** – LLDP フレームの送信も受信も行うことができません。

LLDP エージェントの動作モードが変更されるたびに LLDP は初期化されます。設定可能な再初期化遅延時間を設定することにより、LLDP が頻繁に初期化されるのを防ぐことができます。再初期化遅延時間を設定する場合、LLDP は LLDP 動作モードが変更したのち、指定された期間が終了するまで再初期化を行いません。

II. LLDP フレームの送信

TxRx モードあるいは Tx モードで動作する LLDP エージェントは、定期的およびローカルの設定が変更される場合に、直接接続されている装置へ LLDP フレームを送信します。LLDP フレームがローカルの装置情報を頻繁に変更する際、ネットワークを占有してしまうことを防止するため、LLDP はトークンバケットメカニズムを使用して LLDP フレームを制限します。トークンバケットメカニズムの詳細は、オペレーションマニュアルのセクション 6 *ACL and QoS* ”*ラインレート*”を参照してください。

LLDP は自動的に以下のいずれかの場合を用いて、ただちに LLDP フレームを送信することができます。

- 新しい LLDP フレームが受信され、ローカル装置に新しい装置情報をアドバタイズする場合
- LLDP エージェントの LLDP 動作モードが Disable あるいは Rx から、TxRx あるいは Tx に変更される場合

このメカニズムでは、LLDP 隣接装置がローカル装置を発見できるように、指定した数の LLDP フレームが、設定可能なできるだけ早い送信間隔で連続して送信されます。装置は指定した数の LLDP フレームを送信した後、送信間隔を通常に戻します。

III. LLDP フレームの受信

TxRx モードまたは Rx モードで動作している LLDP エージェントは、受信した LLDP フレームを受信するたびに TLV の有効性を確認します。TLV が有効である場合、LLDP エージェントは情報を保存し、エージングタイマを開始します。エージングタイマのデフォルトは LLDP フレームによってアドバタイズされる Time To Live TLV の TTL と同じ値です。LLDP エージェントが新しい LLDP フレームを受信した場合、エージングタイマは再スタートします。LLDP フレームでアドバタイズされた Time To Live TLV の TTL が 0 になった場合、保存されているすべての情報はエージアウトします。

12.1.3 プロトコルと標準

- IEEE 802.1AB-2005, *Station and Media Access Control Connectivity Discovery*
- IEEE 802.1AB-2009, *Station and Media Access Control Connectivity Discovery*
- ANSI/TIA-1057, *Link Layer Discovery Protocol for Media Endpoint Devices*
- IEEE Std 802.1Qaz-2011, *Media Access Control (MAC) Bridges and Virtual Bridged Local Area Networks-Amendment 18: Enhanced Transmission Selection for Bandwidth Sharing Between Traffic Classes*

12.2 LLDP設定作業リスト

作業リスト
LLDPの基本設定： ● （必須設定項目） LLDPの有効化 ● （オプション設定項目） LLDP動作モードの設定 ● （オプション設定項目） 再初期化遅延時間の設定 ● （オプション設定項目） LLDPポーリングの有効化 ● （オプション設定項目） アドバタイズ可能なTLVの設定 ● （オプション設定項目） 管理アドレスの設定とカプセル化フォーマットの設定 ● （オプション設定項目） LLDPに関する他のパラメータの設定 ● （オプション設定項目） LLDPフレームのカプセル化フォーマットの設定
（オプション設定項目） CDP互換モードの設定
（オプション設定項目） LLDPトラップ、LLDP-MEDトラップの設定

12.3 LLDPの基本設定

12.3.1 LLDP の有効化

LLDP はポートで LLDP を有効にするには、ポートとグローバルの両方で有効にする必要があります。

以下に LLDP を有効化する設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． グローバルで LLDP を有効化する	**lldp global enable**	デフォルト：無効
3． Layer 2 Ethernet interface view あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	―
4． （オプション設定項目）LLDP を有効化する	**lldp enable**	デフォルト：有効

12.3.2 LLDP 動作モードの設定

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

操作	コマンド	補足
2． Layer 2 Ethernet interface view あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	―
3． 動作モードを設定する	● Layer 2 Ethernet interface view での設定： **lldp** [**agent nearest-customer**] **admin-status** { **disable** | **rx** | **tx** | **txrx** } ● aggregate interface viewでの設定： **lldp agent nearest-customer admin-status** { **disable** | **rx** | **tx** | **txrx** }	デフォルト： nearest bridgeエージェント：txrxモードです。 nearest customer bridgeエージェント：disableです。 Ethernet interface viewでエージェントタイプが指定されていない場合、nearest bridgeエージェントで動作モードを設定します。 aggregate interface viewではnearest customer bridgeエージェントの動作モードのみを設定できます。

12.3.3 再初期化遅延時間の設定

ポートの LLDP 動作モードを変更した場合、ポートは遅延時間の経過後、プロトコル状態を初期化します。再初期化遅延時間を設定することで、ポートの LLDP 動作モードが頻繁に変更されることを防ぐことができます。

以下に再初期化遅延時間の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． 再初期化遅延時間を設定する	**lldp timer reinit-delay** *delay*	デフォルト：2秒

12.3.4 LLDP ポーリングの有効化

LLDP ポーリングを有効にした装置はローカルの設定の変更を定期的に確認します。設定の変更を検出すると、装置は隣接装置へ変更を知らせるために LLDP フレームを送信します。

以下に LLDP ポーリングの有効化の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． Layer 2 Ethernet interface view あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	―

操作	コマンド	補足
3. LLDP ポーリングの有効化を設定する	• Layer 2 Ethernet interface view での設定： **lldp** [**agent nearest-customer**] **check-change-interval** *interval* • aggregate interface viewでの設定： **lldp agent nearest-customer check-change-interval** *interval*	デフォルト：無効

12.3.5 アドバタイズ可能な TLV の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. Layer 2 Ethernet interface view あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	—
3. LLDPDU TLV を設定する（Layer 2 Ethernet interface view）	• **lldp tlv-enable** { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [*ip-address* | **interface loopback** *interface-number*] } | **dot1-tlv** { **all** | **port-vlan-id** | **link-aggregation** | **vlan-name** [*vlan-id*] | **management-vid** [*mvlan-id*] } | **dot3-tlv** { **all** | **link-aggregation** | **mac-physic** | **max-frame-size** | **power** } | **med-tlv** { **all** | **capability** | **inventory** | **network-policy** [*vlan-id*] | **power-over-ethernet** | **location-id** { **civic-address** *device-type country-code* { *ca-type ca-value* }&<1-10> | **elin-address** *tel-number* } } } • **lldp agent nearest-customer tlv-enable** { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [*ip-address*] } | **dot1-tlv** { **all** | **port-vlan-id** | **link-aggregation** } | **dot3-tlv** { **all** | **link-aggregation** } }	デフォルト： • Nearest bridgeエージェントはlocation identification TLV, port VLAN ID TLV、protocol VLAN ID TLV、VLAN name TLV、management VLAN ID TLVを除いてすべてのLLDP TLVタイプを送信します。 • Nearest customer bridge エージェントはbasic TLV、IEEE 802.1 organizationally specific TLVを送信します。

操作	コマンド	補足
4． LLDPDU TLV を設定する（aggregate interface view）	● **lldp agent nearest-customer tlv-enable** { **basic-tlv** { **all** | **management-address-tlv** [*ip-address*] | **port-description** | **system-capability** | **system-description** | **system-name** } | **dot1-tlv** { **all** | **port-vlan-id** } } ● **lldp tlv-enable dot1-tlv** { **vlan-name** [*vlan-id*] | **management-vid** [*mvlan-id*] }	デフォルト： ● Nearest customer bridgeエージェントはbasic TLV、IEEE802.1組織指定TLV（VLAN name TLV、management VLAN ID TLVのみ）を送信します ● Nearest bridgeはアグリゲートインタフェースでサポートしていません。

12.3.6 管理アドレスの設定とカプセル化フォーマットの設定

LLDP は管理アドレス TLV の数値形式または string 形式でカプセル化します。

デフォルトでは、管理アドレス TLV は数値形式でカプセル化されています。隣接装置が管理アドレス TLV を string 形式でカプセル化している場合、管理アドレス TLV を string 形式でカプセル化することができます。これにより隣接装置と正常に通信することができます。

以下に管理アドレスのカプセル化フォーマットの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． Layer 2 Ethernet interface view あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	—
3． LLDPDU 内の管理アドレスの設定、管理アドレスの送信を設定する	● Layer 2 Ethernet interface viewでの設定： **lldp** [**agent nearest-customer**] **tlv-enable basic-tlv management-address-tlv** [*ip-address*] ● aggregate interface viewでの設定： **lldp agent nearest-customer** | **tlv-enable basic-tlv management-address-tlv** [*ip-address*]	デフォルト：nearest bridgeエージェントとnearest customer bridgeエージェントはLLDPDUの管理アドレスを送信します。
4． 管理アドレス TLV のカプセル化フォーマットを string 形式として設定する	● Layer 2 Ethernet interface viewでの設定： **lldp** [**agent nearest-customer**] **management-address-format string** ● aggregate interface viewでの設定： **lldp agent nearest-customer management-address-format string**	デフォルト：数値形式

12.3.7 LLDP に関する他のパラメータの設定

LLDPDU でアドバタイズされる Time To Live TLV は、LLDPDU の装置情報の有効時間を決定し、隣接装置で保存されます。

TTL の乗数を設定することにより、隣接装置に送信する LLDPDU の TTL の設定を行うことができます。隣接装置についての情報の TTL は以下の式によって定義されます。

TTL の乗数 × LLDP フレームの 送信間隔 ＋ 1

TTL は最大 65535 秒ということに注意してください。それより大きい場合、65535 秒に丸められます。

以下に LLDPDU に関するパラメータの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． TTL の乗数を設定する	**lldp hold-multiplier** *value*	デフォルト： 4
3． LLDP フレームの送信間隔を設定する	**lldp timer tx-interval** *interval*	デフォルト： 30秒
4． 新しい隣接装置を検出した場合の LLDP フレームの送信回数を設定する	**lldp fast-count** *count*	デフォルト： 4

12.3.8 LLDP フレームのカプセル化フォーマットの設定

LLDPDU は Ethernet II または SNAP フレームにカプセル化されます。

- **Ethernet II**－Ethernet II に設定した場合､LLDP ポートは Ethernet II フレームで LLDP フレームを送信します。
- **SNAP**－SNAP に設定した場合、LLDP ポートは SNAP フレームで LLDP フレームを送信します。

LLDP フレームを処理する初期バージョンの LLDP は、両端で同じカプセル化フォーマットが必要です。初期バージョンの LLDP で動作する装置に隣接したローカル装置は、初期バージョンの LLDP で動作する装置と同じカプセル化フォーマットで設定してください。

以下に SNAP に LLDP フレームのカプセル化フォーマットの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． Layer 2 Ethernet interface view あるいは Layer 2 aggregate interface view に移行する	**interface** *interface-type interface-number*	―
3． SNAP に LLDPDU のカプセル化フォーマットを設定する	● Layer 2 Ethernet interface view での設定： **lldp** [**agent nearest-customer**] **encapsulation snap** ● aggregate interface viewでの設定： **lldp agent nearest-customer encapsulation snap**	デフォルト： Ethernet II

12.4 CDP互換モードの設定

CDP のみをサポートしている Cisco 製品と装置が直接接続されている場合、情報を交換するため、CDP 互換モードを有効に設定することができます。

CDP 互換性モードを有効にした場合、装置は直接接続された装置から CDP パケットを受信し、隣接装置に CDP パケットを送信します。装置が隣接の CDP 装置に送信するパケットは、以下の情報があります。

- device ID
- 隣接装置に接続されているポートの ID
- ポートの IP アドレス
- TTL

ポートの IP アドレスは、VLAN インタフェースがアップ状態のプライマリ IP アドレスです。VLAN インタフェースの VLAN ID はポートで許可されている VLAN のなかでもっとも低い ID にする必要があります。許可された VLAN インタフェースに、IP アドレスが割り当てられていないあるいはすべてのインタフェースがダウンである場合、ポートの IP アドレスはアドバタイズされません。

display lldp neighbor-information コマンドの出力は、装置が認識できる CDP 隣接装置情報を示します。**display lldp neighbor-information** コマンドについての詳細は、コマンドマニュアルのセクション 2 *アクセス”LLDP*”を参照してください。

Cisco の IP 電話と情報を交換する場合、CDP 互換性モードを有効にする必要があります。

LLDP 対応装置が CDP パケットを認識できない場合、装置で設定された Voice VLAN ID の Cisco の IP 電話の要求に応答しません。その結果、Cisco の IP 電話の要求は、装置に VLAN タグなしで音声トラフィックを送信します。装置は音声トラフィックを他のタイプのトラフィックと区別することができません。

CDP の互換モードは、Cisco の IP 電話からの CDP パケットを受信して認識し、Voice VLAN の設定で TLV をアドバタイズする CDP パケットに応答するために有効にします。CDP パケット用に Voice VLAN が設定されていない場合、CDP パケットは、ポートの Voice VLAN あるいは RADIUS サーバによって割り当てられた Voice VLAN をアドバタイズします。割り当てられた Voice VLAN は高い優先度をもちます。Voice VLAN の設定の TLV に従い、IP 電話は自動で Voice VLAN を設定します。その結果、設定された Voice VLAN で音声トラフィックが制限され、他のタイプのトラフィックと区別されます。

Voice VLAN の詳細は、オペレーションマニュアルのセクション 2 *アクセス”Voice VLAN*”を参照してください。

装置がデータポートに接続されているホストをもつ Cisco の IP 電話に接続されている場合、ホストは Cisco の IP 電話を通してネットワークにアクセスする必要があります。データポートがダウンした場合、装置がユーザをログアウトさせるため IP 電話は装置に CDP パケットを送信します。

12.4.1 設定要件

CDP 互換モードの設定を行う前に、以下の設定を行ってください。

- グローバルで LLDP を有効にします。
- CDP をサポートする装置に接続するポートで LLDP を有効にします。
- ポートの LLDP の動作モードを TxRx モードに設定します。

12.4.2 設定手順

CDP 互換モードは以下のモードのいずれかで動作します。

- **TxRx**–CDP パケットを送受信できます。
- **Rx**–CDP パケットを送信できますが受信できません。
- **Disable**–CDP パケットを送受信できません。

指定したポートで CDP 互換モードの設定を行うために、以下の手順を設定します。

1) グローバルで CDP 互換モードを有効にします。
2) TxRx モードで動作するように CDP 互換モードの設定を行います。

CDP で許可される最大 TTL は 255 秒です。Cisco の IP 電話と一緒に運用するために、LLDP フレーム送信間隔の値は、CDP 互換モードの TTL 値の 1/3 以内にする必要があります。

以下に CDP 互換モードの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. グローバルで CDP 互換モードを有効にする	**lldp compliance cdp**	デフォルト：無効
3. Layer 2 Ethernet interface view に移行する	**interface** *interface-type interface-number*	―
4. CDP 互換モードの動作モードを TxRx モードに設定する	**lldp compliance admin-status cdp txrx**	デフォルト：無効

12.5 LLDPトラップの設定

LLDP トラップは、ネットワーク管理システムに新しい隣接装置の検知やリンクの故障などのイベントを知らせるために使用されます。

トポロジが不安定な場合、LLDP トラップの送信間隔の設定を変更することで、指定した時間内での過度な LLDP トラップの送信を防ぐことができます。

以下に LLDP トラップの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Layer 2 Ethernet interface view あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	―
3. LLDP トラップの送信を有効にする	● Layer 2 Ethernet interface view での設定： **lldp** [**agent nearest-customer**] **notification remote-change enable** ● aggregate interface viewでの設定： **lldp agent nearest-customer notification remote-change enable**	デフォルト：無効
4. system view に戻る	**quit**	―

操作	コマンド	補足
5.　（オプション設定項目）LLDP トラップの送信間隔を設定する	**lldp timer notification-interval** *interval*	デフォルト：30秒

12.6 LLDPの表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
ローカルLLDP情報を表示する	**display lldp local-information** [**global** | **interface** *interface-type interface-number*]
隣接装置から受信したLLDP TLVの情報を表示する	**display lldp neighbor-information** [[[**interface** *interface-type interface-number*] [**verbose**]] | **list** [**system-name** *system-name*]]
LLDPの統計情報を表示する	**display lldp statistics** [**global** | [**interface** *interface-type interface-number*]]
ポートのLLDPのステータスを表示する	**display lldp status** [**interface** *interface-type interface-number*]
現在送信されているLLDP TLVのタイプを表示する	**display lldp tlv-config** [**interface** *interface-type interface-number*]

12.7 LLDPの設定例

12.7.1 LLDP の基本的な設定例

I. ネットワーク要件

図 12-5 で示すように、NMS と Switch A は、同じイーサネットネットワークに接続されています。MED 装置と Switch B は、Switch A の GigabitEthernet 1/0/1 と GigabitEthernet 1/0/2 に接続しています。

Switch A と Switch B で以下の処理を実行するためグローバルで LLDP を有効にします。

- Switch A と Switch B のリンクをモニタします。
- Switch A と NMS の MED 装置のリンクをモニタします。

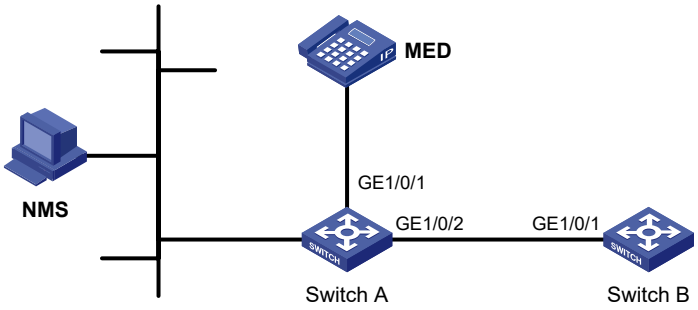


図 12-5 ネットワーク図

II. 設定手順

1) Switch A を設定します。

グローバルで LLDP を有効にします。

```
<SwitchA> system-view
[SwitchA] lldp global enable
```

GigabitEthernet 1/0/1 で LLDP を有効にします。デフォルトではポートで LLDP が有効です。

```
[SwitchA] interface gigabitethernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] lldp enable
```

GigabitEthernet 1/0/1 で LLDP の動作モードを Rx に設定します。

```
[SwitchA-GigabitEthernet1/0/1] lldp admin-status rx
[SwitchA-GigabitEthernet1/0/1] quit
```

GigabitEthernet 1/0/2 で LLDP を有効にします。デフォルトではポートで LLDP が有効です。

```
[SwitchA] interface gigabitethernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] lldp enable
```

GigabitEthernet 1/0/2 で LLDP の動作モードを Rx に設定します。

```
[SwitchA-GigabitEthernet1/0/2] lldp admin-status rx
[SwitchA-GigabitEthernet1/0/2] quit
```

2) Switch B を設定します。

グローバルで LLDP を有効にします。

```
<SwitchB> system-view
[SwitchB] lldp global enable
```

GigabitEthernet 1/0/1 で LLDP を有効にします。デフォルトではポートで LLDP が有効です。

```
[SwitchB] interface gigabitethernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] lldp enable
```

GigabitEthernet 1/0/1 で LLDP の動作モードを Tx に設定します。

```
[SwitchB-GigabitEthernet1/0/1] lldp admin-status tx
[SwitchB-GigabitEthernet1/0/1] quit
```

III. 設定の確認

以下のことを確認します。

- Switch A の GigabitEthernet 1/0/1 が MED 装置に接続しています。
- Switch A の GigabitEthernet 1/0/2 が非 MED 装置に接続しています。
- 両方のポートは Rx モードで動きます。つまり LLDP フレームの受信ができますが、LLDP フレームを送信できません。

[SwitchA] display lldp status

```
Global status of LLDP: Enable
Bridge mode of LLDP: customer-bridge
The current number of LLDP neighbors: 2
The current number of CDP neighbors: 0
LLDP neighbor information last changed time: 0 days, 0 hours, 4 minutes, 40 seconds
Transmit interval              : 30s
Fast transmit interval         : 1s
Transmit max credit            : 5
Hold multiplier                : 4
Reinit delay                   : 2s
Trap interval                  : 30s
Fast start times               : 4

LLDP status information of port 1 [GigabitEthernet1/0/1]:
LLDP agent nearest-bridge:
Port status of LLDP            : Enable
Admin status                   : Rx_Only
Trap flag                      : No
MED trap flag                  : No
Polling interval               : 0s
Number of LLDP neighbors       : 1
Number of MED neighbors        : 1
Number of CDP neighbors        : 0
Number of sent optional TLV    : 21
Number of received unknown TLV : 0

LLDP agent nearest-customer:
Port status of LLDP            : Enable
Admin status                   : Disable
Trap flag                      : No
MED trap flag                  : No
Polling interval               : 0s
Number of LLDP neighbors       : 0
Number of MED neighbors        : 0
Number of CDP neighbors        : 0
Number of sent optional TLV    : 16
Number of received unknown TLV : 0

LLDP status information of port 2 [GigabitEthernet1/0/2]:
LLDP agent nearest-bridge:
Port status of LLDP            : Enable
Admin status                   : Rx_Only
Trap flag                      : No
MED trap flag                  : No
Polling interval               : 0s
Number of LLDP neighbors       : 1
Number of MED neighbors        : 0
Number of CDP neighbors        : 0
Number of sent optional TLV    : 21
Number of received unknown TLV : 3

LLDP agent nearest-nontpmr:
Port status of LLDP            : Enable
Admin status                   : Disable
Trap flag                      : No
MED trap flag                  : No
Polling interval               : 0s
Number of LLDP neighbors       : 0
Number of MED neighbors        : 0
Number of CDP neighbors        : 0
Number of sent optional TLV    : 1
Number of received unknown TLV : 0

LLDP agent nearest-customer:
Port status of LLDP            : Enable
Admin status                   : Disable
Trap flag                      : No
MED trap flag                  : No
```

```
Polling interval               : 0s
Number of LLDP neighbors       : 0
Number of MED neighbors        : 0
Number of CDP neighbors        : 0
Number of sent optional TLV    : 16
Number of received unknown TLV : 0
```

Switch A と Switch B のリンクを切断します。

Switch A の GigabitEthernet 1/0/2 が隣接装置と接続していないことを確認します。

[SwitchA] display lldp status

```
Global status of LLDP: Enable
The current number of LLDP neighbors: 1
The current number of CDP neighbors: 0
LLDP neighbor information last changed time: 0 days, 0 hours, 5 minutes, 20 seconds
Transmit interval              : 30s
Fast transmit interval         : 1s
Transmit max credit            : 5
Hold multiplier                : 4
Reinit delay                   : 2s
Trap interval                  : 30s
Fast start times               : 4

LLDP status information of port 1 [GigabitEthernet1/0/1]:
LLDP agent nearest-bridge:
Port status of LLDP            : Enable
Admin status                   : Rx_Only
Trap flag                      : No
MED trap flag                  : No
Polling interval               : 0s
Number of LLDP neighbors       : 1
Number of MED neighbors        : 1
Number of CDP neighbors        : 0
Number of sent optional TLV    : 0
Number of received unknown TLV : 5

LLDP agent nearest-nontpmr:
Port status of LLDP            : Enable
Admin status                   : Disable
Trap flag                      : No
MED trap flag                  : No
Polling interval               : 0s
Number of LLDP neighbors       : 0
Number of MED neighbors        : 0
Number of CDP neighbors        : 0
Number of sent optional TLV    : 1
Number of received unknown TLV : 0

LLDP status information of port 2 [GigabitEthernet1/0/2]:
LLDP agent nearest-bridge:
Port status of LLDP            : Enable
Admin status                   : Rx_Only
Trap flag                      : No
MED trap flag                  : No
Polling interval               : 0s
Number of LLDP neighbors       : 0
Number of MED neighbors        : 0
Number of CDP neighbors        : 0
Number of sent optional TLV    : 0
Number of received unknown TLV : 0

LLDP agent nearest-nontpmr:
Port status of LLDP            : Enable
Admin status                   : Disable
Trap flag                      : No
MED trap flag                  : No
Polling interval               : 0s
Number of LLDP neighbors       : 0
```

```
Number of MED neighbors         : 0
Number of CDP neighbors         : 0
Number of sent optional TLV     : 1
Number of received unknown TLV : 0

LLDP agent nearest-customer:
Port status of LLDP             : Enable
Admin status                    : Disable
Trap flag                       : No
MED trap flag                   : No
Polling interval                : 0s
Number of LLDP neighbors        : 0
Number of MED neighbors         : 0
Number of CDP neighbors         : 0
Number of sent optional TLV     : 16
Number of received unknown TLV : 0
```

12.7.2 CDP 互換モードの設定例

I. ネットワーク要件

図 12-6 に示すように、Switch A の GigabitEthernet 1/0/1、GigabitEthernet 1/0/2 は VLAN タグがついた音声トラフィックを送信する Cisco の IP 電話に接続されています。

Switch A で Voice VLAN 2 を設定します。Cisco の IP 電話が Voice VLAN を自動で設定できるように Switch A で LLDP の CDP 互換モードを有効にします。Voice VLAN 機能は以下の動作を実行します。

- Voice VLAN に音声トラフィックを制限します。
- 他のトラフィックタイプから音声トラフィックを隔離します。

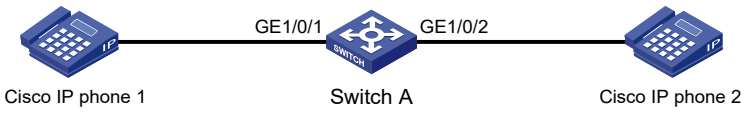


図 12-6 ネットワーク図

II. 設定手順

1) Switch A で Voice VLAN を設定します。

VLAN 2 を作成します。

```
<SwitchA> system-view
[SwitchA] vlan 2
[SwitchA-vlan2] quit
```

GigabitEthernet 1/0/1 と GigabitEthernet 1/0/2 のリンクタイプを trunk に設定し、Voice VLAN を有効にします。

```
[SwitchA] interface gigabitethernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] port link-type trunk
[SwitchA-GigabitEthernet1/0/1] voice vlan 2 enable
[SwitchA-GigabitEthernet1/0/1] quit
[SwitchA] interface gigabitethernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] port link-type trunk
```

```
[SwitchA-GigabitEthernet1/0/2] voice vlan 2 enable
[SwitchA-GigabitEthernet1/0/2] quit
```

2)　Switch A で CDP 互換モードを設定します。

グローバルで LLDP を有効にします。グローバルで CDP 互換モードを有効にします。

```
[SwitchA] lldp global enable
[SwitchA] lldp compliance cdp
```

GigabitEthernet 1/0/1 で LLDP を有効にします。デフォルトではポートで LLDP が有効です。

```
[SwitchA] interface gigabitethernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] lldp enable
```

GigabitEthernet 1/0/1 で LLDP の動作モードを TxRx に設定します。

```
[SwitchA-GigabitEthernet1/0/1] lldp admin-status txrx
```

GigabitEthernet 1/0/1 で LLDP の TxRx の動作モードで動作させるため、CDP 互換モードを設定します。

```
[SwitchA-GigabitEthernet1/0/1] lldp compliance admin-status cdp txrx
[SwitchA-GigabitEthernet1/0/1] quit
```

GigabitEthernet 1/0/2 で LLDP を有効にします。デフォルトではポートで LLDP が有効です。

```
[SwitchA] interface gigabitethernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] lldp enable
```

GigabitEthernet 1/0/2 で LLDP の動作モードを TxRx に設定します。

```
[SwitchA-GigabitEthernet1/0/2] lldp admin-status txrx
```

GigabitEthernet 1/0/2 で LLDP の TxRx の動作モードで動作させるため、CDP 互換モードを設定します。

```
[SwitchA-GigabitEthernet1/0/2] lldp compliance admin-status cdp txrx
[SwitchA-GigabitEthernet1/0/2] quit
```

III. 設定の確認

Switch A が以下の作業が完了していることを確認します。

- GigabitEthernet 1/0/1 と GigabitEthernet 1/0/2 に接続されている IP 電話を検出します。
- IP 電話の情報を取得します。

```
[SwitchA] display lldp neighbor-information

CDP neighbor-information of port 1[GigabitEthernet1/0/1]:
 CDP neighbor index  : 1
 Chassis ID          : SEP00141CBCDBFE
 Port ID             : Port 1
 Software version    : P0030301MFG2
 Platform            : Cisco IP Phone 7960
Duplex              : Full

CDP neighbor-information of port 2[GigabitEthernet1/0/2]:
```

```
CDP neighbor index  : 2
Chassis ID          : SEP00141CBCDBFF
Port ID             : Port 1
Software version    : P0030301MFG2
Platform            : Cisco IP Phone 7960
Duplex              : Full
```

目次

このセクションのページは**2-x-x** です。

13 章 L2PT 13-1
13.1 概要 13-1
13.1.1 背景 13-1
13.1.2 L2PT 動作メカニズム 13-2
13.2 L2PT 設定作業リスト 13-3
13.3 L2PT の有効化 13-3
13.3.1 制限事項とガイドライン 13-3
13.3.2 プロトコルでの L2PT の有効化 13-4
13.3.3 トンネルパケットの宛先マルチキャスト MAC アドレスの設定 13-5
13.4 L2PT の表示と維持 13-5
13.5 L2PT の設定例 13-5
13.5.1 STP での L2PT の設定 13-5

13章 L2PT

13.1 概要

L2PT（Layer 2 Protocol Tunneling）を使用すると地理的に分散されているカスタマネットワークをサービスプロバイダネットワーク経由でレイヤ 2 プロトコルパケットを送信できます。

13.1.1 背景

特定ユーザ向けのレイヤ 2 ネットワークを構築するため、サービスプロバイダネットワークで専用線が使用されます。その結果、カスタマネットワークはサービスプロバイダネットワークの異なるサイドに存在します。

図 13-1に示すようにCustomer Aネットワークはサービスプロバイダによって接続されているネットワーク 1 とネットワーク 2 に分割されています。Customer A ネットワークでレイヤ 2 プロトコルの計算を行うため、レイヤ 2 プロトコルのパケットはサービスプロバイダネットワークを通過して転送される必要があります。

PE がレイヤ 2 プロトコルパケットを受信した場合、PE はカスタマネットワークから受信されたパケットなのかサービスプロバイダネットワークからのパケットなのか判断することができません。このプロセス処理を行うため、CPU にパケットを転送する必要があります。この場合、Customer A ネットワークのレイヤ 2 プロトコルの計算は、サービスプロバイダネットワークのレイヤ 2 プロトコルの計算と一緒に行われます。カスタマネットワークあるいはサービスプロバイダネットワークのどちらも、独立してレイヤ 2 プロトコルの計算を行うことができません。

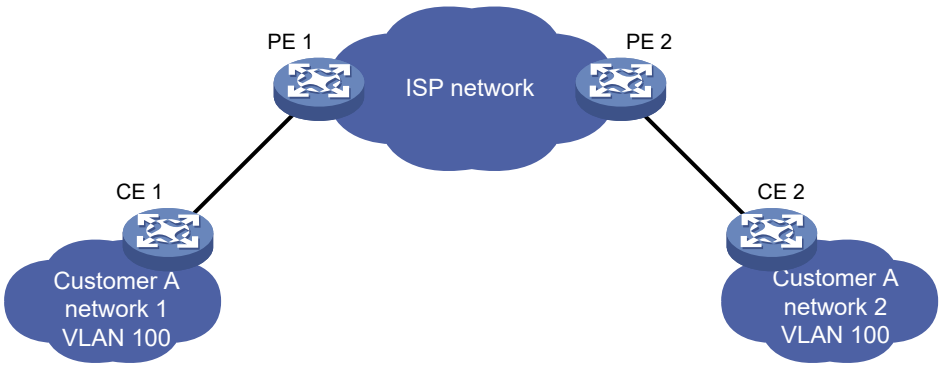


図 13-1 L2PT アプリケーションシナリオ

L2PT はこの問題を解決するために導入されました。L2PT は以下の機能を提供します。

- VLAN のカスタマネットワークからレイヤ 2 プロトコルパケットをマルチキャストします。分割されたカスタマネットワークは独立してレイヤ 2 プロトコルの計算を行うことができます。この計算はサービスプロバイダネットワークに対してトランスペアレントに行われます。
- 異なる VLAN を経由した異なるカスタマネットワークからのレイヤ 2 プロトコルパケットを分離します。

装置は以下のプロトコルを行うため L2PT をサポートします。

- CDP
- DLDP
- GVRP
- LACP
- LLDP
- MVRP
- PAgP
- PVST
- STP（STP、RSTP、MSTP を含みます）
- UDLD
- VTP

13.1.2 L2PT 動作メカニズム

図 13-2に示すように L2PT は以下のように動作します。

- VLAN の PE1 のポートがカスタマネットワークからレイヤ 2 プロトコルパケットを受信した場合、以下の処理を行います。
  - 受信ポートを除く VLAN のすべてのカスタマ側のポートにパケットをマルチキャストします。
  - パケットの宛先マルチキャスト MAC アドレスを指定されたマルチキャスト MAC アドレスに変更し、VLAN のすべての ISP 側のポートにパケットをマルチキャストします。変更されたパケットはトンネルパケットと呼ばれます。
- VLAN の PE2 のポートがサービスプロバイダネットワークからトンネルパケットを受信した場合、以下の処理を行います。
  - 受信ポートを除く VLAN のすべての ISP 側のポートにパケットをマルチキャストします。
  - パケットの宛先マルチキャスト MAC アドレスをもとの MAC アドレスに変更し、VLAN のすべてのカスタマ側のポートにパケットをマルチキャストします。

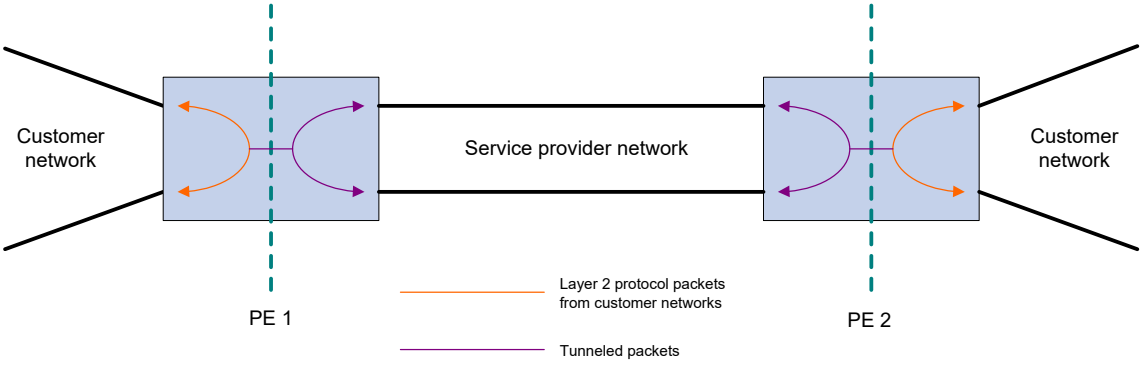


図 13-2 L2PT 動作メカニズム

たとえば、図 13-3に示すように PE1 はネットワーク 1 からネットワーク 2 への STP パケット（BPDU）を受信します。CE はカスタマネットワークの Edge 装置、PE はサービスプロバイダネットワークの Edge 装置です。L2PT は以下のようにパケットを処理します。

1) PE1 は以下の処理を行います。

   a) パケットの宛先MACアドレス0180-c200-0000を、BPDUの指定したマルチキャストMACアドレス（デフォルトは010f-e200-0003）に変更します。

   b) パケットのVLANのすべてのISP側のポートにトンネルパケットを送信します。

2) トンネルパケットを受信すると、PE2 はパケットを復号化し、CE2 に BPDU を送信します。

L2PT を通して ISP ネットワークと Customer A ネットワークは独立したスパニングツリーの計算を行うことができます。

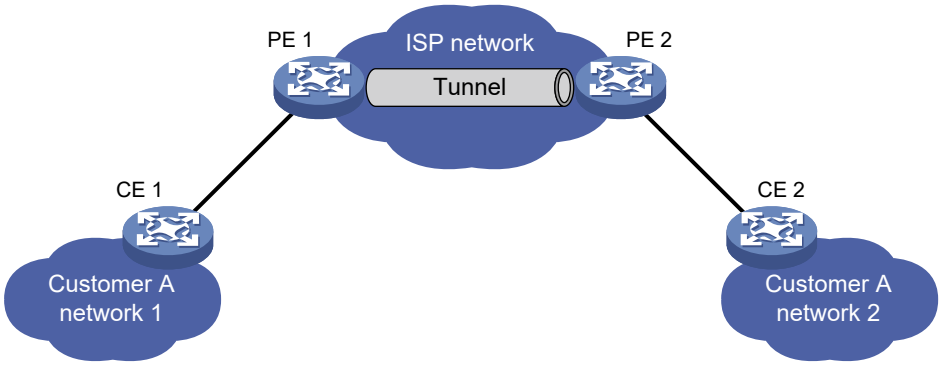


図 13-3 L2PT ネットワーク図

13.2 L2PT設定作業リスト

作業リスト
（必須設定項目）プロトコルでのL2PTの有効化
（オプション設定項目）トンネルパケットの宛先マルチキャストMACアドレスの設定

13.3 L2PTの有効化

13.3.1 制限事項とガイドライン

- ポートのレイヤ 2 プロトコルで L2PT を有効にする前に以下の処理を行ってください。
  - □ 接続された CE のプロトコルを有効にし、ポートでプロトコルを無効にしてください。
  - □ 以下の条件において、CE 上のアグリゲーションインタフェースと接続している PE ポートでは STP などのプロトコルを無効にしてください。
    - プロトコルは CE 上のアグリゲーションインタフェースで動作しています。

- CE 上のアグリゲーションインタフェースが PE 上の L2PT 対応のインタフェースに接続しています。

□ カスタマネットワークに接続された PE ポートで L2PT を有効にしてください。サービスプロバイダネットワークに接続されているポートで L2PT を有効にした場合、L2PT はポートがカスタマネットワークに接続されていると認識します。

□ トンネルパケットがサービスプロバイダネットワークを通して正常に転送できるようにするため、レイヤ 2 プロトコルパケットの VLAN タグが変更あるいは削除されていないことを確認してください。

- L2PT は nearest bridge エージェントのみからの LLDP パケットをサポートします。
- アグリゲーショングループのメンバポートで L2PT の設定を入力することができますが、設定は適用されません。

13.3.2 プロトコルでの L2PT の有効化

I. 制限事項とガイドライン

LACP は Point-to-Point の通信を必要としていますが、L2PT を LACP のインタフェース上で使用する場合は、L2PT はカスタマ側のポートから LACP をマルチキャストします。

2 つの CE 間の通信は Point-to-Point ではないため、LACP パケットを Point-to-Point の通信を保証するには別の機能を使用する必要があります。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. interface view に移行する	• Ethernet interface viewに移行する： **interface** *interface-type interface-number* • aggregate interface viewに移行する： **interface bridge-aggregation** *interface-type interface-number*	―
3. プロトコルの L2PT を有効にする	• Ethernet interface view： **l2protocol** { **cdp** | **dldp** | **gvrp** | **lacp** | **lldp** | **mvrp** | **pagp** | **pvst** | **stp** | **udld** | **vtp** } **tunnel dot1q** • aggregate interface view： **l2protocol** { **gvrp** | **mvrp** | **pvst** | **stp** | **vtp** } **tunnel dot1q**	デフォルト：無効

13.3.3 トンネルパケットの宛先マルチキャスト MAC アドレスの設定

I. 宛先マルチキャスト MAC アドレスについて

使用可能なマルチキャスト MAC アドレスは 010f-e200-0003、0100-0ccd-cdd0、0100-0ccd-cdd1、0100-0ccd-cdd2 です。

II. 制限事項とガイドライン

- トンネルパケットを認識するため、同一カスタマネットワークに接続されている PE では同一の宛先マルチキャスト MAC アドレスを設定してください。
- 異なるカスタマネットワークに接続されている PE では異なる宛先マルチキャスト MAC アドレスを設定します。そのため L2PT は、カスタマネットワークのパケットから、別のカスタマネットワークにパケットを送信することを防ぎます。

III. 設定手順

以下にトンネルパケットの宛先マルチキャスト MAC アドレスの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． トンネルパケットの宛先マルチキャスト MAC アドレスを設定する	**l2protocol tunnel-dmac** *mac-address*	デフォルト：010f-e200-0003

13.4 L2PTの表示と維持

すべての view で **display** コマンドを実行し、user view で **reset** コマンドを実行できます。

操作	コマンド
L2PTの統計情報を表示する	**display l2protocol statistics** [**interface** *interface-type interface-number*]
L2PTの統計情報を削除する	**reset l2protocol statistics** [**interface** *interface-type interface-number*]

13.5 L2PTの設定例

13.5.1 STP での L2PT の設定

I. ネットワーク要件

図 13-4に示すように、CE1 の MAC アドレスは f474-8802-5800、CE2 の MAC アドレスは f474-8802-5802 です。Customer A ネットワークでは MSTP が使用されています。

PE で以下の処理を行います。

- CE に接続するポートをアクセスポートとして設定し、サービスプロバイダネットワークのポートをトランクポートとして設定します。サービスプロバイダネットワークのポートはすべての VLAN からのパケットを許可します。

- サービスプロバイダネットワークを通して、Customer A ネットワークで独立してスパニングツリーの計算を行うため、STP の L2PT を有効にします。
- トンネルパケットの宛先マルチキャスト MAC アドレスを 0100-0ccd-cdd0 に設定します。

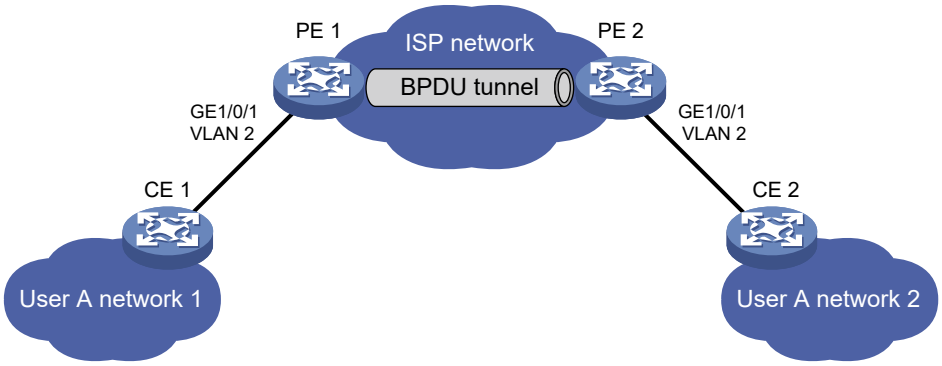


図 13-4 ネットワーク図

II. 設定手順

1)　PE1 を設定します。

トンネルパケットの宛先マルチキャスト MAC アドレスを 0100-0ccd-cdd0 に設定します。

```
<PE1> system-view
[PE1] l2protocol tunnel-dmac 0100-0ccd-cdd0
```

VLAN 2 を作成します。

```
[PE1] vlan 2
[PE1-vlan2] quit
```

GigabitEthernet 1/0/1 をアクセスポートとして設定し、VLAN 2 に割り当てます。

```
[PE1] interface gigabitethernet 1/0/1
[PE1-GigabitEthernet1/0/1] port access vlan 2
```

GigabitEthernet 1/0/1 で STP を無効にし、STP の L2PT を有効にします。

```
[PE1-GigabitEthernet1/0/1] undo stp enable
[PE1-GigabitEthernet1/0/1] l2protocol stp tunnel dot1q
[PE1-GigabitEthernet1/0/1] quit
```

サービスプロバイダに接続されている GigabitEthernet 1/0/2 をトランクポートとして設定し、すべての VLAN に割り当てます。

```
[PE1] interface gigabitethernet 1/0/2
[PE1-GigabitEthernet1/0/2] port link-type trunk
[PE1-GigabitEthernet1/0/2] port trunk permit vlan all
[PE1-GigabitEthernet1/0/2] quit
```

2) PE1 を PE1 の設定と同様に設定します。（詳細は省略します。）

III. 設定の確認

Customer A ネットワークのルートブリッジが CE1 であることを確認します。

```
<CE2> display stp root
 MST ID   Root Bridge ID        ExtPathCost IntPathCost Root Port
 0        32768.f474-8802-5800  0           0
```

サービスプロバイダネットワークのルートブリッジが CE1 でないことを確認します。

```
[PE1] display stp root
 MST ID   Root Bridge ID        ExtPathCost IntPathCost Root Port
 0        32768.0cda-41c5-ba50  0           0
```

目次

このセクションのページは**2-x-x** です。

14 章 Private VLAN 14-1
14.1 概要 14-1
14.2 制限とガイドライン 14-2
14.3 Private VLAN 設定作業リスト 14-2
14.4 プライマリ VLAN の作成 14-2
14.5 セカンダリ VLAN の作成 14-3
14.6 プライマリ VLAN とセカンダリ VLAN の関連付け 14-3
14.7 アップリンクポートの設定 14-3
14.7.1 アップリンクポートについて 14-3
14.7.2 設定手順 14-3
14.8 ダウンリンクポートの設定 14-4
14.8.1 ダウンリンクポートについて 14-4
14.8.2 設定手順 14-4
14.9 セカンダリ VLAN 間のレイヤ 3 通信の設定 14-5
14.10 Private VLAN の表示と維持 14-5
14.11 Private VLAN 設定例 14-5
14.11.1 プロミスカスポートの設定例 14-5
14.11.2 トランクプロミスカスポートの設定例 14-9
14.11.3 トランクプロミスカスとトランクセカンダリの設定例 14-12
14.11.4 セカンダリ VLAN でのレイヤ 3 通信の 設定例 14-16

14章 Private VLAN

14.1 概要

VLAN 機能はカスタマからトラフィックを分離するための方法を提供します。ネットワークのアクセスレイヤでは、セキュリティ確保等の目的でカスタマトラフィックを分離する必要があります。VLAN がユーザ単位に割り当てられている場合、多数の VLAN が必要になります。Private VLAN 機能は VLAN を 2 層構成にすることで VLAN のリソースを抑えることができます。

- **プライマリ VLAN**：アップリンクに接続するために使用します。プライマリ VLAN は複数のセカンダリ VLAN を関連付けできアップリンクの装置はプライマリ VLAN が指定されています。
- **セカンダリ VLANs**：ユーザ側に接続するために使用します。セカンダリ VLAN はレイヤ 2 で分離されます。プライマリ VLAN と関連付けたセカンダリ VLAN の間でレイヤ 3 通信を実現するためには、アップリンク装置ではローカルプロキシ ARP を有効にしてください。

図 14-1のように、Private VLAN 機能は L2 Device B で有効にします。VLAN10 はプライマリ VLAN、VLAN2、5、8 は VLAN10 のセカンダリ VLAN に関連付けられます。L3 Device A は VLAN10 のみ認識します。

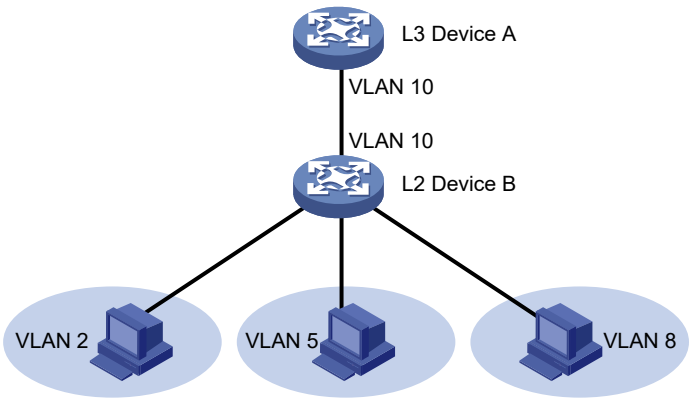


図 14-1 Private VLAN 例

Private VLAN 機能をレイヤ 3 装置上で設定する場合、レイヤ 3 通信を有効にするために以下の方法のいずれかを使用してください。レイヤ 3 通信は同じプライマリ VLAN に関連付けられたセカンダリ VLAN 間や他のネットワークの間で必要となる場合があります。

I. 方法 1:

- セカンダリ VLAN に VLAN インタフェースを作成します。
- セカンダリ VLAN インタフェースに IP アドレスを作成します。

II. 方法 2:

- プライマリ VLAN と関連付けられたセカンダリ VLAN 間でレイヤ 3 通信を有効にします。
- プライマリ VLAN の VLAN インタフェースを作成して、IP アドレスを作成します。（この方法を使用する場合は、セカンダリ VLAN インタフェースを作成しないでください。）
- プライマリ VLAN インタフェースでローカルプロキシ ARP を有効にします。

14.2 制限とガイドライン

- 以下の要件が満たされていることを確認してください。
  - プロミスカスポートの場合
    - プライマリ VLAN はそのポートの PVID であること。
    - そのポートがプライマリ VLAN とセカンダリ VLAN の untagged メンバであること。
  - ホストポートの場合
    - そのポートの PVID はセカンダリ VLAN であること。
    - そのポートはプライマリ VLAN とセカンダリ VLAN の untagged メンバであること。
  - トランクプロミスカスまたはトランクセカンダリポートはプライマリ VLAN とセカンダリ VLAN の tagged メンバであること。
- VLAN1（システムデフォルト VLAN）は Private VLAN 設定をサポートしていません。

14.3 Private VLAN設定作業リスト

作業リスト
（必須設定項目）プライマリVLANの作成
（必須設定項目）セカンダリVLANの作成
（必須設定項目）プライマリVLANとセカンダリVLANの関連付け
（必須設定項目）アップリンクポートの設定
（必須設定項目）ダウンリンクポートの設定
（オプション設定項目）セカンダリVLAN間のレイヤ3通信の設定

14.4 プライマリVLANの作成

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. VLAN を作成し、view へ移行する	**vlan** *vlan-id*	―
3. プライマリ VLAN を作成する	**private-vlan primary**	デフォルト： VLANはプライマリVLANではありません。

14.5 セカンダリVLANの作成

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． VLAN を作成し、view へ移行する	**vlan** { *vlan-id-list* | **all** }	―

14.6 プライマリVLANとセカンダリVLANの関連付け

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． VLAN を作成し、プライマリ VLAN の view へ移行する	**vlan** *vlan-id*	―
3． プライマリ VLAN にセカンダリ VLAN を関連付ける	**private-vlan secondary** *vlan-id-list*	デフォルト：設定なし

14.7 アップリンクポートの設定

14.7.1 アップリンクポートについて

アップリンクポートを以下に従い設定します。

- 1 つだけプライマリ VLAN を許可する場合は、ポートをプライマリ VLAN のプロミスカスポートとして設定し、プロミスカスポートはプライマリ VLAN と関連付けられたセカンダリポートに自動的に割り当てられます。
- 複数のプライマリポートを許可する場合は、ポートをプライマリ VLAN のトランクプロミスカスポートとして設定します。トランクプロミスカスポートはプライマリ VLAN と関連付けられたセカンダリポートに自動的に割り当てられます。

14.7.2 設定手順

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． アップリンクポートの interface view に移行する	**interface** *interface-type interface-number*	―
3． アップリンクポートを指定した VLAN のプロミスカスポートまたはトランクプロミスカスポートに設定する	● プロミスカスポートを設定する場合： **port private-vlan** *vlan-id* **promiscuous** ● トランクプロミスカスポートを設定する場合： **port private-vlan** *vlan-id-list* **trunk promiscuous**	デフォルト：設定なし

14.8 ダウンリンクポートの設定

14.8.1 ダウンリンクポートについて

ダウンリンクポートを以下に従い設定します。

- ダウンリンクポートを 1 つのセカンダリ VLAN のみを許可する場合、そのポートはホストポートとして設定してください。セカンダリ VLAN と関連付けたプライマリ VLAN が自動的に設定されます。
- ダウンリンクポートを複数のセカンダリ VLAN で許可する場合、そのポートはトランクセカンダリポートとして設定してください。セカンダリ VLAN と関連付けたプライマリ VLAN が自動的に設定されます。

14.8.2 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. アップリンクポートの interface view に移行する	**interface** *interface-type interface-number*	―
3. ダウンリンクポートをセカンダリ VLAN に設定する	1. リンクタイプを設定する： **port link-type** { **access** | **hybrid** | **trunk** } 2. アクセス VLAN を設定する： **port access vlan** *vlan-id* 3. トランクポートで許可する VLAN を設定する： **port trunk permit vlan** { *vlan-id-list* | **all** } 4. ハイブリッドポートの VLAN を設定する： **port hybrid vlan** *vlan-id-list* { **tagged** | **untagged** } 2、3、4はリンクタイプの設定に依存します。	デフォルト：設定なし
4. ダウンリンクポートをホストポートまたはトランクセカンダリポートに設定する	1. ホストポートに設定する： **port private-vlan host** 2. トランクセカンダリポートに設定する： **port private-vlan** *vlan-id-list* **trunk secondary**	デフォルト：設定なし
5. System view に戻る	**quit**	―
6. セカンダリ VLAN の VLAN view へ移行する	**vlan** *vlan-id*	―
7. 同じセカンダリ VLAN のポート間でレイヤ 2 通信を有効にする	**undo private-vlan isolated**	(オプション設定項目) デフォルト：レイヤ2通信が可能

14.9 セカンダリVLAN間のレイヤ3通信の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． プライマリ VLAN の VLAN interface view へ移行する	**interface vlan-interface** *interface-number*	―
3． プライマリ VLAN と関連付けたセカンダリ VLAN 間のレイヤ 3 通信を有効にする	**private-vlan secondary** *vlan-id-list*	デフォルト：無効
4． プライマリ VLAN インタフェースに IP アドレスを設定する	**ip address** *ip-address* { *mask-length* | *mask* } [**sub**]	デフォルト：設定なし
5． ローカルプロキシ ARP を設定する	**local-proxy-arp enable**	デフォルト：無効

14.10 Private VLANの表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
プライマリVLANとセカンダリVLANの関連付け情報を表示する	**display private-vlan** [*primary-vlan-id]*

14.11 Private VLAN設定例

14.11.1 プロミスカスポートの設定例

I. ネットワーク要件

図 14-2に示すように設定します。

- Device B は、VLAN5 をプライマリ VLAN としてセカンダリ VLAN に VLAN2 と 3 を関連付けます。GigabitEthernet 1/0/5は VLAN 5、GigabitEthernet 1/0/2は VLAN 2、GigabitEthernet 1/0/3 は VLAN 3 を割り当てます。
- Device C は、VLAN6 をプライマリ VLAN としてセカンダリ VLAN に VLAN3 と 4 を関連付けます。GigabitEthernet 1/0/5は VLAN 6、GigabitEthernet 1/0/3は VLAN 3、GigabitEthernet 1/0/4は VLAN 4 を割り当てます。
- Device A は Device B の VLAN 5、Device C の VLAN 6 に接続します。

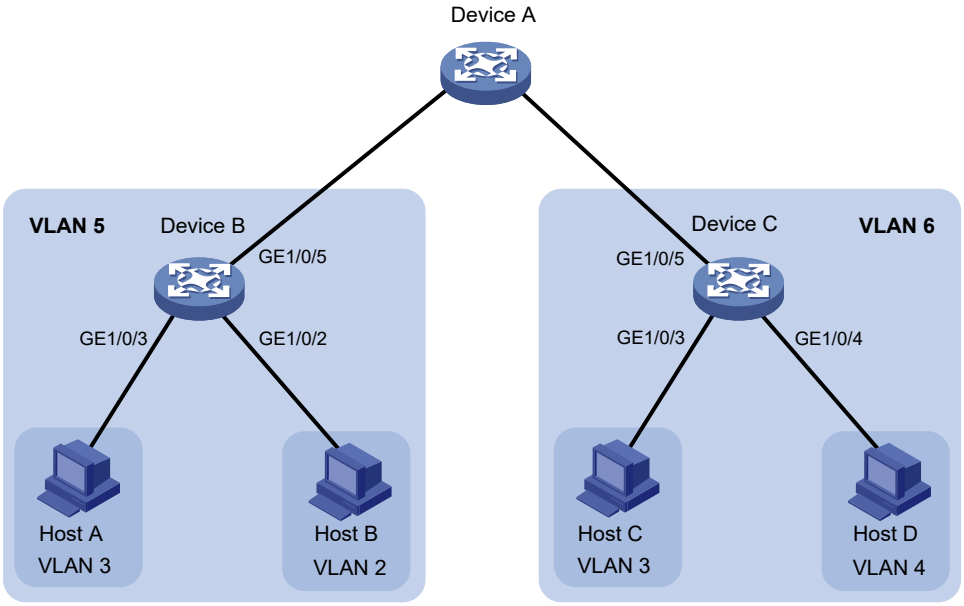


図 14-2 ネットワーク図

II. 設定手順

1)　Device B を設定します。

VLAN5 をプライマリ VLAN に設定します。

```
<DeviceB> system-view
[DeviceB] vlan 5
[DeviceB-vlan5] private-vlan primary
[DeviceB-vlan5] quit
```

VLAN2 と 3 を作成します。

```
[DeviceB] vlan 2 to 3
```

VLAN2 と 3 をプライマリ VLAN5 のセカンダリ VLAN に設定します。

```
[DeviceB] vlan 5
[DeviceB-vlan5] private-vlan secondary 2 to 3
[DeviceB-vlan5] quit
```

GigabitEthernet 1/0/5を VLAN5 のプロミスカスポートに設定します。

```
[DeviceB] interface gigabitethernet 1/0/5
[DeviceB-GigabitEthernet1/0/5] port private-vlan 5 promiscuous
[DeviceB-GigabitEthernet1/0/5] quit
```

GigabitEthernet 1/0/2を VLAN2 に割り当てホストポートに設定します。[DeviceB] interface gigabitethernet 1/0/2

```
[DeviceB-GigabitEthernet1/0/2] port access vlan 2
[DeviceB-GigabitEthernet1/0/2] port private-vlan host
[DeviceB-GigabitEthernet1/0/2] quit
```

GigabitEthernet 1/0/3 を VLAN 3 に割り当てホストポートに設定します。

```
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] port access vlan 3
[DeviceB-GigabitEthernet1/0/3] port private-vlan host
[DeviceB-GigabitEthernet1/0/3] quit
```

2) Device C を設定します。

VLAN6 をプライマリ VLAN に設定します。

```
<DeviceC> system-view
[DeviceC] vlan 6
[DeviceC–vlan6] private-vlan primary
[DeviceC–vlan6] quit
```

VLAN3 と 4 を作成します。

```
[DeviceC] vlan 3 to 4
```

VLAN3 と 4 をプライマリ VLAN6 のセカンダリ VLAN に設定します。

```
[DeviceC] vlan 6
[DeviceC-vlan6] private-vlan secondary 3 to 4
[DeviceC-vlan6] quit
```

GigabitEthernet 1/0/5を VLAN6 のプロミスカスポートに設定します。

```
[DeviceC] interface gigabitethernet 1/0/5
[DeviceC-GigabitEthernet1/0/5] port private-vlan 6 promiscuous
[DeviceC-GigabitEthernet1/0/5] quit
```

GigabitEthernet 1/0/3を VLAN 3 に割り当てホストポートに設定します。

```
[DeviceC] interface gigabitethernet 1/0/3
[DeviceC-GigabitEthernet1/0/3] port access vlan 3
[DeviceC-GigabitEthernet1/0/3] port private-vlan host
[DeviceC-GigabitEthernet1/0/3] quit
```

GigabitEthernet 1/0/4を VLAN 4 に割り当て、ホストポートに設定します。

```
[DeviceC] interface gigabitethernet 1/0/4
[DeviceC-GigabitEthernet1/0/4] port access vlan 4
```

```
[DeviceC-GigabitEthernet1/0/4] port private-vlan host
[DeviceC-GigabitEthernet1/0/4] quit
```

III. 設定の確認

Private VLAN が装置に設定されていることを確認します（Device B を例とします）。

```
[DeviceB] display private-vlan
Primary VLAN ID: 5
Secondary VLAN ID: 2-3

VLAN ID: 5
VLAN type: Static
Private VLAN type: Primary
Route interface: Not configured
Description: VLAN 0005
Name: VLAN 0005
Tagged ports:   None
Untagged ports:
   GigabitEthernet1/0/2
   GigabitEthernet1/0/3
   GigabitEthernet1/0/5

VLAN ID: 2
VLAN type: Static
Private VLAN type: Secondary
Route interface: Not configured
Description: VLAN 0002
Name: VLAN 0002
Tagged ports:   None
Untagged ports:
   GigabitEthernet1/0/2
   GigabitEthernet1/0/5

VLAN ID: 3
VLAN type: Static
Private VLAN type: Secondary
Route interface: Not configured
Description: VLAN 0003
Name: VLAN 0003
Tagged Ports:   None
Untagged Ports:
   GigabitEthernet1/0/3
   GigabitEthernet1/0/5
```

出力は以下を示します。

- プロミスカスポート(GigabitEthernet 1/0/5) はプライマリ VLAN5 とセカンダリ VLAN2 と 3 の untagged メンバです。
- ホストポート(GigabitEthernet 1/0/2)はプライマリ VLAN5 とセカンダリ VLAN2 の untagged メンバです。
- ホストポート(GigabitEthernet 1/0/3)はプライマリ VLAN5 is an untagged member of primary VLAN 5 and secondary VLAN 3.

14.11.2 トランクプロミスカスポートの設定例

I. ネットワーク要件

図 14-3に示すように設定します。

- VLAN5 と VLAN10 を Device B のプライマリ VLAN とします。Device B のアップリンクポート(GigabitEthernet 1/0/1) は VLAN5 と VLAN10 から VLAN タグ付きパケットの転送を許可します。
- Device B は、ダウンリンクポート(GigabitEthernet 1/0/2)でセカンダリ VLAN2 を許可します。ダウンリンクポート(GigabitEthernet 1/0/3)でセカンダリ VLAN3 を許可します。セカンダリ VLAN2 と 3 はプライマリ VLAN5 に関連付けられています。
- Device B は、ダウンリンクポート(GigabitEthernet 1/0/4)でセカンダリ VLAN6 を許可します。ダウンリンクポート(GigabitEthernet 1/0/5)でセカンダリ VLAN8 を許可します。セカンダリ VLAN6 と 8 はプライマリ VLAN10 に関連付けられています。
- Device A は Device B の VLAN5 と 10 に接続します。

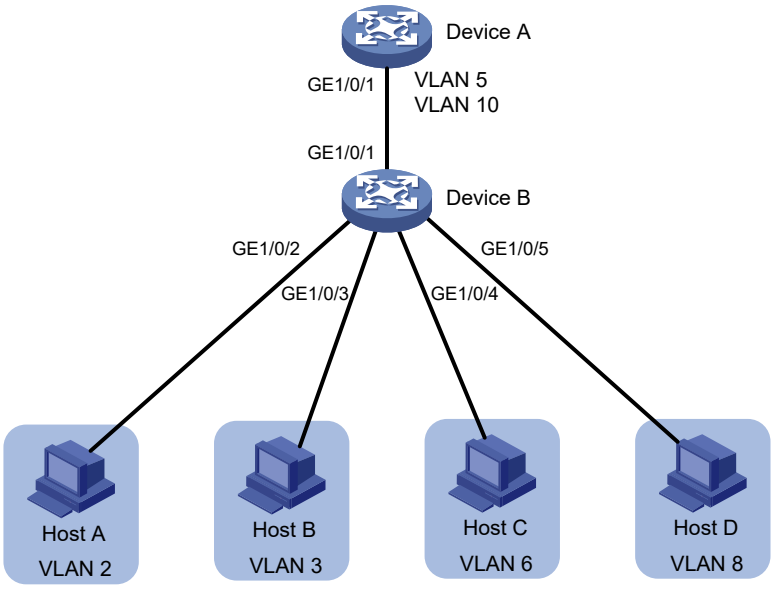


図 14-3 ネットワーク図

II. 設定手順

1)　Device B を設定します。

VLAN5 と 10 をプライマリ VLAN に設定します。

```
<DeviceB> system-view
[DeviceB] vlan 5
[DeviceB-vlan5] private-vlan primary
[DeviceB-vlan5] quit
[DeviceB] vlan 10
```

```
[DeviceB-vlan10] private-vlan primary
[DeviceB-vlan10] quit
```

VLAN2、3、6、8 を作成します。

```
[DeviceB] vlan 2 to 3
[DeviceB] vlan 6
[DeviceB-vlan6] quit
[DeviceB] vlan 8
[DeviceB-vlan8] quit
```

セカンダリ VLAN2 と 3 をプライマリ VLAN5 に関連付けます。

```
[DeviceB] vlan 5
[DeviceB-vlan5] private-vlan secondary 2 to 3
[DeviceB-vlan5] quit
```

セカンダリ VLAN6 と 8 をプライマリ VLAN10 に関連付けます。

```
[DeviceB] vlan 10
[DeviceB-vlan10] private-vlan secondary 6 8
[DeviceB-vlan10] quit
```

GigabitEthernet 1/0/1 を VLAN5 と 10 のトランクプロミスカスポートに設定します。

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port private-vlan 5 10 trunk promiscuous
[DeviceB-GigabitEthernet1/0/1] quit
```

GigabitEthernet 1/0/2 を VLAN2 に割り当て、ホストポートに設定します。

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] port access vlan 2
[DeviceB-GigabitEthernet1/0/2] port private-vlan host
[DeviceB-GigabitEthernet1/0/2] quit
```

GigabitEthernet 1/0/3 を VLAN 3 に割り当て、ホストポートに設定します。

```
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] port access vlan 3
[DeviceB-GigabitEthernet1/0/3] port private-vlan host
[DeviceB-GigabitEthernet1/0/3] quit
```

GigabitEthernet 1/0/4 を VLAN 6 に割り当て、ホストポートに設定します。

```
[DeviceB] interface gigabitethernet 1/0/4
[DeviceB-GigabitEthernet1/0/4] port access vlan 6
```

```
[DeviceB-GigabitEthernet1/0/4] port private-vlan host
[DeviceB-GigabitEthernet1/0/4] quit
```

GigabitEthernet 1/0/5 を VLAN 8 に割り当て、ホストポートに設定します。

```
[DeviceB] interface gigabitethernet 1/0/5
[DeviceB-GigabitEthernet1/0/5] port access vlan 8
[DeviceB-GigabitEthernet1/0/5] port private-vlan host
[DeviceB-GigabitEthernet1/0/5] quit
```

2) Device A を設定します。

VLAN5 と 10 を作成します。

```
[DeviceA] vlan 5
[DeviceA-vlan5] quit
[DeviceA] vlan 10
[DeviceA-vlan10] quit
```

GigabitEthernet 1/0/1 をハイブリッドポートに設定して、VLAN5 と 10 を tagged メンバとして割り当てます。

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-type hybrid
[DeviceA-GigabitEthernet1/0/1] port hybrid vlan 5 10 tagged
[DeviceA-GigabitEthernet1/0/1] quit
```

III. 設定の確認

Device B のプライマリ VLAN 情報を確認します（プライマリ VLAN5 を例とします）。

```
[DeviceB] display private-vlan 5
Primary VLAN ID: 5
Secondary VLAN ID: 2-3

VLAN ID: 5
VLAN type: Static
Private VLAN type: Primary
Route interface: Not configured
Description: VLAN 0005
Name: VLAN 0005
Tagged ports:
   GigabitEthernet1/0/1
Untagged ports:
   GigabitEthernet1/0/2
   GigabitEthernet1/0/3

VLAN ID: 2
VLAN type: Static
Private VLAN type: Secondary
Route interface: Not configured
Description: VLAN 0002
Name: VLAN 0002
Tagged ports:
   GigabitEthernet1/0/1
```

```
Untagged ports:
   GigabitEthernet1/0/2

VLAN ID: 3
VLAN type: Static
Private VLAN type: Secondary
Route interface: Not configured
Description: VLAN 0003
Name: VLAN 0003
Tagged ports:
   GigabitEthernet1/0/1
Untagged ports:
   GigabitEthernet1/0/3
```

出力は以下を示します。

- トランクプロミスカスポート(GigabitEthernet 1/0/1)はプライマリ VLAN5 とセカンダリ VLAN2 と 3 の tagged メンバです。
- ホストポート(GigabitEthernet 1/0/2)はプライマリ VLAN5 とセカンダリ VLAN2 の untagged ポートです。
- ホストポート(GigabitEthernet 1/0/3)はプライマリ VLAN5 とセカンダリ VLAN3 の untagged ポートです。

14.11.3 トランクプロミスカスとトランクセカンダリの設定例

I. ネットワーク要件

図 14-4に示すように設定します。

- VLAN10 と 20 は Device A のプライマリ VLAN です。Device A のアップリンクポート(GigabitEthernet 1/0/5)は VLAN10 と 20 からの VLAN タグ付きパケットの転送を許可します。
- VLAN11、12、21、22 は Device A のセカンダリ VLAN です。
  - ダウンリンクポート(GigabitEthernet 1/0/2)はセカンダリ VLAN11 と 21 からの VLAN タグ付きパケットの転送を許可します。
  - ダウンリンクポート(GigabitEthernet 1/0/1)はセカンダリ VLAN22 を許可します。
  - ダウンリンクポート(GigabitEthernet 1/0/3)はセカンダリ VLAN12 を許可します。
- セカンダリ VLAN11 と 12 はプライマリ VLAN10 と関連付けます。
- セカンダリ VLAN21 と 22 はプライマリ VLAN20 と関連付けます。

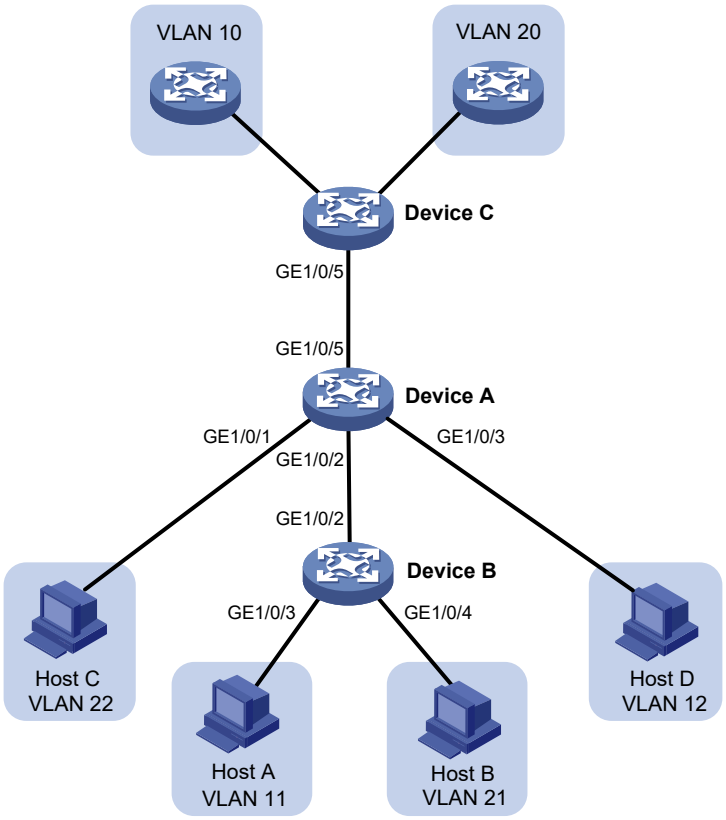


図 14-4 ネットワーク図

II. 設定手順

1)　Device A を設定します。

VLAN10 と 20 はプライマリ VLAN に設定します。

```
<DeviceA> system-view
[DeviceA] vlan 10
[DeviceA-vlan10] private-vlan primary
[DeviceA-vlan10] quit
[DeviceA] vlan 20
[DeviceA-vlan20] private-vlan primary
[DeviceA-vlan20] quit
```

VLAN11、12、21、22 を作成します。

```
[DeviceA] vlan 11 to 12
[DeviceA] vlan 21 to 22
```

セカンダリ VLAN11 と 12 をプライマリ VLAN10 に関連付けます。

```
[DeviceA] vlan 10
[DeviceA-vlan10] private-vlan secondary 11 12
[DeviceA-vlan10] quit
```

セカンダリ VLAN21 と 22 をプライマリ VLAN20 に関連付けます。

```
[DeviceA] vlan 20
[DeviceA-vlan20] private-vlan secondary 21 22
[DeviceA-vlan20] quit
```

GigabitEthernet 1/0/5 を VLAN10 と 20 のトランクプロミスカスポートに設定します。

```
[DeviceA] interface gigabitethernet 1/0/5
[DeviceA-GigabitEthernet1/0/5] port private-vlan 10 20 trunk promiscuous
[DeviceA-GigabitEthernet1/0/5] quit
```

GigabitEthernet 1/0/1 を VLAN 22 に割り当て、ホストポートに設定します。

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port access vlan 22
[DeviceA-GigabitEthernet1/0/1] port private-vlan host
[DeviceA-GigabitEthernet1/0/1] quit
```

GigabitEthernet 1/0/3 を VLAN 12 に割り当て、ホストポートに設定します。

```
[DeviceA] interface gigabitethernet 1/0/3
[DeviceA-GigabitEthernet1/0/3] port access vlan 12
[DeviceA-GigabitEthernet1/0/3] port private-vlan host
[DeviceA-GigabitEthernet1/0/3] quit
```

GigabitEthernet 1/0/2 を VLAN11 と 21 のトランクセカンダリに設定します。

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port private-vlan 11 21 trunk secondary
[DeviceA-GigabitEthernet1/0/2] quit
```

2)　Device B を設定します。

VLAN11 と 21 を作成します。

```
<DeviceB> system-view
[DeviceB] vlan 11
[DeviceB-vlan11] quit
[DeviceB] vlan 21
[DeviceB-vlan21] quit
```

GigabitEthernet 1/0/2をハイブリッドポートに設定して、VLAN11 と 21 を tagged メンバとして割り当てます。

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] port link-type hybrid
[DeviceB-GigabitEthernet1/0/2] port hybrid vlan 11 21 tagged
[DeviceB-GigabitEthernet1/0/2] quit
```

GigabitEthernet 1/0/3 に VLAN 11 を割り当てます。

```
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] port access vlan 11
[DeviceB-GigabitEthernet1/0/3] quit
```

GigabitEthernet 1/0/4 に VLAN 21 を割り当てます。

```
[DeviceB] interface gigabitethernet 1/0/4
[DeviceB-GigabitEthernet1/0/4] port access vlan 21
[DeviceB-GigabitEthernet1/0/4] quit
```

3)　Device C を設定します。

VLAN10 と 20 を作成します。

```
<DeviceC> system-view
[DeviceC] vlan 10
[DeviceC-vlan10] quit
[DeviceC] vlan 20
[DeviceC-vlan20] quit
```

GigabitEthernet 1/0/5 をハイブリッドポートに設定して、VLAN10 と 20 を tagged メンバとして割り当てます。

```
[DeviceC] interface gigabitethernet 1/0/5
[DeviceC-GigabitEthernet1/0/5] port link-type hybrid
[DeviceC-GigabitEthernet1/0/5] port hybrid vlan 10 20 tagged
[DeviceC-GigabitEthernet1/0/5] quit
```

III. 設定の確認

Device A のプライマリ VLAN 情報を確認します（プライマリ VLAN10 を例とします）。

```
[DeviceA] display private-vlan 10
 Primary VLAN ID: 10
 Secondary VLAN ID: 11-12

 VLAN ID: 10
 VLAN type: Static
 Private-vlan type: Primary
 Route interface: Not configured
```

```
Description: VLAN 0010
Name: VLAN 0010
Tagged ports:
   GigabitEthernet1/0/2
   GigabitEthernet1/0/5
Untagged ports:
   GigabitEthernet1/0/3

VLAN ID: 11
VLAN type: Static
Private-vlan type: Secondary
Route interface: Not configured
Description: VLAN 0011
Name: VLAN 0011
Tagged ports:
   GigabitEthernet1/0/2
   GigabitEthernet1/0/5
Untagged ports: None

VLAN ID: 12
VLAN type: Static
Private-vlan type: Secondary
Route interface: Not configured
Description: VLAN 0012
Name: VLAN 0012
Tagged ports:
   GigabitEthernet1/0/5
Untagged ports:
   GigabitEthernet1/0/3
```

出力は以下を示します。

- トランクプロミスカスポート(GigabitEthernet 1/0/5)はプライマリ VLAN10 とセカンダリ VLAN11 と 12 の tagged メンバです。
- トランクセカンダリポート(GigabitEthernet 1/0/2)はプライマリ VLAN10 とセカンダリ VLAN11 の tagged メンバです。
- ホストポート (GigabitEthernet 1/0/3)はプライマリ VLAN10 とセカンダリ VLAN12 の untagged メンバです。

14.11.4 セカンダリ VLAN でのレイヤ 3 通信の 設定例

I. ネットワーク要件

図 14-5に示すように設定します。

- Device A のプライマリ VLAN10 はセカンダリ VLAN2 と 3 に関連付けます。VLAN インタフェース 10 の IP アドレスは 192.168.1.1/24 です。
- GigabitEthernet 1/0/1 は VLAN 10 に所属し、GigabitEthernet 1/0/2 とGigabitEthernet 1/0/3はそれぞれ VLAN 2 と VLAN 3 に所属します。
- セカンダリ VLAN はレイヤ 2 で分離していますが、レイヤ 3 では相互通信します。

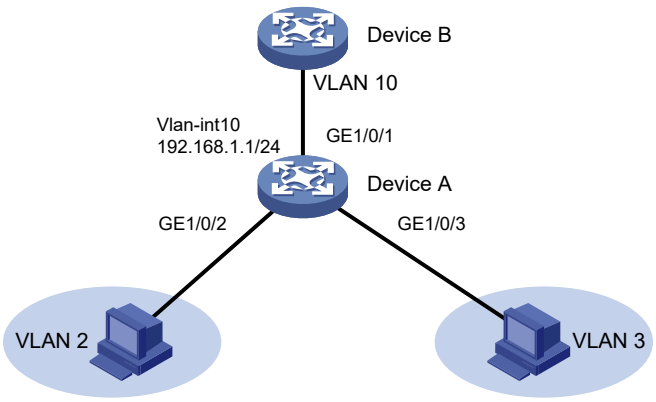


図 14-5 ネットワーク図

II. 設定手順

VLAN10 を作成して、プライマリ VLAN に設定します。

```
<DeviceA> system-view
[DeviceA] vlan 10
[DeviceA-vlan10] private-vlan primary
[DeviceA-vlan10] quit
```

VLAN2 と 3 を作成します。

```
<DeviceA> system-view
[DeviceA] vlan 2 to 3
```

プライマリ VLAN10 をセカンダリ VLAN2 と 3 と関連付けます。

```
[DeviceA] vlan 10
[DeviceA-vlan10] private-vlan secondary 2 3
[DeviceA-vlan10] quit
```

GigabitEthernet 1/0/1 を VLAN10 のプロミスカスポートに設定します。

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port private-vlan 10 promiscuous
[DeviceA-GigabitEthernet1/0/1] quit
```

GigabitEthernet 1/0/2 を VLAN 2 に割り当て、ホストポートに設定します。

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port access vlan 2
[DeviceA-GigabitEthernet1/0/2] port private-vlan host
[DeviceA-GigabitEthernet1/0/2] quit
```

GigabitEthernet 1/0/3 を VLAN 3 に割り当て、ホストポートに設定します。

```
[DeviceA] interface gigabitethernet 1/0/3
[DeviceA-GigabitEthernet1/0/3] port access vlan 3
[DeviceA-GigabitEthernet1/0/3] port private-vlan host
[DeviceA-GigabitEthernet1/0/3] quit
```

プライマリ VLAN10 に関連付けたセカンダリ VLAN2 と 3 間でレイヤ 3 通信を有効にします。

```
[DeviceA] interface vlan-interface 10
[DeviceA-Vlan-interface10] private-vlan secondary 2 3
```

VLAN インタフェース 10 に IP アドレス(192.168.1.1/24)を設定します。

```
[DeviceA-Vlan-interface10] ip address 192.168.1.1 255.255.255.0
```

ローカルプロキシ ARP を VLAN インタフェース 10 で有効にします。

```
[DeviceA-Vlan-interface10] local-proxy-arp enable
[DeviceA-Vlan-interface10] quit
```

III. 設定の確認

プライマリ VLAN10 の設定を確認します。

```
[DeviceA] display private-vlan 10
 Primary VLAN ID: 10
 Secondary VLAN ID: 2-3

 VLAN ID: 10
 VLAN type: Static
 Private VLAN type: Primary
 Route interface: Configured
 IPv4 address: 192.168.1.1
 IPv4 subnet mask: 255.255.255.0
 Description: VLAN 0010
 Name: VLAN 0010
 Tagged ports:   None
 Untagged ports:
    GigabitEthernet1/0/1
    GigabitEthernet1/0/2
    GigabitEthernet1/0/3

 VLAN ID: 2
 VLAN type: Static
 Private VLAN type: Secondary
 Route interface: Configured
 IPv4 address: 192.168.1.1
 IPv4 subnet mask: 255.255.255.0
 Description: VLAN 0002
 Name: VLAN 0002
 Tagged ports:   None
 Untagged ports:
    GigabitEthernet1/0/1
    GigabitEthernet1/0/2

 VLAN ID: 3
 VLAN type: Static
 Private VLAN type: Secondary
 Route interface: Configured
```

```
IPv4 address: 192.168.1.1
IPv4 subnet mask: 255.255.255.0
Description: VLAN 0003
Name: VLAN 0003
Tagged ports:   None
Untagged ports:
   GigabitEthernet1/0/1
   GigabitEthernet1/0/3
```

Route interface 情報が **Configured** と表示され、セカンダリ VLAN2 と 3 がレイヤ 3 で相互通信可能であることを示します。

QX-S1100G シリーズ Ethernet スイッチ

オペレーションマニュアル

3. IP サービス

本マニュアルは以下に示す章で構成されています。

01-ARP

02-Gratuitous ARP

03-IP アドレス

04-DHCP の概要

05-DHCP サーバ

06-DHCP クライアント

07-DHCP スヌーピング

08-BOOTP クライアント

09-DNS

10-IP フォワーディングの基本

11-IP パフォーマンスの最適化

12-UDP ヘルパー

13-IPv6 の基本

14-Proxy ARP

15-DHCPv6 の概要

16-DHCPv6 クライアント

17-ARP snooping

目次

このセクションのページは**3-x-x** です。

1 章 ARP 1-1
1.1 概要 1-1
1.1.1 ARP メッセージフォーマット 1-1
1.1.2 ARP 動作メカニズム 1-2
1.1.3 ARP テーブル 1-3
1.2 スタティック ARP エントリの設定 1-4
1.2.2 インタフェースで学習できる ARP エントリの最大数の設定 1-4
1.3 ダイナミック ARP エントリのエージングタイマの設定 1-5
1.4 ARP エントリチェックの有効化 1-5
1.5 ARP ロギング機能の有効化 1-6
1.6 インタフェースでの ARP エントリと MAC アドレスエントリの整合性のチェックの有効化 1-6
1.7 ARP の表示と維持 1-7
1.8 ARP の設定例 1-7
1.8.1 ロングスタティック ARP の設定例 1-7
1.8.2 ショートスタティック ARP の設定例 1-9

1章 ARP

1.1 概要

ARP（Address Resolution Protocol）は、IP アドレスを基に MAC アドレス（物理アドレス）を調べる仕組みのことです。

1.1.1 ARP メッセージフォーマット

ARP は ARP 要求/応答メッセージの 2 つのメッセージタイプがあります。図 1-1に ARP 要求/応答メッセージのフォーマットを示し、図の数字はフィールド長を示します。

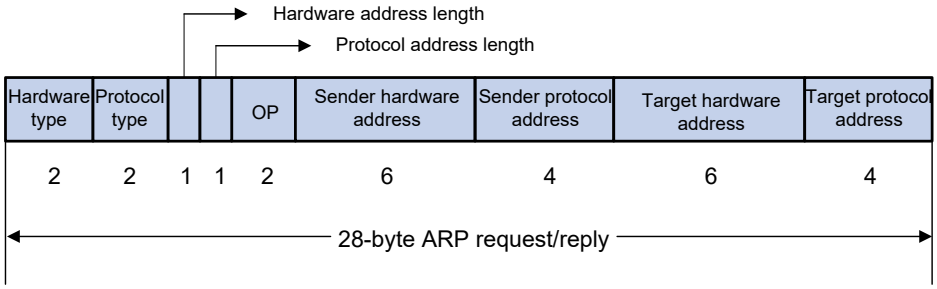


図 1-1 ARP メッセージフォーマット

- **Hardware type**– このフィールドはハードウェアアドレスタイプを指定します。1 は Ethernet を表します。
- **Protocol type**– このフィールドはマッピングされるプロトコルアドレスのタイプを指定します。16 進数で 0x0800 は IP を表します。
- **Hardware address length**、**protocol address length**– ハードウェアアドレスの長さと、プロトコルアドレスの長さをバイト単位で指定します。イーサネットアドレスに関して、Hardware address length の値は 6 です。IPv4 アドレスに関しては、protocol address length の値は 4 です。
- **OP**– このフィールド（Operation code）は ARP メッセージのタイプを指定します。1 は ARP 要求し 2 は ARP 応答を表します。
- **Sender hardware address**– このフィールドはメッセージを送信する装置のハードウェアアドレスを指定します。
- **Sender protocol address**– このフィールドはメッセージを送信する装置のプロトコルアドレスを指定します。
- **Target hardware address**– このフィールドはメッセージが送られる装置のハードウェアアドレスを指定します。
- **Target protocol address**– このフィールドはメッセージが送られる装置のプロトコルアドレスを指定します。

1.1.2 ARP 動作メカニズム

図 1-2に示すように、Host A と Host B は同一サブネットにあります。Host A は Host B に以下のようにパケットを送信します。

1) Host A は Host B の ARP エントリが ARP テーブルにあるか検索します。ARP エントリがある場合、Host A は、ARP エントリの MAC アドレスを使用します。そしてデータリンクレイヤのフレームに IP パケットをカプセル化し、Host B にフレームを送信します。
2) Host B の ARP エントリがない場合、Host A はパケットをバッファし、ARP 要求をブロードキャストします。ARP リクエストのデータの内容は以下の情報が含まれます。
   - **送信元 IP アドレスと送信元 MAC アドレス** – Host A の IP アドレスと MAC アドレス
   - **宛先 IP アドレス** – Host B の IP アドレス
   - **宛先 MAC アドレス** – 値がすべて 0 の MAC アドレス

   サブネットのすべてのホストはブロードキャストリクエストを受信することができますが、パケットを処理するホスト（Host B）のみが ARP 要求を処理します。
3) Host B は自身の IP アドレスと ARP リクエストの宛先 IP アドレスを比較し、同一の場合、以下の処理を行います。
   a) 送信元IPアドレスと送信元MACアドレスをARPテーブルに追加します。
   b) ARP応答に自身のMACアドレスを挿入します。
   c) Host AにARP応答をユニキャストで送信します。
4) ARP 応答を受信した後、Host A は以下の処理を行います。
   a) Host BのMACアドレスをARPテーブルに追加します。
   b) 以降、送信するパケットにHost BのMACアドレスを追加し、Host Bにパケットを送信します。

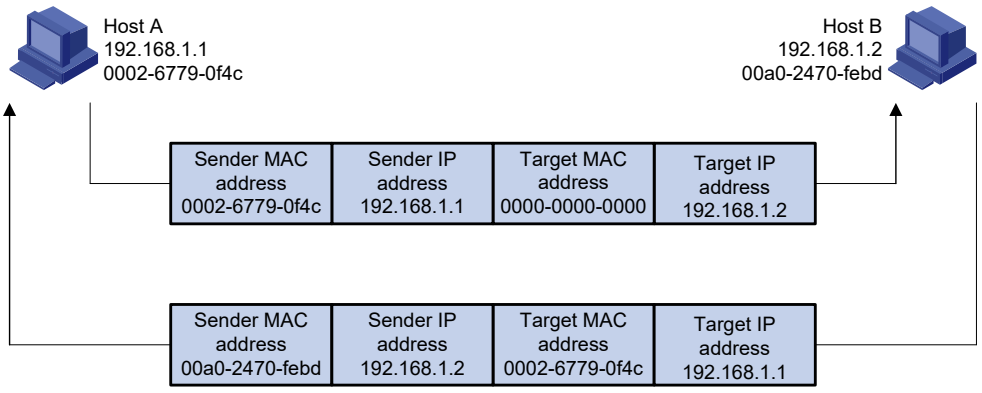


図 1-2 ARP アドレス解決プロセス

Host A と Host B が異なるサブネットにある場合、Host A は Host B に以下のようにパケットを送信します。

1) Host A は、宛先 IP アドレスをゲートウェイの IP アドレスにした ARP 要求をブロードキャストします。
2) ゲートウェイは、ARP 応答を行い、自身の MAC アドレスを Host A に送信します。

3) Host A はゲートウェイの MAC アドレスをパケットに挿入し、ゲートウェイにパケットを送信します。
4) ゲートウェイが Host B の ARP エントリがある場合、Host B にパケットを直接転送します。Host B の ARP エントリがない場合、宛先 IP アドレスを Host B の IP アドレスとして ARP 要求をブロードキャストします。
5) ゲートウェイが Host B の MAC アドレスを取得した後、Host B にパケットを送信します。

1.1.3 ARP テーブル

ARP テーブルはダイナミックとスタティックの ARP エントリがあります。

I. ダイナミック ARP エントリ

ダイナミックエントリは ARP によって自動的に作成し、アップデートされます。エージングタイマが終了した場合、あるいは出力インタフェースがダウンした場合、ダイナミックエントリは削除されます。ダイナミック ARP エントリはスタティック ARP エントリによって上書きされます。

II. スタティック ARP エントリ

スタティック ARP エントリは手動で設定され、維持されます。スタティック ARP エントリはエージングせず、ダイナミック ARP エントリで上書きされることもありません。

スタティック ARP エントリを使用することにより、通信のセキュリティを強化できます。スタティック ARP エントリで IP アドレスと MAC アドレスをマッピングすることにより、指定された IP アドレスと MAC アドレスのマッピングが、攻撃パケットで変更されることはありません。

装置は以下のタイプのスタティック ARP エントリをサポートします。

- **ロングスタティック ARP エントリ**：IP アドレス、MAC アドレス、VLAN インタフェース、入力および出力インタフェースから構成されパケットを転送するのに直接使用されます。
- **ショートスタティック ARP エントリ**：IP アドレス、MAC アドレスのみで構成されます。

  装置はターゲット IP アドレスがショートエントリの IP アドレスである ARP 要求を送信します。受信した ARP 応答の送信元 IP アドレスと MAC アドレスがショートスタティック ARP エントリと一致した場合、装置は以下の処理を行います。

  - ARP エントリを受信したインタフェースはショートスタティック ARP エントリを追加します。
  - IP パケットを転送するため、解決したショートスタティック ARP エントリを使用します。

固定の IP アドレス-MAC アドレスマッピングを使用してホストと通信する場合、装置は、ショートスタティック ARP エントリを設定します。固定の IP アドレス-MAC アドレスマッピングを使用して、指定した VLAN の指定したインタフェースを通してホストと通信する場合、装置はロングスタティック ARP エントリを設定します。

1.2 スタティックARPエントリの設定

スタティック ARP エントリは、装置が正常に動作する場合に適用されます。

I. ショートスタティック ARP エントリの設定

ショートスタティック ARP エントリ は、解決済みの出力インタフェース がダウンした場合や、対応する VLAN または VLAN インタフェース が削除された場合に未解決となります。

II. ロングスタティック ARP エントリの設定

ロングスタティック ARP エントリは次の条件のいずれかに該当する場合は無効となります。無効なロングスタティック ARP エントリは、パケット転送には使用できません。

- ARP エントリの IP アドレスが装置に設定する IP アドレスと同じ場合
- ARP エントリが所属する VLAN インタフェースに、ARP エントリの IP アドレスと同じサブネットの IP アドレスが存在しない場合

VLAN または VLAN インタフェース が削除されると、ロングスタティック ARP は削除されます。

以下にスタティック ARP エントリの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． スタティック ARP エントリを設定する	• ショートスタティック ARPエントリを設定する： **arp static** *ip-address mac-address* • ロングスタティックARP エントリを設定する： **arp static** *ip-address mac-address* [*vlan-id interface-type interface-number*]	デフォルト：設定なし

1.2.2 インタフェースで学習できる ARP エントリの最大数の設定

インタフェースは動的に ARP エントリを学習します。多すぎる ARP エントリを保持しないように、インタフェースが学習できるダイナミック ARP エントリの最大数を設定することができます。設定した最大数に到達すると、ARP エントリの学習を停止します。

ダイナミック ARP エントリの最大数をレイヤ 2 インタフェースと VLAN インタフェースの両方で設定することができます。レイヤ 2 インタフェースはダイナミック ARP エントリが最大値に到達しない場合のみ ARP エントリを学習します。

以下にインタフェースで学習できるダイナミック ARP エントリの最大数の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． interface view に移行する	**interface** *interface-type interface-number*	―
3． ダイナミック ARP エントリの最大数を設定する	**arp max-learning-num** *number*	デフォルト：256 *number* 引数に0を設定した場合、ダイナミックARPエントリの学習を行いません。

1.3 ダイナミックARPエントリのエージングタイマの設定

ARP テーブル上の各ダイナミック ARP エントリは有効期限があります。有効期限はエージングタイマと呼ばれ、有効期限内にダイナミック ARP エントリが使用される度に、エージングタイマはアップデートされます。有効期限切れになる前に更新されなかったダイナミック ARP エントリは、ARP テーブルから削除されます。

system view または interface view で、ダイナミック ARP エントリのエージングタイマを設定できます。interface view で設定されたエージングタイマは、system view で設定されたエージングタイマよりも優先されます。

以下にダイナミック ARP エントリのエージングタイマの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． ダイナミック ARP エントリのエージングタイムを設定する	● system viewでダイナミックARPエントリのエージングタイマを設定する **arp timer aging** *aging-time* ● interface viewでダイナミックARPエントリのエージングタイマを以下の手順で設定する **interface** *interface-type interface-number* **arp timer aging** *aging-time*	デフォルト：system viewでは20分 デフォルト：interface viewではsystem viewで設定されたエージングタイマ

1.4 ARPエントリチェックの有効化

ダイナミック ARP エントリチェック機能は、装置でマルチキャスト MAC アドレスを含むダイナミック ARP エントリのサポートを無効にします。装置は送信元がマルチキャスト MAC アドレスであるダイナミック ARP エントリを学習できません。マルチキャスト MAC アドレスを含むスタティック ARP エントリを手動で学習させることもできません。

ARP エントリチェックを無効にした場合、装置はマルチキャスト MAC アドレスの ARP エントリを学習することができます。手動でマルチキャスト MAC アドレスを含むスタティック ARP エントリを追加することができます。

以下に ARP エントリチェック機能の設定を示します。

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

操作	コマンド	補足
2． ARP エントリチェック機能を有効にする	**arp check enable**	デフォルト：有効

1.5 ARPロギング機能の有効化

ARP が IP アドレスを正常に解決できない場合、装置で ARP イベントをロギングします。以下の ARP イベントをロギングできます。

- インタフェースで proxy ARP が無効な場合、受信した ARP パケットの宛先 IP アドレスは受信インタフェースの IP アドレスのいずれでもありません。
- 受信した ARP エントリの送信元 IP アドレスが受信インタフェースの IP アドレスの 1 つと重複しています。

装置は Information Center に ARP ログメッセージを送信します。Information Center のログ出力ルールを設定するため、**info-center source** コマンドを使用します。Information Center の詳細は、オペレーションマニュアルのセクション 9 *システム管理*“*Information Center*”を参照してください。

以下に ARP ロギング機能の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． ARP ロギング機能を有効にする	**arp check log enable**	デフォルト：無効

1.6 インタフェースでのARPエントリとMACアドレスエントリの整合性のチェックの有効化

不安定なネットワークでは、ユーザからのパケットの受信側インタフェースが変更されることがあります。MAC アドレスエントリのインタフェースはすぐに更新できますが、ARP エントリのインタフェースは更新できません。この場合、ARP エントリに一致するパケットは、正しくないインタフェースから送信されます。この問題を解決するには、この機能を使用して、エントリの ARP および MAC アドレスユーザのインタフェース整合性を定期的にチェックします。インタフェースが同じでない場合、ARP は ARP エントリの VLAN に ARP 要求を送信し、ARP 応答を受信したインタフェースでエントリを更新します。

display mac-address を使用して、MAC アドレスエントリを表示します。詳細はコマンドマニュアルのセクション 2 *アクセス*”*MAC アドレステーブル*”を参照してください。

以下にインタフェースで ARP エントリと MAC アドレスエントリの整合性のチェックを有効にする設定を示します。

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

操作	コマンド	補足
2． インタフェースで ARP エントリと MAC アドレスエントリの整合性のチェックを有効にする	**arp mac-interface-consistency check enable**	デフォルト：有効

1.7 ARPの表示と維持

⚠ **重要：**
ARP テーブルから ARP エントリをクリアすると、通信障害を引き起こす恐れがあります。ARP エントリを削除した場合は、その後の通信に影響がないことを確認してください。

すべての view で **display** コマンドを実行でき、user view で **reset** コマンドが実行できます。

操作	コマンド
ARPエントリを表示する	**display arp** [[**all** | **dynamic** | **static**] [**slot** *slot-number*] | **vlan** *vlan-id* | **interface** *interface-type interface-number*] [**count** | **verbose**]
指定したIPアドレスのARPエントリを表示する	**display arp** *ip-address* [**slot** *slot-number*] [**verbose**]
ダイナミックARPエントリのエージングタイムを表示する	**display arp timer aging**
ARPテーブルからARPエントリを削除する	**reset arp** { **all** | **dynamic** | **interface** *interface-type interface-number* | **slot** *slot-number* | **static** }

1.8 ARPの設定例

1.8.1 ロングスタティック ARP の設定例

I. ネットワーク要件

図 1-3に示すように、Host は、Device B に接続されています。Device B は VLAN 10 の GigabitEthernet 1/0/1 によって Device A に接続されています。

Device A と Device B 間の通信を強化するため、Device B で Device A のロングスタティック ARP エントリの設定を行います。

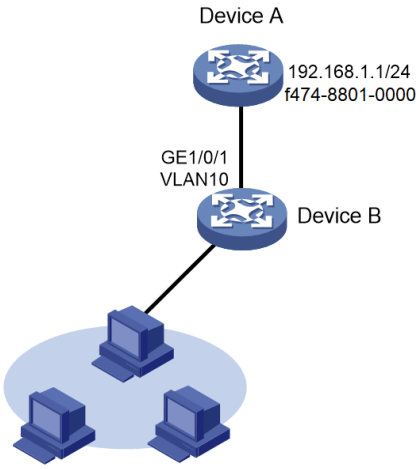


図 1-3 ネットワーク図

II. 設定手順

VLAN 10 を作成します。

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

GigabitEthernet 1/0/1 に VLAN 10 を割り当てます。

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port access vlan 10
[DeviceB-GigabitEthernet1/0/1] quit
```

VLAN インタフェース 10 を作成し、IP アドレスを設定します。

```
[DeviceB] interface vlan-interface 10
[DeviceB-vlan-interface10] ip address 192.168.1.2 24
[DeviceB-vlan-interface10] quit
```

IP アドレス 192.168.1.1 と MAC アドレス f474-8801-0000 のスタティック ARP エントリを作成します。ロングスタティック ARP エントリに対応する出力インタフェースを VLAN 10 に所属する GigabitEthernet 1/0/1 とします。

```
[DeviceB] arp static 192.168.1.1 f474-8801-0000 10 gigabitethernet 1/0/1
```

III. 設定の確認

Device B で Device A のスタティック ARP エントリを表示します。

```
[DeviceB] display arp static
  Type: S-Static   D-Dynamic   O-Openflow   R-Rule   M-Multiport  I-Invalid
IP address      MAC address    VLAN/VSI   Interface                Aging Type
192.168.1.1     f474-8801-0000 10         GE1/0/1                  --    S
```

1.8.2 ショートスタティック ARP の設定例

I. ネットワーク要件

図 1-4に示すように、Host は、Device B に接続されています。Device B は VLAN 10 の GigabitEthernet 1/0/2 によって Device A に接続されています。

Device A と Device B 間の通信を強化するため、Device B で Device A のショートスタティック ARP エントリの設定を行います。

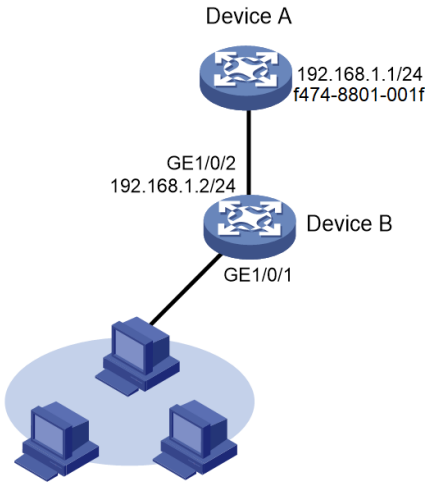


図 1-4 ネットワーク図

II. 設定手順

GigabitEthernet 1/0/2 の IP アドレスを設定します。

```
<DeviceB> system-view
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] ip address 192.168.1.2 24
[DeviceB-GigabitEthernet1/0/2] quit
```

IP アドレス 192.168.1.1 と MAC アドレス f474-8801-001f のショートスタティック ARP エントリを作成します。

```
[DeviceB] arp static 192.168.1.1 f474-8801-001f
```

III. 設定の確認

Device B で Device A のショートスタティック ARP エントリを表示します。

```
[DeviceB] display arp static
  Type: S-Static   D-Dynamic   O-Openflow   R-Rule   M-Multiport  I-Invalid
IP address      MAC address    VLAN/VSI   Interface                Aging Type
192.168.1.1     f474-8801-001f --         --                       --    S
```

目次

このセクションのページは**3-x-x** です。

2 章 Gratuitous ARP 2-1
2.1 概要 2-1
2.1.1 Gratuitous ARP パケットの学習 2-1
2.1.2 Gratuitous ARP パケットの送信間隔の設定 2-1
2.2 設定手順 2-2
2.3 IP 重複通知の有効化 2-2

2章 Gratuitous ARP

2.1 概要

GARP（Gratuitous ARP）は ARP パケットの 1 つであり、装置は以下の目的で Gratuitous ARP パケットを送信します。

- 他のネットワーク装置と、IP アドレスが重複していないかを確認できます。IP アドレスが既に使われていた場合、ARP 応答によって重複していることが通知されます。
- 他のネットワーク装置に MAC アドレス情報を通知して、ARP エントリを更新させます。

Gratuitous ARP パケットにおいて送信元 IP アドレスと宛先 IP アドレスは共に送信する装置の IP アドレスです。

2.1.1 Gratuitous ARP パケットの学習

Gratuitous ARP パケットの学習機能を有効にした場合、Gratuitous ARP パケットを受信すると、受信した Gratuitous ARP パケットの送信元 IP アドレスと MAC アドレスを使用して ARP エントリを作成あるいは更新します。

この機能を無効にした場合、ARP エントリの更新は行いますが、新しい ARP エントリは追加しません。ARP エントリは受信した Gratuitous ARP パケットをもとに ARP エントリを作成しないで、ARP テーブルを節約します。

2.1.2 Gratuitous ARP パケットの送信間隔の設定

定期的に Gratuitous ARP パケットを送信することにより、下流の装置の対応する ARP エントリあるいは MAC アドレスエントリを更新します。この機能は以下の機能をサポートします。

- ゲートウェイスプーフィングの防御

攻撃者がネットワーク上のホストに捏造した Gratuitous ARP パケットを送信するためにゲートウェイアドレスを使用した場合、ゲートウェイスプーフィングが発生します。ホストからゲートウェイ宛のトラフィックは代わりに攻撃者に送信されます。その結果ホストは外部のネットワークにアクセスできません。

ゲートウェイスプーフィングの攻撃を防ぐため、ゲートウェイが Gratuitous ARP パケットを送信する間隔を設定することができます。Gratuitous ARP パケットは、ホストが正しいゲートウェイの情報を学習できるように、ゲートウェイのプライマリ IP アドレスと手動で設定されたセカンダリ IP アドレスが含まれます。

- ARP エントリのエージアウトの防止

ネットワークのトラフィックが非常に多い、あるいはホストの CPU の使用率が高い場合、受信した ARP パケットは廃棄、あるいはすぐに処理されません。そのため、受信ホスト

のダイナミック ARP エントリはエージアウトします。ホストと対応する装置間のトラフィックは、ホストが ARP エントリを再作成するまで中断されます。

この問題を防ぐため、定期的に Gratuitous ARP パケットを送信するゲートウェイを有効にします。受信ホストはすぐに ARP エントリをアップデートすることができます。

2.2 設定手順

以下に Gratuitous ARP の設定を行うため、制限とガイドラインに従ってください。

- 最大 1024 のインタフェースで Gratuitous ARP パケットの送信間隔を設定できます。
- Gratuitous ARP パケットの送信間隔の設定は、以下の状態の場合に適用されます。
  - インタフェースのリンク状態がアップです。
  - IP アドレスが割り当てられています。
- Gratuitous ARP パケットの送信間隔を変更する場合、設定は次の送信間隔から適用されます。
- Gratuitous ARP パケットの送信間隔は以下の状況によって、設定した値よりも長くなる可能性があります。
  - 複数のインタフェースで有効にされた場合
  - 各インタフェースで複数のセカンダリ IP アドレスが設定された場合
  - 複数のインタフェースで有効にされ、各インタフェースで複数のセカンダリ IP アドレスが設定された場合、Gratuitous ARP パケットの送信間隔は設定された送信間隔よりも短くなります。

以下に Gratuitous ARP の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Gratuitous ARP パケット学習機能を有効にする	**gratuitous-arp-learning enable**	デフォルト：無効
3. 他のネットワークセグメントから ARP 要求を受信した際、Gratuitous ARP パケットの送信を有効にする	**gratuitous-arp-sending enable**	デフォルト：無効
4. interface view に移行する	**interface** *interface-type interface-number*	―
5. Gratuitous ARP パケットの定期的な送信を有効化し、送信間隔を設定する	**arp send-gratuitous-arp** [**interval** *interval*]	デフォルト：無効

2.3 IP重複通知の有効化

デフォルトで、受信装置が Gratuitous ARP パケットの送信者の IP アドレスを使用する場合、受信装置は gratuitous ARP 要求を送信します。重複に関する ARP 応答を受信したのち、エラーメッセージを表示します。

このコマンドを使用することで、Gratuitous ARP 応答あるいは要求を送信することなく、装置でエラーメッセージを表示することができます。

以下に IP 重複通知の有効化の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． IP 重複通知を有効にする	**arp ip-conflict log prompt**	デフォルト：無効

目次

このセクションのページは**3-x-x** です。

3 章 IP アドレス 3-1
3.1 概要 3-1
3.1.1 IP アドレスクラス 3-1
3.1.2 特別な IP アドレス 3-2
3.1.3 サブネットとマスク 3-2
3.2 インタフェースへの IP アドレスの割り当て 3-3
3.2.1 設定ガイドライン 3-3
3.2.2 設定手順 3-3
3.3 IP アドレスの表示と維持 3-4
3.4 IP アドレスの設定例 3-4
3.4.1 ネットワーク要件 3-4
3.4.2 設定手順 3-5
3.4.3 設定の確認 3-5

3章 IP アドレス

この章では IP アドレスの基本とインタフェースにアドレスを手動で割り当てる方法について記載し、ダイナミックに IP アドレスを割り当てる方法（BOOTP、DHCP）については記載しません。この章の IP アドレスは特に指定がない限り、IPv4 アドレスについて記載します。

3.1 概要

IP アドレスは、IPv4 ネットワークの各ホストを識別するため、32 ビットアドレスを使用します。たとえば、2 進数では 00001010000000010000000100000001 となります。IP アドレスをわかりやすくするために、32 ビットの整数値を 8 ビットずつ 4 つに分割し、ドット付きの 10 進数で IP アドレスを表します。先ほどの 32 ビットの 2 進数は、10.1.1.1 となります。

3.1.1 IP アドレスクラス

各 IP アドレスは以下のセクションに分類されます。

- **Net ID** – ネットワークを定義します。先頭の数ビットはネットワークを定義するアドレスです。クラスフィールドあるいはクラスビットで、IP アドレスのクラスを識別します。
- **Host ID** – ホストを定義します。

図 3-1に示すように、IP アドレスは 5 つのクラスに分類されます。IP アドレスがどのクラスに所属するのかは、下図の青い部分のアドレスによって決まります。最初の 3 つのクラスは一般的に使用されます。

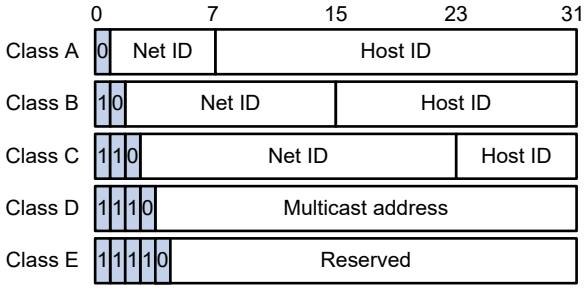


図 3-1 IP アドレスクラス

表 3-1 IP アドレスクラスと範囲

クラス	アドレス範囲	補足
A	0.0.0.0 ～ 127.255.255.255	0.0.0.0はブートストラップ時に一時的にホストが使用するため、有効な宛先アドレスにはなりません。127からはじまるアドレスはループバックテストのために予約されているため、このアドレス宛てのパケットは、入力パケットとしてローカルで処理されます。
B	128.0.0.0 ～ 191.255.255.255	ー
C	192.0.0.0 ～ 223.255.255.255	ー
D	224.0.0.0 ～ 239.255.255.255	マルチキャストアドレス
E	240.0.0.0 ～ 255.255.255.255	予約済みです。255.255.255.255はブロードキャストアドレスです。

3.1.2 特別な IP アドレス

以下の IP アドレスは特別な用途で使用されるため、ホストの IP アドレスに設定することができません。

- **Net ID がすべて 0 の IP アドレス** ー ローカルネットワークのホストを識別します。たとえば、IP アドレス 0.0.0.16 はローカルネットワークの Host ID が 16 のホストを示します
- **Host ID がすべて 0 の IP アドレス** ー ネットワークアドレスを示します。
- **Host ID がすべて 1 の IP アドレス** ー ディレクテッドブロードキャストを示します。たとえば、宛先アドレスが 192.168.1.255 のパケットは、ネットワーク 192.168.1.0 に属するすべてのホストにブロードキャストされます。

3.1.3 サブネットとマスク

サブネットは、Host ID のいくつかのビットを使用して Subnet ID を作成し、ネットワークをサブネットと呼ばれるより小さいネットワークに分割します。

Host ID と、Net ID と Subnet ID の組み合わせの境界を識別するために、サブネットマスクが使用されます。

各サブネットマスクは IP アドレス関連する 32 ビットで構成されています。サブネットマスクは 1 と 0 で構成されています。1 が連続している部分で Net ID と Subnet ID の組み合わせを識別し、0 が連続している部分で Host ID を識別します。

サブネットとなるまえに、クラス A、B、C ネットワークは、それぞれ 255.0.0.0、255.255.0.0、255.255.255.0 のデフォルトマスク（ナチュラルマスクと呼ばれます）を使用します。

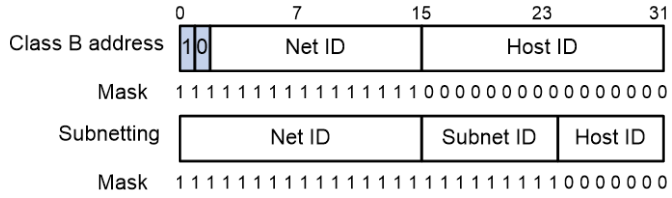


図 3-2 クラス B ネットワークのサブネット

サブネットは、ホストに割り当てることができないアドレスを増大させます。従って、サブネットを使用することは、ある程度少ないホストを適用することになります。

たとえばクラス B ネットワークでは、1022 のサブネットを持つネットワークよりも、512 のサブネットを持つネットワークのほうが、多くのホストを収容することができます。

- **サブネットがないネットワーク** － 65534 個（$2^{16} - 2$）のホストを収容できます。（Host ID がすべて 1 のブロードキャストアドレスと、Host ID すべて 0 のネットワークアドレスを差し引きます。）
- **サブネットネットワーク** － Host-ID の最初の 9 ビットをサブネットに割り当てると、512 個（2^9）のサブネットができます。Host-ID に使用できるのは残りの 7 ビットだけとなり、各サブネットに 126 個（$2^7 - 2$）のホストを収容できます。従って、全部で 64512 個（512 × 126）のホストを収容できます。

3.2 インタフェースへのIPアドレスの割り当て

インタフェースは他のホストと通信するために IP アドレスが必要です。手動でインタフェースに IP アドレスを割り当てるか、BOOTP あるいは DHCP によって IP アドレスを取得することができます。IP アドレスを取得する方法を変更した場合、新しい IP アドレスは古い IP アドレスに上書きします。

インタフェースは 1 つのプライマリアドレスと複数のセカンダリアドレスを持つことができます。

通常、インタフェースのプライマリアドレスを設定する必要があります。インタフェースが複数のサブネットに接続する場合、サブネットが、インタフェースを通して互いに通信できるようにインタフェースにプライマリとセカンダリ IP アドレスを設定します。

3.2.1 設定ガイドライン

インタフェースに IP アドレスを割り当てる場合、以下のガイドラインに従ってください。

- インタフェースは 1 つのプライマリ IP アドレスのみを設定することができます。インタフェースで異なるプライマリ IP アドレスを指定するために **ip address** コマンドを複数回実行すると、最新の設定が有効になります。
- BOOTP または DHCP により IP アドレスを取得する設定をしているインタフェースでは、セカンダリ IP アドレスを設定することはできません。
- インタフェースに設定するプライマリとセカンダリ IP アドレスは同じネットワークセグメントに存在することができます。しかし、装置上の異なるインタフェースは異なるネットワークセグメントにしなければなりません。

3.2.2 設定手順

以下にインタフェースに IP アドレスの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	－
2． interface view に移行する	**interface** *interface-type interface-number*	－

操作	コマンド	補足
3． インタフェースに IP アドレスを設定する	**ip address** *ip-address* { *mask-length* | *mask* } [**sub**]	デフォルト：設定なし

3.3 IPアドレスの表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
指定された、またはすべてのレイヤ3インタフェースの設定と統計情報を表示する	**display ip interface** [*interface-type interface-number*]
指定された、またはすべてのレイヤ3インタフェースの概要情報を表示する	**display ip interface** [*interface-type* [*interface-number*]] **brief**

3.4 IPアドレスの設定例

3.4.1 ネットワーク要件

図 3-3に示すように、Switch の VLAN1 は、IP アドレス 172.16.1.0/24 と IP アドレス 172.16.2.0/24 の 2 つの LAN に接続されています。

Switch を経由して外部ネットワークに接続された 2 つのサブネット上にある Host が互いに通信可能なように設定します。

- VLAN インタフェース 1 に、プライマリ IP アドレスとセカンダリ IP アドレスを割り当てます。
- Switch のプライマリ IP アドレスを、サブネット 172.16.1.0/24 の PC のゲートウェイアドレスに設定し、Switch のセカンダリ IP アドレスを、サブネット 172.16.2.0/24 の PC のゲートウェイアドレスに設定します。

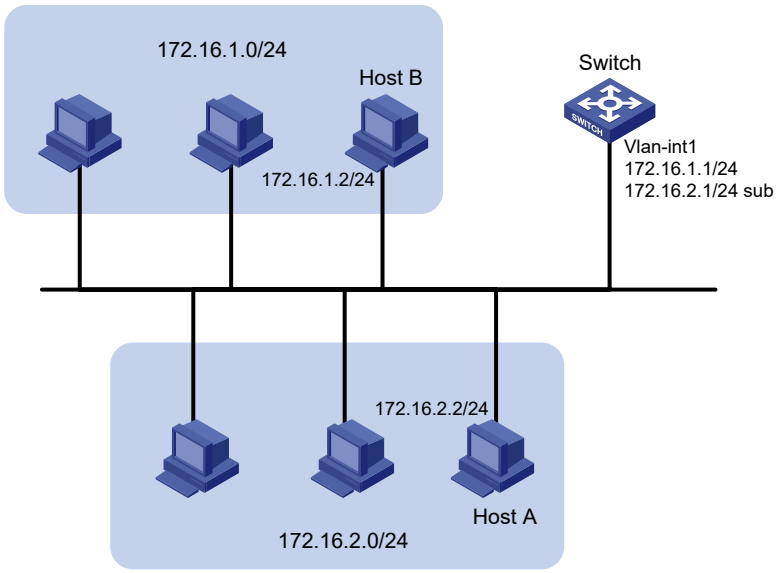


図 3-3 ネットワーク図

3.4.2 設定手順

VLAN インタフェース 1 にプライマリ IP アドレスとセカンダリ IP アドレスを割り当てます。

```
<Switch> system-view
[Switch] interface vlan-interface 1
[Switch-Vlan-interface1] ip address 172.16.1.1 255.255.255.0
[Switch-Vlan-interface1] ip address 172.16.2.1 255.255.255.0 sub
```

サブネット 172.16.1.0/24 に接続された PC にゲートウェイアドレス 172.16.1.1 を設定し、サブネット 172.16.2.0/24 に接続された PC にゲートウェイアドレス 172.16.2.1 を設定します。

3.4.3 設定の確認

接続されているか確認するため、Switch からサブネット 172.16.1.0/24 の Host に ping を実施します。

```
<Switch> ping 172.16.1.2
Ping 172.16.1.2 (172.16.1.2): 56 data bytes, press CTRL_C to break
56 bytes from 172.16.1.2: icmp_seq=0 ttl=128 time=7.000 ms
56 bytes from 172.16.1.2: icmp_seq=1 ttl=128 time=2.000 ms
56 bytes from 172.16.1.2: icmp_seq=2 ttl=128 time=1.000 ms
56 bytes from 172.16.1.2: icmp_seq=3 ttl=128 time=1.000 ms
56 bytes from 172.16.1.2: icmp_seq=4 ttl=128 time=2.000 ms

--- Ping statistics for 172.16.1.2 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.000/2.600/7.000/2.245 ms
```

接続されているか確認するため、Switch からサブネット 172.16.2.0/24 の Host に ping を実施します。

<Switch> ping 172.16.2.2

```
Ping 172.16.2.2 (172.16.2.2): 56 data bytes, press CTRL_C to break
56 bytes from 172.16.2.2: icmp_seq=0 ttl=128 time=2.000 ms
56 bytes from 172.16.2.2: icmp_seq=1 ttl=128 time=7.000 ms
56 bytes from 172.16.2.2: icmp_seq=2 ttl=128 time=1.000 ms
56 bytes from 172.16.2.2: icmp_seq=3 ttl=128 time=2.000 ms
56 bytes from 172.16.2.2: icmp_seq=4 ttl=128 time=1.000 ms

--- Ping statistics for 172.16.2.2 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.000/2.600/7.000/2.245 ms
```

接続されたかどうか確認するため、サブネット 172.16.2.0/24 に接続された Host A からサブネット 172.16.1.0/24 に接続された Host B に ping を実施します。Host B は Host A から ping 応答を受信することができます。

目次

このセクションのページは**3-x-x** です。

4 章 DHCP の概要 4-1
4.1 DHCP アドレスの割り当て 4-1
4.1.1 割り当てメカニズム 4-1
4.1.2 IP アドレスの割り当てプロセス 4-2
4.1.3 IP アドレスのリース延長 4-3
4.2 DHCP メッセージフォーマット 4-3
4.3 DHCP オプション 4-4
4.3.1 一般的な DHCP オプション 4-4
4.3.2 自己定義 DHCP オプション 4-5
4.4 プロトコルと標準 4-8

4章 DHCP の概要

DHCP（Dynamic Host Configuration Protocol）は、ネットワークにおいて通信に必要な基本的な設定を自動的に行う機能を提供します。

図 4-1に示すように、一般的な DHCP の構成は、同一サブネットに DHCP サーバとクライアントがあります。

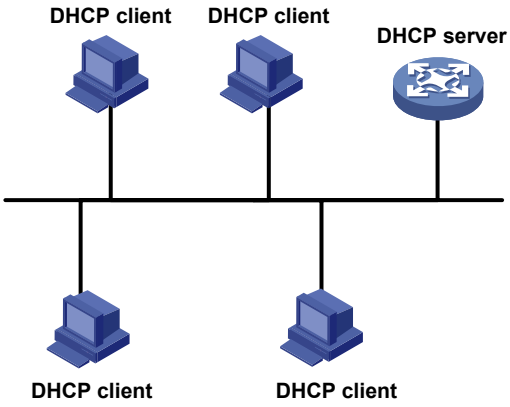


図 4-1 一般的な DHCP の構成

4.1 DHCPアドレスの割り当て

4.1.1 割り当てメカニズム

DHCP は以下の IP アドレスの割り当てメカニズムをサポートします。

- **手動割り当て** － ネットワーク管理者が WWW サーバなどのクライアントに IP アドレスを割り当てます。DHCP が割り当てられたアドレスをクライアントに伝送します。
- **自動割り当て** － DHCP がクライアントに永続的に使用可能な IP アドレスを割り当てます。
- **動的（ダイナミック）割り当て** － DHCP は、クライアントに一定期間（リース期間）使用可能な IP アドレスを割り当てます。ほとんどのクライアントがこの方法でアドレスを取得します。

4.1.2 IP アドレスの割り当てプロセス

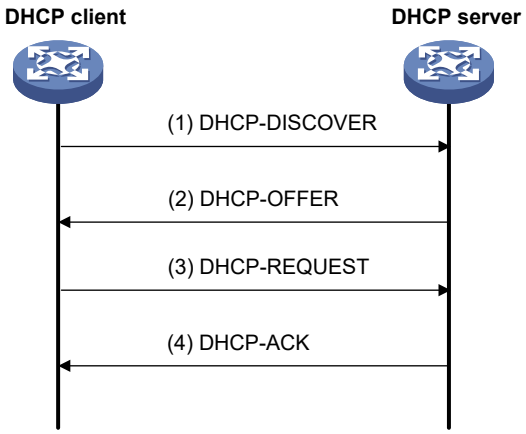


図 4-2 IP アドレスの割り当てプロセス

図 4-2に示すように DHCP サーバは以下の手順で DHCP クライアントに IP アドレスを割り当てます。

1) クライアントは DHCP-DISCOVER メッセージをブロードキャストし、DHCP サーバを特定します。
2) DHCP サーバは、DHCP-OFFER メッセージの中で IP アドレスなどの設定パラメータをクライアントに提供します。DHCP-OFFER の送信モードは DHCP-DISCOVER メッセージのフラグフィールドによって決定します。関連情報は、オペレーションマニュアルのセクション 3 *IP サービス* "*DHCP の概要*"の"*DHCP メッセージフォーマット*"を参照してください。
3) クライアントが複数の DHCP-OFFER を受信した場合、クライアントは最初に受け取った DHCP-OFFER を受け入れ、正式に IP アドレスを要求するために DHCP-REQUEST メッセージをブロードキャストで送信します。(他の DHCP サーバから提供された IP アドレスは他のクライアントに提供することができます。)
4) すべての DHCP サーバが DHCP-REQUEST メッセージを受信します。しかし、クライアントによって選択されたサーバのみ以下の動作を行います。
   - □ サーバは、クライアントに IP アドレスが割り当てられていることを確認して DHCP-ACK メッセージを返します。
   - □ IP アドレスの割り当てを拒否して DHCP-NAK ユニキャストメッセージを返します。

クライアントは DHCP-ACK メッセージを受信した後、クライアントは割り当てられた IP アドレスを使用する前に、詳細を確認します。

- 割り当てられた IP アドレスが使用中であるかどうかを確認します。Gratuitous ARP パケットをブロードキャストで送信することによって、サーバから割り当てられた IP アドレスが使用中かどうかを調べます。一定時間内に応答がなければ、クライアントはこの IP アドレスを使用することができます。
- 割り当てられた IP アドレスがクライアントで使用している IP アドレスと同一サブネットにないかどうかを確認します。

それ以外の場合、クライアントは DHCP-DECLINE メッセージをサーバに送信し、再度 IP アドレスを要求します。

4.1.3 IP アドレスのリース延長

DHCP サーバがクライアントに動的に割り当てた IP アドレスには、リース期間があります。リース期間が経過すると、その IP アドレスは DHCP から返還を要求（回収）されます。クライアントが再び IP アドレスを使用する場合は、リース期間を延長する必要があります。

リース期間の半分が経過したところで、DHCP クライアントはリース期間を延長するために DHCP サーバに DHCP-REQUEST ユニキャストメッセージを送信します。IP アドレスの使用状況に依存して、DHCP サーバは以下のメッセージのいずれか 1 つを返します。

- クライアントのリース期間が延長されていることを確認する DHCP-ACK ユニキャストを返します。
- 要求を拒否する DHCP-NAK ユニキャストメッセージを返します。

クライアントが応答を受信しない場合、クライアントはリース期間が 7/8 経過したところで、リースを延長するために別の DHCP-REQUEST メッセージをブロードキャストします。IP アドレスの使用状況に応じて、DHCP サーバはリース期間を延長されたことを示す DHCP-ACK ユニキャストあるいは DHCP-NAK ユニキャストメッセージを返します。

4.2 DHCPメッセージフォーマット

図 4-3に DHCP メッセージフォーマットを示します。DHCP フィールドのいくつかを異なる方法で使用します。カッコ内の数字は、各フィールドのサイズをバイト数で示したものです。

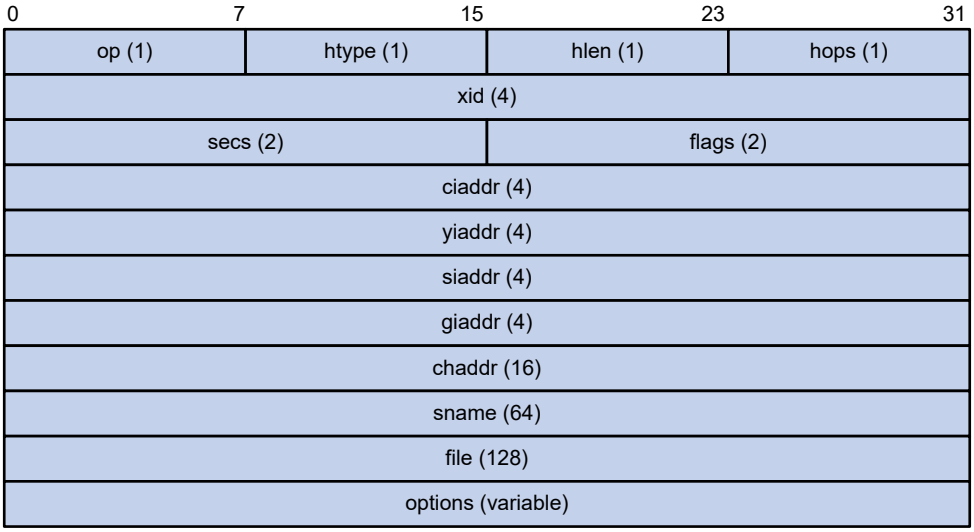


図 4-3 DHCP メッセージフォーマット

- **op**– オプションフィールドに定義されているメッセージタイプです。1 = REQUEST,2 = REPLY
- **htype, hlen**– DHCP クライアントのハードウェアアドレスのタイプと長さです。
- **hops**– 要求メッセージが伝送される（経由する）リレーエージェントの数です。

- **xid**– トランザクション ID で、IP アドレスの割り当てを特定するために、クライアントがランダムに選択した数です。
- **secs**– クライアントがアドレスを取得または更新プロセスを始めてから経過した秒数です。このフィールドは予約されており 0 に設定されています。
- **flags**– 1 ビット目は BROADCAST（B）フラグです。このフラグが 0 に設定されていると、DHCP サーバは応答をユニキャストで返します。このフラグの設定値が 1 の場合は、DHCP サーバはブロードキャストで応答を返します。フラグフィールドの残りのビットは、今後の使用のために予約されています。
- **ciaddr**– 有効で使用可能なクライアントの IP アドレスです。それ以外の場合は、0 に設定されています。（クライアントは、このフィールドを特定の IP アドレスを要求するために使用しません。）
- **yiaddr**– DHCP サーバが DHCP クライアントに割り当てる IP アドレスです。
- **siaddr**– サーバの IP アドレスです。クライアントはここから設定パラメータを取得します。
- **giaddr**– 要求メッセージが最初に伝送されたリレーエージェントのゲートウェイ IP アドレスです。
- **chaddr**– クライアントの MAC アドレスです。
- **sname**– サーバのホスト名です。クライアントはここから設定パラメータを取得します。
- **file**– サーバからクライアントに対して定義されたブートファイル名（システムソフトウェアイメージと呼ばれます）、パス情報です。
- **options**– オプションの可変長パラメータです。メッセージタイプ、リース期間、DNS サーバの IP アドレスおよび WINS サーバの IP アドレスなどが含まれます。

4.3 DHCPオプション

DHCP メッセージは、BOOTP（Bootstrap Protocol）と同じメッセージフォーマットを使用しますが、DHCP は動的な IP アドレス割り当て情報と追加の設定情報をクライアントに送信するため、option フィールドを使用します。

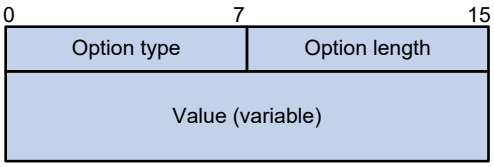


図 4-4 DHCP オプションフォーマット

4.3.1 一般的な DHCP オプション

以下に一般的な DHCP オプションを示します。

- **オプション 3** –　ルータのオプションです。ゲートウェイアドレスを指定します。
- **オプション 6** –　DNS サーバのオプションです。DNS サーバの IP アドレスを指定します。
- **オプション 33** –　スタティックルートオプションです。ルーティングテーブルに追加する必要のあるクラスフルスタティックルート（クラスフルスタティックルートの

宛先アドレス）のリストを指定します。クライアントはルーティングテーブルに追加します。オプション 33 とオプション 121 の両方が存在する場合、オプション 33 は無視されます。

- **オプション 51** – IP アドレスのリースオプションです。
- **オプション 53** – DHCP メッセージタイプのオプションです。DHCP メッセージのタイプを識別します。
- **オプション 55** – パラメータ要求リストのオプションです。DHCP クライアントが、指定の設定パラメータを要求するために使用します。このオプションには、クライアントが要求したパラメータに対応する値が含まれます。
- **オプション 60** – ベンダクラスの識別オプションです。DHCP クライアントがベンダを識別するために使用します。DHCP サーバが、DHCP クライアントを区別し、指定された IP アドレスを割り当てるために使用します。
- **オプション 66** – TFTP サーバ名のオプションです。クライアントに割り当てる TFTP サーバを指定します。
- **オプション 67** – ブートファイル名のオプションです。クライアントに割り当てるブートファイル名を指定します。
- **オプション 121** – クラスレスルートオプションです。クラスレススタティックルート（スタティックルートの宛先ネットワークアドレスがクラスレス）のリストを指定します。クライアントがルーティングテーブルに追加するために要求します。オプション 33 とオプション 121 の両方が存在する場合、オプション 33 は無視されます。
- **オプション 150** – TFTP サーバの IP アドレスのオプションです。クライアントに割り当てる TFTP サーバの IP アドレスを指定します。

DHCP オプションについての詳細は、RFC2132、RFC3442 を参照してください。

4.3.2 自己定義 DHCP オプション

オプション 43、オプション 82、オプション 184 のようなオプションは、RFC2132 で定義されていません。

I. ベンダ指定オプション（オプション 43）

DHCP サーバとクライアントは、ベンダ指定の設定情報を交換するため、オプション 43 を使用します。

DHCP クライアントはオプション 43 を以下の情報を通して取得します。

- ACS の URL、ユーザ名、パスワードを含んだ自動設定パラメータ（ACS パラメータ）です。
- CPE によって DHCP サーバから取得され、ベンダ固有の設定とパラメータを選択するために ACS に送信されるサービスプロバイダ識別子です。
- PXE（Preboot Execution Environment）サーバからブートファイルあるいは、他のコントロール情報を取得するために使用する PXE サーバアドレスです。

1) オプション 43 のフォーマット

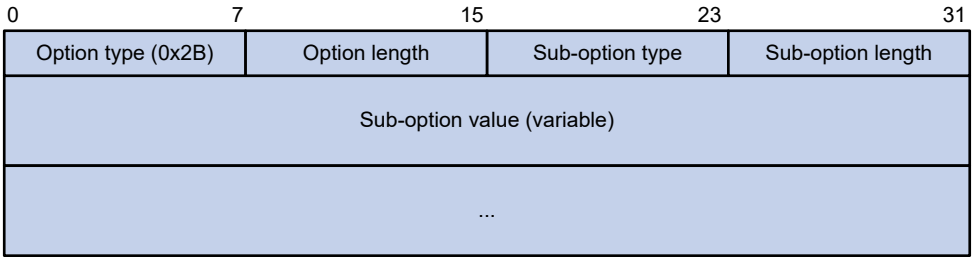


図 4-5 オプション 43 のフォーマット

図 4-5に示すように、ネットワーク設定パラメータは、異なるオプション 43 のサブオプションで送信されます。

- **サブオプションタイプ** ー サブオプションのタイプです。フィールド値は、0x01（ACS パラメータのサブオプション）、0x02（サービスプロバイダ識別子のサブオプション）または 0x80（PXE サーバアドレスのサブオプション）です。
- **サブオプション長** ー サブオプションタイプとサブオプション長フィールドを除くサブオプションの長さです。
- **サブオプション値** ー サブオプションによって値のフォーマットは変更します。

2)　サブオプションフィールドのフォーマット

- **ACS パラメータのサブオプションフィールド**– 図 4-6に示すように、ACS パラメータのサブオプションのフィールドは、ACS の URL、ユーザ名、パスワードです。それぞれの間はスペース（0x20）で分離されます。

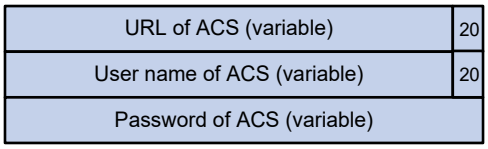


図 4-6 サブオプションフィールドのフォーマット

- **サービスプロバイダ識別子のサブオプションフィールド** ー サービスプロバイダ識別子のサブオプションフィールドは、サービスプロバイダ識別子を含みます。
- **PXE サーバアドレスのサブオプションフィールド** ー 図 4-7に示すように、PXE server type が 0 で、Server number がサブオプションに含まれる PXE サーバの数を示し、Server IP addresses が PXE サーバの IP アドレスを示します。

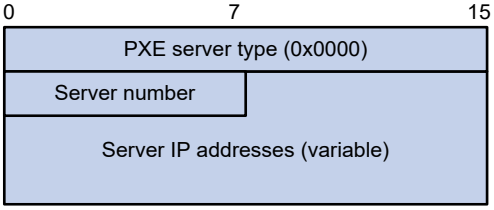


図 4-7 PXE サーバアドレスのサブオプションフィールド

II. リレーエージェントオプション（オプション 82）

オプション 82 は、オプションフィールドにおけるリレーエージェントのオプションです。DHCP クライアントの位置情報を記録します。DHCP リレーエージェントあるいは DHCP snooping がクライアントの要求を受信すると、要求メッセージにオプション 82 を追加してサーバに送信します。

管理者は DHCP クライアントの位置を特定して、セキュリティ管理とアカウンティングを実行することができます。DHCP サーバは、クライアントの個別の設定ポリシーを提供するためにオプション 82 を使用します。

オプション 82 には、最大 255 のサブオプションがあります。少なくとも 1 つのサブオプションを定義する必要があります。オプション 82 は、サブオプション 1（Circuit ID）とサブオプション 2（Remote ID）、サブオプション 5（Link Selection）の 3 つのサブオプションをサポートしています。オプション 82 は標準の定義がありません。ベンダによってパディングフォーマットは変わります。

- Circuit ID は以下に示すパディングフォーマットを持ちます。
  - **文字列パディングフォーマット** – ユーザが定義した文字列を含みます。
  - **標準（Normal）パディングフォーマット** – VLAN ID、クライアントの要求を受信したインタフェースのインタフェース番号を含みます。
  - **詳細（Verbose）パディングフォーマット** – ユーザ定義のアクセスノード識別子、VLAN ID、クライアントの要求を受信したインタフェースの番号、インタフェースのタイプを含みます。
- Remote ID は以下に示すパディングフォーマットを持ちます。
  - **文字列パディングフォーマット** – ユーザが定義した文字列を含みます。
  - **標準（Normal）パディングフォーマット** – DHCP リレーエージェントのインタフェースの MAC アドレスあるいはクライアントの要求を受信した DHCP snooping の MAC アドレスを含みます。
  - **システム名パディングフォーマット** – 装置のシステム名を含みます。装置のシステム名を設定する場合、system view で **sysname** コマンドを使用します。
- Link Selection は、**giaddr** フィールドの IP アドレスあるいは DHCP リレーインタフェースの IP アドレスを送信します。サブオプションはオプション 82 に含まれます。

III. オプション 184

オプション 184 は予約されているオプションです。パラメータを必要に応じて定義することができます。音声機能を持つ DHCP クライアントが DHCP サーバから音声パラメータを取得できるため、装置は音声関連パラメータを含むオプション 184 をサポートします。

オプション 184 は以下のサブオプションがあります。

- **サブオプション 1** – プライマリネットワークコーリングプロセッサの IP アドレスを指定します。プライマリネットワークコーリングプロセッサはネットワークコーリング制御ソースとして機能し、ダウンロード可能なプログラムを提供するサーバです。オプション 184 では、他のサブオプションを適用させるためには、サブオプション 1 を定義する必要があります。
- **サブオプション 2** – プライマリネットワークコーリングプロセッサが到達不可能な場合に、DHCP クライアントがコンタクトをとるバックアップのネットワークコーリングプロセッサの IP アドレスです。
- **サブオプション 3** – 音声 VLAN ID、および DHCP クライアントがこの ID を音声 VLAN として適用するかどうかの結果を示します。

- **サブオプション 4** － ターゲットユーザの IP アドレスと呼び出し番号を含むファイルオーバルートを指定します。プライマリとバックアップのコーリングプロセッサが両方とも到達不可能な場合、SIP VoIP ユーザは直接ターゲットの SIP ユーザに接続を確立するために使用する宛先 IP アドレスと呼び出し番号（SIP ユーザは IP アドレスとナンバを使用して相互に通信する）を指定します。

4.4 プロトコルと標準

- RFC 2131, *Dynamic Host Configuration Protocol*
- RFC 2132, *DHCP Options and BOOTP Vendor Extensions*
- RFC 1542, *Clarifications and Extensions for the Bootstrap Protocol*
- RFC 3046, *DHCP Relay Agent Information Option*
- RFC 3442, *The Classless Static Route Option for Dynamic Host Configuration Protocol (DHCP) version 4*

目次

このセクションのページは**3-x-x** です。

5 章 DHCP サーバ.....5-1
5.1 概要.....5-1
5.1.1 DHCP アドレスプール.....5-1
5.1.2 IP アドレス割り当て順序.....5-3
5.2 DHCP サーバ設定作業リスト.....5-3
5.3 DHCP サーバのアドレスプールの設定.....5-3
5.3.1 設定作業リスト.....5-3
5.3.2 DHCP アドレスプールの作成.....5-4
5.3.3 DHCP アドレスプールの IP アドレス範囲の設定.....5-4
5.3.4 DHCP クライアントのゲートウェイの設定.....5-6
5.3.5 クライアントへのドメイン名サフィックスの設定.....5-7
5.3.6 DHCP クライアントの DNS サーバの設定.....5-7
5.3.7 DHCP クライアントの WINS サーバと NetBIOS ノードタイプの設定.....5-7
5.3.8 DHCP クライアントの BIMS サーバ情報の設定.....5-8
5.3.9 DHCP クライアントのオートコンフィグレーションの設定ファイルの設定.....5-8
5.3.10 DHCP クライアントのサーバの設定.....5-9
5.3.11 DHCP クライアントのオプション 184 パラメータの設定.....5-9
5.3.12 DHCP ユーザクラスの設定.....5-10
5.3.13 カスタマイズ DHCP オプションの設定.....5-10
5.4 DHCP の有効化.....5-12
5.5 インタフェースでの DHCP サーバの有効化.....5-12
5.6 インタフェースでのアドレスプールの適用.....5-12
5.7 IP アドレス競合検出の設定.....5-13
5.8 オプション 82 の処理モードの有効化.....5-13
5.9 DHCP サーバが送信した DHCP パケットの DSCP 値の設定.....5-14
5.10 DHCP サーバの表示と維持.....5-14
5.11 DHCP サーバ設定例.....5-15
5.11.1 スタティック IP アドレスの割り当て設定例.....5-15
5.11.2 ダイナミック IP アドレスの割り当て設定例.....5-17
5.11.3 プライマリ、セカンダリサブネット設定例.....5-19
5.11.4 自己定義オプション設定例.....5-21
5.12 DHCP サーバ設定のトラブルシューティング.....5-22
5.12.1 症状.....5-22
5.12.2 分析.....5-22
5.12.3 解決策.....5-22

5章 DHCP サーバ

5.1 概要

DHCP(Dynamic Host Configuration Protocol)サーバ機能とは、IP アドレスなどのネットワーク利用に必要な設定情報を、各クライアントに自動的に割り当てる機能です。これにより、各クライアントでネットワークの詳細な設定を行わなくても、ネットワークに接続することができます。

DHCP サーバは以下のようなネットワークに適しています。

- 手動の設定や集中管理が難しいネットワーク
- 同時にアクセスできる IP アドレス数が制限されているネットワーク
- 多くのホストで、固定の IP アドレスが必要でないネットワーク

5.1.1 DHCP アドレスプール

各 DHCP アドレスプールは、割り当て可能な IP アドレス、ネットワーク設定パラメータのグループを持っています。DHCP サーバは、アドレスプールから IP アドレスとほかのパラメータを選択し、DHCP クライアントに割り当てます。

I. アドレス割り当てメカニズム

必要に応じて以下のようにアドレス割り当てメカニズムの設定を行います。

- **スタティックアドレス割り当て** － DHCP アドレスプールの IP アドレスをクライアントの MAC アドレスあるいは ID に手動で割り当てます。クライアントが IP アドレスを要求した場合、DHCP サーバは、スタティックバインディングの IP アドレスをクライアントに割り当てます。
- **ダイナミックアドレス割り当て** － DHCP アドレスプールの IP アドレス範囲を設定します。DHCP クライアントからの要求を受信した場合、DHCP サーバは、ダイナミックにアドレスプールの IP アドレス範囲から IP アドレスを選択します。

アドレスプールの IP アドレス範囲を設定する場合、アドレスプールの 1 つのプライマリサブネットと複数のセカンダリサブネットを設定します。

DHCP サーバは最初にプライマリサブネットから IP アドレスを選択します。プライマリサブネットに割り当て可能な IP アドレスがない場合、DHCP サーバは設定された順番でセカンダリサブネットから IP アドレスを選択します。

II. アドレスプール選択の原則

DHCP サーバは以下の原則に従い、アドレスプールを選択してクライアントに IP アドレスを割り当てます。

1) IP アドレスがクライアントの MAC アドレスあるいは ID にスタティックで割り当てられているアドレスプールがある場合は、DHCP サーバが、このアドレスプールを選択し、スタティックに割り当てられている IP アドレスとほかのパラメータをクライアントに割り当てます。
2) 受信インタフェースがアドレスプールに割り当てられている場合、DHCP サーバは、このアドレスプールを選択し、IP アドレスとほかのパラメータをクライアントに割り当てます。
3) 手動で設定したアドレスプールがなく、受信インタフェースに適用されるアドレスプールがない場合、DHCP サーバはクライアントの場所に応じて以下の方法でアドレスプールを選択します。
   - **クライアントとサーバが同一サブネットにある場合**－DHCP サーバは受信インタフェースの IP アドレスをすべてのアドレスプールのプライマリサブネットにマッチさせます。
     - マッチしたプライマリサブネットが複数ある場合、最長一致（ロンゲストマッチ）のルールでアドレスプールを選択します。
     - マッチしたプライマリサブネットがない場合、DHCP サーバはすべてのアドレスプールのセカンダリサブネットにマッチさせます。DHCP サーバは最長一致（ロンゲストマッチ）のルールでアドレスプールを選択します。
   - **クライアントとサーバが異なるサブネットにある場合**－DHCP サーバは DHCP リクエストの **giaddr** フィールドにある IP アドレスをすべてのアドレスプールのプライマリサブネットにマッチさせます。（DHCP リレーエージェントはクライアントとサーバの間にあります）
     - マッチしたプライマリサブネットが複数ある場合、最長一致（ロンゲストマッチ）のルールでアドレスプールを選択します。
     - マッチしたプライマリサブネットがない場合、DHCP サーバはすべてのアドレスプールのセカンダリサブネットにマッチさせます。DHCP サーバは最長一致（ロンゲストマッチ）のルールでアドレスプールを選択します。

たとえば、1.1.1.0/24 と 1.1.1.0/25 の 2 つのアドレスプールが設定可能ですが、DHCP サーバのインタフェースに適用されていないとします。

- 受信したインタフェースの IP アドレスが 1.1.1.1/25 である場合、DHCP サーバはアドレスプール 1.1.1.0/25 を選択します。アドレスプールに割り当て可能な IP アドレスがない場合、DHCP サーバはほかのプールを選択できず、アドレス割り当ては失敗します。
- 受信したインタフェースの IP アドレスが 1.1.1.130/25 である場合、DHCP サーバはアドレスプール 1.1.1.0/24 からクライアントの IP アドレスを選択します。

正しくアドレスの割り当てを行うため、以下のサブネットの 1 つでダイナミック割り当て用の IP アドレスを保持します。

- **クライアントとサーバが同一サブネットにある場合**－DHCP サーバのインタフェースが接続されているサブネット
- **クライアントとサーバが異なるサブネットにある場合**－クライアント側に面し、最初の DHCP リレーのインタフェースが接続されているサブネット

🕮 **メモ：**

ネットワークで最低 1 つの一致したプライマリのサブネットを設定してください。それ以外の場合、最初にセカンダリサブネットを選択します。セカンダリサブネットで割り当て可能な IP アドレス数より多くの DHCP クライアントが存在する場合、すべての DHCP クライアントに IP アドレスの割り当てを行うことができません。

5.1.2 IP アドレス割り当て順序

DHCP サーバはクライアントの IP アドレスを以下の順序で選択します。

1) クライアントの MAC アドレスあるいは ID に手動で割り当てされている IP アドレスです。
2) クライアントに割り当てられていた IP アドレスです。
3) DHCP-DISCOVER メッセージ内のオプション 50 フィールドに設定されている IP アドレスです。

   オプション 50 は、DHCP-DISCOVER メッセージの要求した IP アドレスフィールドです。クライアントが取得したい IP アドレスを設定するために、クライアントにより追加されます。追加される内容は、ユーザが定義します。
4) 適切な DHCP アドレスプールで検出された､最初に割り当て可能な IP アドレスです。
5) 競合していた IP アドレスか、リース期間を過ぎた IP アドレスです。割り当て可能な IP アドレスがない場合、サーバは応答しません。

🕮 **メモ：**

- クライアントが別のサブネットに移動した場合､DHCP サーバは一度クライアントに割り当てた IP アドレスの代わりに、新しいサブネットにマッチする IP アドレスを割り当てます。
- 競合した IP アドレスは 1 時間経過したのち、ほかの DHCP クライアントに割り当てることができます。

5.2 DHCPサーバ設定作業リスト

作業リスト
（必須設定項目） DHCPサーバのアドレスプールの設定
（必須設定項目） DHCPの有効化
（必須設定項目） インタフェースでのDHCPサーバの有効化
（オプション設定項目） インタフェースでのアドレスプールの適用
（オプション設定項目） IPアドレス競合検出の設定
（オプション設定項目） オプション82の処理モードの有効化
（オプション設定項目） DHCPサーバが送信したDHCPパケットのDSCP値の設定

5.3 DHCPサーバのアドレスプールの設定

5.3.1 設定作業リスト

作業リスト
（必須設定項目） DHCPアドレスプールの作成

作業リスト
少なくとも以下の作業の1つを実行します。 • DHCPアドレスプールのIPアドレス範囲の設定 • DHCPクライアントのゲートウェイの設定 • DHCPクライアントへのドメイン名サフィックスの設定 • DHCPクライアントのDNSサーバの設定 • DHCPクライアントのWINSサーバとNetBIOSノードタイプの設定 • DHCPクライアントのBIMSサーバ情報の設定 • DHCPクライアントのオートコンフィグレーションの設定ファイルの設定 • DHCPクライアントのサーバの設定 • クライアントのオプション184パラメータの設定 • DHCPユーザクラスの設定 • 自己定義DHCPオプションの設定

5.3.2 DHCP アドレスプールの作成

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． DHCP アドレスプールを作成し、その view に移行する	**dhcp server ip-pool** *pool-name*	デフォルト：設定なし

5.3.3 DHCP アドレスプールの IP アドレス範囲の設定

DHCP アドレスプールに、スタティックのアドレス割り当ておよびダイナミックアドレスの割り当ての両方を設定することができます。ダイナミックアドレスの割り当ては、1 つのプライマリサブネットに複数のセカンダリサブネットを設定することができます。

I. DHCP アドレスプールのプライマリサブネットと複数のセカンダリサブネットの設定

プライマリサブネットで割り当て可能な IP アドレスがない場合、DHCP サーバは、クライアントに要求するセカンダリサブネットの IP アドレスを割り当てることができます。

DHCP アドレスプールのプライマリサブネットとセカンダリサブネットを設定する場合、以下のガイドラインに従ってください。

- 各アドレスプールに 1 つのプライマリサブネットのみを設定することができます。**network** コマンドを使用して複数設定した場合、最後に行った設定が適用されます。
- 各アドレスプールで最大 32 のセカンダリサブネットを設定することができます。
- **forbidden-ip** コマンドで設定された IP アドレスは、現在のアドレスプールに割り当てすることができません。ほかのアドレスプールに割り当てすることができます。**dhcp server forbidden-ip** コマンドで設定した IP アドレスはアドレスプールに割り当てることができません。

以下に DHCP アドレスプールのプライマリサブネットとセカンダリサブネットを設定する方法を示します。

操作	コマンド	補足
3． system view に移行する	**system-view**	―
4． DHCP アドレスプールを作成し、その view に移行する	**dhcp server ip-pool** *pool-name*	デフォルト：設定なし
5． プライマリサブネットを設定する	**network** *network-address* [*mask-length* | **mask** *mask*]	デフォルト：設定なし
6． （オプション設定項目）セカンダリサブネットを設定する	**network** *network-address* [*mask-length* | **mask** *mask*] **secondary**	デフォルト：設定なし
7． （オプション設定項目）system view に戻る	**quit**	―
8． （オプション設定項目）アドレスのリース期間を設定する	**expired** { **day** *day* [**hour** *hour* [**minute** *minute* [**second** *second*]]] | **unlimited** }	デフォルト：1日
9． （オプション設定項目）ダイナミック割り当てから設定された IP アドレスを除外する	**forbidden-ip** *ip-address*&<1-8>	デフォルト：DHCPアドレスプールすべてのアドレスが割り当て可能です。 複数のアドレス範囲を除外する場合、このステップを繰り返します。
10．system view に戻る	**quit**	―
11．（オプション設定項目）グローバルにダイナミック割り当てから設定された IP アドレスを除外する	**dhcp server forbidden-ip** *start-ip-address* [*end-ip-address*]	デフォルト：DHCPサーバインタフェースのIPアドレスを除いて、DHCPアドレスプールすべてのアドレスが割り当て可能です。 複数のアドレス範囲を除外する場合、このステップを繰り返します。

II. DHCP アドレスプールのスタティック割り当ての設定

WWW サーバのような特定の DHCP クライアントは固定の IP アドレスが必要です。クライアントに固定の IP アドレスを提供する場合、MAC アドレスあるいはクライアントの ID を DHCP アドレスプールの IP アドレスにスタティックで割り当てることができます。

スタティック割り当てを設定する場合、以下のガイドラインに従ってください。

- 1 つの IP アドレスは 1 つの MAC アドレスあるいはクライアントの ID にのみ割り当てることができます。作成されたバインディングは変更することができません。DHCP クライアントのバインディングを変更する場合、最初に既存のバインディングを削除する必要があります。
- スタティックバインディングの IP アドレスは DHCP サーバインタフェースのアドレスにすることができません。そうしないと、IP アドレスの競合が発生し、隣接のクライアントが正常に IP アドレスを取得することができません。
- 同一装置の複数インタフェースはスタティック IP アドレスを要求するため、DHCP を使用します。この場合、要求しているインタフェースを識別するため MAC アドレスよりもクライアントの ID を設定する必要があります。そうしないと、IP アドレスの割り当てが失敗します。

以下にスタティックバインディングを設定する方法を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． DHCP アドレスプールを作成し、その view に移行する	**dhcp server ip-pool** *pool-name*	デフォルト：設定なし
3． スタティックバインディングを設定する	**static-bind ip-address** *ip-address* [*mask-length* | **mask** *mask*] { **client-identifier** *client-identifier* | **hardware-address** *hardware-address* [**ethernet** | **token-ring**] }	デフォルト：設定なし 複数のスタティックバインディングを設定する場合、このステップを繰り返します。
4． （オプション設定項目）アドレスのリース期間を設定する	**expired** { **day** *day* [**hour** *hour* [**minute** *minute* [**second** *second*]]] | **unlimited** }	デフォルト：1日

5.3.4 DHCP クライアントのゲートウェイの設定

DHCP クライアントはほかのネットワークへのパケットをゲートウェイに送信します。DHCP サーバは DHCP クライアントにゲートウェイアドレスを割り当てることができます。

DHCP サーバで各アドレスプールにゲートウェイアドレスを設定することができます。最大 64 つのゲートウェイを DHCP address pool view あるいは secondary subnet view で設定することができます。

DHCP サーバは以下の方法でセカンダリサブネットのクライアントにゲートウェイアドレスを割り当てます。

- address pool view と secondary subnet view の両方でゲートウェイアドレスを設定する場合、DHCP サーバは secondary subnet view で設定されたゲートウェイアドレスを設定します。
- ゲートウェイアドレスが address pool view で設定されているが、secondary subnet view にない場合、DHCP サーバは address pool view のゲートウェイアドレスを割り当てます。

以下に DHCP アドレスプールのゲートウェイを設定する方法を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． DHCP アドレスプールを作成し、その view に移行する	**dhcp server ip-pool** *pool-name*	デフォルト：設定なし
3． ゲートウェイを設定する	**gateway-list** *ip-address*&<1-64>	デフォルト：設定なし
4． （オプション設定項目）secondary subnet view に移行する	**network** *network-address* [*mask-length* | **mask** *mask*] **secondary**	―
5． （オプション設定項目）ゲートウェイを設定する	**gateway-list** *ip-address*&<1-64>	デフォルト：設定なし

5.3.5 クライアントへのドメイン名サフィックスの設定

DHCP サーバの DHCP アドレスプールにドメイン名サフィックス（DNS）を設定することができます。このサフィックスを設定することで、クライアントはドメイン名の入力部分のみ必要となります。システムは名前解決のため、ドメイン名サフィックスを追加します。DNS の詳細は、オペレーションマニュアルのセクション *3 IP サービス "DNS"*を参照してください。

以下に DHCP アドレスプールのドメイン名サフィックスの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． DHCP アドレスプールを作成し、その view に移行する	**dhcp server ip-pool** *pool-name*	デフォルト：設定なし
3． ドメイン名サフィックスを設定する	**domain-name** *domain-name*	デフォルト：設定なし

5.3.6 DHCP クライアントの DNS サーバの設定

インターネット上のホストがドメイン名を使用してアクセスする場合、DHCP クライアントは名前を解決するため、DNS（Domain Name System）サーバにコンタクトをとる必要があります。DHCP アドレスプールで最大 8 つの DNS サーバを設定することができます。

以下に DHCP アドレスプールの DNS サーバの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． DHCP address pool view に移行する	**dhcp server ip-pool** *pool-name*	デフォルト：設定なし
3． DNS サーバを設定する	**dns-list** *ip-address*&<1-8>	デフォルト：設定なし

5.3.7 DHCP クライアントの WINS サーバと NetBIOS ノードタイプの設定

NetBIOS プロトコルを使用している Microsoft DHCP クライアントは、名前解決のために WINS（Windows Internet Naming Service）サーバにコンタクトする必要があります。DHCP アドレスプールのクライアントに最大 8 つの WINS サーバを設定することができます。

クライアントが名前解決できるように、DHCP アドレスプールに NetBIOS ノードタイプを設定する必要があります。NetBIOS ノードタイプには以下の 4 つがあります。

- **b（ブロードキャスト）-ノード** － b-ノードクライアントは、ブロードキャストメッセージで宛先名を送信します。宛先はメッセージを受信後、クライアントに IP アドレスを返します。
- **p（ピアツー-ピア）-ノード** － P-ノードクライアントは WINS サーバにユニキャストメッセージで宛先名を送信します。WINS サーバは宛先の IP アドレスを返します。
- **m（ミックス）-ノード** － m-ノードクライアントは、宛先名をブロードキャストし、応答がない場合は、WINS サーバに宛先名をユニキャストして宛先 IP アドレスを取得します。

- **h（ハイブリッド）-ノード** – h-ノードクライアントは宛先名を WINS サーバにユニキャストし、応答がない場合は、宛先名をブロードキャストして宛先 IP アドレスを取得します。

以下に DHCP アドレスプールの WINS サーバと NetBIOS ノードタイプの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． DHCP アドレスプールを作成し、その view に移行する	**dhcp server ip-pool** *pool-name*	デフォルト：設定なし
3． WINS サーバを設定する	**nbns-list** *ip-address*&<1-8>	b-ノードでは、オプション設定項目です。 デフォルト：設定なし
4． NetBIOS ノードタイプを設定する	**netbios-type** { **b-node** | **h-node** | **m-node** | **p-node** }	デフォルト：設定なし

5.3.8 DHCP クライアントの BIMS サーバ情報の設定

この設定は BIMS サーバの IP アドレス、ポート番号および共有キーをクライアントに提供します。DHCP クライアントは BIMS（branch intelligent management system）サーバから取得した設定ファイルを使用して、ソフトウェアの定期的なアップデートとバックアップを実行します。

以下に DHCP アドレスプールの BIMS サーバの IP アドレス、ポート番号、共有キーの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． DHCP アドレスプールを作成し、その view に移行する	**dhcp server ip-pool** *pool-name*	デフォルト：設定なし
3． BIMS サーバの IP アドレス、ポート番号、共有キーを設定する	**bims-server ip** *ip-address* [**port** *port-number*] **sharekey** { **cipher** | **simple** } *string*	デフォルト：設定なし

5.3.9 DHCP クライアントのオートコンフィグレーションの設定ファイルの設定

オートコンフィグレーションは装置がコンフィグレーションファイルなしで起動する場合、装置がサーバから自動でコンフィグレーションの設定を取得できることを有効にします。DHCP サーバ、DNS サーバ、TFTP サーバの協力が必要です。

コンフィグレーションファイルの取得を行うため DHCP サーバでパラメータを設定する際、以下のガイドラインに従ってください。

- コンフィグレーションファイルが TFTP サーバにある場合、TFTP サーバの IP アドレスあるいはコンフィグレーションファイル名を設定してください。

DHCP クライアントはコンフィグレーションファイルを取得する TFTP サーバとコンタクトをとるため、取得したパラメータを使用します。

以下に DHCP アドレスプールのコンフィグレーションファイル名を設定する方法を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． DHCP アドレスプールを作成し、その view に移行する	**dhcp server ip-pool** *pool-name*	デフォルト：設定なし
3． TFTP サーバの IP アドレスあるいは名前を設定する	● TFTPサーバのIPアドレスを設定する： **tftp-server ip-address** *ip-address* ● TFTPサーバの名前を設定する： **tftp-server domain-name** *domain-name*	IPアドレスあるいはTFTPサーバの名前を設定することができます。 デフォルト：設定なし
4． ブートファイル名を設定する	**bootfile-name** *bootfile-name*	デフォルト：設定なし

5.3.10 DHCP クライアントのサーバの設定

特定の DHCP クライアントは TFTP サーバなどのサーバから設定情報を取得する必要があります。サーバの IP アドレスを設定することができます。DHCP サーバはサーバの IP アドレスを DHCP クライアントにほかの設定情報と共に送信します。

以下にサーバの IP アドレスの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． DHCP アドレスプールを作成し、その view に移行する	**dhcp server ip-pool** *pool-name*	デフォルト：設定なし
3． サーバの IP アドレスを設定する	**next-server** *ip-address*	デフォルト：設定なし

5.3.11 DHCP クライアントのオプション 184 パラメータの設定

音声サービスを備えた DHCP クライアントに音声サービスを割り当てるためには、DHCP サーバにオプション 184 を設定する必要があります。オプション 184 の詳細は、オペレーションマニュアルのセクション 3 *IP サービス”DHCP の概要*”を参照してください。

以下に DHCP アドレスプールのオプション 184 パラメータの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． DHCP アドレスプールを作成し、その view に移行する	**dhcp server ip-pool** *pool-name*	デフォルト：設定なし

操作	コマンド	補足
3． プライマリネットワークコーリングプロセッサの IP アドレスを設定する	**voice-config ncp-ip** *ip-address*	デフォルト：設定なし このコマンドを設定した後、ほかのオプション184のパラメータが適用されます。
4． （オプション設定項目）バックアップサーバの IP アドレスを設定する	**voice-config as-ip** *ip-address*	デフォルト：設定なし
5． （オプション設定項目）音声 VLAN を設定する	**voice-config voice-vlan** *vlan-id* { **disable** | **enable** }	デフォルト：設定なし
6． （オプション設定項目）フェイルオーバーの IP アドレス､ダイヤル番号を設定する	**voice-config fail-over** *ip-address dialer-string*	デフォルト：設定なし

5.3.12 DHCP ユーザクラスの設定

DHCP サーバは、受信した DHCP 要求のハードウェアアドレス、オプション情報、または giaddr フィールドに従って、DHCP ユーザをさまざまなユーザクラスに分類します。サーバは、異なるユーザクラスの DHCP クライアントに IP アドレスと設定パラメータを割り当てます。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． DHCP ユーザクラスを作成し、その view に移行する	**dhcp class** *class-name*	―
3． DHCP ユーザクラスの一致ルールを設定します。	**if-match rule** *rule-number* **{ hardware-address** *hardware-address* **mask** *hardware-address-mask* **| option** *option-code* **[ascii** *ascii-string* **[offset** *offset* **| partial] | hex** *hex-string* **[mask** *mask* **| offset** *offset* **length** *length* **| partial]] | relay-agent** *gateway-address* **}**	デフォルト：設定なし

5.3.13 カスタマイズ DHCP オプションの設定

重要：
カスタマイズ DHCP オプションを設定する場合、DHCP の動作への影響を十分考慮して行ってください。

カスタマイズ DHCP オプションを設定すると、以下のことが可能になります。

- 新規に定義したオプションを追加します。
- オプション 43 のようなベンダ定義のオプションを追加します。

- CLI によって設定できない、専用の設定コマンドのオプションを追加します。たとえば **option 4 ip-address 1.1.1.1** コマンドで DHCP クライアントにタイムサーバアドレス 1.1.1.1 を定義することができます。
- 予約されたオプションの設定コマンドの制限を超過させる場合、すべてのオプションを追加します。たとえば、**dns-list** コマンドを使用して、8 つを超える DNS サーバアドレスを設定することはできません。8 つを超える DNS サーバを設定する場合、すべての DNS サーバで **option 6** コマンドを使用する必要があります。

表 5-1 一般的な DHCP オプション

オプション	オプション名	対応コマンド	コマンドパラメータ
3	Router Option	**gateway-list**	**ip-address**
6	Domain Name Server Option	**dns-list**	**ip-address**
15	Domain Name	**domain-name**	**ascii**
44	NetBIOS over TCP/IP Name Server Option	**nbns-list**	**ip-address**
46	NetBIOS over TCP/IP Node Type Option	**netbios-type**	**hex**
66	TFTP server name	**tftp-server**	**ascii**
67	Boot file name	**bootfile-name**	**ascii**
43	Vendor Specific Information	—	**hex**

I. DHCP アドレスプールでのカスタマイズ DHCP オプション設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. DHCP アドレスプールを作成し、その view に移行する	**dhcp server ip-pool** *pool-name*	デフォルト：設定なし
3. カスタマイズ DHCP オプションを設定する	**option** *code* { **ascii** *ascii-string* | **hex** *hex-string* | **ip-address** *ip-address*&<1-8> }	デフォルト：設定なし DHCPオプショングループで設定されたDHCPオプションはDHCPアドレスプールで設定されたDHCPオプションより優先されます。

II. DHCP オプショングループでのカスタマイズ DHCP オプション設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. DHCP オプショングループを作成し、その view に移行する	**dhcp option-group** *option-group-number*	—
3. カスタマイズ DHCP オプションを設定する	**option** *code* { **ascii** *ascii-string* | **hex** *hex-string* | **ip-address** *ip-address*&<1-8> }	デフォルト：設定なし DHCPオプショングループで設定されたDHCPオプションはDHCPアドレスプールで設定されたDHCPオプションより優先されます。

操作	コマンド	補足
4． system view に移行する	**quit**	―
5． DHCP アドレスプールを作成し、その view に移行する	**dhcp server ip-pool** *pool-name*	デフォルト：設定なし
6． DHCP ユーザクラスに DHCP オプショングループを指定する。	**class** *class-name* **option-group** *option-group-number*	デフォルト：設定なし DHCPユーザクラスは事前に作成しておく必要があります。

5.4 DHCPの有効化

ほかの DHCP 設定を有効にするには、DHCP を有効にする必要があります。

以下に DHCP の有効化の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． DHCP を有効にする	**dhcp enable**	デフォルト：無効

5.5 インタフェースでのDHCPサーバの有効化

インタフェースで DHCP サーバを有効にする場合、この設定を行います。インタフェースで DHCP 要求を受信すると、DHCP サーバは DHCP アドレスプールから DHCP クライアントに IP アドレスとほかの設定パラメータを割り当てます。

以下にインタフェースでの DHCP サーバの有効化の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． interface view に移行する	**interface** *interface-type interface-number*	―
3． インタフェースで DHCP サーバを有効にする	**dhcp select server**	デフォルト：有効

5.6 インタフェースでのアドレスプールの適用

インタフェースに DHCP アドレスプールを適用する場合、この設定を行います。

インタフェースから DHCP 要求を受信すると、DHCP サーバは以下の方法でアドレスを割り当てます。

- DHCP 要求にスタティックバインディングがある場合、DHCP サーバはスタティックバインディングが含まれるアドレスプールからスタティックバインディング IP アドレスと設定パラメータをクライアントに割り当てます。
- DHCP 要求にスタティックバインディングがない場合、DHCP サーバはアドレスプールと設定パラメータのために適用されたアドレスプールを選択します。

以下にインタフェースにアドレスプールを適用する設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． interface view に移行する	**interface** *interface-type interface-number*	ー
3． インタフェースにアドレスプールを適用する	**dhcp server apply ip-pool** *pool-name*	デフォルト : 適用されていません。 アドレスプールがない場合、DHCPサーバはダイナミックアドレスの割り当てに失敗します。

5.7 IPアドレス競合検出の設定

IP アドレスを割り当てる前に、DHCP サーバは、ping パケットを送信して、割り当てるアドレスが使用中かどうかを調べます。

- DHCP サーバが設定した期間内に ping 応答を受信した場合、サーバは別の IP アドレスに ping を行います。
- 応答がない場合、指定数の ping パケットが送信されるまでサーバは IP アドレスに ping を行います。応答がない場合は、サーバは要求元のクライアントに IP アドレスを割り当てます。DHCP クライアントは gratuitous ARP パケットを送信して IP アドレスが競合しているかどうかを調べます。

以下に IP アドレス競合検出の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． （オプション設定項目）IP アドレス競合検出の ping パケットの最大数を設定する	**dhcp server ping packets** *number*	デフォルト：1 **0**に設定した場合、IPアドレスの競合検出を行いません。
3． （オプション設定項目）ping に対する応答の待機タイムアウトを設定する	**dhcp server ping timeout** *milliseconds*	デフォルト：500ms **0**に設定した場合、IPアドレスの競合検出を行いません。

5.8 オプション82の処理モードの有効化

DHCP サーバがオプション 82 を処理するように設定されている場合、オプション 82 のメッセージを受信すると、DHCP サーバは DHCP 応答メッセージにオプション 82 を追加します。

DHCP サーバがオプション 82 を無視するように設定されている場合、DHCP 応答メッセージにオプション 82 を追加しません。

オプション 82 のパラメータが正常に動作するために、DHCP サーバと DHCP リレーエージェントの両方でオプション 82 を処理するように有効にする必要があります。

以下に DHCP サーバでのオプション 82 の処理モードの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． オプション 82 の処理モードを有効にする	**dhcp server relay information enable**	デフォルト：有効

5.9 DHCPサーバが送信したDHCPパケットのDSCP値の設定

パケットの DSCP 値は、パケットの優先度レベルを設定し、パケットの優先度に影響します。

以下に DHCP サーバが送信した DHCP パケットの DSCP 値の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． DHCP サーバが送信した DHCP パケットの DHCP 値を設定する	**dhcp dscp** *dscp-value*	デフォルト：56

5.10 DHCPサーバの表示と維持

重要：

DHCP サーバの再起動あるいは、**reset dhcp server ip-in-use** コマンドが実行されると、すべてのリース情報を削除します。DHCP サーバは DHCP クライアントからのリース期間延長要求を拒否するので、クライアントは再度 IP アドレスを要求する必要があります。

すべての view で **display** コマンドを実行でき、user view で **reset** コマンドを実行できます。

操作	コマンド
IPアドレスの競合に関する情報を表示する	**display dhcp server conflict** [**ip** *ip-address*]
リース期限切れに関する情報を表示する	**display dhcp server expired** [**ip** *ip-address* | **pool** *pool-name*]
割り当て可能なIPアドレスに関する情報を表示する	**display dhcp server free-ip** [**pool** *pool-name*]
割り当てられたIPアドレス情報を表示する	**display dhcp server ip-in-use** [**ip** *ip-address* | **pool** *pool-name*]
DHCPサーバの統計情報を表示する	**display dhcp server statistics** [**pool** *pool-name*]
DHCPアドレスプールの情報を表示する	**display dhcp server pool** [*pool-name*]
IPアドレスの競合に関する情報を削除する	**reset dhcp server conflict** [**ip** *ip-address*]
リース期限切れに関する情報を削除する	**reset dhcp server expired** [**ip** *ip-address* | **pool** *pool-name*]

操作	コマンド
割り当てられたIPアドレス情報を削除する	**reset dhcp server ip-in-use** [**ip** *ip-address* | **pool** *pool-name*]
DHCPサーバの統計情報を削除する	**reset dhcp server statistics**

5.11 DHCPサーバ設定例

DHCP のネットワークの構築は以下のタイプがあります。

- 同一サブネット上の DHCP サーバと DHCP クライアントは、直接メッセージを交換できます。
- 異なるサブネット上の DHCP サーバと DHCP クライアントは、DHCP リレーエージェントを介して相互に通信します。

DHCP サーバの設定は、どちらのタイプでも同じです。

5.11.1 スタティック IP アドレスの割り当て設定例

I. ネットワーク要件

図 5-1に示すように、Switch B（DHCP クライアント）、Switch C（BOOTP クライアント）は Switch A（DHCP サーバ）からスタティック IP アドレス、DNS サーバアドレス、ゲートウェイアドレスを取得します。

Switch B の VLAN インタフェース 2 のクライアント ID は以下です。

0030-3030-662e-6532-3030-2e30-3030-322d-4574-6865-726e-6574

Switch C の VLAN インタフェース 2 の MAC アドレスは 000f-e200-01c0 です。

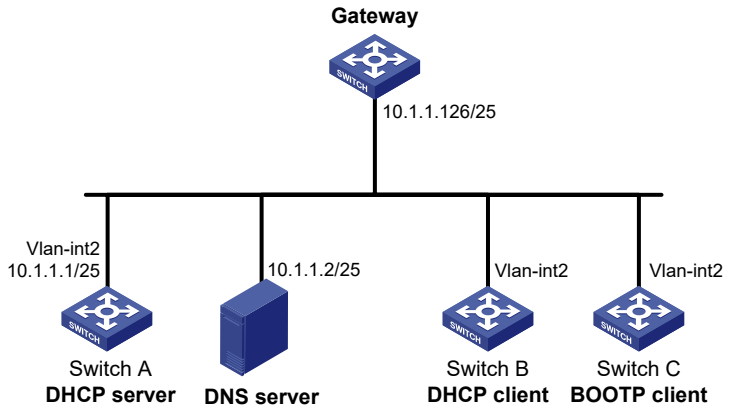


図 5-1 ネットワーク図

II. 設定手順

1)　Switch A の VLAN インタフェース 2 に IP アドレスを設定します。

```
<SwitchA> system-view
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ip address 10.1.1.1 25
[SwitchA-Vlan-interface2] quit
```

2)　DHCP サーバを設定します。

DHCP を有効にします。

```
[SwitchA] dhcp enable
```

VLAN インタフェース 2 で DHCP サーバを有効にします。

```
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] dhcp select server
[SwitchA-Vlan-interface2] quit
```

DHCP アドレスプール 0 を作成します。

```
[SwitchA] dhcp server ip-pool 0
```

Switch B のスタティックバインディングの設定をします。

```
[SwitchA-dhcp-pool-0] static-bind ip-address 10.1.1.5 25 client-identifier 0030-3030-662e-6532-3030-2e30-3030-322d-4574-6865-726e-6574
```

Switch C のスタティックバインディングの設定をします。

```
[SwitchA-dhcp-pool-0] static-bind ip-address 10.1.1.6 25 hardware-address 000f-e200-01c0
```

DNS サーバ、ゲートウェイを設定します。

```
[SwitchA-dhcp-pool-0] dns-list 10.1.1.2
[SwitchA-dhcp-pool-0] gateway-list 10.1.1.126
[SwitchA-dhcp-pool-0] quit
```

III. 設定の確認

Switch B は Switch A から IP アドレス 10.1.1.5 とほかのパラメータを取得します。（詳細は省略します。）

Switch C は Switch A から IP アドレス 10.1.1.6 とほかのパラメータを取得します。（詳細は省略します。）

DHCP サーバでクライアントに割り当てられた IP アドレスを表示します。

```
[SwitchA] display dhcp server ip-in-use
IP address       Client-identifier/     Lease expiration      Type
                 Hardware address
10.1.1.5         0030-3030-662e-6532-   Jan 21 14:27:27 2014  Static(C)
                 3030-2e30-3030-322d-
                 4574-6865-726e-6574
10.1.1.6         000f-e200-01c0         Unlimited             Static(C)
```

5.11.2 ダイナミック IP アドレスの割り当て設定例

I. ネットワーク要件

図 5-2に示すように、DHCP サーバ（Switch A）はサブネット 10.1.1.0/24 のクライアントに IP アドレスを割り当てます。10.1.1.0/24 はさらに 10.1.1.0/25 と 10.1.1.128/25 にサブネット化されます。

Switch A の DHCP サーバで以下の割り当てを行います。

表 5-2 割り当て方法

DHCP クライアント	IP アドレス	リース期間	ほかの設定パラメータ
VLANインタフェース10に接続するクライアント	10.1.1.0/25	10日間と12時間	• ゲートウェイアドレス：10.1.1.126/25 • DNSサーバ：10.1.1.2/25 • ドメイン名：aabbcc.com • WINSサーバ：10.1.1.4/25
VLANインタフェース20に接続するクライアント	10.1.1.128/25	5日間	• ゲートウェイアドレス：10.1.1.254/25 • DNSサーバ：10.1.1.2/25 • ドメイン名：aabbcc.com

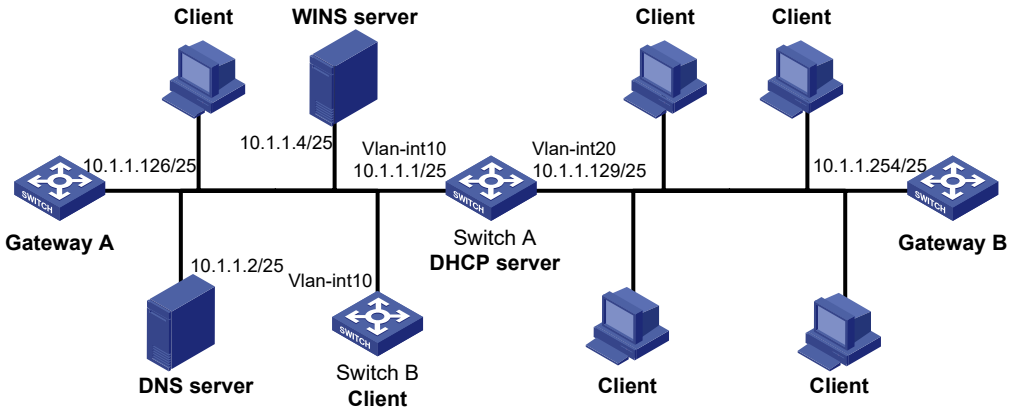


図 5-2 ネットワーク図

II. 設定手順

VLAN インタフェースに IP アドレスを設定します。（詳細は省略します。）

1)　DHCP サーバを設定します。

DHCP を有効にします。

```
<SwitchA> system-view
[SwitchA] dhcp enable
```

VLAN インタフェース 10、VLAN インタフェース 20 で DHCP サーバを有効にします。

```
[SwitchA] interface vlan-interface 10
[SwitchA-Vlan-interface10] dhcp select server
[SwitchA-Vlan-interface10] quit
[SwitchA] interface vlan-interface 20
[SwitchA-Vlan-interface20] dhcp select server
[SwitchA-Vlan-interface20] quit
```

ダイナミック割り当てから DNS サーバアドレス、WINS サーバアドレス、ゲートウェイアドレスを除外します。

```
[SwitchA] dhcp server forbidden-ip 10.1.1.2
[SwitchA] dhcp server forbidden-ip 10.1.1.4
[SwitchA] dhcp server forbidden-ip 10.1.1.126
[SwitchA] dhcp server forbidden-ip 10.1.1.254
```

サブネット 10.1.1.0/25 のクライアントに IP アドレス、ほかのパラメータを割り当てるように DHCP アドレスプール 1 を設定します。

```
[SwitchA] dhcp server ip-pool 1
[SwitchA-dhcp-pool-1] network 10.1.1.0 mask 255.255.255.128
[SwitchA-dhcp-pool-1] expired day 10 hour 12[SwitchA-dhcp-pool-1] domain-name aabbcc.com
[SwitchA-dhcp-pool-1] dns-list 10.1.1.2
[SwitchA-dhcp-pool-1] gateway-list 10.1.1.126
[SwitchA-dhcp-pool-1] nbns-list 10.1.1.4
[SwitchA-dhcp-pool-1] quit
```

サブネット 10.1.128/25 のクライアントに IP アドレス、ほかのパラメータを割り当てるように DHCP アドレスプール 2 を設定します。

```
[SwitchA] dhcp server ip-pool 2
[SwitchA-dhcp-pool-2] network 10.1.1.128 mask 255.255.255.128
[SwitchA-dhcp-pool-2] expired day 5
[SwitchA-dhcp-pool-2] domain-name aabbcc.com
```

```
[SwitchA-dhcp-pool-2] dns-list 10.1.1.2
[SwitchA-dhcp-pool-2] gateway-list 10.1.1.254
[SwitchA-dhcp-pool-2] quit
```

III. 設定の確認

サブネット 10.1.1.0/25 と 10.1.1.128/25 のクライアントが Switch A から正しい IP アドレスとほかのパラメータを取得することを確認します。（詳細は省略します。）

DHCP サーバでクライアントに割り当てられた IP アドレスを表示します。

```
[SwitchA] display dhcp server ip-in-use
IP address       Client-identifier/    Lease expiration      Type
                 Hardware address
10.1.1.3         0031-3865-392e-6262-  Jan 14 22:25:03 2015  Auto(C)
                 3363-2e30-3230-352d-
                 4745-302f-30
10.1.1.5         0031-fe65-4203-7e02-  Jan 14 22:25:03 2015  Auto(C)
                 3063-5b30-3230-4702-
                 620e-712f-5e
10.1.1.130       3030-3030-2e30-3030-  Jan 9 10:45:11 2015   Auto(C)
                 662e-3030-3033-2d45-
                 7568-6572-1e
10.1.1.131       3030-0020-fe02-3020-  Jan 9 10:45:11 2015   Auto(C)
                 7052-0201-2013-1e02
                 0201-9068-23
10.1.1.132       2020-1220-1102-3021-  Jan 9 10:45:11 2015   Auto(C)
                 7e52-0211-2025-3402
                 0201-9068-9a
10.1.1.133       2021-d012-0202-4221-  Jan 9 10:45:11 2015   Auto(C)
                 8852-0203-2022-55e0
                 3921-0104-31
```

5.11.3 プライマリ、セカンダリサブネット設定例

I. ネットワーク要件

図 5-3に示すように、DHCP サーバ（Switch A）は LAN 上のクライアントにダイナミックに IP アドレスを割り当てます。

DHCP サーバのアドレスプールにプライマリサブネット 10.1.1.0/24、セカンダリサブネット 10.1.2.0/24 を設定します。プライマリサブネットで割り当てるアドレスがない場合、DHCP サーバは、セカンダリサブネットの IP アドレスを選択します。

Switch A は以下のパラメータを割り当てます。

- サブネット 10.1.1.0/24 のクライアントにデフォルトゲートウェイ 10.1.1.254/24 を割り当てます。
- サブネット 10.1.2.0/24 のクライアントにデフォルトゲートウェイ 10.1.2.254/24 を割り当てます。

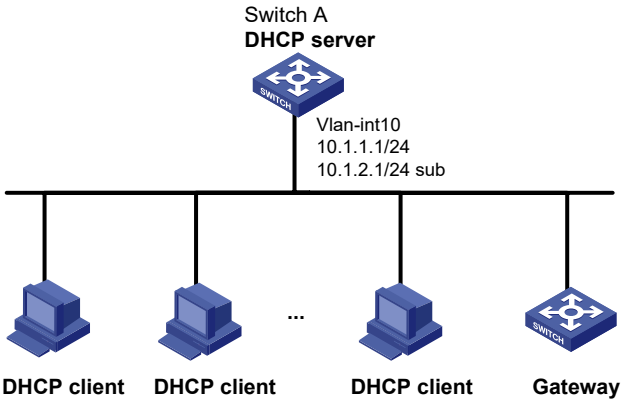


図 5-3 ネットワーク図

II. 設定手順

DHCP を有効にします。

```
<SwitchA> system-view
[SwitchA] dhcp enable
```

VLAN インタフェース 10 のプライマリ IP アドレス、セカンダリ IP アドレスを設定します。

```
[SwitchA] interface vlan-interface 10
[SwitchA-Vlan-interface10] ip address 10.1.1.1 24
[SwitchA-Vlan-interface10] ip address 10.1.2.1 24 sub
```

VLAN インタフェース 10 で DHCP サーバを有効にします。

```
[SwitchA-Vlan-interface10] dhcp select server
[SwitchA-Vlan-interface10] quit
```

DHCP アドレスプール aa を作成します。

```
[SwitchA] dhcp server ip-pool aa
```

ダイナミック割り当てのプライマリアドレス、ゲートウェイアドレスを設定します。

```
[SwitchA-dhcp-pool-aa] network 10.1.1.0 mask 255.255.255.0
[SwitchA-dhcp-pool-aa] gateway-list 10.1.1.254
```

ダイナミック割り当てのセカンダリサブネット、ゲートウェイアドレスを設定します。

```
[SwitchA-dhcp-pool-aa] network 10.1.2.0 mask 255.255.255.0 secondary
[SwitchA-dhcp-pool-aa-secondary] gateway-list 10.1.2.254
[SwitchA-dhcp-pool-aa-secondary] quit
[SwitchA-dhcp-pool-aa] quit
```

III. 設定の確認

プライマリサブネットで割り当て可能なアドレスがない場合、DHCP サーバはセカンダリサブネットから割り当てることを確認します。（詳細は省略します。）

DHCP サーバが割り当てたプライマリ、セカンダリサブネット IP アドレスを表示します。

```
[SwitchA] display dhcp server ip-in-use
IP address       Client-identifier/     Lease expiration      Type
                 Hardware address
10.1.1.2         0031-3865-392e-6262-   Jan 14 22:25:03 2015  Auto(C)
                 3363-2e30-3230-352d-
                 4745-302f-30
10.1.2.2         3030-3030-2e30-3030-   Jan 14 22:25:03 2015  Auto(C)
                 662e-3030-3033-2d45-
                 7568-6572-1e
```

5.11.4 自己定義オプション設定例

I. ネットワーク要件

図 5-4に示すように、DHCP クライアント（Switch B）は DHCP サーバ（Switch A）から、IP アドレスと PXE サーバアドレスを取得します。IP アドレスはサブネット 10.1.1.0/24 に属しています。PXE サーバアドレスは、1.2.3.4 と 2.2.2.2 です。

DHCP サーバは、オプション 43（自己定義オプション）を通して、PXE サーバアドレスを DHCP クライアントに割り当てます。オプション 43 のフォーマットと PXE サーバアドレスのサブオプションは、オペレーションマニュアルのセクション 3 *IP サービス* "*DHCP の概要*"を参照してください。この例では、DHCP サーバで設定されるオプション 43 の値は、80 0B 00 00 02 01 02 03 04 02 02 02 02 です。

- 番号 80 は、サブオプションタイプの値です。
- 番号 0B は、サブオプション長の値です。
- 番号 00 00 は、PXE サーバタイプの値です。
- 番号 02 は、サーバの数を示します。
- 番号 01 02 03 04 02 02 02 02 は、PXE サーバアドレスが 1.2.3.4 と 2.2.2.2 であることを示します。

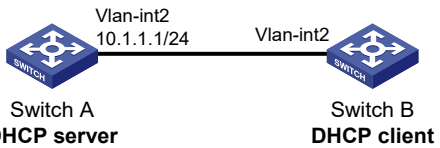


図 5-4 ネットワーク図

II. 設定手順

1) インタフェースに IP アドレスを設定します。（詳細は省略します。）
2) DHCP サーバを設定します。

DHCP を有効にします。

```
<SwitchA> system-view
[SwitchA] dhcp enable
```

VLAN インタフェース 2 で DHCP サーバを有効にします。

```
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] dhcp select server
[SwitchA-Vlan-interface2] quit
```

DHCP アドレスプール 0 を設定します。

```
[SwitchA] dhcp server ip-pool 0
```

ダイナミックアドレス割り当てのサブネットを設定します。

```
[SwitchA-dhcp-pool-0] network 10.1.1.0 mask 255.255.255.0
```

自己定義オプション 43 を設定します。

```
[SwitchA-dhcp-pool-0] option 43 hex 800B000002010203040202020202
```

III. 設定の確認

Switch B は Switch A から 10.1.1.0/24 の IP アドレスと PXE サーバアドレスを取得できることを確認します。（詳細は省略します。）

DHCP サーバでクライアントに割り当てられた IP アドレスを表示します。

```
[SwitchA] display dhcp server ip-in-use
IP address       Client-identifier/    Lease expiration      Type
                 Hardware address
10.1.1.2         aabb-aabb-ab01        Jan 14 22:25:03 2015  Auto(C)
```

5.12 DHCPサーバ設定のトラブルシューティング

5.12.1 症状

DHCP サーバから取得したクライアントの IP アドレスが別の IP アドレスと競合しています。

5.12.2 分析

サブネットの別のホストが同一 IP アドレスを持っている可能性があります。

5.12.3 解決策

1) クライアントのネットワークアダプタを無効にする、もしくはネットワークケーブルの接続を切断します。別のホストにあるクライアントの IP アドレスに ping を行い、同じ IP アドレスを使用しているホストがあるかを確認します。

2) ping に対する応答があれば、そのホストには IP アドレスが手動で設定されています。DHCP サーバで **dhcp server forbidden-ip** コマンドを実行して、ダイナミックな割り当てからその IP アドレスを除外します。
3) クライアントのネットワークアダプタを有効にする、もしくはネットワークケーブルを接続します。クライアントの IP アドレスを解放し、IP アドレスを再取得します。Windows の DHCP クライアントの場合、以下のように行います。

a) DOS環境で**cmd**コマンドを実行し、コマンドプロンプトを起動します。

b) **ipconfig /release**を実行してIPアドレスを放棄します。

c) **ipconfig /renew**を実行し、IPアドレスの再取得を行います。

目次

このセクションのページは**3-x-x** です。

6 章 DHCP クライアント 6-1
6.1 インタフェースでの DHCP クライアントの有効化 6-1
6.2 アドレス重複検出の有効化 6-1
6.3 DHCP クライアントが送信する DHCP パケットの DSCP の設定 6-2
6.4 DHCP クライアントの表示と維持 6-2
6.5 DHCP クライアント設定例 6-2
6.5.1 ネットワーク要件 6-2
6.5.2 設定手順 6-3
6.5.3 設定の確認 6-4

6章 DHCP クライアント

装置は DHCP クライアントが有効である場合、DHCP サーバから IP アドレスを含む設定パラメータを取得できます。

DHCP クライアントの設定は VLAN インタフェースでのみサポートします。

6.1 インタフェースでのDHCPクライアントの有効化

インタフェースで DHCP クライアントを有効にするため、以下のガイドラインに従ってください。

- IP アドレス要求の失敗数がシステムで定義した値に到達した場合、DHCP クライアントが有効なインタフェースはデフォルトの IP アドレスを使用します。
- インタフェースは何度も IP アドレスを取得することができますが、古い設定が新しい設定に上書きされ、新しい設定が適用されます。
- DHCP クライアントが有効になったインタフェースはセカンダリ IP アドレスを設定することができません。
- DHCP サーバから割り当てられた IP アドレスが装置上のほかのインタフェースの IP アドレスとネットワークセグメントを共有していた場合、インタフェースは割り当てられた IP アドレスを使用しません。その代わり、DHCP サーバから新しい IP アドレスを要求します。

以下にインタフェースでの DHCP クライアントの有効化の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. interface view に移行する	**interface** *interface-type interface-number*	―
3. インタフェースで DHCP クライアントを有効にする	**ip address dhcp-alloc**	デフォルト：無効 初期設定と工場出荷時のデフォルトの詳細は、オペレーションマニュアルのセクション1 *はじめに”コンフィグレーションファイル管理”* を参照してください。

6.2 アドレス重複検出の有効化

DHCP クライアントは、ARP パケットを使用して IP アドレスの重複があるかどうかを検出します。攻撃者は、サーバが割り当てた IP アドレスを使用できなくさせるため、ARP 応答を送信し、IP アドレスのオーナーとして動作します。ARP 攻撃がネットワークに存在する場合、アドレス重複検出機能を無効にすることを推奨します。

以下にアドレス重複検出の有効化の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． アドレス重複検出を有効にする	**dhcp client dad enable**	デフォルト : インタフェースで有効

6.3 DHCPクライアントが送信するDHCPパケットのDSCPの設定

パケットの DSCP は、パケットの優先度レベルを指定し、パケットの優先度に影響します。

以下に DHCP クライアントが送信した DHCP パケットの DSCP の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． DHCP クライアントが送信する DHCP パケットの DSCP を設定する	**dhcp client dscp** *dscp-value*	デフォルト：56

6.4 DHCPクライアントの表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
DHCPクライアント情報を表示する	**display dhcp client** [**verbose**] [**interface** *interface-type interface-number*]

6.5 DHCPクライアント設定例

6.5.1 ネットワーク要件

図 6-2に示すように、LAN で Switch B は VLAN インタフェース 2 を通して DHCP サーバと接続し、IP アドレス、DNS サーバアドレス、スタティックルート情報を取得します。DHCP クライアントのアドレスはネットワーク 10.1.1.0/24 にあり、DNS サーバアドレスは 20.1.1.1、スタティックルートの 20.1.1.0/24 のネットワークのネクストホップアドレスは、10.1.1.2 です。

DHCP サーバは DHCP クライアントにスタティックルートの情報を割り当てるため、オプション 121 を使用します。図 6-1にオプション 121 のフォーマットを示します。Destination descriptor フィールドは、16 進数で記載されたサブネットマスク長、宛先ネットワークアドレスの情報が含まれます。この例では Destination descriptor は 18 14 01 01（10 進数でサブネットマスク長が 24、ネットワークアドレスが 20.1.1.0）です。ネクストホップアドレスは 0A 01 01 02（10 進数で 10.1.1.2）です。

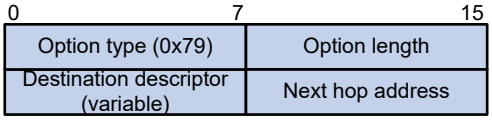


図 6-1 オプション 121 フォーマット

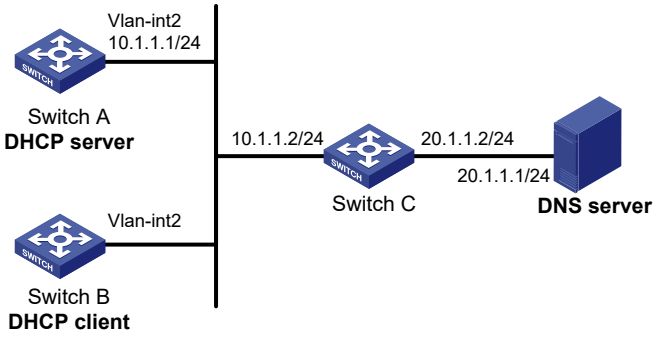


図 6-2 ネットワーク図

6.5.2 設定手順

1)　Switch A を設定します。

VLAN インタフェース 2 の IP アドレスを指定します。

```
<SwitchA> system-view
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ip address 10.1.1.1 24
[SwitchA-Vlan-interface2] quit
```

DHCP を有効にします。

```
[SwitchA] dhcp enable
```

自動割り当てから除外する IP アドレスを指定します。

```
[SwitchA] dhcp server forbidden-ip 10.1.1.2
```

DHCP アドレスプール 0 を設定します。サブネット、リース期間、DNS サーバアドレス、スタティックルートのサブネット 20.1.1.0/24 を指定します。

```
[SwitchA] dhcp server ip-pool 0
[SwitchA-dhcp-pool-0] network 10.1.1.0 mask 255.255.255.0
[SwitchA-dhcp-pool-0] expired day 10
[SwitchA-dhcp-pool-0] dns-list 20.1.1.1
[SwitchA-dhcp-pool-0] option 121 hex 18 14 01 01 0A 01 01 02
```

2)　Switch B を設定します。

IP アドレスを取得するため、VLAN インタフェース 2 で DHCP クライアントを有効にします。

```
<SwitchB> system-view
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] ip address dhcp-alloc
[SwitchB-Vlan-interface2] quit
```

6.5.3 設定の確認

Switch B に割り当てられた IP アドレス、他のネットワークパラメータを表示します。

```
[SwitchB-Vlan-interface2] display dhcp client verbose
Vlan-interface2 DHCP client information:
 Current state: BOUND
 Allocated IP: 10.1.1.3 255.255.255.0
 Allocated lease: 864000 seconds, T1: 331858 seconds, T2: 756000 seconds
 Lease from May 21 19:00:29 2012   to   May 31 19:00:29 2012
 DHCP server: 10.1.1.1
 Transaction ID: 0xcde72232
 Classless static routes:
   Destination: 20.1.1.0, Mask: 255.255.255.0, NextHop: 10.1.1.2
 DNS servers: 20.1.1.1
 Client ID type: acsii(type value=00)
 Client ID value: 000c.29d3.8659-Vlan2
 Client ID (with type) hex: 0030-3030-632e-3239-
                            6433-2e38-3635-392d-
                            4574-6830-2f30-2f32
 T1 will timeout in 3 days 19 hours 48 minutes 43 seconds
```

Switch B のルート情報を表示します。ルーティングテーブルにスタティックルートのネットワーク 20.1.1.0/24 が追加されています。

```
[SwitchB] display ip routing-table

Destinations : 11        Routes : 11

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
10.1.1.0/24         Direct 0    0            10.1.1.3        Vlan2
10.1.1.3/32         Direct 0    0            127.0.0.1       InLoop0
20.1.1.0/24         Static 70   0            10.1.1.2        Vlan2
10.1.1.255/32       Direct 0    0            10.1.1.3        Vlan2
127.0.0.0/8         Direct 0    0            127.0.0.1       InLoop0
127.0.0.0/32        Direct 0    0            127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0            127.0.0.1       InLoop0
127.255.255.255/32  Direct 0    0            127.0.0.1       InLoop0
224.0.0.0/4         Direct 0    0            0.0.0.0         NULL0
224.0.0.0/24        Direct 0    0            0.0.0.0         NULL0
255.255.255.255/32  Direct 0    0            127.0.0.1       InLoop0
```

目次

このセクションのページは**3-x-x** です。

7 章 DHCP スヌーピング 7-1
7.1 概要 7-1
7.1.1 トラステッドポートと非トラステッドポートのアプリケーション 7-1
7.1.2 DHCP snooping でのオプション 82 のサポート 7-2
7.2 DHCP snooping 設定作業リスト 7-3
7.3 DHCP snooping の基本機能の設定 7-3
7.4 オプション 82 の設定 7-4
7.5 DHCP snooping の表示と維持 7-5
7.6 DHCP snooping 設定例 7-6
7.6.1 DHCP snooping の基本機能の設定例 7-6
7.6.2 オプション 82 設定例 7-7

7章 DHCP スヌーピング

7.1 概要

DHCP スヌーピング（DHCP snooping）は、DHCP サーバと DHCP クライアント間でやりとりされる DHCP メッセージを監視して動的な IP ソースフィルタリングを行う機能です。本機能を利用することで、DHCP サーバを用いたネットワーク環境において、正当な DHCP クライアントにだけ IP 通信を許可することができる DHCP セキュリティ機能です。

セキュリティの目的から DHCP クライアントの IP アドレスと MAC アドレスバインディング（DHCP snooping エントリと呼ばれます）を記録します。

DHCP snooping は DHCP サーバと DHCP リレーエージェント間では動作しません。

DHCP snooping は許可された DHCP サーバからのみ IP アドレスを取得することができるように、トラステッド（trusted）ポートと非トラステッド（untrusted）ポートを定義します。

- **トラステッド（Trusted）** – DHCP メッセージを正常に転送し、DHCP クライアントが承認された DHCP サーバから IP アドレスを取得できることを確実にします。
- **非トラステッド（Untrusted）** – 不正な DHCP サーバからの IP アドレスの割り当てを防ぐため、受信した DHCP-ACK パケットまたは DHCP-OFFER パケットを廃棄します。

DHCP snooping は DHCP snooping エントリを作成するため、トラステッドポートから受信した DHCP-ACK メッセージと、DHCP-REQUEST メッセージを読み込みます。DHCP snooping エントリはクライアントの MAC アドレスと IP アドレス、DHCP クライアントに接続するポート、VLAN 情報を含みます。

DHCP snooping エントリを使用するため、以下の機能が必要となります。

- **ARP detection** – 承認されたクライアントからの ARP パケットかどうか、DHCP Snooping エントリにもとづいて決定します。この機能は、不正なクライアントからの ARP 攻撃を防ぐことができます。詳細はオペレーションマニュアルのセクション 7 *セキュリティ "ARP アタックプロテクション"*を参照してください。
- **IP ソースガード** – ポート毎に不正なパケットをフィルタするために使用します。詳細はオペレーションマニュアルのセクション 7 *セキュリティ "IP ソースガード"*を参照してください。

7.1.1 トラステッドポートと非トラステッドポートのアプリケーション

DHCP サーバに接続されているポートをトラステッドポートとして設定し、他のポートを非トラステッドポートとして設定します。

図 7-1に示すように、DHCP サーバに接続している DHCP snooping 装置のポートをトラステッドポートとして設定します。トラステッドポートは DHCP サーバからクライアントに応答メッセージを転送します。許可されていない DHCP サーバに接続されている非トラステッドポートは入力した DHCP 応答メッセージを廃棄します。

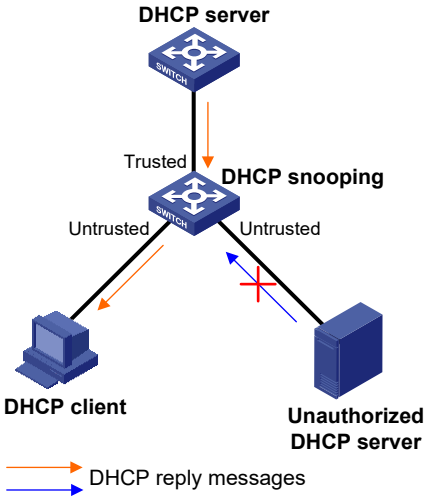


図 7-1　トラステッドポートと非トラステッドポート

図 7-2に示すようなカスケードネットワーク構成では、DHCP サーバに面しているポートはトラステッドポートとして設定する必要があります。システムリソースを節約するため、直接DHCPクライアントに接続されている非トラステッドポートのみが、DHCP snooping エントリを記録することができます。

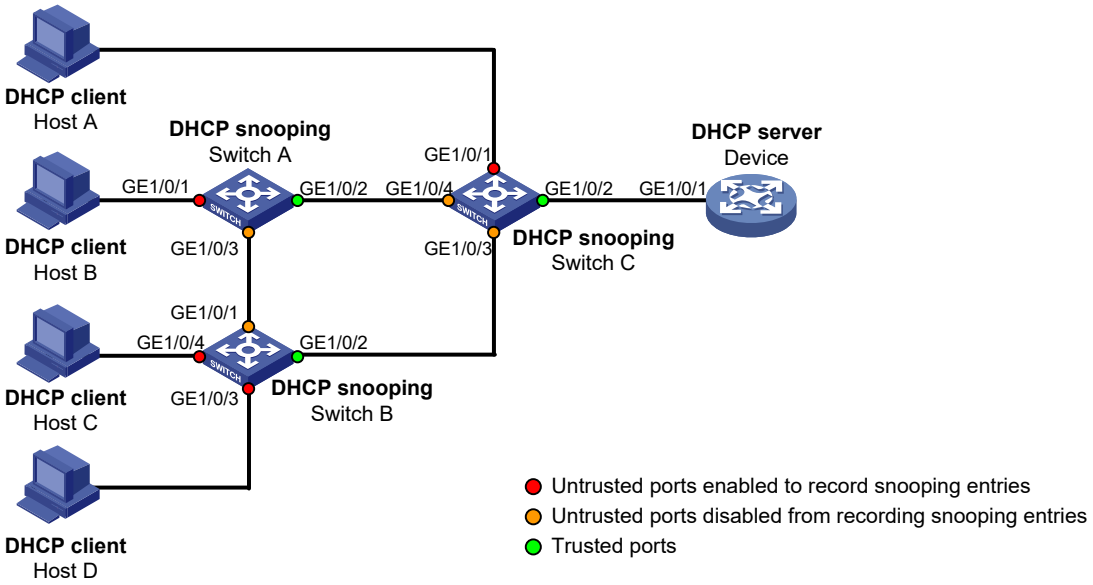


図 7-2　カスケードネットワーク構成のトラステッドポートと非トラステッドポート

7.1.2　DHCP snooping でのオプション 82 のサポート

オプション 82 は DHCP クライアントの位置情報を記録します。管理者はセキュリティとアカウンティングのため、DHCP クライアントを特定することができます。オプション

82 の詳細は、オペレーションマニュアルのセクション 3 *IP サービス* "*DHCP の概要*"を参照してください。

Option 82 のサブオプション 9（ベンダー固有）は、DHCP スヌーピング装置でのみサポートされます。**append** Option 82 処理を持つ各 DHCP スヌーピング装置は、受信した DHCP 要求のサブオプションに次の情報を追加します。

- 現在の DHCP スヌーピング装置のノード識別子
- クライアント側インタフェースに関する情報
- DHCP クライアントの VLAN

管理装置は、DHCP 要求を受信した後、要求が移動したネットワークトポロジを特定し、DHCP クライアントを見つけることができます。

DHCP snooping は表 7-1に示すように、DHCP リクエストメッセージのオプション 82 を処理するため、DHCP リレーエージェントと同様の処理を行います。DHCP サーバからの応答にオプション 82 が含まれている場合は、クライアントに応答を転送する前に DHCP Snooping 装置がオプション 82 を取り除きます。応答にオプション 82 が含まれていない場合、そのまま転送します。

表 7-1 DHCP snooping の動作

クライアントの要求メッセージに含まれるオプション	処理方法	DHCP Snooping の動作
Option 82	Append	オプション82を変更せずにメッセージを転送します。
	Drop	メッセージを破棄します。
	Keep	オプション82を変更せずにメッセージを転送します。
	Replace	もとのオプション82を設定されたパディング形式、パディングの内容、コードタイプに従って、新しいオプション82に置き換えてからメッセージを転送します。
No Option 82	ー	設定されたパディング形式、パディングの内容、コードタイプに従って、もとのオプション82に追加し、メッセージを転送します。

7.2 DHCP snooping設定作業リスト

アグリゲーショングループに接続されているレイヤ 2 Ethernet インタフェースに DHCP snooping を設定する場合、アグリゲーショングループからインタフェースを削除するまで設定は適用されません。

作業リスト
（必須設定項目） DHCP snoopingの基本機能の設定
（オプション設定項目） オプション82の設定

7.3 DHCP snoopingの基本機能の設定

DHCP snooping の基本機能の設定を行う場合、以下のガイドラインに従ってください。

- 許可された DHCP サーバに接続されているポートをトラステッドポートとして指定し、DHCP クライアントが確実に有効な IP アドレスを取得できるようにします。トラステッドポートと、DHCP クライアントに接続されているポートは同じ VLAN 内になければなりません。
- レイヤ 2 Ethernet インタフェースとアグリゲートインタフェースは、トラステッドポートとして指定できます。アグリゲートインタフェースの詳細は、オペレーションマニュアルのセクション 2 *アクセス ” リンクアグリゲーション*”を参照してください。
- アグリゲーショングループに追加された Ethernet インタフェースで DHCP snooping の設定を行う場合、アグリゲーショングループからインタフェースが削除されるまで設定内容は適用されません。

以下に DHCP snooping の基本機能の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． DHCP snooping を有効にする	**dhcp snooping enable**	デフォルト：無効
3． interface view に移行する	**interface** *interface-type interface-number*	インタフェースはDHCPサーバに接続する必要があります。
4． トラステッドポートとしてポートを指定する	**dhcp snooping trust**	デフォルト：DHCP snoopingが有効になった後、すべてのポートは非トラステッドポートとなります。
5． system view に戻る	**quit**	―
6． interface view に移行する	**interface** *interface-type interface-number*	インタフェースはDHCPクライアントに接続する必要があります。
7． （オプション設定項目）DHCP snooping エントリの記録を有効にする	**dhcp snooping binding record**	デフォルト：DHCP snoopingが有効になった後、DHCP snoopingエントリの記録は無効です。

7.4 オプション82の設定

オプション 82 を設定する場合、以下のガイドラインに従ってください。

- アグリゲーショングループに追加された Ethernet インタフェースでオプション 82 の設定を行う場合、アグリゲーショングループからインタフェースが削除されるまで設定内容は適用されません。
- オプション 82 をサポートする場合、DHCP サーバと DHCP snooping 装置の両方でオプション 82 を設定する必要があります。DHCP サーバのオプション 82 の設定の詳細は、オペレーションマニュアルのセクション 3 *IP サービス "DHCP サーバ"*を参照してください。
- DHCP Snooping が有効になっている装置の処理方法が **replace** と設定されている場合、オプション 82 のパディングフォーマットを設定する必要があります。処理方法が **keep** または **drop** の場合は、パディングフォーマットを設定する必要はありません。
- オプション 82 がノードの装置名でパディングされる場合、装置名にスペースを含めることはできません。含まれている場合、DHCP Snooping が有効になっている装置

はメッセージを破棄します。**sysname** コマンドを使用して装置名を指定することができます。コマンドの詳細は、コマンドマニュアルのセクション 1 *はじめに*”*装置管理*”を参照してください。

- 以下の状況が存在している場合、verbose パディングフォーマットのオプション 82 のサブオプション 1 の VLAN ID フィールドを満たすため、“外部 VLAN タグ.内部 VLAN タグ”を使用します。
  - □ DHCP snooping が 2 つの VLAN タグの DHCP パケットを受信する場合

  たとえば、外部 VLAN タグが 10、内部 VLAN タグが 20 である場合、VLAN ID フィールドは 000a.0014 です。16 進数で表記される 000a は外部 VLAN タグ 10 を示し、16 進数で表記される 0014 は内部 VLAN タグ 20 を示します。
- オプション 82 のサブオプション 1 がノードの装置名（**sysname**）でパディングされている場合､装置名はスペースを含んではいけません｡スペースが含まれている場合、DHCP snooping はオプション 82 の追加、更新に失敗します。

以下にオプション 82 をサポートする DHCP snooping の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． interface view に移行する	**interface** *interface-type interface-number*	―
3． オプション 82 をサポートする DHCP snooping を有効にする	**dhcp snooping information enable**	デフォルト：無効
4． （オプション設定項目）オプション 82 が含まれている要求メッセージの処理方法を設定する	**dhcp snooping information strategy** { **append** | **drop** | **keep** | **replace** }	デフォルト：**replace**
5． （オプション設定項目）サーキット ID サブオプションのパディング内容とコードタイプを設定する	**dhcp snooping information circuit-id** { [**vlan** *vlan-id*] **string** *circuit-id* | { **normal** | **verbose** [**node-identifier** { **mac** | **sysname** | **user-defined** *node-identifier* }] } [**format** { **ascii** | **hex** }] }	デフォルト：パディング内容は**normal**、サーキット ID サブオプションは**hex**です。
6． （オプション設定項目）リモート ID サブオプションのパディング内容とコードタイプを設定する	**dhcp snooping information remote-id** { **normal** [**format** { **ascii** | **hex** }] | [**vlan** *vlan-id*] { **string** *remote-id* | **sysname** } }	デフォルト：パディング内容は**normal**、リモート ID サブオプションは**hex**です。

7.5 DHCP snoopingの表示と維持

すべての view で **display** コマンドを実行でき、user view で **reset** コマンドを実行できます。

操作	コマンド
DHCP snoopingエントリを表示する	**display dhcp snooping binding** [**ip** *ip-address* [**vlan** *vlan-id*]]
DHCP Snooping装置でオプション82の設定に関する情報を表示する	**display dhcp snooping information** { **all** | **interface** *interface-type interface-number* }
DHCP Snooping装置のDHCPパケット統計情報を表示する	**display dhcp snooping packet statistics** [**slot** *slot-number*]

操作	コマンド
トラステッドポートの情報を表示する	**display dhcp snooping trust**
DHCP snoopingエントリを削除する	**reset dhcp snooping binding** { **all** | **ip** *ip-address* [**vlan** *vlan-id*] }
DHCP Snooping装置のDHCPパケット統計情報を削除する	**reset dhcp snooping packet statistics** [**slot** *slot-number*]

7.6 DHCP snooping設定例

7.6.1 DHCP snooping の基本機能の設定例

I. ネットワーク要件

図 7-3に示すように設定します。GigabitEthernet 1/0/1 をトラステッドポートとして DHCP サーバに接続します。GigabitEthernet 1/0/3 は許可されていない DHCP サーバに接続します。GigabitEthernet 1/0/2 を通して DHCP クライアントに接続します。

DHCP サーバからの応答を転送するため、許可されている DHCP サーバにのみ接続するように設定します。トラステッドポートから受信した DHCP-REQUEST メッセージと DHCP-ACK メッセージを確認することで、DHCP snooping がクライアントの IP-MAC バインディングを記録するようにします。

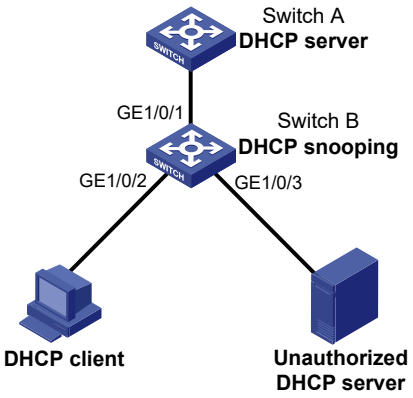


図 7-3 ネットワーク図

II. 設定手順

DHCP snooping を有効にします。

```
<SwitchB> system-view
[SwitchB] dhcp snooping enable
```

トラステッドポートとして GigabitEthernet 1/0/1 を設定します。

```
[SwitchB] interface gigabitethernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] dhcp snooping trust
[SwitchB-GigabitEthernet1/0/1] quit
```

GigabitEthernet 1/0/2 でクライアントの IP-MAC バインディングを記録することを有効にします。

```
[SwitchB] interface gigabitethernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] dhcp snooping binding record
[SwitchB-GigabitEthernet1/0/2] quit
```

III. 設定の確認

DHCP クライアントは許可された DHCP サーバからのみ IP アドレスと他の設定パラメータを取得できることを確認します。（詳細は省略します。）

クライアントの記録された DHCP snooping エントリを表示します。

```
[SwitchB] display dhcp snooping binding
```

7.6.2 オプション 82 設定例

I. ネットワーク要件

図 7-4に示すように、DHCP snooping を有効にし、以下のように Switch B のオプション 82 の設定を行います。

- オプション 82 が含まれる DHCP 要求の処理方法を **replace** に設定します。
- GigabitEthernet 1/0/2 のパディング内容のサーキット ID のサブオプションを **company001**、リモート ID サブオプションを **device001** に設定します。
- サーキット ID サブオプションの GigabitEthernet 1/0/3 のパディングフォーマットを **verbose**、アクセスノードの識別子を **sysname**、コードタイプを **ascii** に設定します。リモート ID サブオプションのパディングフォーマットを **device001** に設定します。

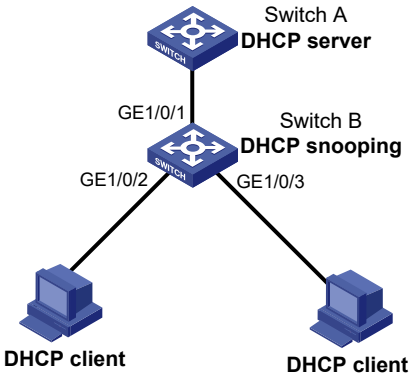


図 7-4 ネットワーク図

II. 設定手順

DHCP snooping を有効にします。

```
<SwitchB> system-view
[SwitchB] dhcp snooping enable
```

トラステッドポートとして GigabitEthernet 1/0/1 を設定します。

```
[SwitchB] interface gigabitethernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] dhcp snooping trust
[SwitchB-GigabitEthernet1/0/1] quit
```

GigabitEthernet 1/0/2 でオプション 82 を設定します。

```
[SwitchB] interface gigabitethernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] dhcp snooping information enable
[SwitchB-GigabitEthernet1/0/2] dhcp snooping information strategy replace
[SwitchB-GigabitEthernet1/0/2] dhcp snooping information circuit-id string company001
[SwitchB-GigabitEthernet1/0/2] dhcp snooping information remote-id string device001
[SwitchB-GigabitEthernet1/0/2] quit
```

GigabitEthernet 1/0/3 でオプション 82 を設定します。

```
[SwitchB] interface gigabitethernet 1/0/3
[SwitchB-GigabitEthernet1/0/3] dhcp snooping information enable
[SwitchB-GigabitEthernet1/0/3] dhcp snooping information strategy replace
[SwitchB-GigabitEthernet1/0/3] dhcp snooping information circuit-id verbose node-identifier sysname format ascii
[SwitchB-GigabitEthernet1/0/3] dhcp snooping information remote-id string device001
```

III. 設定の確認

DHCP snooping 装置の GigabitEthernet 1/0/2 と GigabitEthernet 1/0/3 のオプション 82 の設定情報を表示します。

```
[SwitchB] display dhcp snooping information
```

目次

このセクションのページは**3-x-x** です。

8 章 BOOTP クライアント 8-1
8.1 BOOTP アプリケーション 8-1
8.2 動的 IP アドレスの取得 8-1
8.3 プロトコルと標準 8-1
8.4 インタフェースでの BOOTP を使用した IP アドレスの取得の設定 8-2
8.5 BOOTP クライアントの表示と維持 8-2
8.6 BOOTP クライアントの設定例 8-2
8.6.1 ネットワーク要件 8-2
8.6.2 設定手順 8-3
8.6.3 設定の確認 8-3

8章 BOOTP クライアント

BOOTP（ブートストラッププロトコル）は、コンピュータネットワークに接続されたクライアントが、IP アドレスやホスト名、サブネットマスク等を自動的に取得するためのプロトコルです。

BOOTP クライアントは VLAN インタフェースでのみサポートします。

8.1 BOOTPアプリケーション

BOOTP クライアントとして指定したインタフェースは BOOTP を使用して BOOTP サーバから情報（IP アドレスなど）を入手することができます。

BOOTP を使用するため、管理者は各 BOOTP クライアントに対し BOOTP パラメータファイルを BOOTP サーバ上に用意する必要があります。パラメータファイルには、BOOTP クライアントの IP アドレス、MAC アドレスなどの情報が含まれます。BOOTP クライアントが BOOTP サーバに要求を送信すると、BOOTP サーバは BOOTP パラメータファイルを検索し、対応する設定情報を返信します。

一般的に BOOTP は安定した環境で使用します。ネットワーク環境が頻繁に変わる場合、DHCP が適しています。

DHCP サーバは BOOTP クライアントと相互に対応しています。そのため、BOOTP クライアントの IP アドレスを変更する場合、BOOTP サーバを使用しないで DHCP サーバを使用することができます。

8.2 動的IPアドレスの取得

BOOTP クライアントは以下のように BOOTP サーバから動的に IP アドレスを取得します。

1) BOOTP クライアントは自身の MAC アドレスを含めた、BOOTP 要求をブロードキャストします。
2) BOOTP サーバは、BOOTP 要求を受信するとクライアントの MAC アドレスに対応する IP アドレスの情報を検索します。
3) BOOTP サーバは BOOTP クライアントに BOOTP 応答を返信します。
4) BOOTP クライアントは受信した応答から IP アドレスを取得します。

DHCP サーバは BOOTP サーバの代わりに動的に IP アドレスを取得することができます。

8.3 プロトコルと標準

- RFC 951, *Bootstrap Protocol (BOOTP)*
- RFC 2132, *DHCP Options and BOOTP Vendor Extensions*
- RFC 1542, *Clarifications and Extensions for the Bootstrap Protocol*

8.4 インタフェースでのBOOTPを使用したIPアドレスの取得の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． interface view に移行する	**interface** *interface-type interface-number*	―
3． インタフェースで BOOTP を使用した IP アドレスの取得を設定する	**ip address bootp-alloc**	デフォルト：設定なし

8.5 BOOTPクライアントの表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
BOOTPクライアント情報を表示する	**display bootp client** [**interface** *interface-type interface-number*]

8.6 BOOTPクライアントの設定例

8.6.1 ネットワーク要件

図 8-1に示すように、Switch B の VLAN10 に属しているポートは、LAN に接続しています。VLAN インタフェース 10 は BOOTP を使用して DHCP サーバから IP アドレスを取得します。

BOOTP クライアントが DHCP サーバから IP アドレスを取得するため、DHCP サーバの設定を行う必要があります。詳細はオペレーションマニュアルのセクション 3 *IP サービス”DHCP サーバ”*を参照してください。

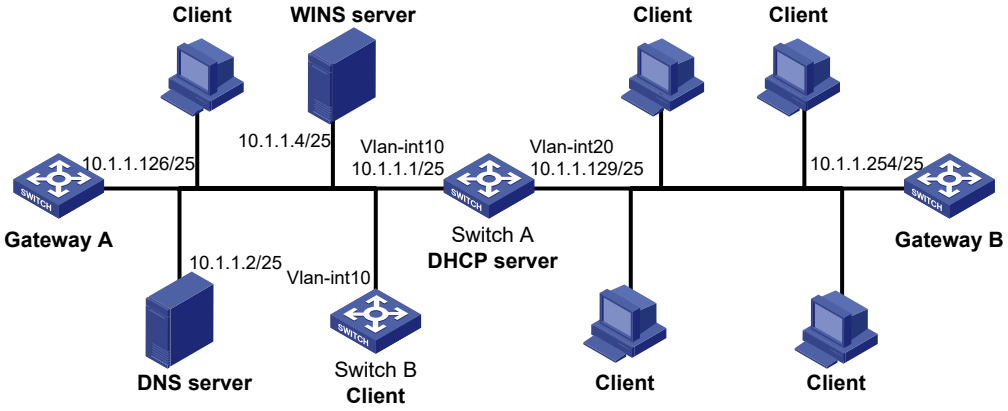


図 8-1 ネットワーク図

8.6.2 設定手順

以下の手順は、Switch B をクライアントとして動作させる設定です。

VLAN インタフェース 10 が DHCP サーバから動的に IP アドレスを取得できるように設定します。

```
<SwitchB> system-view
[SwitchB] interface vlan-interface 10
[SwitchB-Vlan-interface10] ip address bootp-alloc
```

8.6.3 設定の確認

BOOTP クライアントに割り当てられている IP アドレスを表示します。

```
[SwitchB] display bootp client
```

目次

このセクションのページは**3-x-x** です。

9 章 DNS 9-1
9.1 概要 9-1
9.1.1 スタティックドメイン名解決 9-1
9.1.2 ダイナミックドメイン名解決 9-1
9.1.3 DNS プロキシ 9-3
9.2 DNS 設定作業リスト 9-3
9.3 IPv4 DNS クライアントの設定 9-4
9.3.1 スタティックドメイン名解決の設定 9-4
9.3.2 ダイナミックドメイン名解決の設定 9-4
9.4 DNS プロキシの設定 9-5
9.5 送信される DNS パケットの DSCP 値の設定 9-5
9.6 IPv4 DNS の表示と維持 9-5
9.7 IPv4 DNS 設定例 9-6
9.7.1 スタティックドメイン名解決の設定例 9-6
9.7.2 ダイナミックドメイン名解決の設定例 9-7
9.7.3 DNS プロキシの設定例 9-11
9.8 IPv4 DNS 設定のトラブルシューティング 9-12
9.8.1 症状 9-12
9.8.2 解決策 9-12

9章 DNS

9.1 概要

DNS（Domain Name System）は、DNS サーバから DNS プロトコルを介してホスト名を IP アドレスにマッピングできる分散データベースです。各固有の IP アドレスには、ホスト名を関連付けることができますドメイン名－IP アドレスのマッピングは DNS エントリと呼ばれます。

DNS サービスには、スタティックとダイナミックの 2 種類があります。ユーザが名前を指定したのち、装置はスタティックの名前解決のデータベースで IP アドレスを調べます。有効な IP アドレスがない場合、ダイナミック（動的）な名前を解決するために DNS サーバに問い合わせを行います。これは、スタティック（静的）な名前解決の場合よりも時間がかかります。そこで効率化のために、よく照会される名前と IP アドレスのマッピングがローカルのスタティックな名前解決のデータベーステーブルに保存されています。

9.1.1 スタティックドメイン名解決

スタティックドメイン名解決は、ドメイン名と IP アドレスの間にマッピングを手動で作成します。たとえば、Telnet などのアプリケーションを使用する際に、装置のスタティックドメイン名解決のマッピングを作成することができます。

9.1.2 ダイナミックドメイン名解決

I. 解決手段

1) ユーザプログラムは、DNS クライアントの解決者にネームクエリを送信します。
2) DNS の解決者は、ローカルでドメイン名を適合させるためにキャッシュを調べます。適合するものがあれば、それに対応する IP アドレスを返送します。適合するものがなければ、DNS サーバにネームクエリを送信します。
3) DNS サーバはドメイン名を適合させるために名前解決のデータベースを調べます。適合するものがなければ、他のより高レベルの DNS サーバにネームクエリを送信します。このプロセスは、結果（成功、もしくは失敗）が返ってくるまで続けられます。
4) DNS サーバから応答を受信した後、DNS クライアントはユーザプログラムに解決結果を返信します。

図 9-1に、ユーザプログラム、DNS クライアントおよび DNS サーバ間の関係を示しています。

解決者（Resolver）とキャッシュ（Cache）は DNS クライアントによって構成されます。通常、ユーザプログラムと DNS クライアントは同じ装置あるいは異なる装置で動作しますが、DNS サーバと DNS クライアントが異なる装置間で動作します。

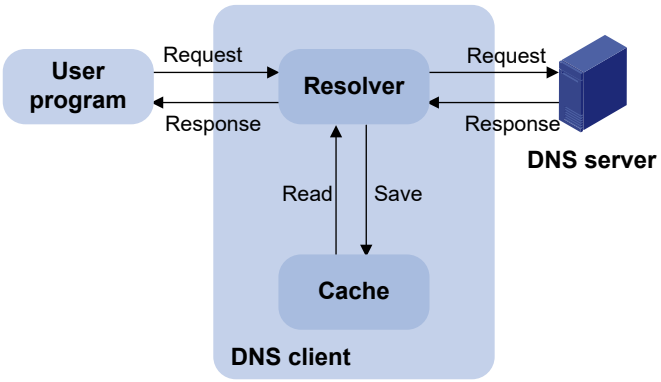


図 9-1 ダイナミックドメイン名解決

ダイナミックドメイン名解決は、DNS クライアントがダイナミックドメイン名のキャッシュに、DNS エントリを格納するようにします。有効期間内に度重なるクエリ用に DNS 要求を DNS サーバに送信する必要はありません。有効期間が満了した場合、DNS サーバからのエントリが最新であることを確認するため、DNS エントリを削除します。DNS サーバはマッピングの有効な期間を決定します。DNS クライアントは DNS 応答からエージング情報を取得します。

II. DNS サフィックス

DNS クライアントは、通常、ユーザによって定義することのできるサフィックスのリストを保持します。それは解決する名前が完全に一致しない場合に使用します。解決者は不明な部分を提供することができます。

たとえば、ユーザは aabbcc.com のためのサフィックスとして com を設定することができます。これによって、ユーザは、aabbcc を入力するだけで aabbcc.com の IP アドレスを取得することができます。解決者は DNS サーバに名前を通過させる前に、サフィックスとデリミタ（区切り記号）を付加します。

名前解決は、ユーザが入力したドメインネームにもとづくクエリを処理します。

- ユーザがドット（.）なしでドメイン名を入力した場合（たとえば aabbcc）、解決者はホスト名と認識し、処理する前にホスト名に DNS サフィックスを追加します。すべての DNS の検索に失敗した場合、解決者は IP アドレスのクエリのためにユーザが入力したドメイン名（たとえば aabbcc）を使用します。
- 文字の間にドメイン名にドット（.）がある場合（たとえば www.aabbcc）、解決者は最初に DNS の検索を行うために、このドメイン名を直接使用します。DNS の検索に失敗した場合、解決者は他の DNS を検索するために DNS サフィックスを追加します。
- ドメイン名の末尾にドット（.）がある場合（たとえば、aabbcc.com.）、解決者は、ドメイン名を FQDN（Fully Qualified Domain Name、完全修飾ドメイン名）と認識し、クエリが正常に処理されたかエラーが発生したか、結果が解決者から返信されます。このため、ドメイン名末尾のドット（.）は終端記号と認識されます。

装置は、スタティック DNS サービスおよびダイナミック DNS サービスをサポートしています。

DNS サーバでドメイン名にエイリアスが設定されている場合、そのエイリアスをホストの IP アドレスに変換できます。

9.1.3 DNS プロキシ

図 9-2に示すように、DNS プロキシは以下のように動作します。

- DNS クライアント（DNS client）は指定された DNS サーバ(DNS server)に要求を送信します。
- DNS サーバから指定された DNS クライアントに応答が送信されます。

DNS プロキシは、ネットワーク管理を容易にします。DNS サーバのアドレスが変更された場合、DNS プロキシの設定を変更するだけで、各 DNS クライアントの設定を変更する必要がなくなります。

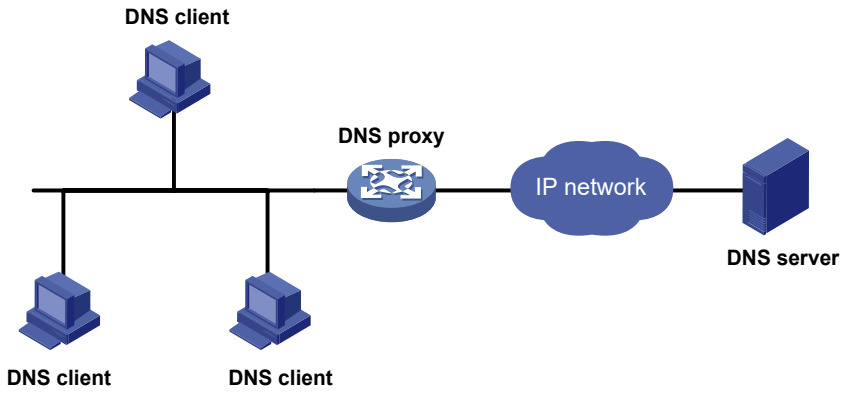


図 9-2 DNS プロキシアプリケーション

DNS プロキシは以下のように動作します。

1) DNS クライアントは DNS プロキシを DNS サーバと認識し、DNS プロキシに DNS 要求を送信します。要求の宛先アドレスは DNS プロキシの IP アドレスです。
2) DNS プロキシは要求を受信すると、ローカルスタティックドメイン名解決テーブルおよびダイナミックドメイン名解決テーブルを検索します。要求された情報がテーブル内にあれば、DNS プロキシはクライアントに DNS 応答を返します。
3) 要求された情報が見つからない場合は、DNS プロキシから指定の DNS サーバに要求が送信され、ドメイン名の解決を行います。
4) DNS サーバから応答を受け取ると、DNS プロキシは IP アドレスードメイン名のマッピングを記録し、応答を DNS クライアントに転送します。

DNS サーバが存在しない、あるいは、指定された DNS サーバへのルートがない場合、DNS プロキシは DNS 要求を転送しません。

9.2 DNS設定作業リスト

作業リスト
IPv4 DNSクライアントの設定
（オプション設定項目） DNSプロキシの設定
（オプション設定項目） 送信されるDNSパケットのDSCP値の設定

9.3 IPv4 DNSクライアントの設定

9.3.1 スタティックドメイン名解決の設定

スタティックドメイン名解決は、IPv4 アドレスの代わりにホスト名を使用してホストに接続する Telnet のようなアプリケーションを提供します。

スタティックドメイン名解決の設定を行う場合、以下のガイドラインに従ってください。

- 各ホスト名は 1 つの IPv4 アドレスのみ割り当てられます。既にホスト名に割り当てられた IPv4 アドレスがある場合、最後に行われた設定が適用されます。
- IPv4 DNS エントリを最大 1024 まで設定することができます。

以下にスタティックドメイン名解決の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． スタティック名前解決テーブルでホスト名と IPv4 アドレスの間のマッピングを設定する	**ip host** *host-name ip-address*	デフォルト：設定なし

9.3.2 ダイナミックドメイン名解決の設定

ダイナミックドメイン名解決を使用する場合、正しいサーバに DNS クエリを送信できるように DNS サーバを設定します。DNS サーバは DHCP を通して動的に取得した設定よりも、手動の設定が優先されます。複数設定を行った場合、最初に行った設定が優先されます。最初に最も高い優先度の DNS サーバにドメイン名解決リクエストを送信します。DNS サーバからの応答がない場合、順番に 2 番目の優先度のドメイン名解決リクエストが DNS サーバに送信されます。

加えて、取得したドメイン名を、システムが自動で追加するように DNS サフィックスを設定することができます。DNS サフィックスは DHCP を通して動的に取得した設定よりも、手動での設定が優先されます。複数設定を行った場合、最初に行った設定が優先されます。DNS 解決者は最初に最も高い優先度のサフィックスを使用します。名前解決に失敗した場合、順番に 2 番目の優先度のサフィックスを使用します。

I. 設定ガイドライン

ダイナミックドメイン名解決の設定を行う場合、以下のガイドラインに従ってください。

- DNS サーバは最大 6 台まで設定することができます。
- DNS サフィックスは最大 16 まで設定できます。

II. 設定手順

以下にダイナミックドメイン名解決の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． DNS サーバの IP アドレスを設定する	**dns server** *ip-address*	デフォルト：設定なし
3． （オプション設定項目）ドメイン名のサフィックスを設定する	**dns domain** *domain-name*	デフォルト：設定なし 定義済みのドメイン名のみ解決します。

9.4 DNSプロキシの設定

複数の DNS サーバを指定することができます。DNS プロキシは最も高い優先度の DNS サーバに要求を転送します。DNS サーバから応答がない場合、2 番目以降の優先度の DNS サーバに要求を転送します。

以下に DNS プロキシの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． DNS プロキシを有効にする	**dns proxy enable**	デフォルト：無効
3． DNS サーバの IP アドレスを指定する	**dns server** *ip-address*	デフォルト：指定なし

9.5 送信されるDNSパケットのDSCP値の設定

パケットの DSCP は、パケットの優先度レベルを指定し、パケットの優先度に影響します。DSCP が高いほど、優先度が高くなります。

以下に出力される DNS パケットの DSCP の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． 出力される DNS パケットの DSCP 値を設定する	**dns dscp** *dscp-value*	デフォルト：0 この設定はDNSクライアント、DNSプロキシの装置で有効です。

9.6 IPv4 DNSの表示と維持

すべての view で **display** コマンドを実行でき、user view で **reset** コマンドを実行できます。

操作	コマンド
ドメイン名解決テーブルを表示する	**display dns host** [**ip**]

操作	コマンド
IPv4 DNSサーバ情報を表示する	**display dns server** [**dynamic**]
DNSサフィックスを表示する	**display dns domain** [**dynamic**]
ダイナミックドメイン名キャッシュの情報を削除する	**reset dns host** [**ip**]

9.7 IPv4 DNS設定例

9.7.1 スタティックドメイン名解決の設定例

I. ネットワーク要件

図 9-3に示すように、Device は IP アドレスよりも、覚えやすいドメイン名を使用して、Host にアクセスします。

ドメイン名 host.com で IP アドレス 10.1.1.2 のホストにアクセスできるように、Device にスタティックドメイン名解決の設定を行います。

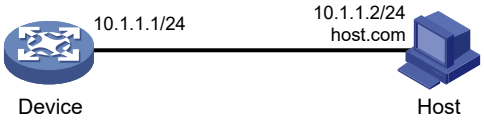


図 9-3 ネットワーク図

II. 設定手順

ホスト名 host.com と IP アドレス 10.1.1.2 のマッピングを設定します。

```
<Switch> system-view
[Switch] ip host host.com 10.1.1.2
```

ping host.com コマンドを使用します。Device がスタティックドメイン名解決により、host.com に対応する IP アドレスの 10.1.1.2 を取得できることを確認します。

```
[Switch] ping host.com
Ping host.com (10.1.1.2): 56 data bytes, press CTRL_C to break
56 bytes from 10.1.1.2: icmp_seq=0 ttl=255 time=1.000 ms
56 bytes from 10.1.1.2: icmp_seq=1 ttl=255 time=1.000 ms
56 bytes from 10.1.1.2: icmp_seq=2 ttl=255 time=1.000 ms
56 bytes from 10.1.1.2: icmp_seq=3 ttl=255 time=1.000 ms
56 bytes from 10.1.1.2: icmp_seq=4 ttl=255 time=2.000 ms

--- Ping statistics for host.com ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.000/1.200/2.000/0.400 ms
```

9.7.2 ダイナミックドメイン名解決の設定例

I. ネットワーク要件

図 9-4に示すように、Device を以下のように設定します。

- IP アドレスよりも、覚えやすいドメイン名を使用して Host にアクセスします。
- ダイナミック DNS を使用し、DNS server に IP アドレスの要求を行います。

DNS server の IP アドレスは 2.1.1.2/16 で、ドメインは com で、IP アドレス 3.1.1.1/16 とドメイン名 host のマッピングは com に保存されます。

DNS client として動作する Device でダイナミック DNS、DNS サフィックス com を設定します。Device は、Device がドメイン名 host.com と IP アドレス 3.1.1.1/16 で Host にアクセスできるように設定します。

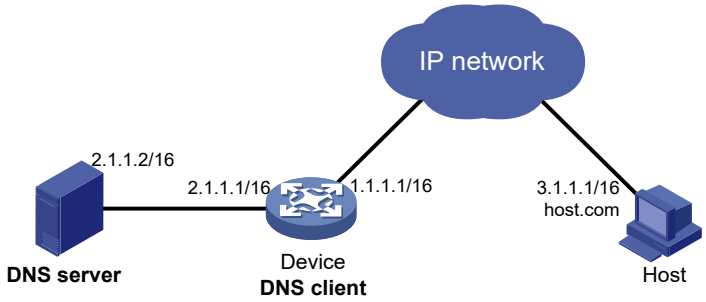


図 9-4 ネットワーク図

II. 設定手順

設定を行う前に、以下を確認してください。

- Device と Host が互いに通信可能できることを確認してください。
- インタフェースの IP アドレスが、図 9-4に示すように設定されていることを確認してください。

1) DNS server を設定します。

設定は DNS server によって異なります。以下の設定は、Windows 2008 R2 server で行われています。

a) “Start” > “Programs” > “Administrative Tools” > “DNS” を選択します。図 9-5 に示すようにDNS serverの設定ページが表示されます。

b) “Forward Lookup Zones” を右クリックし、“New zone” を選択します。指示に従って、新しいゾーンcomを作成します。

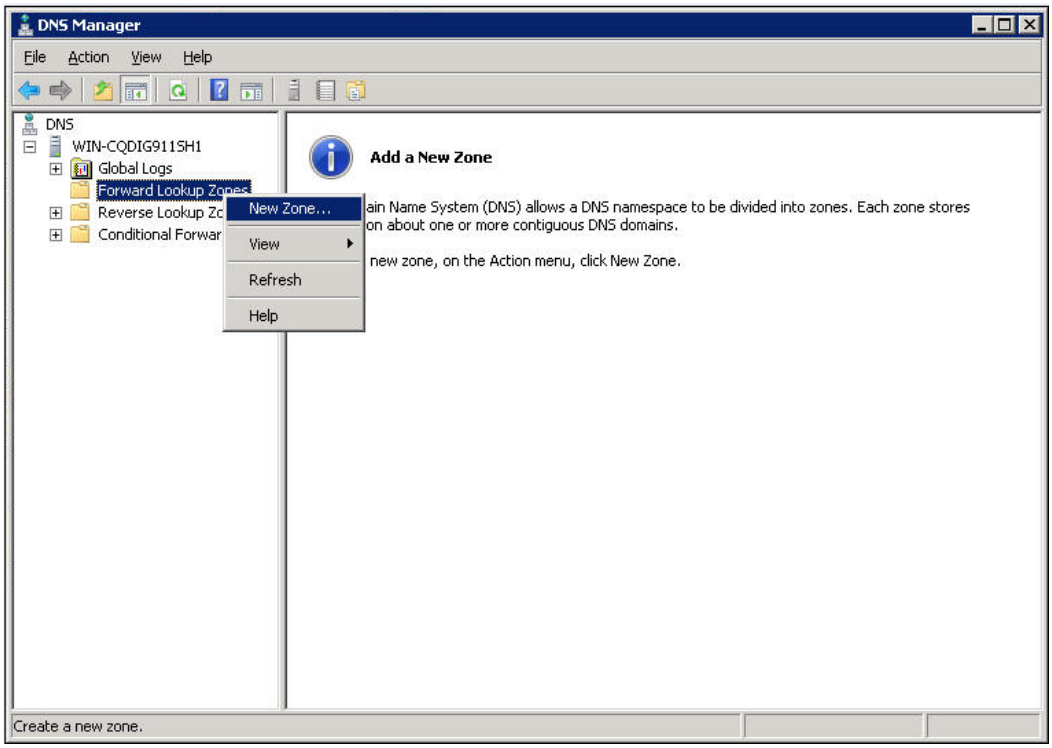


図 9-5 ゾーンの作成

c)　DNS server設定ページで、ゾーンcomを右クリックし、“New Host”を選択します。

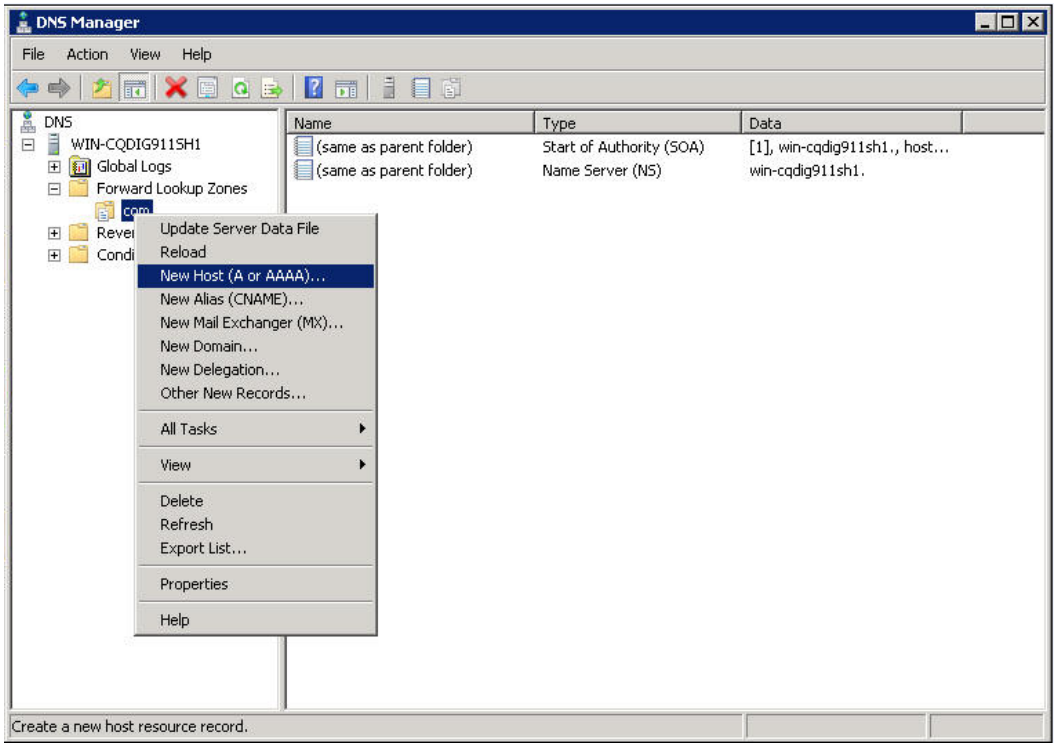


図 9-6 ホストの追加

d) ダイアログボックスで、ホスト名host、IPアドレス3.1.1.1を入力します。

e) “Add Host”をクリックします。IPアドレスとホスト名間のマッピングが作成されます。

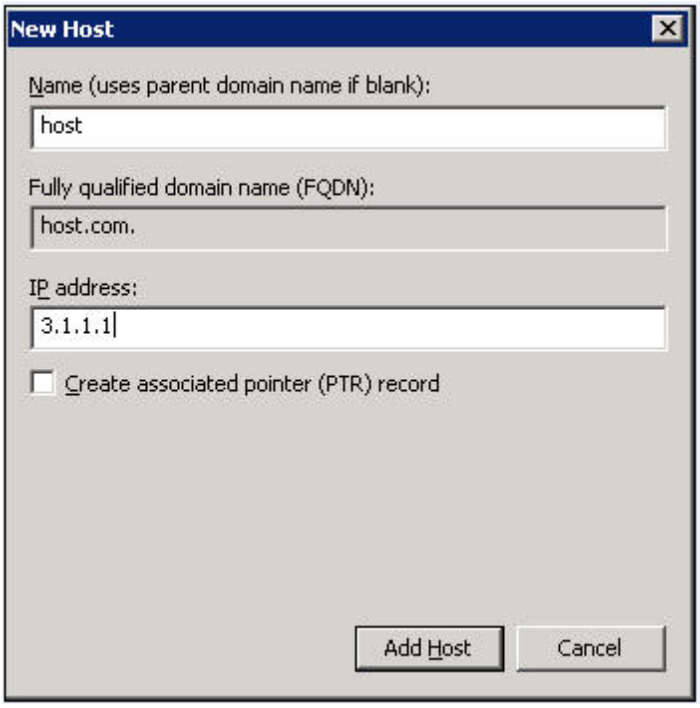


図 9-7 IP アドレスとホスト名間のマッピングの作成

2)　DNS client を設定します。

IP アドレスとして 2.1.1.2 を指定します。

```
<Switch> system-view
[Switch] dns server 2.1.1.2
```

#ドメイン名のサフィックスとして com を設定します。

```
[Switch] dns domain com
```

III. 設定の確認

Device で **ping** host コマンドを使用します。Device と host 間の通信が正常であり、ドメイン名 host.com に対応する宛先 IP アドレスが 3.1.1.1 であることを確認します。

```
[Switch] ping host
Ping host.com (3.1.1.1): 56 data bytes, press CTRL_C to break
56 bytes from 3.1.1.1: icmp_seq=0 ttl=255 time=1.000 ms
56 bytes from 3.1.1.1: icmp_seq=1 ttl=255 time=1.000 ms
56 bytes from 3.1.1.1: icmp_seq=2 ttl=255 time=1.000 ms
56 bytes from 3.1.1.1: icmp_seq=3 ttl=255 time=1.000 ms
56 bytes from 3.1.1.1: icmp_seq=4 ttl=255 time=2.000 ms

--- Ping statistics for host ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.000/1.200/2.000/0.400 ms
```

9.7.3 DNS プロキシの設定例

I. ネットワーク要件

図 9-8に示すように Device B（DNS client）と DNS server 間で DNS パケットを転送する DNS プロキシとして Device A を設定します。DNS server の IP アドレスは 4.1.1.1 です。

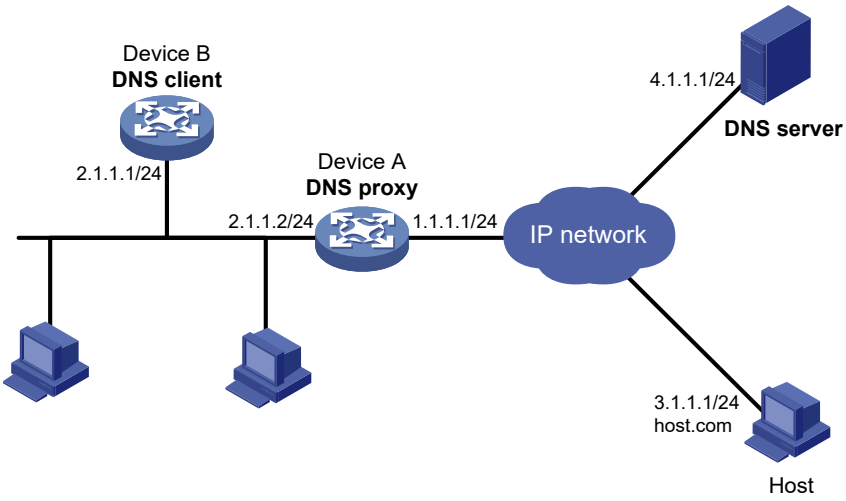


図 9-8 ネットワーク図

II. 設定手順

設定を行う前に、以下のことを確認してください。

- Device A と DNS server、Host の間が互いに通信可能であることを確認してください
- インタフェースの IP アドレスが、図 9-8に示すように設定されていることを確認してください

1) DNS server を設定します。

この設定は DNS server によって異なります。Windows 2008 R2 server を DNS server として使用する場合、オペレーションマニュアルのセクション 3 *IP サービス”DNS“の“ダイナミックドメイン名解決の設定例“*を参照してください。

2) DNS proxy を設定します。

DNS server の IP アドレスとして、4.1.1.1 を指定します。

```
<DeviceA> system-view
[DeviceA] dns server 4.1.1.1
```

DNS プロキシを有効にします。

```
[DeviceA] dns proxy enable
```

3) DNS client を設定します。

```
<DeviceB> system-view
```

DNS server の IP アドレスとして、2.1.1.2 を指定します。

```
[DeviceB] dns server 2.1.1.2
```

III. 設定の確認

Device A で DNS プロキシが有効であることを確認します。

```
[DeviceB] ping host.com
Ping host.com (3.1.1.1): 56 data bytes, press CTRL_C to break
56 bytes from 3.1.1.1: icmp_seq=0 ttl=255 time=1.000 ms
56 bytes from 3.1.1.1: icmp_seq=1 ttl=255 time=1.000 ms
56 bytes from 3.1.1.1: icmp_seq=2 ttl=255 time=1.000 ms
56 bytes from 3.1.1.1: icmp_seq=3 ttl=255 time=1.000 ms
56 bytes from 3.1.1.1: icmp_seq=4 ttl=255 time=2.000 ms

--- Ping statistics for host.com ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.000/1.200/2.000/0.400 ms
```

9.8 IPv4 DNS設定のトラブルシューティング

9.8.1 症状

ダイナミックドメイン名解決を有効にした後、ユーザが正しい IP アドレスを取得することができません。

9.8.2 解決策

1) **display dns host ip** コマンドを使用して、指定されたドメイン名がキャッシュにあることを確認してください。
2) 定義済みのドメイン名がない場合、ダイナミックドメイン名解決を有効にし、DNS クライアントと DNS サーバ間の通信が可能なことを確認してください。
3) キャッシュに特定のドメイン名はあっても、IP アドレスが正しくない場合、DNS クライアントが DNS サーバの正しい IP アドレスであることを確認してください。
4) DNS サーバのドメイン名と IP アドレス間のマッピングが正しいことを確認してください。

目次

このセクションのページは**3-x-x** です。

10 章 IP フォワーディングの基本 10-1
10.1 FIB テーブル 10-1
10.2 FIB テーブルエントリの表示と維持 10-2

10章 IP フォワーディングの基本

装置は、パケットを受信した際、FIB（forwarding information base）テーブルにマッチするかどうか検索するため、パケットの宛先 IP アドレスを使用します。マッチしたエントリを使用して、パケットを転送します。

10.1 FIBテーブル

装置はルーティングテーブルから最適なルートを選択し、FIB テーブルにルートを記載します。各 FIB エントリは、指定したサブネットあるいはホストにパケットを転送するため、ネクストホップの IP アドレスと出力インタフェースを指定しています。

ルーティングテーブルの詳細は、オペレーションマニュアルのセクション 4 *ルーティングプロトコル”IP ルーティングの基本*”を参照してください。

display fib コマンドを使用して FIB テーブルのエントリを表示します。以下に FIB テーブルの表示例を示します。

```
<Switch> display fib

Destination count: 8 FIB entry count: 8Destination count: 4 FIB entry count: 4

Flag:
  U:Usable   G:Gateway   H:Host   B:Blackhole   D:Dynamic   S:Static
  R:Relay     F:FRR

Destination/Mask   Nexthop         Flag     OutInterface/Token       Label
0.0.0.0/32         127.0.0.1       UH       InLoop0                  Null
127.0.0.0/8        127.0.0.1       U        InLoop0                  Null
127.0.0.0/32       127.0.0.1       UH       InLoop0                  Null
127.0.0.1/32       127.0.0.1       UH       InLoop0                  Null
127.255.255.255/32 127.0.0.1       UH       InLoop0                  Null
224.0.0.0/4        0.0.0.0         UB       NULL0                    Null
224.0.0.0/24       0.0.0.0         UB       NULL0                    Null
255.255.255.255/32 127.0.0.1       UH       InLoop0                  Null
```

FIB エントリは以下のアイテムが含まれます。

- **Destination** － 宛先 IP アドレスです。
- **Mask** － ネットワークマスクです。マスクと宛先アドレスは宛先ネットワークを識別します。宛先アドレスとネットワークマスク間の論理的 AND を行い、宛先ネットワークのアドレスを算出します。たとえば、宛先アドレスが 192.168.1.40、マスクが 255.255.255.0 である場合、宛先ネットワークのアドレスは、192.168.1.0 です。ネットワークマスクは、2 進数で連続した 1 と 0 で構成され、最上位から連続した 1 の数で表されます。またドットを用いて 10 進数で表すこともできます。
- **Nexthop** － ネクストホップの IP アドレスです。
- **Flag** － ルートのフラグです。
- **OutInterface** － 出力インタフェースです。
- **Token** － MPLS ラベルスイッチングパスインデックス番号です。
- **Label** － 内部ラベルです。

10.2 FIBテーブルエントリの表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
FIBエントリを表示する	**display fib** [*ip-address* [*mask* | *mask-length*]]

目次

このセクションのページは**3-x-x** です。

11 章 IP パフォーマンスの最適化 11-1
11.1 ダイレクトブロードキャストの送受信の有効化 11-1
11.1.1 設定手順 11-1
11.1.2 設定例 11-2
11.2 インタフェースの MTU サイズの設定 11-3
11.3 TCP path MTU discovery の設定 11-3
11.4 TCP バッファサイズの設定 11-4
11.5 TCP タイマの設定 11-4
11.6 ICMP エラーパケットの送信設定 11-5
11.7 ICMP エラーメッセージのレートリミットの設定 11-7
11.8 ICMP パフォーマンスの最適化の表示と維持 11-7

11章 IP パフォーマンスの最適化

装置の設定を最適化することで、IP パフォーマンス全体を最適にすることができます。この章では設定を最適化するための、さまざまな技術について記載します。

11.1 ダイレクトブロードキャストの送受信の有効化

ダイレクトブロードキャストパケットは、特定のネットワークのすべてのホストに送信されるブロードキャストパケットのことです。ダイレクトブロードキャストパケットの宛先 IP アドレスの、ネットワーク ID は宛先ネットワークを識別し、ホスト ID は値がすべて 1 です。

インタフェースが、ダイレクトブロードキャストをネットワークに転送することを許可した場合、ハッカーがこの機能を悪用し、宛先ネットワークに攻撃する可能性があります。しかし、あるシナリオではインタフェースが UDP ヘルパー、Wake on LAN をサポートするため、ダイレクトブロードキャストパケットのように送受信する必要があります。

UDP ヘルパー機能によって、インタフェースが直接接続されたネットワークからダイレクトブロードキャストパケットの送受信を有効にすることができます。UDP ヘルパーはダイレクトブロードキャストパケットをユニキャストパケットに変換し、特定のサーバへ転送することにより、本機能を有効にできます。

この処理は、インタフェースが直接接続されたネットワークへのダイレクトブロードキャストパケットを転送し、Wake on LAN をサポートするため、別のサブネットから受信します。Wake on LAN は宛先ネットワークのホストを起動させるためにダイレクトブロードキャストを送信します。

11.1.1 設定手順

以下に、インタフェースで、直接接続されたネットワークにダイレクトブロードキャストの送受信を有効にする設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． interface view に移行する	**interface** *interface-type interface-number*	―
3． 直接接続されたネットワークにダイレクトブロードキャストの送受信を有効にする	**ip forward-broadcast**	デフォルト：無効

11.1.2 設定例

I. ネットワーク要件

図 11-1に示すように、Host のデフォルトゲートウェイは Switch の VLAN インタフェース 3 の IP アドレス 1.1.1.2/24 です。

Server が Host から IP アドレス 2.2.2.255 にダイレクトブロードキャストを受信できるようにするため、VLAN インタフェース 2 が直接接続されたネットワークへのブロードキャストを転送できるように有効にします。

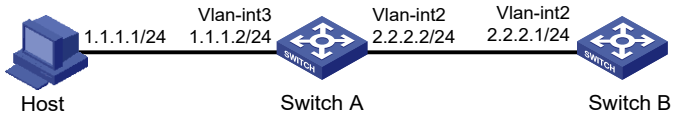


図 11-1 ネットワーク図

II. 設定手順

1)　Switch A を設定します。

VLAN インタフェース 2、VLAN インタフェース 3 の IP アドレスを設定します。

```
<SwitchA> system-view
[SwitchA] interface vlan-interface 3
[SwitchA-Vlan-interface3] ip address 1.1.1.2 24
[SwitchA-Vlan-interface3] quit
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ip address 2.2.2.2 24
```

VLAN インタフェース 2 で直接接続されたネットワークのダイレクトブロードキャストの転送を有効にします。

```
[SwitchA-Vlan-interface2] ip forward-broadcast
```

2)　Switch B を設定します。

ホストへのスタティックルートを設定します。

```
<SwitchB> system-view
[SwitchB] ip route-static 1.1.1.1 24 2.2.2.2
```

VLAN インタフェース 2 の IP アドレスを設定します。

```
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] ip address 2.2.2.1 24
```

設定を行った後、ホストでサブネットに直接接続されたブロードキャストアドレス 2.2.2.255 に ping を行った場合、Switch B の VLAN インタフェース 2 は ping パケットを受信できます。Switch で **ip forward-broadcast** コマンドの設定を削除した場合、インタフェースは ping パケットを受信することができません。

11.2 インタフェースのMTUサイズの設定

IPv4 パケットが出力インタフェースの MTU サイズを超えた場合、装置は、以下のどちらかの処理を行います。

- パケットのフラグメントが禁止されている場合、装置はパケットを廃棄します。
- パケットのフラグメントが許可されている場合、装置はパケットを分割し、フラグメントしたパケットを転送します。

フラグメントと再構築は、システムリソースを消費します。フラグメントを防ぐため、ネットワーク環境にもとづいて、適切にインタフェースの MTU サイズを設定します。

以下にインタフェースの MTU サイズの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． interface view に移行する	**interface** *interface-type interface-number*	―
3． インタフェースの MTU サイズを設定する	**ip mtu** *mtu-size*	デフォルト：設定なし

11.3 TCP path MTU discoveryの設定

⚠ **重要**：

TCP 経路のすべての装置は **ip unreachables enable** コマンドを使用して、ICMP エラーメッセージの送信を有効にする必要があります。

TCP path MTU discovery（RFC1191）は、TCP 接続の送信元と宛先間の経路 MTU を探索します。以下のように動作します。

1) TCP 送信元の装置はフラグメント禁止（DF）ビットを設定して、パケットを送信します。
2) ルータは、出力インタフェースで MTU サイズを超過したパケットを廃棄します。出力インタフェースの MTU サイズが含まれた ICMP エラーメッセージを送信します。
3) ICMP エラーメッセージを受信した TCP 送信元の装置は、TCP 接続の現在の経路 MTU を計算します。
4) TCP 送信元の装置は、MSS よりも小さい TCP セグメントの次のパケットを送信します。（MSS ＝ 経路 MTU － IP ヘッダ長 － TCP ヘッダ長）

MSS が 32 バイトよりも小さい状態で、TCP 送信元の装置が ICMP エラーメッセージを受信する場合、TCP 送信元の装置はパケットをフラグメントします。

RFC1191 をサポートしていないルータから ICMP エラーメッセージを受信した場合、出カインタフェースの MTU は 0 に設定されます。ICMP エラーメッセージを受信した際、TCP 送信元の装置は、RFC1191 に記載されているように TCP MSS を計算するため、MTU テーブルから、現在の経路 MTU よりも小さい経路 MTU を選択します。MTU テーブルは、68、296、508、1006、1280、1492、2002、4352、8166、17914、32000、65535 バイトの MTU 値を含んでいます。最小 TCP MSS の値はシステムで 32 バイトと決められているため、実際の最小 MTU は 72 バイトです。

TCP path MTU discovery を有効にした後、すべての新しい TCP 接続は、経路 MTU を見つけます。装置は IP のフラグメントを発生させないように MSS の計算をするため、経路 MTU を使用します。

経路上で最小リンク MTU が増加した場合、送信元の装置の経路 MTU を増加させることができるように、経路 MTU は以下に示すエージングメカニズムを使用します。

- TCP 送信元の装置が ICMP エラーメッセージを受信した場合、経路 MTU を減少させ、経路 MTU のエージングタイマを開始します。
- エージングタイマが終了した後、送信元の装置は、RFC1191 に記載されているように、MTU テーブルで大きい値の MSS を使用します。
- ICMP エラーメッセージを 2 分以内に受信しない場合、送信元の装置は、TCP 3WAY ハンドシェイクでネゴシエートできる最大の MSS の値まで MSS を増加させます。

以下に TCP path MTU discovery の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. TCP path MTU discovery を有効にする	**tcp path-mtu-discovery** [**aging** *age-time* | **no-aging**]	デフォルト：無効

11.4 TCPバッファサイズの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. TCP 受信/送信バッファのサイズの設定をする	**tcp window** *window-size*	デフォルト：63KB

11.5 TCPタイマの設定

以下の TCP タイマを設定することができます。

- **SYN wait timer** – SYN パケットを送信したのち、TCP は SYN wait タイマを開始します。SYN wait タイマ間隔以内に応答パケットを受信しない場合、TCP 接続は確立しません。
- **FIN wait timer** – TCP 接続が FIN_WAIT_2 状態に変更される場合、FIN wait タイマを開始します。タイマ間隔以内に FIN パケットを受信しない場合、TCP 接続は終了します。FIN パケットを受信した場合、TCP 接続状態は TIME_WAIT に変わります。FIN パケットを受信しない場合、タイマを再スタートします。タイマが満了した場合、接続は切断されます。

以下に TCP タイマの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． TCP タイマを設定する	● TCP SYN waitタイマを設定する： **tcp timer syn-timeout** *time-value* ● TCP FIN waitタイマを設定する： **tcp timer fin-timeout** *time-value*	デフォルト： ● TCP SYN waitタイマ：75秒 ● TCP FIN waitタイマ：675秒

11.6 ICMPエラーパケットの送信設定

ICMP エラーパケットには、リダイレクトパケット、タイムアウトパケット、宛先到達不能パケットの 3 種類のパケットがあります。この機能は ICMP エラーメッセージの送信を有効にします。

- ICMP リダイレクトメッセージ

ホストはすべてのパケットをデフォルトゲートウェイに送信します。デフォルトゲートウェイは、以降のパケットを送信するために正しいネクストホップを再選択するよう、以下のルールで、ホストに ICMP リダイレクトパケットを送信します。

- □ 受信と送信が同じインタフェースです。
- □ 選択したルートがリダイレクトパケットで作成されていない、あるいは変更されていません。
- □ 選択されたルートが 0.0.0.0 の装置へのデフォルトルートではありません。
- □ 受信したパケットに送信元ルートオプションがありません。

ICMP リダイレクトパケット機能はホストの管理を簡略化し、最適なルートを見つけ出すために、ホストが正しいルーティングテーブルを徐々に確立することができます。

- ICMP タイムアウトパケット

装置は以下のルールで ICMP タイムアウトパケットを送信します。

- □ 以下の場合、装置は送信元に ICMP TTL Expired の ICMP エラーパケットを送信します。
  - □ 受信パケットが装置へのパケットではありません。
  - □ パケットの TTL フィールドが 1 です。
- □ 宛先が装置自身である IP データグラムの最初のフラグメントパケットを、装置が受信した場合、タイマを始動します。データグラムのすべてのフラグメントパケットを受信する前にタイマが満了した場合、装置は ICMP Fragment Reassembly Timeout の ICMP エラーパケットを送信します。

- ICMP 宛先到達不能パケット

装置は以下のルールで ICMP 宛先不能パケットを送信します。

- □ パケットを転送するためのルートとデフォルトルートが入手できない場合、
- □ 以下の場合、装置は ICMP Network Unreachable の ICMP エラーパケットを送信元に送信します。
  - □ パケットを転送するためのルートがありません。
  - □ ルーティングテーブルにデフォルトルートが存在しません。
- □ 以下の場合、装置は ICMP Protocol Unreachable の ICMP エラーパケットを送信元に送信します。
  - □ パケットの宛先が装置です。

- □ パケットのトランスポート層プロトコルが装置でサポートしていません。

🕮 **メモ：**

DHCP 対応の装置が ICMP エコー要求を送信しないで、ICMP エコー返答を受信する場合、装置はどのようなプロトコルの ICMP 到達不能のエラーパケットも送信元に送信しません。DHCP の詳細は、オペレーションマニュアルのセクション 3 *IP サービス”DHCP の概要”* を参照してください。

- □ 以下の場合、装置は ICMP Port Unreachable の ICMP エラーパケットを送信元に送信します。
  - □ UDP パケットの宛先が装置です。
  - □ パケットのポート番号が実行中のプロセスと一致していません。
- □ 以下の場合、装置は ICMP Source Route Failed の ICMP エラーパケットを送信元に送信します。
  - □ パケットの送信元が、Strict Source Routing を使用しています。
  - □ 中継装置が、送信元により指定されたネクストホップが直接接続されていないことを検出しました。
- □ 以下の場合、装置は ICMP Fragmentation Needed and DF-set の ICMP エラーパケットを送信元に送信します。
  - □ パケットを転送するとき、送信インタフェースの MTU がパケットより小さいです。
  - □ パケットに DF セット（フラグメント禁止）が付与されています。

以下に ICMP エラーパケットの送信の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. ICMP エラーパケットの送信を有効にする	• ICMPリダイレクトパケットの送信を有効にする：**ip redirects enable** • ICMPタイムアウトパケットの送信を有効にする：**ip ttl-expires enable** • ICMP宛先到達不能パケットの送信を有効にする：**ip unreachables enable**	デフォルト：無効

多くの ICMP パケットを送信するとネットワークトラフィックが増加します。多くの ICMP エラーによる悪意のあるパケットを受信した場合、装置のパフォーマンスが下がります。

このような問題を防止するために、装置は ICMP エラーパケットを送信しないように設定を無効にすることができます。ICMP タイムアウトパケットの送信が無効の場合、装置は ICMP TTL Expired メッセージの ICMP エラーパケットを送信しません。ICMP Fragment Reassembly Timeout の ICMP エラーパケットは正常に送信します。

11.7 ICMPエラーメッセージのレートリミットの設定

ネットワークの混雑状態を引き起こす可能性のある短い期間内に、過度の ICMP エラーメッセージを送信することを避けるため、ICMP エラーメッセージの送信レートを制限することができます。トークンバケット（bucket）アルゴリズムは、1 つの ICMP エラーメッセージを示す 1 つのトークンが用いられます。バケットに入ることができるトークンの最大数に達するまで、トークンは指定された間隔でバケットに配置されます。ICMP エラーメッセージが送信される場合に、トークンはバケットから取り除かれます。バケットが空の場合に、新しいトークンがバケットに配置されるまで、ICMP エラーメッセージは送信されません。

以下に ICMP エラーメッセージのレートリミットの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． ICMP エラーメッセージの間隔とトークンバケットサイズを設定する	**ip icmp error-interval** *interval* [*bucketsize*]	デフォルト：100ミリ秒間隔で最大10トークンが配置されます。 ICMPレートリミットを無効にするには、間隔を0ミリ秒に設定します。

11.8 ICMPパフォーマンスの最適化の表示と維持

すべての view で **display** コマンドを実行でき、user view で **reset** コマンドを実行できます。

操作	コマンド
RawIP接続の概要情報を表示する	**display rawip** [**slot** *slot-number*]
RawIP接続の詳細情報を表示する	**display rawip verbose** [**slot** *slot-number* [**pcb** *pcb-index*]]
TCP接続の概要情報を表示する	**display tcp** [**slot** *slot-number*]
TCP接続の詳細情報を表示する	**display tcp verbose** [**slot** *slot-number* [**pcb** *pcb-index*]]
UCP接続の概要情報を表示する	**display udp** [**slot** *slot-number*]
TCP接続の詳細情報を表示する	**display udp verbose** [**slot** *slot-number* [**pcb** *pcb-index*]]
IPパケットの統計情報を表示する	**display ip statistics** [**slot** *slot-number*]
TCPトラフィックの統計情報を表示する	**display tcp statistics** [**slot** *slot-number*]
UCPトラフィックの統計情報を表示する	**display udp statistics** [**slot** *slot-number*]
ICMPの統計情報を表示する	**display icmp statistics** [**slot** *slot-number*]
IPパケットの統計情報を削除する	**reset ip statistics** [**slot** *slot-number*]
TCPトラフィックの統計情報を削除する	**reset tcp statistics**

操作	コマンド
UDP トラフィックの統計情報を削除する	**reset udp statistics**

目次

このセクションのページは**3-x-x** です。

12 章 UDP ヘルパー 12-1
12.1 概要 12-1
12.2 設定の制限とガイドライン 12-1
12.3 ブロードキャストパケットからユニキャストパケットへの変換 12-1
12.4 UDP ヘルパーの表示と維持 12-2
12.5 UDP ヘルパー設定例 12-2
12.5.1 ネットワーク要件 12-2
12.5.2 設定手順 12-3
12.5.3 設定の確認 12-3

12章 UDP ヘルパー

12.1 概要

UDP ヘルパーは、指定した UDP 宛先ポート番号にパケットを変換することができます。

- 受信した UDP ブロードキャストパケットをユニキャストパケットに変換し、転送します。
- 受信した UDP ブロードキャストパケットをマルチキャストパケットに変換し、転送します。

12.2 設定の制限とガイドライン

UDP ヘルパーを設定する場合、以下の制限とガイドラインに従ってください。

- 装置のインタフェースでは、直接接続されたネットワークへのダイレクトブロードキャストの受信はデフォルトで無効となっています。UDP ヘルパーを使用するため、interface view で **ip forward-broadcast** コマンドを実行してください。ダイレクトブロードキャストの送受信についての詳細は、オペレーションマニュアルのセクション 3 *IP サービス* "*IP パフォーマンスの最適化*"を参照してください。
- UDP ヘルパーは宛先ポート 67 および 68 を使用する DHCP ブロードキャストパケットを転送できません。UDP ポート番号は、**udp-helper port** コマンドを使用してポート 67 および 68 を除外してください。
- UDP ポート番号は、最大で 256 個を設定可能です。
- UDP パケットを転送する宛先 IP アドレスとして、最大 20 個設定が可能です。

12.3 ブロードキャストパケットからユニキャストパケットへの変換

UDP ヘルパーでは、UDP 宛先ポート番号で、UDP ブロードキャストパケットを転送するかを判断します。

UDP ブロードキャストパケットを受信した場合、UDP ヘルパーはパケットの UDP 宛先ポート番号が、設定された UDP ポートに一致するか確認します。

- 受信した UDP ブロードキャストパケットの UDP 宛先ポート番号が、設定されたポート番号に一致した場合、UDP ヘルパーはパケットをコピーし、設定されたユニキャストアドレスにコピーした宛先 IP アドレスを変換します。UDP ヘルパーはユニキャストアドレスにパケットを転送します。
- 受信した UDP ブロードキャストパケットの UDP 宛先ポート番号が、設定されたポート番号に一致しない場合、UDP ヘルパーはパケットを処理しません。

以下にブロードキャストをユニキャストに変換する設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． UDP ヘルパーを有効にする	**udp-helper enable**	デフォルト：無効
3． UDP ポート番号を指定する	**udp-helper port** { *port-number* | **dns** | **netbios-ds** | **netbios-ns** | **tacacs** | **tftp** | **time** }	デフォルト：指定なし
4． interface view に移行する	**interface** *interface-type interface-number*	―
5． 宛先サーバの IP アドレスを指定する	**udp-helper server** *ip-address*	デフォルト：指定なし 複数の宛先サーバを指定する場合、UDPヘルパーはサーバに1つのコピーを作成します。 ブロードキャストパケットを受信するインタフェースで指定してください。

12.4 UDPヘルパーの表示と維持

すべての view で **display** コマンドを実行でき、user view で **reset** コマンドを実行できます。

操作	コマンド
UDPヘルパー機能によって転送されたパケット情報を表示する	**display udp-helper interface** *interface-type interface-number*
UDPヘルパーの統計情報を削除する	**reset udp-helper statistics**

12.5 UDPヘルパー設定例

12.5.1 ネットワーク要件

図 12-1に示すように、Switch A の VLAN インタフェース 1 のブロードキャストパケットをユニキャストパケットに変換します。UDP 宛先ポート番号が 55 のブロードキャストパケットを宛先サーバの IP アドレス 10.2.1.1/16 に転送します。

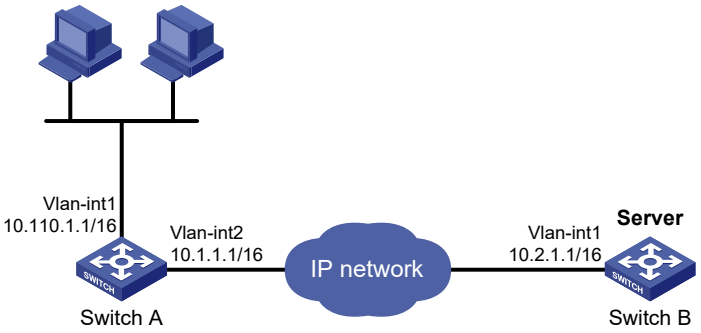


図 12-1 ネットワーク図

12.5.2 設定手順

Switch A がサブネット 10.2.0.0/16 と通信可能であることを確認してください。

UDP ヘルパーを有効にします。

```
[SwitchA] System-view
[SwitchA] udp-helper enable
```

UDP ポート番号 55 のブロードキャストパケットを転送するように設定します。

```
[SwitchA] udp-helper port 55
```

VLAN インタフェース 1 のブロードキャストパケットをユニキャストパケットに変換するため、UDP ヘルパーの宛先サーバ 10.2.1.1 を指定します。

```
[SwitchA] interface vlan-interface 1
[SwitchA-Vlan-interface1] ip address 10.110.1.1 16
[SwitchA-Vlan-interface1] udp-helper server 10.2.1.1
```

12.5.3 設定の確認

VLAN インタフェース 1 で UDP ヘルパーによって転送されたパケットの情報を表示します。

```
[SwitchA-Vlan-interface1] display udp-helper interface vlan-interface 1
Interface              Server VPN instance          Server address Packets sent
Vlan-interface1          N/A                            10.2.1.1       5
```

目次

このセクションのページは**3-x-x** です。

13 章 IPv6 の基本 13-1
13.1 概要 13-1
13.1.1 IPv6 の機能 13-1
13.1.2 IPv6 アドレス 13-3
13.1.3 IPv6 ND プロトコル 13-5
13.1.4 IPv6 path MTU discovery（IPv6 PMTU 探索） 13-8
13.2 IPv6 変換技術 13-9
13.3 プロトコルと標準 13-9
13.4 IPv6 の基本の設定作業リスト 13-10
13.5 インタフェースへの IPv6 アドレスの割り当て 13-10
13.5.1 IPv6 グローバルユニキャストアドレスの設定 13-10
13.5.2 IPv6 リンクローカルアドレスの設定 13-12
13.5.3 IPv6 エニーキャストアドレスの設定 13-13
13.6 IPv6 ND の設定 13-13
13.6.1 スタティックネイバエントリの設定 13-13
13.6.2 動的に学習されるネイバの最大数の設定 13-14
13.6.3 STALE 状態での ND エントリのエージングタイマの設定 13-14
13.6.4 Hop Limit の設定 13-15
13.6.5 RA メッセージのパラメータの設定 13-15
13.6.6 DAD のための NS メッセージ送信試行回数の設定 13-17
13.7 PMTU 探索（ディスカバリ）の設定 13-18
13.7.1 インタフェースの MTU の設定 13-18
13.7.2 IPv6 アドレスのスタティック PMTU の設定 13-18
13.7.3 ダイナミック PMTU のエージングタイマの設定 13-19
13.8 ICMPv6 メッセージ送信の管理 13-19
13.8.1 ICMPv6 エラーメッセージのレートリミットの設定 13-19
13.8.2 マルチキャストエコー要求への応答の有効化 13-20
13.8.3 ICMPv6 宛先到達不能メッセージの有効化 13-20
13.8.4 ICMPv6 時間超過メッセージの送信の有効化 13-20
13.9 IPv6 の基本設定の表示と維持 13-21
13.10 IPv6 の基本設定例 13-22
13.10.1 IPv6 の基本設定例 13-22
13.11 IPv6 の基本のトラブルシューティング 13-26
13.11.1 症状 13-26
13.11.2 分析 13-26

13章 IPv6 の基本

13.1 概要

IPv6（Internet Protocol Version 6）は IPv4（Internet Protocol Version 4）の後継のプロトコルです。IPv4 はアドレス長が 32 ビットなので最大 4.3×10 の 9 乗個の割り当てが可能ですが、世界的に利用者が急増したことで、IP アドレスが枯渇する可能性があり、IPv6（Internet Protocol Version 6）が開発されました。IPv6 はアドレス長が 128 ビットなので最大 3.4×10 の 38 乗個と事実上無限に近い IP アドレスを割り当てることができます。

13.1.1 IPv6 の機能

I. ヘッダフォーマットの簡易化

IPv6 は IPv4 ヘッダフィールドを縮小、または IPv6 拡張ヘッダに移動することにより、基本の IPv6 ヘッダの長さを短くしました。IPv6 は固定長の基本ヘッダを使用し、IPv6 パケットの処理を簡単にして転送効率を高めています。IPv6 のアドレスサイズは IPv4 アドレスの 4 倍ですが、IPv6 の基本ヘッダのサイズは 40 バイトで、IPv4 ヘッダのわずか 2 倍となっています（Options フィールドを除きます）。

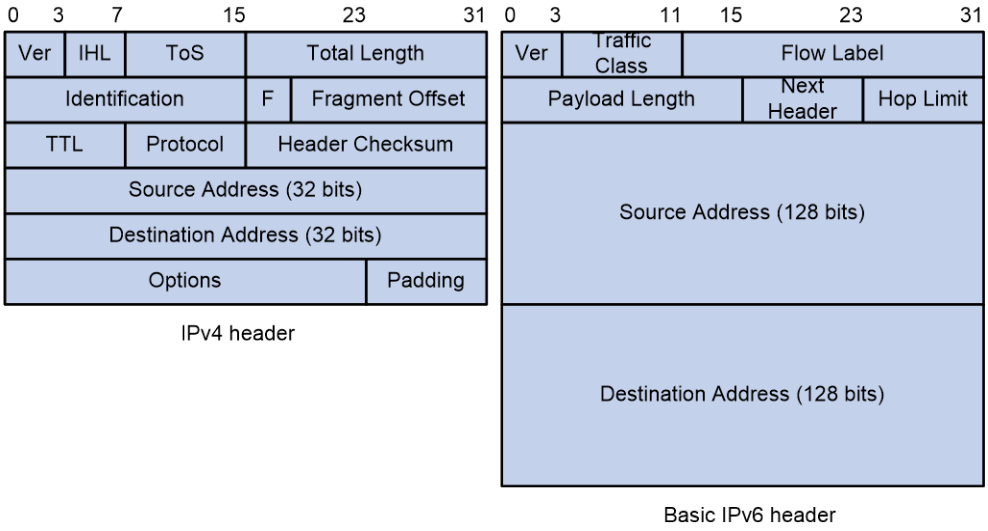


図 13-1 IPv4 パケットと基本 IPv6 パケットのヘッダフォーマットの違い

II. 大きなアドレス空間

IPv6 には 3.4 × 10^{38} アドレスが用意されており、パブリックネットワークとプライベートネットワークの階層的なアドレス割り当ての要件を満たします。

III. 階層アドレス構造

IPv6 は階層アドレス構造を使用しています。ルート検索を速め、ルートの集約を行い、IPv6 ルーティングテーブルに占有されるシステムリソースを減少させます。

IV. アドレス自動設定

ホストの設定を簡単にするために、IPv6 ではステートフルおよびステートレスのアドレス設定がサポートされています。

- ステートフルアドレス設定によって、ホストがサーバ（たとえば、DHCPv6 サーバ）から IPv6 アドレスおよび他の設定情報を取得します。
- ステートレスアドレス設定は、ホストがリンクレイヤアドレスとルータから広告されたプレフィックス情報にもとづいて、自動的に IPv6 アドレスおよび他の設定情報の作成を有効にします。

同一リンク上の他のホストと通信する場合、ホストはリンクレイヤアドレスとリンクローカルアドレスのプレフィックス（FE80::/10）にもとづいてリンクローカルアドレスを自動的に作成します。

V. QoS サポート

IPv6 ヘッダの Flow Label フィールドを使用すると、装置がフロー内のパケットにラベルを付けて、それらのパケットを特別に処理することができます。

VI. 強化されたネイバ検索（ディスカバリ）メカニズム

IPv6 ネイバ探索（ディスカバリ）プロトコルは、同一リンクにある隣接ノード間の情報交換を管理する ICMPv6（Internet Control Message Protocol Version 6）メッセージグループによって実行されます。ICMPv6 メッセージのグループは ARP（Address Resolution Protocol）メッセージ、ICMPv4（Internet Control Message Protocol version 4）ルータディスカバリメッセージ、および ICMPv4 リダイレクトメッセージに取って代わるもので、一連の他の機能を備えています。

VII. 柔軟性のある拡張ヘッダ

IPv6 は IPv4 パケットのオプションフィールドを削除し、複数の拡張ヘッダを導入しています。このように、IPv6 によって柔軟性が大きく高められ、IP に拡張性がもたらされます。処理の効率も向上します。IPv4 パケットのオプションフィールドに含まれるものは最大でも 40 バイトですが、IPv6 拡張ヘッダのサイズは IPv6 パケットのオプションフィールドによって制限されます。

13.1.2 IPv6 アドレス

I. IPv6 アドレスフォーマット

IPv6 アドレスは、コロン（:）で区切られた 16 ビットの 16 進数として表されます。IPv6 アドレスは 8 つのグループに分割され、各グループの 16 ビットはコロンで区切られ、4 つの 16 進数によって示されます。たとえば、2001:0000:130F:0000:0000:09C0:876A:130B です。

IPv6 アドレスの表現を簡単にするために、IPv6 アドレスのゼロを以下のように処理することができます。

- 各グループが 0000 の場合は 0 で表すことができます。たとえば、前述のアドレスは短縮した形式で表すと、2001:0:130F:0:0:9C0:876A:130B となります。
- ゼロの連続グループが 2 つ以上あれば、それらはダブルコロン（::）で置き換えることができます。たとえば、前述のアドレスは最短の形式で表すと、2001:0:130F::9C0:876A:130B となります。

⚠ **重要：**

ダブルコロン（::）は、IPv6 アドレスで 1 回だけ使用できます。複数回使用すると、ゼロに変換して 128 ビットの IPv6 アドレスに復元する場合、ダブルコロンがいくつのゼロを表しているのか判別できなくなります。

IPv6 アドレスは、アドレスプレフィックスとインタフェース ID から構成されます。アドレスプレフィックスとインタフェース ID はそれぞれ IPv4 アドレスのネットワーク ID とホスト ID に相当します。

IPv6 アドレスプレフィックスは IPv6 アドレス/プレフィックスの表記で記載されます。プレフィックス長はアドレスプレフィックスに相当する IPv6 アドレスの左端（先頭）からのビット数を示す 10 進数です。

II. IPv6 アドレスタイプ

IPv6 アドレスは以下のタイプに分類されます。

- **ユニキャストアドレス** － 単一インタフェースの識別番号で、IPv4 ユニキャストアドレスと同様です。ユニキャストアドレスに送られたパケットは、そのアドレスに識別されたインタフェースに配信されます。
- **マルチキャストアドレス** － （通常さまざまなノードに属している）インタフェースの集合の識別番号で、IPv4 マルチキャストアドレスに類似しています。マルチキャストアドレスに送られたパケットは、そのアドレスに識別されたすべてのインタフェースに配信されます。

  ブロードキャストはマルチキャストアドレスによって置き換えられます。
- **エニーキャストアドレス** － （通常はさまざまなノードに属している）インタフェースの集合の識別番号です。エニーキャストアドレスに送られたパケットは、そのアドレスに識別されたインタフェースに配信されます。インタフェースはルーティングプロトコルの距離測定に従って、もっとも近くにある装置のインタフェースです。

IPv6 アドレスのタイプは、フォーマットプレフィックスと呼ばれる先頭の数ビットによって指定されます。表 13-1に、アドレスのタイプとフォーマットプレフィックスの間のマッピング一覧を示します。

表 13-1 アドレスのタイプとフォーマットプレフィックスの間のマッピング

タイプ		フォーマットプレフィックス（バイナリ）	IPv6 プレフィックス ID
ユニキャストアドレス	未割り当てアドレス	00...0（128ビット）	::/128
	ループバックアドレス	00...1（128ビット）	::1/128
	リンクローカルアドレス	1111111010	FE80::/10
	グローバルユニキャストアドレス	他のフォーマット	―
マルチキャストアドレス		11111111	FF00::/8
エニーキャストアドレス		エニーキャストアドレスはユニキャストアドレス空間から取得されるもので、構文的にはユニキャストアドレスとの区別がつきません。	

III. ユニキャストアドレス

ユニキャストアドレスは、グローバルユニキャストアドレス、リンクローカルユニキャストアドレス、ループバックアドレス、未割り当てアドレスがあります。

- **グローバルユニキャストアドレス** ― グローバルユニキャストアドレスは IPv4 のパブリックアドレスに相当し、インタネットサービスプロバイダ向けに提供されています。アドレスのタイプを使用すると、効率的なルートプレフィックス集約によってグローバルなルーティングエントリの数を制限することができます。
- **リンクローカルアドレス** ― リンクローカルアドレスは、ネイバ探索やステートレス自動設定におけるリンクローカルノード間の通信に使用します。リンクローカルの送信元や宛先アドレスのパケットを他のリンクに転送することはできません。
- **ループバックアドレス** ― ユニキャストアドレス 0:0:0:0:0:0:0:1（もっとも短縮した形式で表すと ::1）はループバックアドレスと呼ばれ、物理インタフェースに割り当てることはありません。IPv4 のループバックアドレスのように、ノードは、ループバックアドレス自体に IPv6 パケットを送信する場合があります。
- **未割り当てアドレス** ― ユニキャストアドレス 0:0:0:0:0:0:0:0（もっとも短縮した形式で示すと:）は未割り当てアドレスと呼ばれ、ノードに割り当てることはできません。有効な IPv6 アドレスを取得する前に、ノードは未割り当てアドレスを IPv6 パケットの送信元アドレスフィールドに入力する場合があります。未割り当てアドレスは、宛先 IPv6 アドレスとして使用することはできません。

IV. マルチキャストアドレス

表 13-2に示す IPv6 マルチキャストアドレスは、特別な目的のために予約されています。

表 13-2 予約済みの IPv6 マルチキャストアドレス

アドレス	適用範囲
FF01::1	ノードローカルスコープ全ノードマルチキャストアドレス
FF02::1	リンクローカルスコープ全ノードマルチキャストアドレス
FF01::2	ノードローカルスコープ全ルータマルチキャストアドレス

アドレス	適用範囲
FF02::2	リンクローカルスコープ全ルータマルチキャストアドレス

マルチキャストアドレスにはもう 1 つのタイプの要請（solicited）ノードアドレスがあります。要請ノードマルチキャストアドレスは、同一リンク上にあるネイバノードのリンクレイヤアドレスを取得する場合に使用します。また、重複アドレス検出（DAD）にも使用します。IPv6 ユニキャストアドレスあるいはエニーキャストアドレスには、それぞれ 1 つずつ対応する要請ノードアドレスがあります。要請ノードマルチキャストアドレスの形式は FF02:0:0:0:0:1:FFXX:XXXX です。FF02:0:0:0:0:1 FF は固定値で、104 ビットで構成されています。XX:XXXX は、IPv6 ユニキャストアドレスまたはエニーキャストアドレスの下部 24 ビットです。

V. IEEE EUI-64 フォーマットのインタフェース識別子

インタフェース識別子は 64 ビット長です。IPv6 ユニキャストアドレスのインタフェース識別子は、リンク上のインタフェースを識別するために使用されます。インタフェースのリンクレイヤアドレス（通常 MAC アドレス）から派生したものです。MAC アドレスは 48 ビット長です。

IEEE EUI-64 フォーマットのインタフェース識別子を取得する場合、以下のステップに従います。

a) 16ビットの2進数1111111111111110（16進数でFFFEです）をMACアドレスの高位24ビットの後に挿入します。

b) U/L（ユニバーサル/ローカル）ビット（上位7番目のビット）を挿入します。この処理はインタフェース識別子がMACアドレスのように同じローカルあるいはグローバルで固有です。

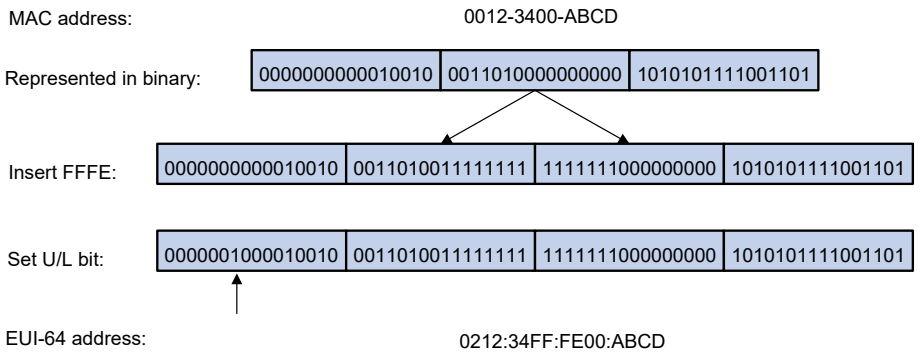


図 13-2 MAC アドレスから EUI-64 インタフェース識別子への変換

13.1.3 IPv6 ND プロトコル

IPv6 ND（Neighbor Discovery）プロトコルは、以下の ICMPv6 メッセージを使用します。

表 13-3 ND によって使用される ICMPv6 メッセージ

ICMPv6 メッセージ	タイプ	機能
ネイバ要請（NS）	135	ネイバのリンクレイヤアドレスの取得に使用します。
		ネイバに到達可能か確認するために使用します。
		DAD（重複アドレス検出）を行うために使用します。
ネイバ広告（NA）	136	NSメッセージへの応答に使用します。
		ネイバノードにリンクレイヤの変更を通知します。
ルータ要請（RS）	133	起動後、オートコンフィギュレーションのためノードはルータにアドレスプレフィックスおよびその他の設定情報を要求します。
ルータ広告（RA）	134	RSメッセージへの応答に使用します。
		ルータはプレフィックス情報オプションやフラグビットなどの情報が含まれるRAメッセージを送信します。
リダイレクト	137	一定の条件が満たされると、パケット転送に適したネクストホップルータを再選択できるように、デフォルトのゲートウェイが送信元ホストにリダイレクトメッセージを送信します。

I. アドレス解決

この機能は IPv4 の ARP に類似しています。IPv6 ノードは NS メッセージおよび NA メッセージを介して同一リンク上にあるネイバノードのリンクレイヤアドレスを取得します。図 13-3に Host A が同一リンク上の Host B のリンクレイヤアドレスを取得する方法を示します。

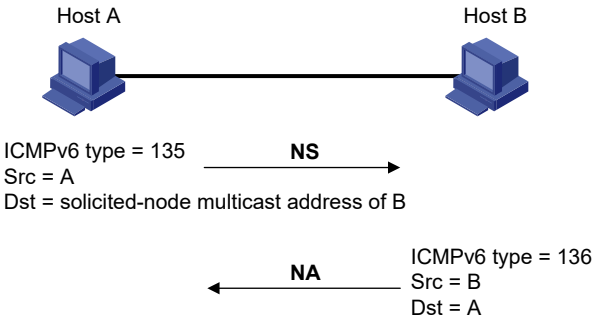


図 13-3 アドレス解決

以下にアドレス解決の手順を示します。

1) Host A は NS メッセージをマルチキャストします。NS メッセージの送信元アドレスは Host A の送信インタフェースの IPv6 アドレスです。宛先アドレスは Host B の要請ノードマルチキャストアドレスです。NS メッセージには、Host A のリンクレイヤアドレスと宛先 IPv6 アドレスが含まれています。
2) NS メッセージを受信した後、Host B はパケットの宛先アドレスが要請ノードマルチキャストアドレスであるかどうかを判断します。要請ノードマルチキャストアドレスである場合は、Host B は Host A のリンクレイヤアドレスを確認し、そのリンクレイヤアドレスが含まれる NA メッセージをユニキャストします。
3) Host A は NA メッセージから Host B のリンクレイヤアドレスを取得します。

II. ネイバ到達可能性探索

Host A がネイバの Host B のリンクレイヤアドレスを取得した後、Host A は NS メッセージと NA メッセージに従って、以下のように Host B が到達可能であるかどうかを確認することができます。

1) Host A は、Host B の IPv6 アドレスを宛先アドレスにした NS メッセージを送ります。
2) Host A が Host B から NA メッセージを受信すると、Host A は Host B が到達可能であると認識します。NA メッセージを受信しない場合、Host B は到達不可能と認識します。

III. 重複アドレスの検出

Host A は IPv6 アドレスを取得すると、DAD（Duplicate Address Detection、重複アドレス検出）を実行してアドレスが他のノードに使用されているかどうかを判断します。IPv4 の gratuitous ARP 機能と同様です。DAD は NS メッセージおよび NA メッセージによって実行されます。

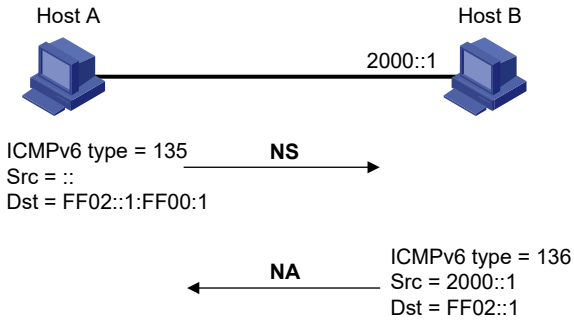


図 13-4 重複アドレスの検出

1) Host A は NS メッセージを送信します。この NS メッセージの送信元アドレスは未割り当てアドレスで、宛先アドレスは検出対象の IPv6 アドレスに対応する要請ノードマルチキャストアドレスです。NS メッセージには IPv6 アドレスが含まれています。
2) Host B がこの IPv6 アドレスを使用する場合、Host B は NA メッセージを返します。NA メッセージには Host B の IPv6 アドレスが含まれます。
3) Host A は Host B から NA メッセージを受信して、IPv6 アドレスが Host B によって使用されていることを知ります。NA メッセージを受信しない場合、Host B は IPv6 アドレスを使用していないと認識し、Host A がこの IPv6 アドレスを使用します。

IV. ルータ/プレフィックスの発見およびアドレスのオートコンフィギュレーション

ノードは、以下のようにルータ/プレフィックスの発見とオートコンフィギュレーションを行います。

1) 起動時、ノードは RS メッセージを送信し、オートコンフィギュレーションのためアドレスプレフィックスやその他の設定情報をルータに要求します。

2) ルータは、プレフィックス情報オプションや他の設定など情報が含まれる RA メッセージを返します。（ルータは定期的に RA メッセージを送信します）
3) RA メッセージのアドレスプレフィックスやその他の設定情報に従って、ノードはインタフェースに IPv6 アドレスおよびその他の設定情報を自動的に作成します。

プレフィックス情報オプションは、アドレスプレフィックスの preferred（推奨）期限と有効期限が含まれています。定期的な RA メッセージを受信すると、ノードはアドレスプレフィックスの preferred 期限と有効期限を更新します。

自動生成された IPv6 アドレスは有効期限内に適用できるものであり、有効期限が期限切れになると削除されます。

有効期限が期限切れになった後、ノードは、新しい接続を確立するために作成された IPv6 アドレスを使用することができませんが、IPv6 アドレスに関連づけられたパケットを受信することができます。preferred 期限は有効期限より大きくすることができません。

V. リダイレクション

ホストからパケットを受信する際、以下の条件である場合、ゲートウェイは最適なネクストホップのホストを通知するため、ICMPv6 リダイレクトメッセージをホストに通知します。

- 受信インタフェースがパケットを転送するインタフェースと同一です。
- 選択ルート自体は IPv6 ICMP リダイレクトメッセージによって作成、変更されることがありません。
- 選択ルートは装置のデフォルトルートではありません。
- 転送された IPv6 パケットに、ルーティング拡張ヘッダが含まれていません。

13.1.4 IPv6 path MTU discovery（IPv6 PMTU 探索）

パケットが送信元から宛先に通過するリンクは、さまざまな MTU を持つ可能性があります。MTU の最小値がパスの MTU です。IPv6 では、パケットサイズがリンクの MTU を超過している場合は、転送装置で処理を行う負荷を軽減し、ネットワークリソースを合理的に活用するために、パケットが送信元エンドでフラグメント化（分割）されます。

PMTU（path MTU）探索（ディスカバリ）メカニズムは、送信元から宛先までのパスにおけるすべてのリンクの MTU 最小値を発見します。

図 13-5に PMTU ディスカバリの動作手順を示します。

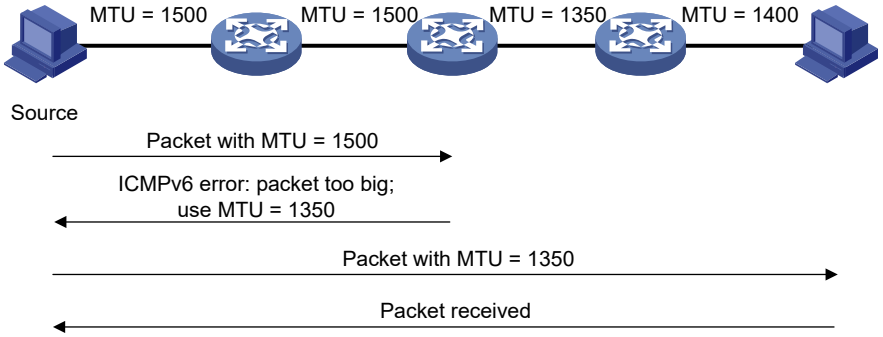


図 13-5 PMTU 探索（ディスカバリ）の処理

1) 送信元ホストは MTU よりも大きいパケットを宛先ホストに送信します。
2) 装置の出力インタフェースによってサポートされている MTU がパケットサイズよりも小さい場合、装置は以下の処理を行います。
   - □ パケットを破棄します。
   - □ インタフェースの MTU が含まれる ICMPv6 エラーパケットを送信元ホストに返します。
3) ICMPv6 エラーパケットを受信したのち、送信元ホストは以下の処理を行います。
   - □ 返された MTU を使用してパケットサイズを制限します。
   - □ パケットをフラグメント化します。
   - □ 宛先ホストに送信します。
4) 宛先ホストがパケットを受信するまで、手順 2～3 を繰り返します。このようにして、送信元ホストから宛先ホストまでのパスにある全リンクの最小 MTU が決定します。

13.2 IPv6変換技術

Dual Stack は、IPv6 ノードに IPv4 ノードとの互換性を持たせるためのもっとも直接的な方法です。Dual Stack ノードと呼ばれているネットワークノードは IPv4 と IPv6 の両方をサポートしています。IPv4 と IPv6 の両方をサポートする上位レイヤアプリケーションのために、トランスポート層で TCP か UDP を選択することができますが、ネットワーク層では IPv6 スタックが優先されます。

IPv4 アドレスと IPv6 アドレスが設定されている Dual Stack ノードは、IPv4 と IPv6 の両方のパケットを送信させることができます。Dual Stack ノードはグローバルで固有な IPv4 アドレスが必要なため、IPv4 アドレスの枯渇問題を解決することはできません。

13.3 プロトコルと標準

IPv6 に関連したプロトコルおよび規格を以下に示します。

- RFC 1881, *IPv6 Address Allocation Management*
- RFC 1887, *An Architecture for IPv6 Unicast Address Allocation*
- RFC 1981, *Path MTU Discovery for IP version 6*
- RFC 2375, *IPv6 Multicast Address Assignments*
- RFC 2460, *Internet Protocol, Version 6 (IPv6) Specification*
- RFC 2464, *Transmission of IPv6 Packets over Ethernet Networks*

- RFC 2526, *Reserved IPv6 Subnet Anycast Addresses*
- RFC 3307, *Allocation Guidelines for IPv6 Multicast Addresses*
- RFC 4191, *Default Router Preferences and More-Specific Routes*
- RFC 4291, *IP Version 6 Addressing Architecture*
- RFC 4443, *Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification*
- RFC 4861, *Neighbor Discovery for IP Version 6 (IPv6)*
- RFC 4862, *IPv6 Stateless Address Autoconfiguration*
- RFC 8106, *IPv6 Router Advertisement Options for DNS Configuration*

13.4 IPv6の基本の設定作業リスト

作業リスト
（必須設定項目） インタフェースへのIPv6アドレスの割り当て • IPv6グローバルユニキャストアドレスの設定 • IPv6リンクローカルアドレスの設定 • IPv6エニーキャストアドレスの設定
（オプション設定項目） IPv6 NDの設定 • スタティックネイバエントリの設定 • 動的に学習されるネイバの最大数の設定 • STALE状態でのNDエントリのエージングタイマの設定 • Hop Limitの設定 • RAメッセージのパラメータの設定 • DADのためのNSメッセージ送信試行回数の設定
（オプション設定項目） PMTU探索（ディスカバリ）の設定 • インタフェースのMTUの設定 • IPv6アドレスのスタティックPMTUの設定 • ダイナミックPMTUのエージングタイマの設定
（オプション設定項目） ICMPv6メッセージ送信の管理: • ICMPv6エラーメッセージのレートリミットの設定 • マルチキャストエコー要求への応答の有効化 • ICMPv6宛先到達不能メッセージの有効化 • ICMPv6時間超過パケットの送信の有効化

13.5 インタフェースへのIPv6アドレスの割り当て

この章は IPv6 グローバルユニキャストアドレス、IPv6 リンクローカルアドレス、IPv6 エニーキャストアドレスの設定について記載します。

13.5.1 IPv6 グローバルユニキャストアドレスの設定

IPv6 グローバルユニキャストアドレスは、以下のいずれかの方法で設定することができます。

- **EUI-64 フォーマット IPv6 アドレス** － IPv6 アドレスプレフィックスは手動で設定し、インタフェース ID はインタフェースで自動作成されます。
- **手動設定** － IPv6 グローバルユニキャストアドレスが手動で設定されます。
- **ステートレスアドレス自動設定** － RA メッセージに含まれるアドレスプレフィックス情報をもとにして自動的に IPv6 グローバルユニキャストアドレスを作成します。

インタフェースに複数の IPv6 グローバルユニキャストアドレスを設定することができます。

手動で設定されたグローバルユニキャストアドレス（EUI-64 フォーマット IPv6 アドレスを含みます）は、自動で作成されたアドレスよりも優先されます。同じアドレスプレフィックスとは別の設定を行った場合、インタフェースで自動生成されたグローバルユニキャストアドレスは、手動で設定されたアドレスで上書きされます。上書きされた自動生成されたグローバルユニキャストアドレスは、手動で設定されたアドレスが削除されても、もとに戻りません。そのかわり、次回インタフェースに受信された RA メッセージをもとにして、新しいグローバルユニキャストアドレスが自動で生成されます。

I. EUI-64 フォーマット IPv6 アドレス

以下に EUI-64 フォーマット IPv6 アドレスの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	－
2． interface view に移行する	**interface** *interface-type interface-number*	－
3． EUI-64 フォーマット IPv6 アドレスを作成するため、インタフェースを設定する	**ipv6 address** { *ipv6-address prefix-length* | *ipv6-address*/*prefix-length* } **eui-64**	デフォルト：設定なし

II. 手動設定

以下に IPv6 グローバルユニキャストアドレスの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	－
2． interface view に移行する	**interface** *interface-type interface-number*	－
3． 手動で IPv6 グローバルユニキャストアドレスを設定する	**ipv6 address** { *ipv6-address prefix-length* | *ipv6-address*/*prefix-length* }	デフォルト：設定なし

III. ステートレスアドレス自動設定

以下にステートレスアドレス自動設定での IPv6 アドレスの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	－
2． interface view に移行する	**interface** *interface-type interface-number*	－

操作	コマンド	補足
3． ステートレスアドレス自動設定を有効にする	**ipv6 address auto**	デフォルト：設定なし インタフェースで**undo ipv6 address auto** コマンドを使用して、インタフェースに自動で作成されたすべてのIPv6グローバルユニキャストアドレスとリンクローカルアドレスを削除できます。

13.5.2 IPv6 リンクローカルアドレスの設定

IPv6 リンクローカルアドレスは、以下のいずれかの方法で設定することができます。

- **自動生成** － インタフェースのリンクローカルアドレスプレフィックス（FE80::/10）およびリンクレイヤアドレスに従って、装置はインタフェースのリンクローカルアドレスを自動的に生成します。
- **手動割り当て** － インタフェースの IPv6 リンクローカルアドレスを手動で割り当てることができます。

インタフェースは 1 つの IPv6 リンクローカルアドレスのみ持つことができます。リンクローカルアドレスの重複を避けるため、自動生成方式を使用します。

手動割り当ては、自動生成より優先されます。

- 最初に自動生成を採用し、次に手動割り当てを行った場合、手動で割り当てたリンクローカルアドレスが自動生成アドレスを上書きします。
- 最初に手動割り当てを行い、次に自動生成を取り入れた場合は、以下の両方が発生します。
  - □ インタフェースのリンクローカルアドレスは手動割り当てのものがそのまま使用されます。
  - □ 自動で生成されたリンクローカルアドレスは有効になりません。手動で割り当てられたアドレスを削除すると、自動生成のリンクローカルアドレスが有効になります。

I. IPv6 リンクローカルアドレスの自動生成の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	－
2． interface view に移行する	**interface** *interface-type interface-number*	－
3． IPv6 リンクローカルアドレスを自動生成するため、インタフェースを設定する	**ipv6 address auto link-local**	デフォルト：設定なし インタフェースにIPv6グローバルユニキャストアドレスが設定された後、リンクローカルアドレスが自動生成されます。

II. IPv6 リンクローカルアドレスの手動割り当ての設定

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． interface view に移行する	**interface** *interface-type interface-number*	―
3． IPv6 リンクローカルアドレスを手動で割り当てる	**ipv6 address** { *ipv6-address* [*prefix-length*] | *ipv6-address/prefix-length* } **link-local**	デフォルト：設定なし インタフェースにIPv6グローバルユニキャストアドレスが設定された後、リンクローカルアドレスが自動生成されます。

インタフェースに IPv6 グローバルユニキャストアドレスが設定された後、インタフェースはリンクローカルアドレスを自動的に生成します。自動的に生成されたリンクローカルアドレスは、**ipv6 address auto link-local** コマンドを使用して生成されたものと同じです。インタフェースにリンクローカルアドレスを手動で割り当てた場合、このリンクローカルアドレスが有効になります。手動で割り当てられたリンクローカルアドレスが削除されると、自動生成されたリンクローカルアドレスが有効になります。

インタフェースで **undo ipv6 address auto link-local** コマンドを使用することでのみ、**ipv6 address auto link-local** コマンドで生成されたリンクローカルアドレスを削除できます。インタフェースに IPv6 グローバルユニキャストアドレスが既に設定されている場合、インタフェースはリンクローカルアドレスを保持します。インタフェースに IPv6 グローバルユニキャストアドレスが設定されていない場合、インタフェースはリンクローカルアドレスを保持しません。

13.5.3 IPv6 エニーキャストアドレスの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． interface view に移行する	**interface** *interface-type interface-number*	―
3． IPv6 エニーキャストアドレスを設定する	**ipv6 address** { *ipv6-address prefix-length* | *ipv6-address*/*prefix-length* } **anycast**	デフォルト：設定なし

13.6 IPv6 NDの設定

この章は IPv6 ND プロトコルの設定方法について記載します。

13.6.1 スタティックネイバエントリの設定

ネイバエントリはリンクローカルノードの情報を記録します。エントリは、NS メッセージおよび NA メッセージを介して動的、あるいは手動で設定することができます。

装置はネイバの IPv6 アドレスとローカルのレイヤ 3 インタフェース番号によってスタティックネイバエントリを固有に識別します。以下のいずれかの方法を使用することでスタティックネイバエントリを設定することができます。

- **方法 1** – ローカルのレイヤ 3 インタフェースにネイバの IPv6 アドレスとリンクレイヤアドレスを関連づけます。

  方法 1 を使用する場合、装置はネイバに接続するレイヤ 2 ポートを自動的に検索します。

- **方法 2** – VLAN のレイヤ 2 ポートにネイバの IPv6 アドレスとリンクレイヤアドレスを設定します。

  方法 2 を使用する場合、対応する VLAN インタフェースが存在しており、*port-type port-number* によって指定されたレイヤ 2 ポートが、*vlan-id* で指定されている VLAN に属していることを確認してください。装置はスタティックネイバエントリを識別するため、VLAN インタフェースをネイバの IPv6 アドレスに関連づけます。

以下にスタティックネイバエントリの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	–
2. スタティックネイバエントリを設定する	**ipv6 neighbor** *ipv6-address mac-address* { *vlan-id port-type port-number* | **interface** *interface-type interface-number* }	デフォルト：設定なし

13.6.2 動的に学習されるネイバの最大数の設定

装置は、ネイバノードのリンクレイヤアドレスを動的に取得して、NS メッセージおよび NA メッセージを介してネイバテーブルに追加することができます。ネイバエントリが動的に取得できるネイバテーブルが上限に到達すると、インタフェースはネイバ情報の学習を停止します。インタフェースでの多くのネイバテーブルによるリソースの枯渇を防ぐため、インタフェースが動的に学習できるネイバの最大数を設定することができます。

以下に動的に学習されるネイバの最大数の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	–
2. interface view に移行する	**interface** *interface-type interface-number*	–
3. 動的に学習されるネイバの最大数を設定する	**ipv6 neighbors max-learning-num** *max-number*	デフォルト：16384

13.6.3 STALE 状態での ND エントリのエージングタイマの設定

ND エントリは、エージングタイマを持っています。エージングタイマが終了する前に、STALE 状態の ND エントリが更新されない場合、ND エントリは DELAY 状態に遷移します。5 秒以内に更新されない場合、PROBE 状態に遷移し、装置は 3 回 NS メッセージを送信します。応答がない場合、ND エントリを削除します。

以下に ND エントリのエージングタイマの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. ND エントリのエージングタイマを設定する	**ipv6 neighbor stale-aging** *aging-time*	デフォルト：240分

13.6.4 Hop Limit の設定

装置は RA メッセージの Hop Limit を通知します。RA メッセージを受信するすべてのホストは送信する IPv6 パケットの Hop Limit フィールドの値を埋めるため、通知された値を使用します。

以下に Hop Limit の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. Hop Limit フィールドを設定する	**ipv6 hop-limit** *value*	デフォルト：64

13.6.5 RA メッセージのパラメータの設定

インタフェースが RA メッセージを送るかどうか、および RA メッセージを送信する間隔および RA メッセージのパラメータを設定することができます。RA メッセージを受信すると、ホストはこれらのパラメータを使用して、対応する動作を実行することができます。

表 13-4に RA メッセージに含まれる設定可能なパラメータを示します。

表 13-4 RA メッセージに含まれる設定可能なパラメータと説明

パラメータ	説明
Hop Limit	RAメッセージの最大ホップ数です。RAメッセージを受信したホストはIPv6パケットを送信するHop Limitフィールドに、この値を入れます。
Prefix information	装置によって広告されたプレフィックス情報を受信した後、同一リンク上のホストはステートレスオートコンフィギュレーションを実行することができます。
MTU	同じMTU値を使用するリンクのすべてのノードを保証します。
Boot file URL	RAメッセージでBoot fileをダウンロードするためのURLアドレスを指定します。DHCPv6を使用する代わりに、装置はNDプロトコルを使用して、自動設定用のIPv6アドレスとBoot file URLの両方を取得できます。
M flag	このフィールドは、ホストがIPv6アドレス取得のためにステートフルオートコンフィギュレーションを使用するかどうかを決定します。 Mフラグが1に設定されると、ホストはステートフルオートコンフィギュレーションを使用して（たとえばDHCPv6サーバ）IPv6アドレスを取得します。その他の場合は、ホストはステートレスオートコンフィギュレーションを使用してIPv6アドレスを取得します。

パラメータ	説明
O flag	このフィールドは、ホストがIPv6アドレス以外の情報を取得するために、ステートフルオートコンフィギュレーションを使用するかどうかを決定します。 Oフラグが1に設定されると、ホストはステートフルオートコンフィギュレーション（たとえばDHCPv6サーバ）を使用してIPv6アドレス以外の情報を取得します。その他の場合は、ホストはステートレスオートコンフィギュレーションを使用してIPv6アドレス以外の情報を取得します。
Router Lifetime	このフィールドは、RAメッセージを送信してホストのデフォルトルータとして機能するルータの有効期限を設定する場合に使用します。 有効期限が0の場合、ルータはデフォルトゲートウェイとして使用することができません。
Retrans Timer	NSメッセージを送信した後、この指定時間内に応答メッセージを装置が受信できなかった場合、装置はNSメッセージを再送信します。
Reachable Time	ネイバの到達可能性を検出することによってネイバが到達可能であることが示されると、この到達可能時間内に到達できるものと装置はみなします。到達可能時間が終了した後、ネイバにパケットを送信する必要がある場合は、装置は宛先が到達可能か再確認します。
Router Preference	RAメッセージのルータ優先度です。ホストはRouter Preferenceの値に従ってデフォルトゲートウェイとしてルータを選択します。Router Preferenceの値が同一である場合、ホストは最初にRAメッセージを受信したルータを選択します。
DNS server option	IPv6ホストのDNSサーバ情報です。ホストは、DHCPv6を使用する代わりに、受信したRAメッセージからDNSサーバ情報を取得できます。
DNS suffix information in DNS Search List (DNSSL) option	Pv6ホストのDNSサフィックス情報です。ホストは、DHCPv6を使用する代わりに、受信したRAメッセージからDNSサフィックス情報を取得できます。

ルータがRAメッセージをアップデートできるように､RAメッセージ送信の最大間隔は、RA メッセージのルータ有効期限と等しいか、それよりも短くしてください。

インタフェースに対して設定された Retrans Timer フィールドと Reachable Time フィールドの値は、RA メッセージを介してホストに送られます。さらに、このインタフェースは Retrans Timer の間隔で NS メッセージを送信し、ネイバを Reachable Time の時間内に到達可能であるとみなします。

I. RA メッセージの送信の有効化

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. interface view に移行する	**interface** *interface-type interface-number*	―
3. RA メッセージ送信の抑制を有効にする	**undo ipv6 nd ra halt**	デフォルト：無効
4. RA メッセージの送信間隔の最大値と最小値を設定する	**ipv6 nd ra interval** *max-interval min-interval*	デフォルト:RAメッセージの送信間隔は最長で600秒、最短で200秒です。 RAメッセージは最長と最短の間隔の中でランダムに送信されます。 最短間隔は最長間隔の0.75倍以内に設定してください。

II. RA メッセージのパラメータの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． interface view に移行する	**interface** *interface-type interface-number*	―
3． RA メッセージのプレフィックス情報のオプションを設定する	**ipv6 nd ra prefix** { *ipv6-prefix prefix-length* | *ipv6-prefix*/*prefix-length* } [*valid-lifetime preferred-lifetime* [**no-autoconfig** | **off-link** | **prefix-preference** *level*] *]	デフォルト：設定なし RAメッセージを送信するインタフェースのIPv6アドレスはプレフィックス情報として使用されます。 IPv6アドレスが手動で設定された場合、*valid-lifetime*は2592000秒（30日）、*preferred-lifetime*は604800秒（7日）の固定の値を使用します。 IPv6アドレスを自動で取得した場合、プレフィックスは設定された*valid-lifetime*と*preferred-lifetime*を使用します。
4． M フラグビットを 1 に設定する	**ipv6 nd autoconfig managed-address-flag**	デフォルト：0 ホストがステートレスオートコンフィギュレーションによってIPv6アドレスを取得します。
5． O フラグビットを 1 に設定する	**ipv6 nd autoconfig other-flag**	デフォルト：0 ホストがステートレスオートコンフィギュレーションによってその他の情報を取得します。
6． RA メッセージのルータの有効期限を設定する	**ipv6 nd ra router-lifetime** *time*	デフォルト：1800秒
7． NS retrans タイマを設定する	**ipv6 nd ns retrans-timer** *value*	デフォルト：1000ミリ秒の間隔でNSメッセージが送信され、RAメッセージのRetrans Timerフィールドは0です。
8． 到達可能な時間を設定する	**ipv6 nd nud reachable-time** *time*	デフォルト：ネイバ到達可能時間は1200000ミリ秒で、RAメッセージのReachable Timerフィールドは0です。

13.6.6 DAD のための NS メッセージ送信試行回数の設定

IPv6 アドレスを取得した後、インタフェースは IPv6 アドレスが重複しているか検出する DAD（Duplicate Address Detection）を行うため、NS メッセージを送信します。インタフェースが（**ipv6 nd ns retrans-timer** コマンドによって決定される）指定時間内に応答を受信できなかった場合は、NS メッセージの送信を続けます。**ipv6 nd dad attempts** コマンドで設定される NS メッセージの送信試行回数が、最大に達しても応答が得られなかった場合は、取得したアドレスが使用可能であるとみなされます。

以下に DAD のための NS メッセージ送信試行回数の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． interface view に移行する	**interface** *interface-type interface-number*	―
3． DAD のための NS メッセージ送信試行回数を設定する	**ipv6 nd dad attempts** *times*	デフォルト：1 0はDADが無効であることを示します。

13.7 PMTU探索（ディスカバリ）の設定

13.7.1 インタフェースの MTU の設定

IPv6 ルータはパケットのフラグメントをサポートしていません。パケットサイズが出力インタフェースの MTU を超過すると、IPv6 ルータはパケットを廃棄し、送信元ホストに Packet Too Big メッセージを送信します。送信元ホストは MTU に従ってパケットを分割します。この問題を防ぐため、インタフェースで適切に MTU を設定します。

以下にインタフェースの MTU の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． interface view に移行する	**interface** *interface-type interface-number*	―
3． インタフェースの MTU を設定する	**ipv6 mtu** *size*	デフォルト：設定なし

13.7.2 IPv6 アドレスのスタティック PMTU の設定

宛先 IPv6 アドレスにスタティック PMTU を設定することができます。IPv6 アドレスのパケットを送信する前に、装置は出力インタフェースの MTU をスタティック PMTU と比較します。パケットサイズが 2 つの値で小さい方を超える場合は、ホストは小さい方の値に従ってパケットをフラグメント化します。フラグメントした後、装置はダイナミックに宛先ホストに PMTU を検出することができます。（オペレーションマニュアルのセクション 3 *IP サービス*”*IPv6 の基本*”の”*IPv6 path MTU discovery（IPv6 PMTU 探索）*”を参照してください。）

以下に指定した IPv6 アドレスのスタティック PMTU の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． 宛先 IPv6 アドレスにスタティック PMTU を設定する	**ipv6 pathmtu** *ipv6-address value*	デフォルト：設定なし

13.7.3 ダイナミック PMTU のエージングタイマの設定

送信元ホストから宛先ホストまでのパスの MTU が動的に決定すると（オペレーションマニュアルのセクション 3 *IP サービス "IPv6 の基本"の"IPv6 path MTU discovery（IPv6 PMTU 探索）"*を参照してください）、装置は以下の処理を行います。

- パスの MTU にもとづいて宛先ホストにパケットを送信します。
- エージングタイマを開始します。

エージングタイマが終了すると、動的に決定した PMTU が削除されます。送信元ホストは再度 MTU を決定し、PMTU メカニズムによってパケットを送信します。

以下にダイナミック PMTU のエージングタイマの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. ダイナミック PMTU のエージング時間を設定する	**ipv6 pathmtu age** *age-time*	デフォルト：10分 スタティックPMTUへのエージングタイマは無効です。

13.8 ICMPv6メッセージ送信の管理

この章は ICMPv6 メッセージの送信に関する設定方法について記載します。

13.8.1 ICMPv6 エラーメッセージのレートリミットの設定

ネットワークの混雑状態を引き起こす可能性のある短い期間内に、過度の ICMPv6 エラーメッセージを送信することを避けるため、ICMPv6 エラーメッセージの送信レートを制限することができます。トークンバケット（bucket）アルゴリズムは、1 つの ICMPv6 エラーメッセージを示す 1 つのトークンが用いられます。

バケットに入ることができるトークンの最大数に達するまで、トークンは指定された間隔でバケットに配置されます。

ICMPv6 エラーメッセージが送信される場合に、トークンはバケットから取り除かれます。バケットが空の場合、新しいトークンがバケットに配置されるまで、ICMPv6 エラーメッセージは送信されません。

以下に ICMPv6 エラーメッセージのレートリミットの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. ICMPv6 エラーメッセージの間隔とトークンバケットサイズを設定する	**ipv6 icmpv6 error-interval** *interval* [*bucketsize*]	デフォルト：100ミリ秒間隔で最大10トークンが配置されます。 ICMPv6レートリミットを無効にするには、間隔を0ミリ秒に設定します。

13.8.2 マルチキャストエコー要求への応答の有効化

装置はデフォルトでマルチキャストエコー要求の返答は無効です。しかし、いくつかのシナリオでは、送信元ホストが必要な情報を取得できるようにするため、マルチキャストエコー要求に応答する必要があります。

以下にマルチキャストエコー要求への応答の有効化の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. マルチキャストエコー要求への応答を有効にする	**ipv6 icmpv6 multicast-echo-reply enable**	デフォルト：無効

13.8.3 ICMPv6 宛先到達不能メッセージの有効化

装置は ICMPv6 宛先到達不能メッセージを以下のように送信します。

- **ICMPv6 No Route to Destination メッセージ**– 転送されたパケットがすべてのルートに一致しません。
- **ICMPv6 Communication with Destination Administratively Prohibited メッセージ**– 装置が宛先へのパケットの転送を禁止しています。通常、装置で Firewall フィルタや ACL などによって行われます。
- **ICMPv6 Beyond Scope of Source Address メッセージ**– 宛先が送信元 IPv6 アドレスの境界を超えています。たとえば、宛先 IPv6 アドレスがグローバルユニキャストアドレスで、送信元 IPv6 アドレスがリンクローカルアドレスです。
- **ICMPv6 Address Unreachable メッセージ**– 装置がパケットの宛先 IPv6 アドレスのリンクレイヤアドレスを解決できません。
- **ICMPv6 Port Unreachable メッセージ**– 装置向けの UDP パケットを受信したが UDP 宛先ポート番号が存在しません。

装置が間違って ICMPv6 宛先到達不能メッセージを作成する場合、攻撃リスクを防ぐため、ICMPv6 宛先到達不能メッセージの送信を無効にします。

以下に ICMPv6 宛先到達不能メッセージを送信する設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. ICMPv6 宛先到達不能メッセージの送信を有効にする	**ipv6 unreachables enable**	デフォルト：無効

13.8.4 ICMPv6 時間超過メッセージの送信の有効化

装置は、以下に従って ICMPv6 時間超過メッセージを送信します

- 受信した IPv6 パケットが装置向けではなく、Hop Limit が 1 の場合、装置は ICMPv6 Hop Limit Exceeded メッセージを送信元に送信します。
- 宛先 IP アドレスが装置向けである IPv6 データグラムのフラグメントされた最初のパケットを受信すると、タイマがスタートします。フラグメントされたすべてのパケッ

トが届く前に、タイマが終了になった場合、ICMPv6 Fragment Reassembly Timeout メッセージを送信元に送信します。

悪意のあるパケットを大量に受信した場合、ICMP 時間超過メッセージにより装置のパフォーマンスが低下します。この攻撃を防ぐため、ICMPv6 時間超過メッセージの送信を無効にすることができます。

以下に ICMPv6 時間超過メッセージの送信の有効化の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． ICMPv6 時間超過メッセージの送信を有効にする	**ipv6 hoplimit-expires enable**	デフォルト：有効

13.9 IPv6の基本設定の表示と維持

すべての view で **display** コマンドを実行でき、user view で **reset** コマンドを実行できます。

操作	コマンド
IPv6 FIBエントリを表示する	**display ipv6 fib** [*ipv6-address* [*prefix-length*]]
インタフェースのIPv6情報を表示する	**display ipv6 interface** [*interface-type* [*interface-number*]] [**brief**]
ネイバ情報を表示する	**display ipv6 neighbors** { { *ipv6-address* | **all** | **dynamic** | **static** } [**slot** *slot-number*] | **interface** *interface-type interface-number* | **vlan** *vlan-id* } [**verbose**]
ネイバエントリの総数を表示する	**display ipv6 neighbors** { { **all** | **dynamic** | **static** } [**slot** *slot-number*] | **interface** *interface-type interface-number* | **vlan** *vlan-id* } **count**
IPv6アドレスのPMTU情報を表示する	**display ipv6 pathmtu** { *ipv6-address* | { **all** | **dynamic** | **static** } [**count**] }
IPv6パケットとICMPv6パケットの統計情報を表示する	**display ipv6 statistics** [**slot** *slot-number*]
IPv6 RawIP接続の概要情報を表示する	**display ipv6 rawip** [**slot** *slot-number*]
IPv6 RawIP接続の詳細情報を表示する	**display ipv6 rawip verbose** [**slot** *slot-number* [**pcb** *pcb-index*]]
IPv6 TCP接続の概要情報を表示する	**display ipv6 tcp** [**slot** *slot-number*]
IPv6 TCP接続の詳細情報を表示する	**display ipv6 tcp verbose** [**slot** *slot-number* [**pcb** *pcb-index*]]
IPv6 UDP接続の概要情報を表示する	**display ipv6 udp** [**slot** *slot-number*]
IPv6 UDP接続の詳細情報を表示する	**display ipv6 udp verbose** [**slot** *slot-number* [**pcb** *pcb-index*]]
IPv6 TCP接続の統計情報を表示する	**display tcp statistics** [**slot** *slot-number*]
IPv6 UDP接続の統計情報を表示する	**display udp statistics** [**slot** *slot-number*]
IPv6ネイバ情報を削除する	**reset ipv6 neighbors** { **all** | **dynamic** | **interface** *interface-type interface-number* | **slot** *slot-number* | **static** }
IPv6アドレスのPMTU情報を削除する	**reset ipv6 pathmtu** { **all** | **dynamic** | **static** }

操作	コマンド
IPv6パケットとICMPv6パケットの統計情報を削除する	**reset ipv6 statistics** [**slot** *slot-number*]
IPv6 TCP接続の統計情報を削除する	**reset tcp statistics**
IPv6 UDP接続の統計情報を削除する	**reset udp statistics**

13.10 IPv6の基本設定例

13.10.1 IPv6 の基本設定例

I. ネットワーク要件

図 13-6に示すように、Host、Switch A、Switch B が Ethernet ポートを通して接続されています。Ethernet ポートに VLAN を設定し、VLAN インタフェースに IPv6 アドレスを設定します。Switch B と Host 間で通信可能となります。

Host で IPv6 を有効にし、IPv6 ND によって IPv6 アドレスを自動的に取得します。

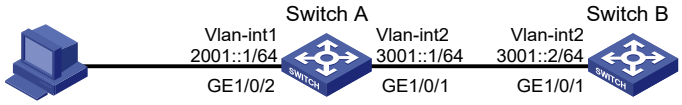


図 13-6 ネットワーク図

II. 設定手順

この例では、各 Switch で、各 VLAN インタフェースを事前に作成されていると仮定します。

1)　Switch A を設定します。

VLAN インタフェース 2 にグローバルユニキャストアドレスを設定します。

```
<SwitchA> system-view
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ipv6 address 3001::1/64
[SwitchA-Vlan-interface2] quit
```

VLAN インタフェース 1 にグローバルユニキャストアドレスを指定し、RA メッセージ（デフォルトでインタフェースは RA メッセージを送信しません）を送信するようにします。

```
[SwitchA] interface vlan-interface 1
[SwitchA-Vlan-interface1] ipv6 address 2001::1/64
[SwitchA-Vlan-interface1] undo ipv6 nd ra halt
[SwitchA-Vlan-interface1] quit
```

2)　Switch B を設定します。

VLAN インタフェース 2 にグローバルユニキャストアドレスを設定します。

```
<SwitchB> system-view
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] ipv6 address 3001::2/64
[SwitchB-Vlan-interface2] quit
```

宛先 IP アドレス 2001::/64 への IPv6 スタティックルート、ネクストホップアドレス 3001::1 を設定します。

```
[SwitchB] ipv6 route-static 2001:: 64 3001::1
```

3)　host を設定します。

IPv6 ND を通して、IPv6 アドレスを自動で取得する設定を有効にします。

Switch A の GigabitEthernet 1/0/2 のネイバ情報を表示します。

```
[SwitchA] display ipv6 neighbors interface gigabitethernet 1/0/2
Type: S-Static    D-Dynamic     O-Openflow     R-Rule    IS-Invalid static
IPv6 address              MAC address    VID  Interface          State T  Aging
FE80::215:E9FF:FEA6:7D14  0015-e9a6-7d14 1    GE1/0/2             STALE D  1238
2001::15B:E0EA:3524:E791  0015-e9a6-7d14 1    GE1/0/2             STALE D  1248
```

出力は、Host が取得した IPv6 グローバルユニキャストアドレスが 2001::15B:E0EA:3524:E791 であることを示しています。

III. 設定の確認

Switch A で IPv6 インタフェースの設定を表示します。インタフェースで設定されたすべての IPv6 グローバルユニキャストアドレスが表示されます。

```
[SwitchA] display ipv6 interface vlan-interface 2
Vlan-interface2 current state: UP
Line protocol current state: UP
IPv6 is enabled, link-local address is FE80::20F:E2FF:FE00:2
  Global unicast address(es):
    3001::1, subnet is 3001::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF00:1
    FF02::1:FF00:2
  MTU is 1500 bytes
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND retransmit interval is 1000 milliseconds
  Hosts use stateless autoconfig for addresses
IPv6 Packet statistics:
  InReceives:                    25829
  InTooShorts:                   0
  InTruncatedPkts:               0
```

```
  InHopLimitExceeds:              0
  InBadHeaders:                   0
  InBadOptions:                   0
  ReasmReqds:                     0
  ReasmOKs:                       0
  InFragDrops:                    0
  InFragTimeouts:                 0
  OutFragFails:                   0
  InUnknownProtos:                0
  InDelivers:                     47
  OutRequests:                    89
  OutForwDatagrams:               48
  InNoRoutes:                     0
  InTooBigErrors:                 0
  OutFragOKs:                     0
  OutFragCreates:                 0
  InMcastPkts:                    6
  InMcastNotMembers:              25747
  OutMcastPkts:                   48
  InAddrErrors:                   0
  InDiscards:                     0
  OutDiscards:                    0
```

[SwitchA] display ipv6 interface vlan-interface 1

```
Vlan-interface1 current state: UP
Line protocol current state: UP
IPv6 is enabled, link-local address is FE80::20F:E2FF:FE00:1C0
  Global unicast address(es):
    2001::1, subnet is 2001::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF00:1
    FF02::1:FF00:1C0
  MTU is 1500 bytes
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND retransmit interval is 1000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 600 seconds
  ND router advertisements live for 1800 seconds
  Hosts use stateless autoconfig for addresses
IPv6 Packet statistics:
  InReceives:                     272
  InTooShorts:                    0
  InTruncatedPkts:                0
  InHopLimitExceeds:              0
  InBadHeaders:                   0
  InBadOptions:                   0
  ReasmReqds:                     0
  ReasmOKs:                       0
  InFragDrops:                    0
  InFragTimeouts:                 0
  OutFragFails:                   0
  InUnknownProtos:                0
  InDelivers:                     159
  OutRequests:                    1012
  OutForwDatagrams:               35
  InNoRoutes:                     0
  InTooBigErrors:                 0
  OutFragOKs:                     0
  OutFragCreates:                 0
  InMcastPkts:                    79
  InMcastNotMembers:              65
  OutMcastPkts:                   938
  InAddrErrors:                   0
  InDiscards:                     0
  OutDiscards:                    0
```

Switch B で IPv6 インタフェースの設定を表示します。インタフェースで設定されたすべての IPv6 グローバルユニキャストアドレスが表示されます。

```
[SwitchB] display ipv6 interface vlan-interface 2
Vlan-interface2 current state :UP
Line protocol current state :UP
IPv6 is enabled, link-local address is FE80::20F:E2FF:FE00:1234
  Global unicast address(es):
    3001::2, subnet is 3001::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF00:2
    FF02::1:FF00:1234
  MTU is 1500 bytes
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND retransmit interval is 1000 milliseconds
  Hosts use stateless autoconfig for addresses
IPv6 Packet statistics:
  InReceives:                    117
  InTooShorts:                   0
  InTruncatedPkts:               0
  InHopLimitExceeds:             0
  InBadHeaders:                  0
  InBadOptions:                  0
  ReasmReqds:                    0
  ReasmOKs:                      0
  InFragDrops:                   0
  InFragTimeouts:                0
  OutFragFails:                  0
  InUnknownProtos:               0
  InDelivers:                    117
  OutRequests:                   83
  OutForwDatagrams:              0
  InNoRoutes:                    0
  InTooBigErrors:                0
  OutFragOKs:                    0
  OutFragCreates:                0
  InMcastPkts:                   28
  InMcastNotMembers:             0
  OutMcastPkts:                  7
  InAddrErrors:                  0
  InDiscards:                    0
  OutDiscards:                   0
```

Host で Switch A、Switch B 間で ping を行い、Switch A、Switch B、Host が接続されていることを確認します。

🕮 メモ：

リンクローカルアドレスに ping を行う際、パラメータ“**-i**”を使用してください

```
[SwitchB] ping ipv6 -c 1 3001::1
Ping6(56 data bytes) 3001::2 --> 3001::1, press CTRL_C to break
56 bytes from 3001::1, icmp_seq=0 hlim=64 time=4.404 ms

--- Ping6 statistics for 3001::1 ---
1 packet(s) transmitted, 1 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 4.404/4.404/4.404/0.000 ms
[SwitchB] ping ipv6 -c 1 2001::15B:E0EA:3524:E791
Ping6(56 data bytes) 3001::2 --> 2001::15B:E0EA:3524:E791, press CTRL_C to break
56 bytes from 2001::15B:E0EA:3524:E791, icmp_seq=0 hlim=64 time=5.404 ms
```

```
--- Ping6 statistics for 2001::15B:E0EA:3524:E791 ---
1 packet(s) transmitted, 1 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 5.404/5.404/5.404/0.000 ms
```

出力では、Switch B が Switch A、Host に ping が実行できることを示しています。また Host が Switch B、Switch A に ping が実行できることを示しています。

13.11 IPv6の基本のトラブルシューティング

13.11.1 症状

対向の IPv6 アドレスに対して ping ができません。

13.11.2 分析

1) 任意の view で **display ipv6 interface** コマンドを使用し、出力インタフェースの IPv6 アドレスが正常で、インタフェースが up であることを確認します。
2) IPv6 パケットのデバッグを有効にし、故障箇所を究明するため、user view で **debugging ipv6 packet** コマンドを使用します。

目次

このセクションのページは**3-x-x** です。

14 章 Proxy ARP..... 14-1
14.1 一般的な Proxy ARP の有効化..... 14-1
14.2 ローカル Proxy ARP の有効化..... 14-1
14.3 Proxy ARP の表示と維持..... 14-1
14.4 一般的な Proxy ARP 設定例..... 14-2
14.4.1 ネットワーク要件..... 14-2
14.4.2 設定手順..... 14-2
14.4.3 設定の確認..... 14-3

14章 Proxy ARP

Proxy ARP が有効な装置で、別のネットワークの IP アドレスの ARP リクエストに応答します。Proxy ARP を有効にすることで、異なるブロードキャストドメインのホストが同一のブロードキャストドメインにいるように互いに通信できるようにします。

Proxy ARP は一般的な Proxy ARP とローカル Proxy ARP があります。

- **一般的な Proxy ARP**－異なるレイヤ 3 インタフェースに接続され、異なるブロードキャストドメインに存在するホスト間で通信することができます。
- **ローカル Proxy ARP**－同一のレイヤ 3 インタフェースに接続され、異なるブロードキャストドメインに存在するホスト間で通信することができます。

14.1 一般的なProxy ARPの有効化

操作	コマンド	補足
1． system view に移行する	**system-view**	－
2． VLAN interface view に移行する	**interface** *vlan-interface vlan-interface-id*	－
3． 一般的な Proxy ARP を有効にする	**proxy-arp enable**	デフォルト：無効

14.2 ローカルProxy ARPの有効化

操作	コマンド	補足
1． system view に移行する	**system-view**	－
2． VLAN interface view に移行する	**interface** *vlan-interface vlan-interface-id*	－
3． ローカル Proxy ARP を有効にする	**local-proxy-arp enable** [**ip-range** *startIP* **to** *endIP*]	デフォルト：無効

14.3 Proxy ARPの表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
一般的なProxy ARPの状態を表示する	**display proxy-arp** [**interface** *interface-type interface-number*]
ローカルProxy ARPの状態を表示する	**display local-proxy-arp** [**interface** *interface-type interface-number*]

14.4 一般的なProxy ARP設定例

14.4.1 ネットワーク要件

図 14-1に示すように、Host A と Host D は同一 IP アドレスとマスクを持ちますが、Switch によって異なるサブネットに分離されています。Host A は VLAN1、Host D は VLAN2 に所属しています。Host A と Host D のデフォルトゲートウェイは設定されていません。

2 つの Host 間で通信ができるように Switch で一般的な Proxy ARP を設定します。

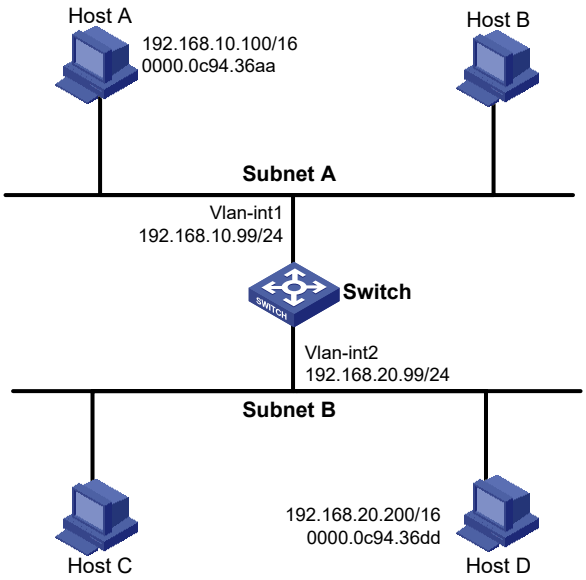


図 14-1 ネットワーク図

14.4.2 設定手順

VLAN 2 を作成します。

```
<Switch> system-view
[Switch] vlan 2
[Switch-vlan2] quit
```

VLAN インタフェース 1 の IP アドレスを設定します。

```
[Switch] interface vlan-interface 1
[Switch-Vlan-interface1] ip address 192.168.10.99 255.255.255.0
```

VLAN インタフェース 1 で一般的な Proxy ARP を有効にします。

```
[Switch-Vlan-interface1] proxy-arp enable
[Switch-Vlan-interface1] quit
```

VLAN インタフェース 2 の IP アドレスを設定します。

```
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ip address 192.168.20.99 255.255.255.0
```

VLAN インタフェース 2 で一般的な Proxy ARP を有効にします。

```
[Switch-Vlan-interface2] proxy-arp enable
```

14.4.3 設定の確認

Host A と Host D で互いに ping ができるかどうか確認してください。

目次

このセクションのページは**3-x-x** です。

15 章 DHCPv6 の概要 15-1
15.1 DHCPv6 アドレス/プレフィックス割り当て 15-1
15.1.1 2 つのメッセージによる高速割り当て 15-1
15.1.2 4 つのメッセージによる割り当て 15-1
15.2 アドレス/プレフィックスのリース更新 15-2
15.3 ステートレス DHCPv6 15-3
15.4 DHCPv6 オプション 15-4
15.4.1 オプション 18 15-4
15.4.2 オプション 37 15-5
15.4.3 オプション 79 15-5
15.5 プロトコルと標準 15-6

15章 DHCPv6 の概要

DHCPv6 は、IPv6 プレフィックス、IPv6 アドレスやほかの設定パラメータをホストに割り当てます。

15.1 DHCPv6アドレス/プレフィックス割り当て

DHCPv6 アドレス/プレフィックスの割り当てのプロセスは 2 つあるいは 4 つのメッセージがあります。

15.1.1 2 つのメッセージによる高速割り当て

図 15-1に示すように高速割り当て(Rapid assignment)のプロセスの動作を以下に示します。

1) DHCPv6 クライアントは高速割り当てを行うため、Rapid Commit オプションを含む Solicit メッセージを送信します。
2) DHCPv6 サーバが高速割り当てをサポートしている場合、割り当てられる IPv6 アドレス/プレフィックスとほかの設定パラメータを含んだ Reply メッセージで応答します。DHCPv6 サーバが高速割り当てをサポートしていない場合、4 つのメッセージによる割り当てを行います。

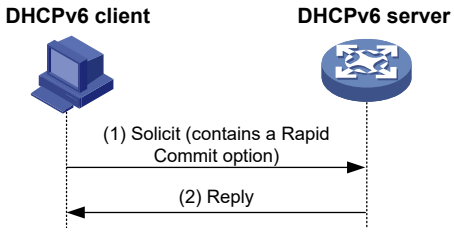


図 15-1 2 つのメッセージによる高速割り当て

15.1.2 4 つのメッセージによる割り当て

図 15-2に示すように 4 メッセージ割り当て(Assignment)でのプロセスの動作を以下に示します。

1) DHCPv6 クライアントは、IPv6 アドレス/プレフィックスとほかの設定パラメータを要求するため、Solicit メッセージを送信します。
2) 以下のどちらかの状況である場合、DHCPv6 サーバは割り当て可能な IPv6 アドレス/プレフィックスとほかの設定パラメータを含む Advertise メッセージで応答します。
   - Solicit メッセージが Rapid Commit オプションを含んでいない場合
   - Solicit メッセージが Rapid Commit オプションを含んでいるが DHCPv6 サーバが高速割り当てをサポートしていない場合

3) DHCPv6 クライアントは異なる DHCPv6 サーバによって提供される複数の Advertise メッセージを受信することができます。受信した番号、サーバ優先度に従って Advertise メッセージを選択し、確認のために選択したサーバに Request メッセージを送信します。
4) DHCPv6 サーバはアドレス/プレフィックスとほかの設定パラメータを割り当てるため、クライアントに Reply メッセージを送信します。

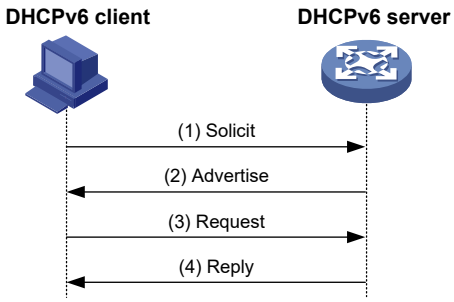


図 15-2 4 つのメッセージによる割り当て

15.2 アドレス/プレフィックスのリース更新

DHCPv6 サーバによって割り当てられた IPv6 アドレス/プレフィックスはリースできる有効期間があります。有効期間が終了すると、DHCPv6 クライアントは IPv6 アドレス/プレフィックスを使用することができません。IPv6 アドレス/プレフィックスを使用するため、DHCPv6 クライアントはリース期間を更新する必要があります。

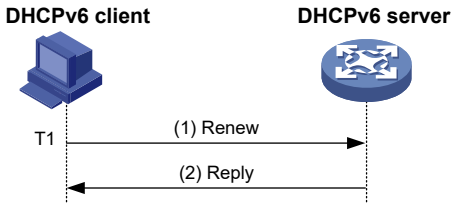


図 15-3 Renew メッセージを使用したアドレス/プレフィックスの更新

図 15-4に示すように、T1 で DHCPv6 クライアントは DHCPv6 サーバに Renew メッセージを送信します。T1 で推奨する値は、preferred 期限の半分の値です。DHCPv6 サーバは、クライアントに、リースが更新されるかどうかを通知するため、Reply メッセージで応答します。

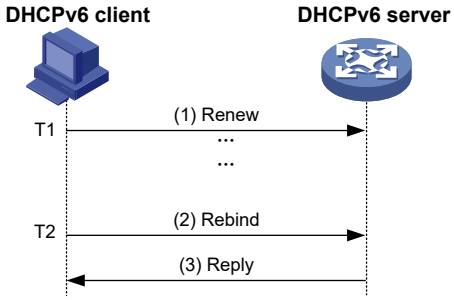


図 15-4 Rebind メッセージを使用したアドレス/プレフィックスリースの更新

図 15-4に示すように、処理します。

- DHCPv6 クライアントが T1 で Renew メッセージを送信した後、DHCPv6 サーバから応答が無い場合、T2 ですべての DHCPv6 サーバに Rebind メッセージをマルチキャストします。一般的に T2 は preferred 期限の 80%です。
- DHCPv6 サーバは、クライアントに、リースが更新されるかどうかを通知するため、Reply メッセージで応答します。
- DHCPv6 クライアントが、有効期限が終了する前にいずれの DHCPv6 サーバから応答を受信しない場合、クライアントはアドレス/プレフィックスの使用を中止します。
- 有効期限と preferred 期限についての詳細は、オペレーションマニュアルのセクション 3 *IP サービス* "*IPv6 の基本*"を参照してください。

15.3 ステートレスDHCPv6

IPv6 アドレス/プレフィックスを取得した装置は、ステートレス DHCPv6 を使用して DHCPv6 サーバからほかの設定パラメータを取得することができます。

装置はステートレス自動アドレス設定を行う間、ルータから受信した以下の RA メッセージのフラグによって、ステートレス DHCPv6 を実行します。

- 管理されたアドレス設定フラグ(M フラグ)が 0 に設定されています。
- ほかのステートフルフラグ(O フラグ)が 1 に設定されています。

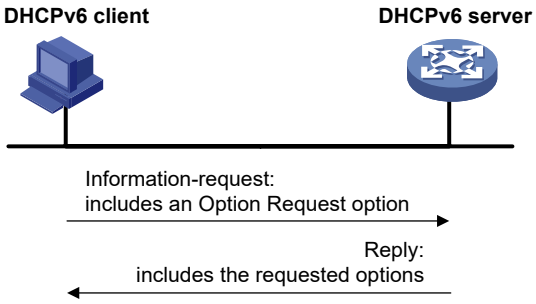


図 15-5 ステートレス DHCPv6 の動作

図 15-5におけるステートレス DHCPv6 の動作を以下に示します。

1) DHCPv6 クライアントは、すべての DHCPv6 サーバと DHCPv6 リレーエージェントに Information-request メッセージをマルチキャストします。Information-request メッセージは、DHCPv6 サーバからクライアントがリクエストする設定パラメータを指定した Option Request オプションが含まれます。
2) DHCPv6 サーバは、リクエストされた設定パラメータが含まれる Reply メッセージをクライアントに応答します。
3) クライアントは Reply メッセージをチェックします。取得した設定パラメータが Information-request メッセージのリクエストした内容にマッチした場合、クライアントはパラメータを使用してネットワーク設定を行います。一致しない場合、クライアントは設定パラメータを無視します。クライアントが複数の応答を受信した場合、最初に受信した応答を使用します。

15.4 DHCPv6オプション

15.4.1 オプション 18

オプション 18 はインタフェース ID と呼ばれます。RELAY-REPLY メッセージを転送するためにインタフェースを決定する DHCPv6 リレーエージェントによって使用されます。

DHCPv6 snooping 装置は DHCPv6 サーバに転送する前に受信した DHCPv6 要求メッセージにオプション 18 を追加します。サーバはオプション 18 のクライアント情報をもとにしてクライアントに IP アドレスを割り当てます。

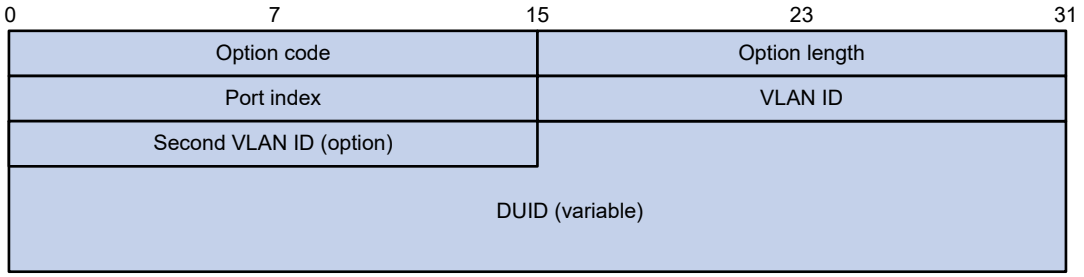


図 15-6 オプション 18 フォーマット

図 15-6にオプション 18 のフォーマットを示します。以下のフィールドを示します。

- **Option code**– オプションコードです。値は 18 です。
- **Option length**– オプションデータのサイズです。
- **Port index**– クライアントから DHCPv6 要求を受信したポートです。
- **VLAN ID**– 外部 VLAN の ID です。
- **Second VLAN ID**– 内部 VLAN の ID です。このフィールドはオプションです。受信した DHCPv6 要求に 2 番目の VLAN が含まれていない場合、オプション 18 も含まれません。
- **DUID**– DHCPv6 クライアントの DUID です。

15.4.2 オプション 37

オプションはリモート ID オプションと呼ばれます。クライアントを識別するために使用します。

DHCPv6 snooping 装置は DHCPv6 サーバに転送する前に受信した DHCPv6 要求メッセージにオプション 37 を追加します。オプションはアドレス割り当てについてのクライアント情報を提供します。

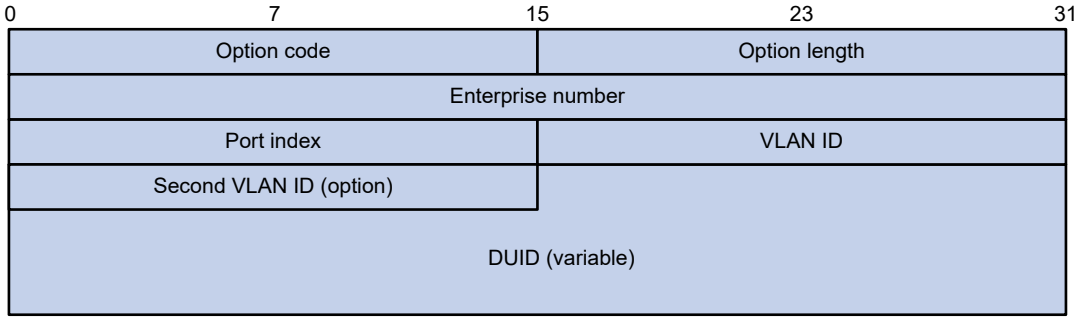


図 15-7 オプション 37 フォーマット

図 15-7にオプション 37 のフォーマットを示します。以下のフィールドを示します。

- **Option code**– オプションコードです。値は 37 です。
- **Option length**– オプションデータのサイズです。
- **Enterprise number**– エンタープライズ番号です。
- **Port index**– クライアントから DHCPv6 要求を受信したポートです。
- **VLAN ID**– 外部 VLAN の ID です。
- **Second VLAN ID**– 内部 VLAN の ID です。このフィールドはオプションです。受信した DHCPv6 要求に 2 番目の VLAN が含まれていない場合、オプション 37 も含まれません。
- **DUID**– DHCPv6 クライアントの DUID です。

15.4.3 オプション 79

クライアントリンクレイヤアドレスオプションとも呼ばれるオプション 79 は、DHCPv6 クライアントの MAC アドレスを記録するために使用されます。DHCPv6 要求が渡す最初のリレーエージェントは、クライアントの MAC アドレスを学習し、このアドレスを要求のリレー転送メッセージのオプション 79 にカプセル化します。DHCPv6 サーバは、クライアントを検証するか、クライアントの MAC アドレスに基づいて IPv6 アドレス/プレフィックスをクライアントに割り当てます。

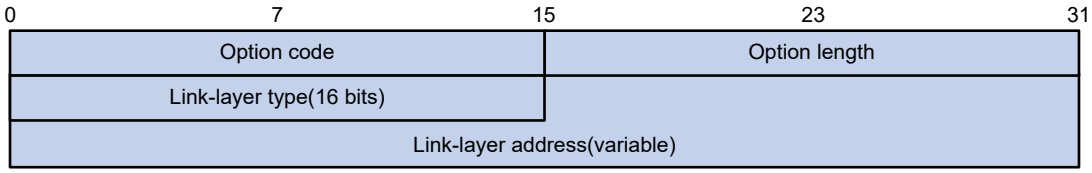


図 15-8 オプション 79 フォーマット

図 15-8にオプション 79 のフォーマットを示します。以下のフィールドを示します。

- **Option code**– オプションコードです。値は 79 です。
- **Option length**– オプションデータのサイズです。
- **Link-layer type**– クライアントのリンクレイヤアドレスタイプです。
- **Link-layer address**– クライアントのリンクレイヤアドレスです。

15.5 プロトコルと標準

- RFC 3736, *Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6*
- RFC 3315, *Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*
- RFC 2462, *IPv6 Stateless Address Autoconfiguration*
- RFC 3633, IPv6 *Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6*
- RFC 6939, *Client Link-Layer Address Option in DHCPv6*

目次

このセクションのページは**3-x-x** です。

16 章 DHCPv6 クライアント 16-1
16.1 概要 16-1
16.2 制限とガイドライン: DHCPv6 クライアント設定 16-1
16.3 DHCPv6 クライアント設定作業リスト 16-1
16.4 IPv6 アドレス取得の設定 16-1
16.5 DHCPv6 クライアントの表示および保守コマンド 16-2
16.6 DHCPv6 クライアント設定の例 16-2
16.6.1 IPv6 アドレス取得の設定例 16-2
16.6.2 ステートレス DHCPv6 の設定例 16-4

16章 DHCPv6 クライアント

装置は DHCPv6 クライアントが有効である場合、DHCPv6 クライアントとして機能し、DHCPv6 サーバから IP アドレスを含む設定パラメータを取得できます。

16.1 概要

DHCPv6 クライアントを設定すると、インタフェースは DHCPv6 サーバから設定パラメータを取得できます。

DHCPv6 クライアントは、DHCPv6 を使用して次の機能を実行できます。

- IPv6 アドレス、IPv6 プレフィックス、またはその両方を取得し、他の設定パラメータを取得します。DHCPv6 サーバが装置で有効になっている場合、クライアントは取得したパラメータを DHCPv6 オプショングループに自動的に保存できます。取得した IPv6 プレフィックスを使用して、クライアントはグローバルユニキャストアドレスを生成できます。
- ステートレス DHCPv6 をサポートし､IPv6 アドレスと IPv6 プレフィックスを除く設定パラメータを取得します。クライアントは、ステートレス IPv6 アドレス自動設定によって IPv6 アドレスを取得します。クライアントがアドレス取得中に、M フラグを 0、O フラグを 1 に設定した RA メッセージを受信すると、ステートレス DHCPv6 が起動します。

16.2 制限とガイドライン: DHCPv6クライアント設定

DHCPv6クライアントをDHCPv6サーバと同じインタフェースに設定しないでください。

16.3 DHCPv6クライアント設定作業リスト

作業リスト
(必須設定項目) IPv6アドレス取得の設定

16.4 IPv6アドレス取得の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. interface view に移行する	**interface** *interface-type interface-number*	―
3. DHCPv6 を使用して IPv6 アドレスとその他の設定パラメータを取得するようにインタフェースを設定する	**ipv6 address dhcp-alloc** [**option-group** *group-number* | **rapid-commit**] *	デフォルトでは、インタフェースはIPv6アドレス取得にDHCPv6を使用しません。

16.5 DHCPv6クライアントの表示および保守コマンド

操作	コマンド
DHCPv6クライアント情報を表示する	**display ipv6 dhcp client** [**interface** *interface-type interface-number*]
DHCPv6クライアント統計情報を表示する	**display ipv6 dhcp client statistics** [**interface** *interface-type interface-number*]
DHCPv6クライアント統計情報をクリアする	**reset ipv6 dhcp client statistics** [**interface** *interface-type interface-number*]

16.6 DHCPv6クライアント設定の例

16.6.1 IPv6 アドレス取得の設定例

I. ネットワーク要件

図 16-1に示すよう、DHCPv6 を使用して DHCPv6 サーバから設定パラメータを取得するようにスイッチを設定するパラメータには、IPv6 アドレス、DNS サーバアドレス、ドメイン名サフィックス、SIP サーバアドレス、および SIP サーバドメイン名が含まれます。

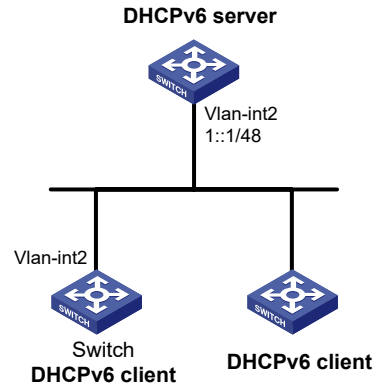


図 16-1 ネットワーク図

II. 設定手順

DHCPv6クライアントを設定する前に、まずDHCPv6サーバを設定する必要があります。

IPv6 アドレス取得のために DHCPv6 クライアントとして VLAN-interface 2 を設定します。DHCPv6 高速アドレス割り当てをサポートするために DHCPv6 クライアントを設定します。DHCPv6 クライアントを設定して、設定パラメータを保存するための動的 DHCPv6 オプショングループを作成します。

```
<Switch> system-view
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ipv6 address dhcp-alloc rapid-commit option-group 1
[Switch-Vlan-interface2] quit
```

III. 設定の確認

クライアントがサーバから IPv6 アドレスと他の設定パラメータを取得したことを確認します。

[Switch] display ipv6 dhcp client

```
Vlan-interface2:
  Type: Stateful client requesting address
    State: OPEN
    Client DUID: 0003000100e002000000
    Preferred server:
      Reachable via address: FE80::2E0:1FF:FE00:18
      Server DUID: 0003000100e001000000
    IA_NA: IAID 0x00000642, T1 50 sec, T2 80 sec
      Address: 1:1::2/128
       Preferred lifetime 100 sec, valid lifetime 200 sec
       Will expire on Mar 27 2014 at 08:06:57 (198 seconds left)
    DNS server addresses:
      2000::FF
    Domain name:
      example.com
    SIP server addresses:
      2:2::4
    SIP server domain names:
      bbb.com
```

装置で DHCPv6 サーバを有効にした後、設定パラメータが動的 DHCPv6 オプショングループに保存されていることを確認します。

[Switch] display ipv6 dhcp option-group 1

```
DHCPv6 option group: 1
  DNS server addresses:
    Type: Dynamic (DHCPv6 address allocation)
    Interface: Vlan-interface2
    2000::FF
  Domain name:
    Type: Dynamic (DHCPv6 address allocation)
    Interface: Vlan-interface2
    example.com
  SIP server addresses:
    Type: Dynamic (DHCPv6 address allocation)
    Interface: Vlan-interface2
    2:2::4
  SIP server domain names:
    Type: Dynamic (DHCPv6 address allocation)
    Interface: Vlan-interface2
    bbb.com
```

DHCPv6 クライアントが IPv6 アドレスを取得していることを確認します。

[Switch] display ipv6 interface brief

```
*down: administratively down
(s): spoofing
Interface                          Physical   Protocol   IPv6 Address
Vlan-interface2                    up         up         1:1::2
```

16.6.2 ステートレス DHCPv6 の設定例

I. ネットワーク要件

図 16-2に示すように、IPv6 アドレスと IPv6 プレフィックス以外の設定パラメータを取得するためにステートレス DHCPv6 を使用するように Switch A を設定しています。Switch B はゲートウェイとして機能し、RA メッセージを定期的に配信します。

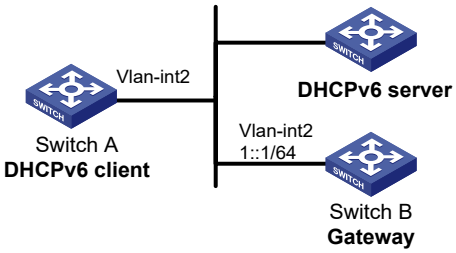


図 16-2 ネットワーク図

II. 設定手順

DHCPv6 クライアントを設定する前に、まず DHCPv6 サーバを設定する必要があります。

1)　ゲートウェイ Switch B を設定します。

VLAN-interface 2 のために IPv6 アドレスを設定します。

```
<SwitchB> system-view
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] ipv6 address 1::1 64
```

VLAN-interface 2 で送信する RA アドバタイズメントの O flag を 1 に設定します。RA アドバタイズメントを受信するホストは、DHCPv6 を介して IPv6 アドレス以外の情報を取得します。

```
[SwitchB-Vlan-interface2] ipv6 nd autoconfig other-flag
```

VLAN-interface 2 で RA メッセージの抑制を無効にします。

```
[SwitchB-Vlan-interface2] undo ipv6 nd ra halt
```

2)　DHCPv6 クライアント Switch A を設定します。

VLAN-interface 2 でステートレス IPv6 アドレス自動設定を有効にします。

```
<SwitchA> system-view
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ipv6 address auto
```

ステートレス IPv6 アドレス自動設定が有効になっているが、VLAN-interface 2 用に IPv6 アドレスが設定されていない場合、Switch A はリンクローカルアドレスを自動的に生成します。Switch B に RS メッセージを送信し、IPv6 アドレス生成のための設定情報を要求します。RS メッセージを受信すると、Switch B は RA メッセージを返信します。M flag を 0、O flag を 1 に設定した RA メッセージを受信した後、Switch A はステートレス DHCPv6 を実行して他の設定パラメータを取得します。

III. 設定の確認

DHCPv6 クライアント情報を表示します。

```
[SwitchA-Vlan-interface2] display ipv6 dhcp client interface vlan-interface 2
Vlan-interface2:
 Type: Stateless client
    State: OPEN
    Client DUID: 00030001000fe2ff0000
    Preferred server:
      Reachable via address: FE80::213:7FFF:FEF6:C818
      Server DUID: 0003000100137ff6c818
    DNS server addresses:
      1:2:4::5
      1:2:4::7
    Domain name:
      abc.com
```

DHCPv6 クライアント統計情報を表示します。

```
[SwitchA-Vlan-interface2] display ipv6 dhcp client statistics
Interface                    :  Vlan-interface2
Packets received             :  1
        Reply                :  1
        Advertise            :  0
        Reconfigure          :  0
        Invalid              :  0
Packets sent                 :  5
        Solicit              :  0
        Request              :  0
        Renew                :  0
        Rebind               :  0
        Information-request  :  5
        Release              :  0
        Decline              :  0
```

目次

このセクションのページは **3-x-x** です。

17 章 ARP snooping 17-1
17.1 設定手順..... 17-1
17.2 ARP snooping の表示と維持 17-1

17章 ARP snooping

ARP snooping はレイヤ 2 ネットワークで使用されます。ARP パケットの情報を使用することで、ARP snooping エントリを作成します。

VLAN で ARP snooping を有効にした場合、VLAN 内のインタフェースで受信された ARP パケットは CPU にリダイレクトされます。VLAN の場合、CPU は ARP snooping エントリを作成するため、ARP パケットの送信元 IP アドレスと送信元 MAC アドレス、受信する VLAN、ポートを使用します。

ARP snooping エントリのエージタイマは 25 分で有効期限は 15 分です。ARP snooping エントリが 15 分以内にアップデートされない場合、ARP snooping エントリは無効になり、使用できなくなります。その後、送信元 IP アドレスと送信元 MAC アドレスがエントリと一致する ARP パケットを受信すると、エントリが有効になり、エージタイマが再スタートします。エントリがエージアウトすると削除されます。

有効な ARP エントリとして、同じ送信元 IP アドレスで異なる送信元 MAC アドレスの ARP パケットを受信すると、装置は攻撃者からのアタックが発生していると認識します。ARP エントリは無効になり、25 分後に削除されます。

17.1 設定手順

以下に VLAN での ARP snooping の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． VLAN view に移行する	**vlan** *vlan-id*	ー
3． ARP snooping を有効にする	**arp snooping enable**	デフォルト：無効

17.2 ARP snoopingの表示と維持

すべての view で **display** コマンドが実行でき、user view で **reset** コマンドが実行できます。

操作	コマンド
ARP snoopingエントリを表示する	**display arp snooping vlan** [*vlan-id*] [**slot** *slot-number*] [**count**] **display arp snooping vlan ip** *ip-address* [**slot** *slot-number*]
ARP snoopingエントリを削除する	**reset arp snooping vlan** [*vlan-id*] **reset arp snooping vlan ip** *ip-address*

QX-S1100G シリーズ Ethernet スイッチ

オペレーションマニュアル

4. ルーティングプロトコル

本マニュアルは以下に示す章で構成されています。

01-IP ルーティングの基本
02-デフォルトルート
03-IPv6 デフォルトルート

目次

このセクションのページは**4-x-x** です。

1 章 IP ルーティングの基本 1-1
1.1 ルーティングテーブル 1-1
1.2 ルートの優先度 1-2
1.3 ロードバランス 1-2
1.4 ルートバックアップ 1-2
1.5 ルート再帰 1-3
1.6 ルート再分配 1-3
1.7 ルーティングテーブルの表示と維持 1-3

1章 IP ルーティングの基本

IP ルーティングはルーティングテーブルをもとにルータ上で IP パケットの転送を行います。この章はユニキャストルーティングプロトコルについて説明します。

1.1 ルーティングテーブル

RIB (routing information base)はルート再帰、ルート再分配、ルート拡張情報を含んだグローバルルーティングテーブルと関連する情報が含まれます。ルータはルーティングテーブルから最適なルートを選択し、FIB (forwarding information base)テーブルに格納します。ルータはパケットを転送するために FIB テーブルを使用します。FIB テーブルの詳細は、オペレーションマニュアルのセクション 3 *IP サービス”IP フォワーディングの基本*”を参照してください。

表 1-1にルートのカテゴリを示します。

表 1-1 ルートのカテゴリ

基準	カテゴリ
宛先	• **ネットワークルート**—宛先がネットワークです。サブネットマスクは32ビット未満です。 • **ホストルート**—宛先がホストです。サブネットマスクは32ビットです。
宛先が直接接続されているかどうか	• **ダイレクトルート**—宛先が直接接続されています。 • **インダイレクトルート**—宛先が直接接続されていません。
作成元	• **ダイレクトルート**—ダイレクトルートがインタフェースのデータリンクプロトコルによって検出されました。インタフェースルートと呼ばれます。 • **スタティックルート**—管理者によって手動で設定されたルートです。 • **ダイナミックルート**—ルーティングプロトコルによって自動に検出されたルートです。

ルーティングテーブルの概要を表示する場合、**display ip routing-table** コマンドを使用します。

```
<Switch> display ip routing-table
Destinations : 9        Routes : 9

Destination/Mask   Proto   Pre Cost        NextHop         Interface
0.0.0.0/32         Direct  0   0           127.0.0.1       InLoop0
3.3.3.3/32         Direct  0   0           127.0.0.1       InLoop0
127.0.0.0/8        Direct  0   0           127.0.0.1       InLoop0
127.0.0.0/32       Direct  0   0           127.0.0.1       InLoop0
127.0.0.1/32       Direct  0   0           127.0.0.1       InLoop0
127.255.255.255/32 Direct  0   0           127.0.0.1       InLoop0
```

ルーティングエントリは以下の項目が含まれます。

- **Destination**(宛先アドレス)—宛先ホストあるいはネットワークの IP アドレスです。
- **Mask**(ネットワークマスク)—IP アドレスのマスク長です。
- **Proto**(プロトコル)—ルートを追加したプロトコルです。
- **Pre**(プリファレンス)—ルートの優先度です。同一宛先へのルートがある場合、最も高い優先度を持つルートが最適なルートとなります。
- **Cost**(コスト)— 宛先へのルートが複数あり、同一優先度である場合、最も小さいコストの値を持つルートが最適なルートとなります。
- **NextHop**(ネクストホップ)— ネクストホップの IP アドレスを示します。
- **Interface**(インタフェース)—IP パケットの転送に使用する出力先のインタフェースを示します。

1.2 ルートの優先度

スタティックルーティング、ダイナミックルーティングを含むルーティングプロトコルは、デフォルトで優先度を持ちます。同一宛先に複数のルートがある場合、ルータは最適なルートとして最も高い優先度を持つルートを選択します。ダイレクトルートのプリファレンスは 0 で、変更できません。各スタティックルートとダイナミックルーティングプロトコルのプリファレンスを設定することができます。表 1-2にルートタイプとデフォルトのプリファレンスを示します。値が小さいほど優先度が高くなります。

表 1-2 ルートタイプとデフォルトルートプリファレンス

ルートタイプ	プリファレンス
Direct route	0
Unicast static route	60
Unknown(信用されていない送信元からのルート)	256

1.3 ロードバランス

ルーティングプロトコルは、同一宛先への複数の最適な同一コストのルートを持ちます。これらのルートの優先順位は同じであり、同一コストで複数パス(ECMP)のロードバランス（負荷分散）を行い転送できます。

スタティックルーティング、IPv6 スタティックルーティングがロードバランスをサポートしています。

1.4 ルートバックアップ

ルートバックアップはネットワークの信頼性を向上させます。ルートバックアップを用いて、最も優先度が高いルートをプライマリルートに設定し、残りをセカンダリルートにすることで、同一宛先に複数のルートを設定することができます。

通常時、パケットはプライマリルートで転送されます。障害などが発生した場合、セカンダリルートの中で最も優先度が高いルートでパケットが転送されます。障害が復旧した場合、ルートの選択が行われ、プライマリルートでパケットが転送されます。

1.5 ルート再帰

ネクストホップに直接接続されていないスタティックルートを使用する場合、ルータはネクストホップに届く出力インタフェースを検索するため、ルート再帰を行う必要があります。リンクステートプロトコルはルート再帰の必要がありません。リンクステートプロトコルはルートの計算を通して直接接続されたネクストホップを取得します。

RIB は、関連したルート、ルート再帰のパス、およびルート再帰の depth についての概要情報を含めて、ルート再帰情報を記録し、保存します。

1.6 ルート再分配

ルート再分配はお互いにルート情報を学習するルーティングプロトコルで有効となります。ダイナミックルーティングプロトコルは、ダイレクト、スタティックルーティングを含む他のルーティングプロトコルからのルートを再分配することができます。詳細は*オペレーションマニュアル*の関連する章を参照してください。

RIB はルーティングプロトコルの再分配の情報を記録します。

1.7 ルーティングテーブルの表示と維持

すべての view で **display** コマンドを実行でき、user view で **reset** コマンドを実行できます。

操作	コマンド
ルーティングテーブルの情報を表示する	**display ip routing-table** [**verbose**]
標準IPv4 ACLで許可されているルーティング情報を表示する	**display ip routing-table acl** *ipv4-acl-number* [**verbose**]
指定した宛先アドレスへのルート情報を表示する	**display ip routing-table** *ip-address* [*mask-length* | *mask*] [**longer-match**] [**verbose**]
指定した範囲内の宛先アドレスを持つルート情報を表示する	**display ip routing-table** *ip-address1* **to** *ip-address2* [**verbose**]
IPプレフィックスリストで許可されているルーティング情報を表示する	**display ip routing-table prefix-list** *prefix-list-name* [**verbose**]
ルートのルーティングプロトコルを表示する	**display ip routing-table protocol** *protocol* [**inactive** | **verbose**]
IPv4ルーティングテーブルの統計情報を表示する	**display ip routing-table statistics**

操作	コマンド
IPv4ルーティングテーブルの統計情報を削除する	**reset ip routing-table statistics protocol** { *protocol* | **all** }
IPv6ルーティングテーブルの統計情報を表示する	**display ipv6 routing-table** [**verbose**]
IPv6宛先アドレスへのルート情報を表示する	**display ipv6 routing-table** *ipv6-address* [*prefix-length*] [**longer-match**] [**verbose**]
標準IPv6 ACLで許可されているルーティング情報を表示する	**display ipv6 routing-table acl** *ipv6-acl-number* [**verbose**]
指定した範囲内のIPv6宛先アドレスを持つルート情報を表示する	**display ipv6 routing-table** *ipv6-address1* **to** *ipv6-address2* [**verbose**]
IPv6プレフィックスリストで許可されているルーティング情報を表示する	**display ipv6 routing-table prefix-list** *prefix-list-name* [**verbose**]
ルートのIPv6ルーティングプロトコルを表示する	**display ipv6 routing-table protocol** *protocol* [**inactive** | **verbose**]
IPv6ルーティングテーブルの統計情報を表示する	**display ipv6 routing-table statistics**
IPv6ルーティングテーブルの統計情報を削除する	**reset ipv6 routing-table statistics protocol** { *protocol* | **all** }

目次

このセクションのページは**4-x-x** です。

2 章 デフォルトルート 2-1

2章 デフォルトルート

デフォルトルートはルーティングテーブルの指定したルーティングエントリにマッチしないパケットを転送するのに使用されます。デフォルトルートが設定されていない場合、ルーティングエントリにマッチしないパケットは廃棄されます。

デフォルトルートは以下の方法で設定することができます。

- ネットワーク管理者が宛先アドレスとマスクを 0.0.0.0 に設定します。詳細はオペレーションマニュアルのセクション 4 *ルーティングプロトコル* を参照してください。

目次

このセクションのページは**4-x-x** です。

3 章 IPv6 デフォルトルート 3-1

3章 IPv6 デフォルトルート

IPv6 デフォルトルートは IPv6 ルーティングテーブルの指定した IPv6 ルーティングエントリにマッチしないパケットを転送するのに使用されます。

IPv6 デフォルトルートは以下のいずれかの方法で設定することができます。

- ネットワーク管理者が宛先アドレスとマスクを::/0 に設定します。詳細はオペレーションマニュアルのセクション 4 *ルーティングプロトコル* を参照してください。

QX-S1100G シリーズ Ethernet スイッチ

オペレーションマニュアル

5. マルチキャスト

本マニュアルは以下に示す章で構成されています。

01-マルチキャストの概要
02-IGMP スヌーピング
03-MLD スヌーピング

目次

このセクションのページは**5-x-x** です。

1 章 マルチキャストの概要 1-1
1.1 マルチキャストの導入 1-1
1.1.1 情報通信技術 1-1
1.1.2 マルチキャストの機能 1-4
1.1.3 マルチキャストの一般的な表記方法 1-4
1.1.4 マルチキャストの利点とアプリケーション 1-5
1.2 マルチキャストモデル 1-5
1.3 マルチキャストアーキテクチャ 1-6
1.3.1 マルチキャストアドレス 1-6
1.3.2 マルチキャストプロトコル 1-10
1.4 マルチキャストパケットの転送メカニズム 1-13

1章 マルチキャストの概要

1.1 マルチキャストの導入

ユニキャストおよびブロードキャストと共存する技術として、マルチキャスト技術はポイントツーマルチポイントデータ送信の問題を効果的に対処します。ネットワーク上で効率の高いポイントツーマルチポイントデータ送信を行うことで、マルチキャストはネットワーク帯域幅を大きく節約し、ネットワーク負荷を低減します。

マルチキャスト技術により、ネットワークオペレータは新しい付加価値のあるサービスを容易に提供することが可能となります。たとえば、Web キャスティング、Web TV、遠隔学習、遠隔医療、Web ラジオ、リアルタイムビデオカンファレンスなどの他に、帯域幅や時間が重要な情報サービスです。

1.1.1 情報通信技術

情報通信技術はユニキャスト、ブロードキャスト、マルチキャストを含みます。

I. ユニキャスト

ユニキャストでは、情報を必要とする各ホスト（Receiver）へ情報送信元（Source）から情報のコピーが個別に送信されます。

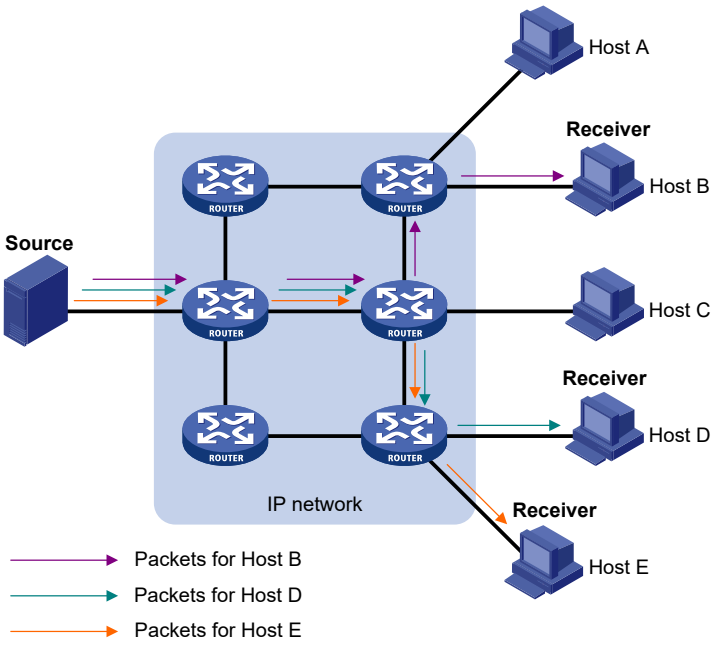


図 1-1 ユニキャスト通信

図 1-1において、Host B と Host D と Host E は情報を必要とします。個別の通信チャネルは情報送信元から各ホストに対して確立する必要があります。

ユニキャスト通信では、ネットワーク上のトラフィックは情報を必要とするホストの数に比例します。非常に多くのユーザが情報を必要とする場合、情報送信元は各ユーザに同じ情報のコピーを送信する必要があります。これは情報送信元とネットワーク帯域幅に相当な負荷をかけることになります。

ユニキャスト通信は情報のバッチ送信には適していません。

II. ブロードキャスト

ブロードキャストでは、情報を必要としていないホストがあったとしても、情報送信元からネットワーク上のすべてのホストに情報が送信されます。

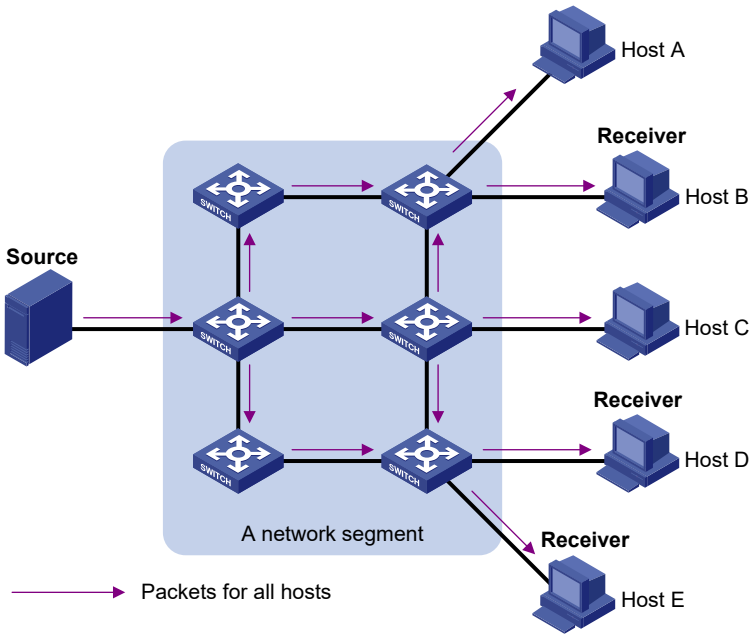


図 1-2 ブロードキャスト通信

図 1-2に示すように、Host B と Host D と Host E は情報を必要とします。情報が同一ネットワーク上にブロードキャストされた場合、Host A と Host C も情報を受信してしまいます。これにより、情報セキュリティの問題に加えて、同一ネットワーク上でトラフィックフラッディングも発生してしまいます。

特定のホストにデータを送信する場合、ブロードキャストは効率的ではありません。ブロードキャストの送信は多くのネットワークリソースを浪費します。

III. マルチキャスト

マルチキャストはネットワークリソースの消費を最小限に抑えてポイントツーマルチポイント送信を実現することができます。ネットワーク上のいくつかのホストがマルチキャスト情報を必要とした場合、情報の送信者あるいはマルチキャスト送信元は情報のコピーを 1 つだけ送信します。マルチキャストルーティングプロトコルによってマルチキャスト配信ツリーが構成され、ツリーが分岐するノードでのみパケットがコピーされます。

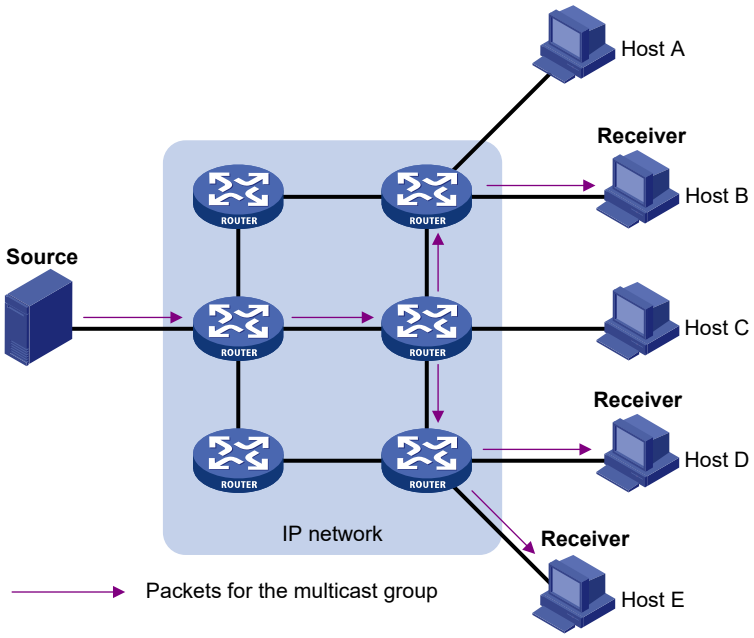


図 1-3 マルチキャスト通信

マルチキャスト送信元（Source）は情報のコピーを 1 つだけマルチキャストグループへ送信します。情報の受信者である Host B、Host D、Host E は、マルチキャストグループに参加する必要があります。ネットワーク上のルータはグループメンバの配置にもとづいて情報を複製して転送します。最終的に、情報は Host B と Host D と Host E に正確に送信されます。

要約すると、マルチキャストの利点を以下に示します。

- **ユニキャストからの利点** － ユニキャストに対しては、マルチキャストトラフィックは送信元から可能な限り遠いノードに流れてから複製、配信されるため、ホストの数が増加した場合でも送信元とネットワークの負荷を増やすことはありません。
- **ブロードキャストからの利点** － ブロードキャストに対しては、必要としている受信者だけにマルチキャストデータが送信されるので、マルチキャストは合理的にネットワーク帯域幅を使用し、ネットワークセキュリティを強化します。さらに、ブロードキャストの配信は同一ネットワークに限定されますが、マルチキャストの配信は同一ネットワークに限定されません。

1.1.2 マルチキャストの機能

- マルチキャストグループは IP マルチキャストアドレスによって識別されて配置されるマルチキャストレシーバです。ホストはマルチキャストグループ宛に送信されたマルチキャストデータを受信できるようになる前に、マルチキャストグループのメンバになるためにマルチキャストグループに参加します。通常、マルチキャストソースはマルチキャストグループに参加する必要はありません。
- マルチキャストソースは情報の送信者です。マルチキャストソースは同時に複数のマルチキャストグループにデータを送信することができます、そして、複数のマルチキャストソースは同時に同一のマルチキャストグループにデータを送信することができます。
- グループメンバは動的です。ホストは、いつでもマルチキャストグループに参加あるいは離脱することができます。マルチキャストグループは、地理的な制約を受けません。
- レイヤ 3 マルチキャストをサポートするルータまたはレイヤ 3 スイッチは、マルチキャストルータまたはレイヤ 3 マルチキャスト装置と呼ばれます。マルチキャストルーティング機能の提供に加えて、マルチキャストルータはグループメンバに所属しているスタブサブネットのマルチキャストグループメンバを管理することもできます。マルチキャストルータ自身は、マルチキャストグループメンバになることができます。

マルチキャストの概念をより良く理解するために、マルチキャスト配信を TV 番組の配信に例えることができます。

表 1-1 TV 番組の配信とマルチキャスト通信の比較

TV 番組の配信	マルチキャスト配信
TV 局がチャンネルを介して TV 番組を放送します。	マルチキャストソースがマルチキャストグループにマルチキャストデータを送信します。
ユーザが TV をチャンネルに合わせます。	レシーバがマルチキャストグループに参加します。
チャンネルを介してTV 局から放送される TV 番組の視聴をユーザが開始します。	ソースからマルチキャストグループに送信されたマルチキャストデータをレシーバが受信し始めます。
ユーザが TV の電源を切るか、他のチャンネルに合わせます。	レシーバがマルチキャストグループから離脱するか、他のグループに参加します。

1.1.3 マルチキャストの一般的な表記方法

マルチキャストでは一般的に 2 つの表記法が使用されます。

- **(*, G)** － RPT（rendezvous point tree）または、あらゆるマルチキャストソースがマルチキャストグループ G へ送信したマルチキャストパケットを表します。（*）はあらゆるマルチキャストソース、(G) は特定のマルチキャストグループを表します。
- **(S, G)** － SPT（shortest path tree）または、マルチキャストソース S がマルチキャストグループ G へ送信したマルチキャストパケットを表します。（S）は特定のマルチキャストソース、（G）は特定のマルチキャストグループを表します。

1.1.4 マルチキャストの利点とアプリケーション

I. マルチキャストの利点

- **効率の向上** － 情報送信元サーバとネットワーク装置の CPU 負荷を低減します。
- **最適なパフォーマンス** － 冗長なトラフィックを低減します。
- **配信アプリケーション** － 最小限のネットワークリソースで、ポイントツーマルチポイントアプリケーションを可能にします。

II. マルチキャストアプリケーション

- マルチメディアとストリーミングアプリケーションがあります。たとえば Web TV、Web ラジオ、リアルタイムビデオ/オーディオ会議などがあります。
- 通信教育や遠隔医療などの研修および協力運用の通信があります。
- データウェアハウスと財務アプリケーション（株価情報）があります。
- その他のポイントツーマルチポイントデータ配信アプリケーションがあります。

1.2 マルチキャストモデル

レシーバ（受信者）がマルチキャストソース（送信元）をどのように扱うかによって、ASM（any-source multicast）、SFM（source-filtered multicast）、SSM（source-specific multicast）の 3 つのマルチキャストモデルがあります。

I. ASM モデル

ASM モデルでは、すべてのマルチキャストソースはマルチキャストグループへ情報を送信できます。レシーバ（受信者）がグループアドレスによって識別されたマルチキャストグループに参加し、そのマルチキャストグループ宛てのマルチキャスト情報を取得することができます。このモデルでは、レシーバ（受信者）はあらかじめマルチキャストソースの位置を認識していません。

II. SFM モデル

SFM モデルは ASM モデルから派生しています。センダ（送信者）の観点からは、2 つのモデルは同じマルチキャストメンバシップのアーキテクチャです。

SFM モデルは ASM モデルの機能拡張版です。SFM モデルでは、上位レイヤソフトウェアが受信したマルチキャストの送信元アドレスをチェックし、指定した送信元からのマルチキャストトラフィックを許可または拒否します。これにより、レシーバ（受信者）は一部のマルチキャストソースからのだけマルチキャストデータを受信することができます。レシーバ（受信者）の観点からは、マルチキャストソース（送信元）がすべて有効というわけではありません。マルチキャストソースはフィルタされます。

III. SSM モデル

SSM モデルは、マルチキャストレシーバが、必要となるマルチキャストソースを指定することができる転送サービスを提供します。

SSM モデルと ASM モデルの根本的な違いは、SSM モデルではレシーバ（受信者）が何らかの方法でマルチキャストソースの位置を既に知っていることです。これは SSM モデルと ASM モデルの主な相違点です。さらに、SSM モデルでは ASM /SFM モデルの場合とは異なるマルチキャストアドレス範囲を使用します。レシーバと指定のマルチキャストソースの間に専用のマルチキャスト転送パスが確立されます。

1.3 マルチキャストアーキテクチャ

IP マルチキャストは以下の問題を解決します。

- マルチキャストソースはどこに情報を送信するべきか？（マルチキャストアドレッシング）
- ネットワーク上にはどんなレシーバ（受信者）が存在するか？（ホストレジストレーション）
- レシーバが受信する必要があるマルチキャストデータのマルチキャストソース（送信元）がどこにいるのか？（マルチキャストソースディスカバリ）
- 情報がどのようにしてレシーバ（受信者）に転送されるのか？（マルチキャストルーティング）

IP マルチキャストはエンドツーエンドサービスの 1 つです。マルチキャストアーキテクチャには以下の 4 つのパートがあります。

- **アドレッシングメカニズム** － マルチキャストソースはマルチキャストアドレスを介してレシーバのグループへ情報を送信します。
- **ホストレジストレーション** － レシーバホストはマルチキャストグループへの参加と離脱を動的に行うことができます。このメカニズムはグループメンバシップ管理の基礎になります。
- **マルチキャストルーティング** － マルチキャストソースからレシーバへマルチキャストデータを配信するために、マルチキャスト配信ツリー（ネットワーク上でのマルチキャストデータの転送パスツリー）が構築されます。
- **マルチキャストアプリケーション** － ビデオ会議などのマルチキャストアプリケーションをサポートするソフトウェアシステムを、マルチキャストソース（送信元）とレシーバホスト（受信者）にインストールする必要があります。そして、TCP/IP スタックはマルチキャストデータの送受信をサポートする必要があります。

1.3.1 マルチキャストアドレス

I. IP マルチキャストアドレス

- IPv4 マルチキャストアドレス

IANA（Internet Assigned Numbers Authority）は IPv4 マルチキャストにクラス D アドレス（224.0.0.0～239.255.255.255）を割り当てました。

表 1-2 クラス D アドレスブロックと説明

アドレスブロック	説明
224.0.0.0 ～ 224.0.0.255	予約されている永久的なグループアドレスです。IPアドレス 224.0.0.0 は予約されており、その他のIPアドレスはルーティングプロトコルによって、そしてトポロジ検索、プロトコルの維持管理などのために使用されることができます。一般的な永久グループアドレスの一覧は表 1-3に示されています。このブロックアドレス宛のパケットは、IPヘッダのTTL （Time to Live） 値に関わらず、ローカルサブネットを越えて転送されることはありません。
224.0.1.0 ～ 238.255.255.255	グローバルスコープグループアドレスです。このブロックには2種類の指定グループアドレスがあります。 ● **232.0.0.0/8** ― SSMグループアドレス ● **233.0.0.0/8** ― Glopグループアドレス
239.0.0.0 ～ 239.255.255.255	管理上、範囲指定されたマルチキャストアドレスです。これらのアドレスはグローバルにではなくローカルに一意とみなされ、異なる組織が管理しているドメインで衝突を起こすことなく再利用できます。詳細はRFC2365を参照してください。

🕮 **メモ：**

“Glop”は、異なる自律システム （AS） 間でマルチキャストアドレスを割り当てるメカニズムです。233.0.0.0 の中間の 2 バイトに AS の数字を入力することで、その AS に 255 のマルチキャストアドレスが得られます。詳細については、RFC2770 を参照してください。

表 1-3 一般的な予約済みマルチキャストグループアドレス

アドレス	説明
224.0.0.1	ホストとルータを含む、サブネット上のすべてのシステム
224.0.0.2	サブネット上のすべてのマルチキャストルータ
224.0.0.3	未割り当て
224.0.0.4	DVMRP（Distance Vector Multicast Routing Protocol）ルータ
224.0.0.5	OSPF（Open Shortest Path First）ルータ。
224.0.0.6	OSPFのDRまたはバックアップDR
224.0.0.7	STルータ
224.0.0.8	STホスト
224.0.0.9	RIPv2（Routing Information Protocol version 2）ルータ
224.0.0.11	モバイルエージェント
224.0.0.12	DHCP（Dynamic Host Configuration Protocol）サーバまたはリレーエージェント
224.0.0.13	すべてのPIM（Protocol Independent Multicast）ルータ
224.0.0.14	RSVP（Resource Reservation Protocol）のカプセル化
224.0.0.15	すべてのCBT（Core-Based Tree）ルータ
224.0.0.16	指定されたSBM（Subnetwork Bandwidth Management）
224.0.0.17	すべてのSBM
224.0.0.18	VRRP（Virtual Router Redundancy Protocol）

- IPv6 マルチキャストアドレス

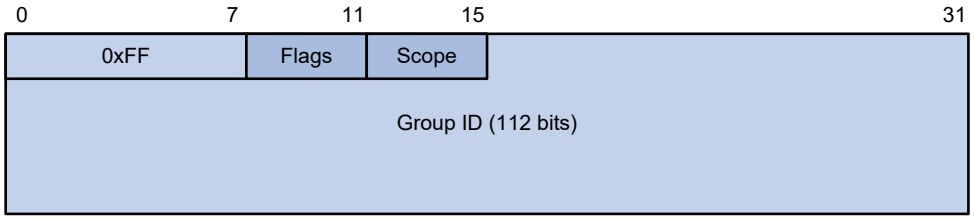


図 1-4 IPv6 マルチキャストフォーマット

以下に IPv6 マルチキャストアドレスのフィールドの説明を示します。

- **0xFF** － 8 ビットで 11111111 です。このアドレスが IPv6 マルチキャストアドレスであることを示します。
- **Flags** － 4 ビットのフラグフィールドです。



図 1-5 Flags フィールドフォーマット

表 1-4 フラグフィールドの説明

ビット	説明
0	予約済みです。常に0です。
R	• 0の場合、RPアドレスが埋め込まれていないIPv6マルチキャストアドレスであることを示します。 • 1の場合、RPアドレスが埋め込まれているIPv6マルチキャストアドレスであることを示します。（PビットとTビットも1にセットされます）
P	• 0の場合、ユニキャストプレフィックスにもとづかないIPv6マルチキャストアドレスであることを示します。 • 1の場合、ユニキャストプレフィックスにもとづくIPv6マルチキャストアドレスであることを示します。（Tビットも1にセットされます）
T	• 0の場合、IANAによって永続的に割り当てられた既知のIPv6マルチキャストアドレスであることを示します。 • 1の場合、一時的あるいはダイナミックに使用される（非永続的な）マルチキャストアドレスであることを示します。

- **Scope** － 4 ビットの IPv6 マルチキャストアドレスの有効範囲を示すフィールドです。

表 1-5 Scope フィールドの値

値	意味
0、F	予約済み
1	インタフェースノードローカル
2	リンクローカル
3	サブネットローカル
4	アドミンローカル
5	サイトローカル

値	意味
6、7、9 ～ D	未割り当て
8	組織ローカル
E	グローバル

- **Group ID** – 112 ビットで IPv6 マルチキャストグループを識別します。Scope フィールドが定義する範囲で IPv6 マルチキャストグループを一意に識別します。

II. イーサネットマルチキャスト MAC アドレス

- IPv4 マルチキャスト MAC アドレス

IANA によって定義されているように、IPv4 マルチキャスト MAC アドレスの上位 24 ビットは 0x01005E、25 ビット目は 0x0、および下位 23 ビットはマルチキャスト IPv4 アドレスの低位 23 ビットです。

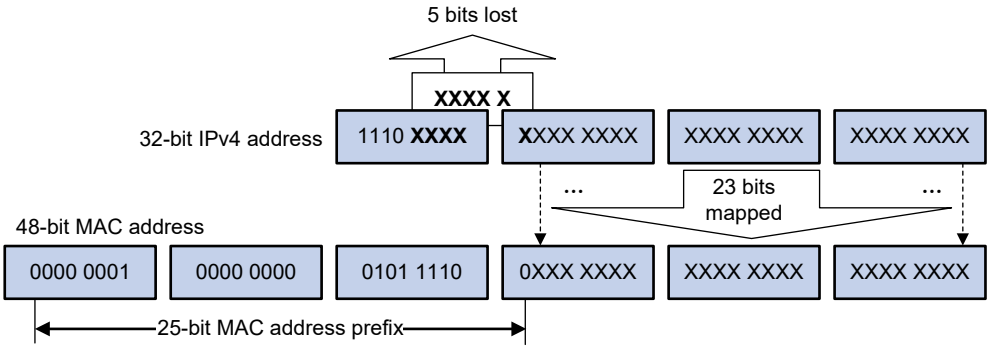


図 1-6 IPv4 アドレスと MAC アドレスのマッピング

IPv4 マルチキャストアドレスの上位 4 ビットは 1110 で固定です。IPv4 アドレスと MAC アドレスのマッピングで使用され、IPv4 マルチキャストアドレスの 5 ビットは失われます。その結果、32 個のマルチキャスト IPv4 アドレスは同じ MAC アドレスにマッピングされます。そのため、レイヤ 2 マルチキャスト転送においては、他の IPv4 マルチキャストグループに宛てたマルチキャストデータを受け取る場合があります。そのような冗長データは上位層によってフィルタする必要があります。

- IPv6 マルチキャスト MAC アドレス

IPv6 マルチキャスト MAC アドレスの上位 16 ビットは 0x3333 です。下位 32 ビットはマルチキャスト IPv6 アドレスの下位 32 ビットにマッピングされます。これは IPv4 アドレスから MAC アドレスのマッピングと同じように、IPv6 から MAC アドレスのマッピングが重複する問題があります。

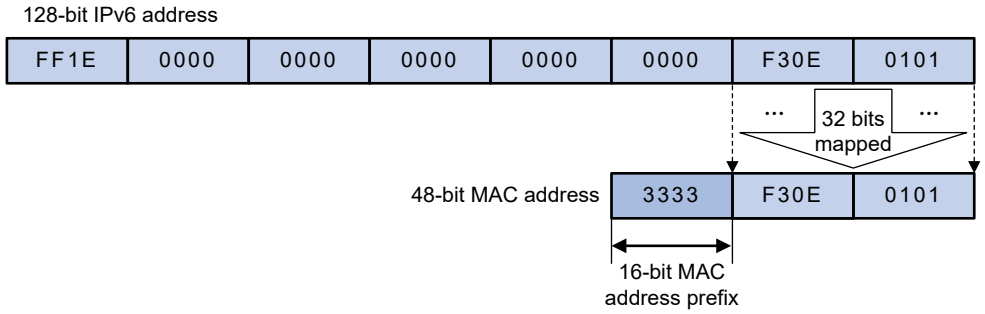


図 1-7 IPv6 アドレスと MAC アドレスのマッピング例

1.3.2 マルチキャストプロトコル

マルチキャストプロトコルは以下のカテゴリに分けられます。

- レイヤ 3、レイヤ 2 マルチキャストプロトコル
  - ネットワークレイヤで動作する IP マルチキャストのレイヤ 3 マルチキャスト

    レイヤ 3 マルチキャストプロトコル － IGMP、MLD、PIM、IPv6 PIM、MSDP、MBGP、IPv6 MBGP
  - データリンクレイヤで動作する IP マルチキャストのレイヤ 2 マルチキャスト

    レイヤ 2 マルチキャストプロトコル － IGMP snooping、MLD snooping、PIM snooping、IPv6 PIM snooping、マルチキャスト VLAN、IPv6 マルチキャスト VLAN
- IPv4、IPv6 マルチキャストプロトコル
  - **IPv4 ネットワーク** － IGMP snooping、PIM snooping、マルチキャスト VLAN、IGMP、PIM、MSDP、MBGP
  - **IPv6 ネットワーク** － MLD snooping、IPv6 PIM snooping、IPv6 マルチキャスト VLAN、MLD、IPv6 PIM、IPv6 MBGP

この章ではレイヤ 2、レイヤ 3 マルチキャストプロトコルの一般的なアプリケーションと機能について記載します。QX-S1100G シリーズでサポートしている IGMP snooping と MLD snooping に関する詳細は、関連する章を参照してください。

I. レイヤ 3 マルチキャストプロトコル

レイヤ 3 マルチキャストプロトコルには、マルチキャストグループ管理プロトコルやマルチキャストルーティングプロトコルがあります。

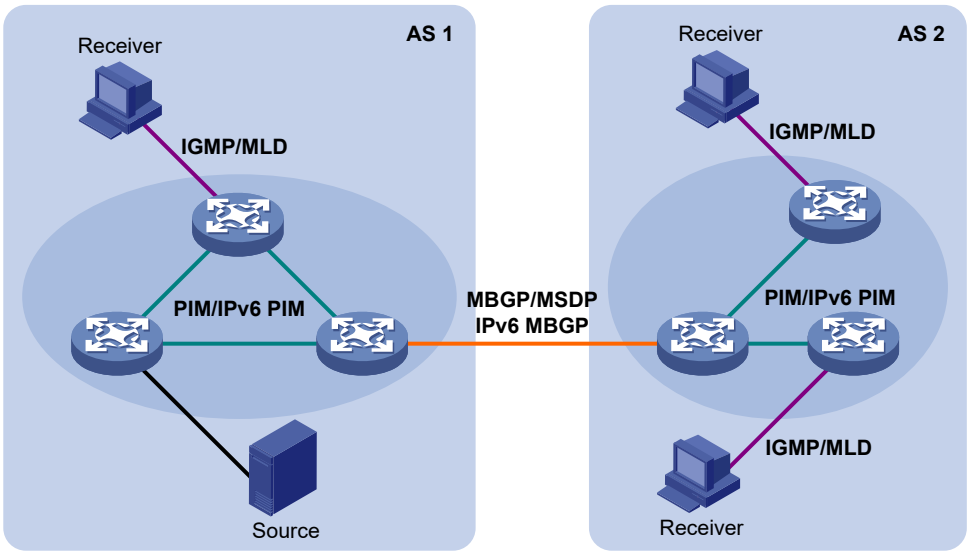


図 1-8 レイヤ 3 マルチキャストプロトコルの位置

- マルチキャストグループ管理プロトコル

通常は、IGMP（internet group management protocol）、MLD（multicast listener discovery protocol）はマルチキャストグループ管理プロトコルです。通常、これらのプロトコルは、ホストとレイヤ 3 マルチキャスト装置の間でグループメンバシップを確立して維持するメカニズムを定義します。

- マルチキャストルーティングプロトコル

マルチキャストルーティングプロトコルはレイヤ 3 マルチキャスト装置上で動作し、マルチキャストルートを確立して維持します。そして、マルチキャストパケットを正確に効率よく転送します。マルチキャストルートは、データソースから複数のレシーバまでループのないデータ転送パス（マルチキャスト配信ツリーとして知られます。）を構成します。

ASM モデルでは、マルチキャストルートはドメイン内ルートとドメイン間ルートがあります。

- □ マルチキャストデータをレシーバに配信するために、ドメイン内マルチキャストルーティングプロトコルを使用してマルチキャストソースの発見、AS 内マルチキャスト配信ツリーの構築を行います。 さまざまな成熟したドメイン内マルチキャストルーティングプロトコルの中でも、PIM（protocol independent multicast）はよく使用されています。PIM にはスパースモード （PIM-SM） があります。
- □ ドメイン間マルチキャストルーティングプロトコルは 2 つの AS 間でマルチキャストの情報を発見するのに使われます。このプロトコルには、MSDP（Multicast Source Discovery Protocol）、MBGP が含まれます。MSDP は異なる AS 間でマルチキャスト送信元情報を送信します。MBGP は異なる AS 間でマルチキャストルーティング情報を交換するため、MP-BGP を拡張したものです。

SSM モデルでは、マルチキャストルートはドメイン間ルートおよびドメイン内ルートに分割されません。レシーバはマルチキャストソースの位置を知っているため、マルチキャスト情報の転送には PIM-SM によって確立されたチャネルで十分です。

II. レイヤ 2 マルチキャストプロトコル

レイヤ 2 マルチキャストプロトコルには、IGMP Snooping、MLD Snooping、PIM Snooping、IPv6 PIM Snooping、マルチキャスト VLAN、IPv6 マルチキャスト VLAN があります。

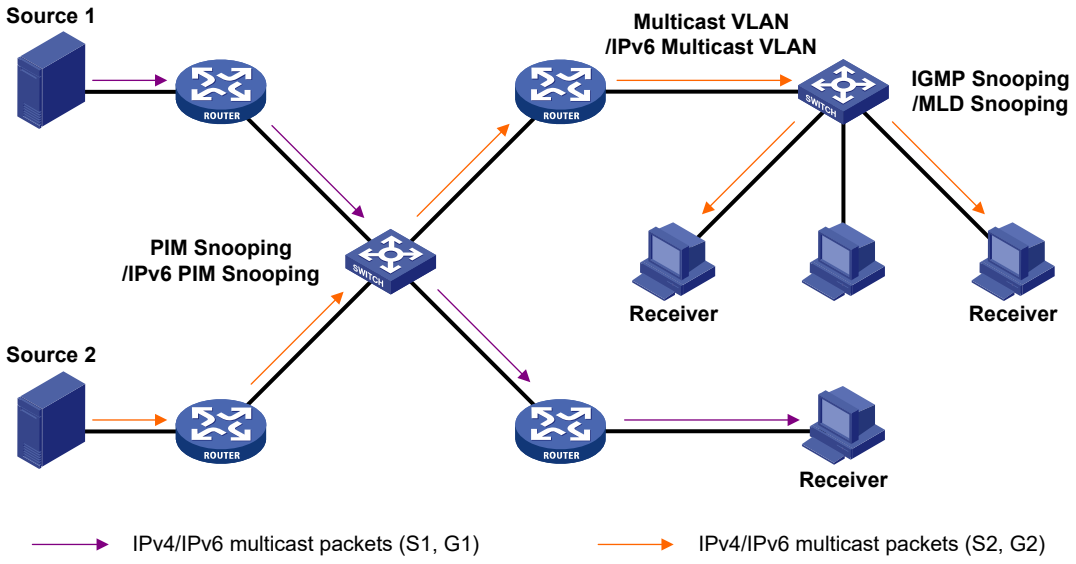


図 1-9 レイヤ 2 マルチキャストプロトコルの位置

- IGMP snooping、MLD snooping

マルチキャストの転送効率を改良するため PIM Snooping および IPv6 PIM Snooping はレイヤ 2 装置で動作するマルチキャスト構成メカニズムです。ホストとレイヤ 3 マルチキャスト装置の間で交換される IGMP または MLD メッセージをモニタ、解析することによって、マルチキャストグループを管理、制御します。このメカニズムはレイヤ 2 ネットワークでマルチキャストデータのフラッディングを制御するのに効率的です。

- PIM snooping、IPv6 PIM snooping

PIM Snooping および IPv6 PIM Snooping はレイヤ 2 装置で動作します。受信した PIM メッセージを解析するため、PIM snooping や IPv6 PIM snooping を動作させます。PIM snooping ルーティングエントリや IPv6 PIM snooping ルーティングエントリに、指定したマルチキャストデータに関連するポートのみを追加します。これによって、マルチキャストデータは、関連するポートに対してのみ転送します。

- マルチキャスト VLAN、IPv6 マルチキャスト VLAN

異なる VLAN に同一グループのマルチキャストレシーバが存在するところで、マルチキャストネットワークのレイヤ 2 装置でマルチキャスト VLAN、IPv6 マルチキャスト VLAN が動作します。これらのプロトコルでは、レイヤ 3 マルチキャスト装置はレイヤ 2 装置のマルチキャスト VLAN または IPv6 マルチキャスト VLAN へマルチキャストデータのコピーを 1 つだけ送信します。これにより、レイヤ 3 装置上のネットワーク帯域幅の浪費や余分な負荷を回避します。

1.4 マルチキャストパケットの転送メカニズム

マルチキャストモデルでは、マルチキャストグループのマルチキャストレシーバは通常、ネットワークの異なるエリアに存在します。これらのマルチキャストレシーバは同じマルチキャストグループアドレスによって識別されます。ネットワーク上の異なる位置に存在するレシーバにマルチキャストパケットを配信するため、宛先アドレスとして IP パケットのマルチキャストデータをマルチキャストグループアドレスにカプセル化します。通常は転送パス上のマルチキャストルータが 1 つの受信インタフェースで受信したマルチキャストパケットを複数の送信インタフェースに転送します。ユニキャストモデルと比較して、マルチキャストモデルは以下でユニキャストより複雑になっています。

- ネットワークにおいてマルチキャストパケットの転送を確実にするために、マルチキャストの転送に異なるルーティングテーブルが使用されます。ユニキャストルーティングテーブル、マルチキャストのルーティングテーブル（たとえば、MBGP ルーティングテーブル）、スタティックマルチキャストルーティングテーブルが含まれます。
- 異なるピアから発信され、同じ装置の異なるインタフェースで受信された同一マルチキャスト情報を処理するため、各マルチキャストパケットの RPF チェックを実行します。RPF チェックの結果によって、パケットの転送または破棄が決定されます。RPF チェックメカニズムは、マルチキャスト転送を実行するほとんどのマルチキャストルーティングプロトコルの基礎になっています。

目次

このセクションのページは**5-x-x** です。

2 章 IGMP スヌーピング 2-1
2.1 概要 2-1
2.1.1 IGMP snooping のポート 2-1
2.1.2 IGMP snooping の動作 2-3
2.1.3 IGMP snooping プロキシー機能 2-5
2.2 プロトコルと標準 2-6
2.3 VLAN ベースの IGMP snooping 設定作業リスト 2-6
2.4 IGMP snooping の基本機能の設定 2-7
2.4.1 IGMP snooping の有効化 2-7
2.4.2 IGMP snooping のバージョンの設定 2-8
2.4.3 IGMP snooping 転送エントリの最大数の設定 2-8
2.4.4 スタティックマルチキャスト MAC アドレスエントリの設定 2-9
2.4.5 IGMP last member クエリ間隔の設定 2-9
2.5 IGMP snooping ポート機能の設定 2-10
2.5.1 ダイナミックポートのエージングタイマの設定 2-10
2.5.2 スタティックポートの設定 2-11
2.5.3 シミュレーティッドメンバホストの設定 2-12
2.5.4 fast-leave 処理の有効化 2-12
2.6 IGMP snooping クエリの設定 2-13
2.6.1 設定要件 2-13
2.6.2 IGMP snooping クエリアの有効化 2-14
2.6.3 IGMP クエリと response のパラメータの設定 2-14
2.7 IGMP snooping プロキシー機能の有効化 2-15
2.8 IGMP メッセージのパラメータの設定 2-15
2.8.1 設定要件 2-16
2.8.2 IGMP メッセージの送信元 IP アドレスの設定 2-16
2.8.3 IGMP メッセージの 802.1p 優先度の設定 2-17
2.9 IGMP snooping ポリシーの設定 2-18
2.9.1 マルチキャストグループポリシーの設定 2-18
2.9.2 マルチキャストソースポートフィルタの設定 2-19
2.9.3 未知のマルチキャストデータ廃棄機能の有効化 2-20
2.9.4 IGMP report 抑制機能の有効化 2-20
2.9.5 ポートで参加可能なマルチキャストグループの最大数の設定 2-21
2.9.6 マルチキャストグループ置き換え機能の有効化 2-21
2.10 IGMP snooping の表示と維持 2-22
2.11 IGMP snooping 設定例 2-23
2.11.1 VLAN ベースのグループポリシーとシミュレーティッドメンバホストの設定例 2-23
2.11.2 VLAN ベースのスタティックポートの設定例 2-25
2.11.3 VLAN ベースの IGMP snooping クエリアの設定例 2-29
2.11.4 VLAN ベースの IGMP snooping プロキシー機能の設定例 2-32
2.12 IGMP snooping のトラブルシューティング 2-34
2.12.1 レイヤ 2 マルチキャスト転送ができない 2-34
2.12.2 マルチキャストグループポリシーが動作しない 2-34

2章 IGMP スヌーピング

2.1 概要

IGMP snooping はマルチキャスト転送時のネットワークへの負荷を軽減するためのメカニズムです。

図 2-1に示すように、IGMP snooping を有効にしない場合、マルチキャストパケットはすべてのポートにフラッディングされます。レイヤ 2 装置で IGMP snooping を有効にすると、既知のマルチキャストグループからのマルチキャストパケットは、Receiver へのみ転送されます。IGMP snooping を有効にすることで、不要なマルチキャストトラフィックのフラッディングを抑止し、ネットワークを効率的に利用することができます。

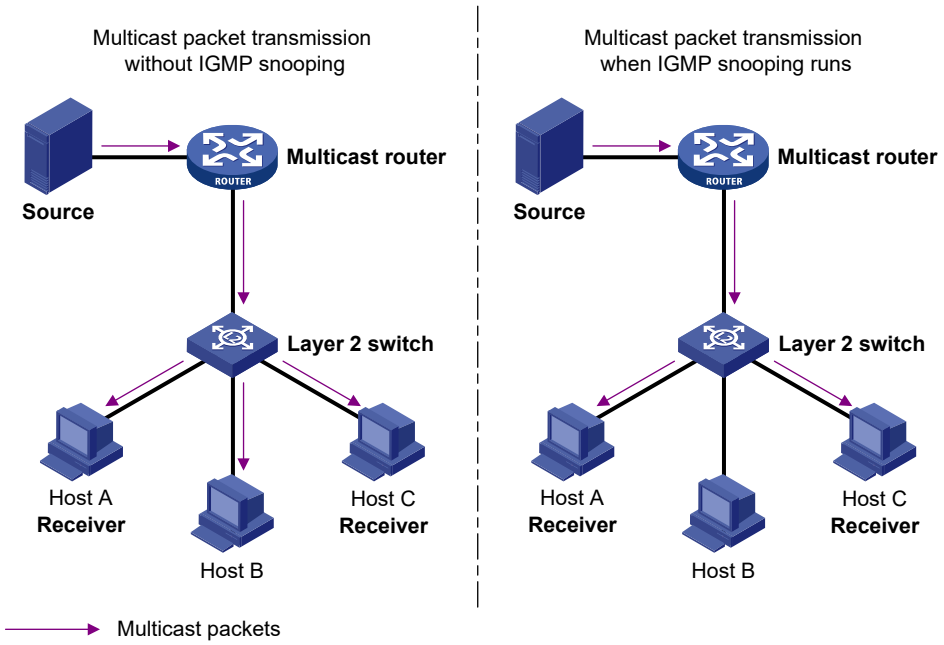


図 2-1 IGMP snooping を有効にする前と有効にした後のマルチキャストパケットの転送

2.1.1 IGMP snooping のポート

図 2-2に示すように、IGMP snooping は Switch A と Switch B で動作し、Host A と Host C はマルチキャストグループの Receiver です。IGMP snooping のポートはメンバポートとルータポートに分類されます。

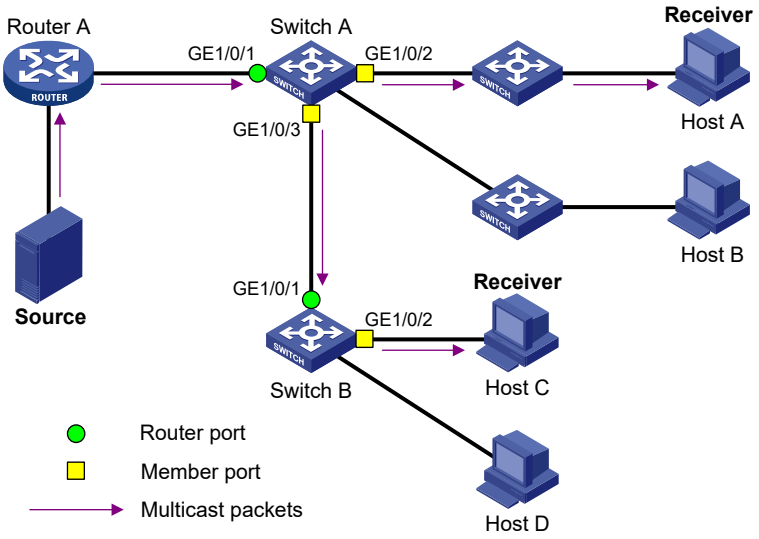


図 2-2 IGMP snooping 関連ポート

I. ルータポート

IGMP snooping のレイヤ 2 装置で、レイヤ 3 マルチキャストへのポートはルータポートと呼ばれます。図 2-2では、Switch A の GigabitEthernet 1/0/1 と Switch B の GigabitEthernet 1/0/1 がルータポートです。

ルータポートは以下のタイプがあります。

- **ダイナミックルータポート**－ポートで 0.0.0.0 以外の送信元アドレスの IGMP general クエリあるいは PIM Hello メッセージを受信した場合、ダイナミックルータポートリストにポートを追加します。同時にポートのタイマを開始します。タイマが満了する前にメッセージを受信しない場合、ポートはダイナミックルータポートリストからポートを削除します。
- **スタティックルータポート**－ポートがルータポートとしてスタティックに設定された場合、スタティックルータポートリストにポートを追加します。スタティックルータポートはエージアウトしません。手動でのみ削除することができます。

IGMP snooping のルータポートをレイヤ 3 インタフェースのルーテッドインタフェースと混同しないでください。IGMP snooping のルータポートはレイヤ 2 インタフェースです。

II. メンバポート

IGMP snooping のレイヤ 2 装置で、マルチキャスト Receiver へのポートはメンバポートと呼ばれます。図 2-2では、Switch A の GigabitEthernet 1/0/2 と GigabitEthernet 1/0/3、Switch B の GigabitEthernet 1/0/2 がメンバポートです。

メンバポートは以下のタイプがあります。

- **ダイナミックメンバポート**－ポートが IGMP report を受信した場合、出力インタフェースとして関連づけられたダイナミック IGMP snooping 転送エントリに追加されます。同時にポートのタイマを開始します。タイマが満了する前にメッセージを受信しない場合、ポートはダイナミック転送エントリからからポートを削除します。

- **スタティックメンバポート**－ポートがメンバポートとしてスタティックに設定された場合、出力インタフェースとして関連づけられたスタティック IGMP snooping 転送エントリに追加されます。スタティックメンバポートはエージアウトしません。手動でのみ削除することができます。

特に指定しない限り、この章のルータポートとメンバポートは、ダイナミック、スタティックの両方を示します。

2.1.2 IGMP snooping の動作

この章のポートはダイナミックポートです。スタティックポートの設定、削除方法については、オペレーションマニュアルのセクション 5 *マルチキャスト”IGMP スヌーピング*”の”*スタティックポートの設定*”を参照してください。

IGMP メッセージのタイプは、general クエリ、IGMP report、leave メッセージを含みます。IGMP snooping が有効なレイヤ 2 装置は、受信した IGMP メッセージによってそれぞれ異なる動作をします。

I. General クエリ

IGMP クエリアは、アクティブなマルチキャストグループメンバが存在するかどうかを調べるために、ローカルサブネット上のすべてのホストとルータへ IGMP general クエリを定期的に送信します。

IGMP クエリアから IGMP general クエリを受信すると、装置はメッセージを受信したポートと同じ VLAN に属する、受信したポート以外のすべてのポートへ IGMP general クエリを転送します。受信ポートに対しては以下を実施します。

- 受信ポートがルータポートリストに存在するルータポートの場合、装置はこのルータポートのエージングタイマを再起動します。
- 受信ポートがルータポートリストに存在しない場合、装置はその受信ポートをルータポートリストに追加し、このルータポートのエージングタイマを開始します。

II. IGMP report

ホストは以下の目的により IGMP report を IGMP クエリアへ送信します。

- ホストがマルチキャストグループメンバである場合、IGMP クエリに応答します。
- マルチキャストグループ membership を適用します。

IGMP report を受信すると、装置は VLAN 内のすべてのルータポートからそれを転送し、報告されたマルチキャストグループのアドレスを解決します。そして、転送テーブルを検索します。

- 報告されたグループの転送テーブルエントリが存在しない場合、装置はエントリを作成して、受信したポートを転送エントリにダイナミックメンバポートとして追加します。そして、そのポートでメンバポートエージングタイマを起動します。
- 報告されたグループの転送テーブルエントリは存在するが、そのグループの発信ポートリストにポートが含まれていない場合、装置はポートをダイナミックメンバポートとして転送エントリに追加します。そのポートのメンバポートエージングタイマを起動します。

- 報告されたグループの転送テーブルエントリが存在し、転送エントリに受信ポートが含まれている場合、装置はそのポートのメンバポートエージングタイマをリセットします。

IGMP snooping が有効な装置でマルチキャストグループポリシーの設定がある際、ユーザがマルチキャストプログラムを要求した場合、ユーザのホストは IGMP report を初期化します。この IGMP report を受信した後、装置は IGMP report のマルチキャストグループアドレスを解決し、IGMP report の ACL によるフィルタリングを実行します。ACL のフィルタリングにパスした場合、出力インタフェースとして受信したポートの IGMP snooping 転送エントリを作成し、転送エントリにポートを追加します。パスしない場合、装置は IGMP report を廃棄します。ユーザはマルチキャストグループに加入できず、マルチキャストプログラムを要求することができないことを示します。

装置は IGMP report の抑制を行わないため、非ルータポートを通して IGMP report の転送を行いません。

III. Leave メッセージ

IGMPv1 ホストがマルチキャストグループを離脱する場合、ホストは IGMP leave メッセージを送信しません。レシーバホストに接続されているポートのエージングタイマが終了するまで、装置はホストに対応するメンバポートの転送エントリを転送テーブルから削除しません。この場合、ポートのマルチキャストグループのエージングタイマが終了するまで関連する転送エントリの出力インタフェースリストからポートを削除しません。

IGMPv2 ホストあるいは IGMPv3 ホストがマルチキャストグループを離脱する場合、マルチキャストルータに IGMP leave メッセージを送信します。

装置がダイナミックメンバポートで IGMP leave メッセージを受信した場合、装置はメッセージのグループアドレスが転送エントリに存在するかどうかを確認します。

- 転送テーブルエントリが存在しない場合、装置は IGMP leave メッセージを破棄します。
- 転送テーブルエントリが存在するが受信ポートが転送エントリの出力インタフェースでない場合、装置は IGMP leave メッセージを破棄します。
- 転送テーブルエントリが存在するが、受信ポートが唯一の転送エントリの出力インタフェースでない場合、以下の処理を行います。
  - □ IGMP leave メッセージを廃棄します。
  - □ 受信ポートに接続されたアクティブレシーバがグループにあるかどうかを確認するため、IGMP group-specific クエリを送信します。
  - □ 受信ポートのエージングタイマを IGMP last member クエリ間隔の 2 倍に設定します。
- 転送テーブルエントリが存在するが、受信ポートが唯一の転送エントリの出力インタフェースである場合、以下の処理を行います。
  - □ VLAN のすべてのルータポートに IGMP leave メッセージを転送します。
  - □ 受信ポートに接続されたアクティブレシーバがグループにあるかどうかを確認するため、IGMP group-specific クエリを送信します。
  - □ 受信ポートのエージングタイマを IGMP last member クエリ間隔の 2 倍に設定します。

ポートで IGMP leave メッセージを受信したのち、IGMP クエリアはメッセージのマルチキャストグループアドレスを解決します。そして、受信ポートを通してマルチキャストグループに IGMP group-specific クエリを送信します。

IGMP group-specific クエリを受信したのち、装置は VLAN 内のすべてのルータポートとメンバポートを通して、クエリを転送します。そして、直接接続されたレシーバから IGMP report の応答を待ちます。leave メッセージを受信したダイナミックメンバポートのため、装置は以下のいずれかのアクションを実行します。

- メンバポートのエージングタイマが切れる前に、装置はそのポートのエージングタイマを再起動します。
- 装置はエージングタイマが終了すると、マルチキャストグループの転送テーブルエントリからポートを削除します。

2.1.3 IGMP snooping プロキシー機能

図 2-3に示すように、上流装置で受信される IGMP report メッセージ、IGMP leave メッセージの数を削減する場合、エッジ装置で IGMP snooping プロキシー機能を有効にします。IGMP snooping プロキシー機能を有効にした場合、IGMP report メッセージ、IGMP leave メッセージを Router A に送信するため、上流の IGMP snooping クエリアのエッジ装置はホストとして動作します。

エッジ装置でホスト IGMP report の抑制メカニズムは適用しません。

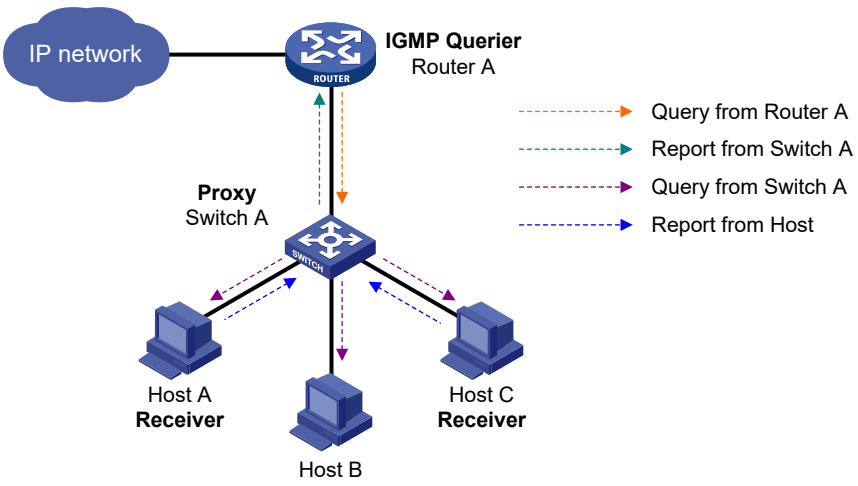


図 2-3 IGMP snooping プロキシー機能

IGMP snooping プロキシー機能が有効な装置は異なる IGMP メッセージを処理します。

- General クエリ

IGMP general クエリを受信したのち、装置は受信ポートを除く VLAN のすべてのポートにクエリを転送します。装置はローカルメンバシップ情報をもとにして IGMP report を作成し、すべてのルータポートに送信します。

- Group-specific クエリあるいは group-and-source-specific クエリ

IGMP group-specific クエリ あるいは IGMP group-and-source-specific クエリを受信したのち、装置は受信ポートを除く VLAN のすべてのポートにクエリを転送します。転送エントリにメンバポートがある場合、装置は VLAN のすべてのルータポートに report を送信します。

- Report

ホストから IGMP report を受信したのち、装置は以下のように一致するエントリを転送テーブルから検索します。

  - □ エントリが一致し、転送エントリに受信ポートを含んでいる場合、装置はポートのエージングタイマをリセットします。
  - □ エントリが一致するが、転送エントリに受信ポートが含まれない場合、装置は出力インタフェースリストに受信ポートを追加します。そして受信ポートをダイナミックメンバポートとしてマーキングし、ポートのエージングタイマを開始します。
  - □ エントリが一致しない場合、装置は出力インタフェースを受信ポートとして転送エントリを作成します。受信ポートをダイナミックメンバポートとしてマーキングし、ポートのエージングタイマを開始します。そしてすべてのルータポートに report を送信します。

- Leave メッセージ

ポートで IGMP leave メッセージを受信したのち、装置は受信ポートを通して IGMP group-specific クエリを送信します。last メンバポートが転送エントリから削除された場合のみすべてのルータポートに IGMP leave メッセージを送信します。

2.2 プロトコルと標準

RFC 4541, *Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches*

2.3 VLANベースのIGMP snooping設定作業リスト

作業リスト
IGMP snoopingの基本機能の設定 ● （必須設定項目）IGMP snoopingの有効化 ● （オプション設定項目）IGMP snoopingのバージョンの設定 ● （オプション設定項目）IGMP snooping転送エントリの最大数の設定 ● （オプション設定項目）スタティックマルチキャストアドレスエントリの設定 ● （オプション設定項目）IGMP last member クエリ間隔の設定
IGMP snoopingポート機能の設定 ● （オプション設定項目）ダイナミックポートのエージングタイマの設定 ● （オプション設定項目）スタティックポートの設定 ● （オプション設定項目）シミュレーティッドメンバホストの設定 ● （オプション設定項目）fast-leave処理の有効化
IGMP snooping クエリの設定 ● （オプション設定項目）IGMP snoopingクエリアの有効化 ● （オプション設定項目）IGMP クエリとresponseのパラメータの設定
（オプション設定項目）IGMP snooping プロキシー機能の有効化

作業リスト
IGMPメッセージパラメータの設定 • （オプション設定項目）IGMPメッセージの送信元IPアドレスの設定 • （オプション設定項目）IGMPメッセージの802.1p優先度の設定
IGMP snooping ポリシーの設定 • （オプション設定項目）マルチキャストグループポリシーの設定 • （オプション設定項目）マルチキャストソースポートフィルタの設定 • （オプション設定項目）未知のマルチキャストデータ廃棄機能の有効化 • （オプション設定項目）IGMP report抑制機能の有効化 • （オプション設定項目）ポートで参加可能なマルチキャストグループの最大数の設定 • （オプション設定項目）マルチキャストグループ置き換え機能の有効化

IGMP snooping において、アグリゲートインタフェース上での設定は、そのメンバポートの設定に干渉しないし、アグリゲーション計算にも参加しません。アグリゲートグループのメンバポートでの設定は、アグリゲートグループから離脱するまで有効になりません。

2.4 IGMP snoopingの基本機能の設定

IGMP snooping の基本機能の設定をする前に、以下の作業を完了させてください。

- 対応する VLAN を設定してください。
- IGMP snooping のバージョンを定義してください。
- IGMP snooping 転送エントリの最大数を定義してください。
- IGMP last member クエリの間隔を定義してください。

2.4.1 IGMP snooping の有効化

IGMP snooping を有効にする場合、以下のガイドラインに従ってください。

- VLAN で IGMP snooping を有効にする前に、グローバルで有効にしてください。
- VLAN 用の IGMP snooping は、VLAN のメンバポートでのみ動作します。

以下に IGMP snooping の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. IGMP snooping をグローバルで有効にし、IGMP-snooping view に移行する	**igmp-snooping**	デフォルト：無効
3. system view に戻る	**quit**	―
4. VLAN view に移行する	**vlan** *vlan-id*	―
5. VLAN で IGMP snooping を有効にする	**igmp-snooping enable**	デフォルト：無効

2.4.2 IGMP snooping のバージョンの設定

IGMP snooping のバージョンが異なると、IGMP メッセージの異なるバージョンを処理することができます。

- IGMPv2 snooping は IGMPv1 と IGMPv2 メッセージを処理することができますが、IGMPv3 メッセージは処理することはできず、VLAN 上にフラッディングされてしまいます。
- IGMPv3 snooping は IGMPv1、IGMPv2、IGMPv3 メッセージを処理することができます。

IGMPv3 snooping を IGMPv2 snooping に変更する場合、装置は以下のことを行います。

- ダイナミックに追加されたすべての IGMP snooping 転送エントリを削除します。
- IGMPv3 snooping スタティック（* , G）の転送エントリは維持します。
- IGMPv3 snooping スタティック（S , G）の転送エントリは削除します。IGMP snooping が IGMPv3 snooping に切り替わった場合復元されます。

スタティック IGMP snooping 転送エントリの詳細については、オペレーションマニュアルのセクション 5 *マルチキャスト” IGMP スヌーピング”の” スタティックポートの設定”* を参照してください。

以下に IGMP snooping のバージョンの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． VLAN view に移行する	**vlan** *vlan-id*	―
3． IGMP snooping のバージョンを指定する	**igmp-snooping version** *version-number*	デフォルト：2

2.4.3 IGMP snooping 転送エントリの最大数の設定

IGMP snooping 転送テーブルの最大エントリ数をグローバルに設定できます。この最大エントリ数はダイナミックエントリ、スタティックを含みます。装置の転送エントリ数が上限に達すると、装置は、いくつかのエントリがタイムアウトするか、手動で削除されるまで、転送エントリを生成することができません。新しいエントリを作成するため、手動でエントリを削除することを推奨します。

以下に IGMP snooping 転送エントリの最大数の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． IGMP-snooping view に移行する	**igmp-snooping**	―
3． IGMP snooping 転送エントリの最大数を設定する	**entry-limit** *limit*	デフォルト：4294967295

2.4.4 スタティックマルチキャスト MAC アドレスエントリの設定

レイヤ 2 マルチキャストにおいて、マルチキャスト MAC アドレスエントリは IGMP snooping などのレイヤ 2 マルチキャストプロトコルによってダイナミックに作成することができます。またマルチキャスト MAC アドレスと、マルチキャストデータの宛先ポートを制御するポートを関連づけることでスタティックマルチキャスト MAC アドレスエントリを手動で設定することができます。

I. 設定の制限とガイドライン

スタティックマルチキャスト MAC アドレスエントリを設定する場合、以下の設定の制限とガイドラインに従ってください。

- 設定する前に IP マルチキャストルーティングを有効にする必要はありません。
- スタティックマルチキャスト MAC アドレスエントリを設定する場合、使用していないマルチキャスト MAC アドレスを指定してください。マルチキャスト MAC アドレスは最上位オクテットの最下位ビット（LSB）が 1 です。
- system view で指定したインタフェース、あるいは interface view で現在のインタフェースにスタティックマルチキャスト MAC アドレスエントリを設定することができます。

II. system view でのスタティックマルチキャスト MAC アドレスエントリの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. スタティックマルチキャスト MAC アドレスエントリを設定する	**mac-address multicast** *mac-address* **interface** *interface-list* **vlan** *vlan-id*	デフォルト：設定なし

III. interface view でのスタティックマルチキャスト MAC アドレスエントリの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Layer 2 Ethernet interface view あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	―
3. スタティックマルチキャスト MAC アドレスエントリを設定する	**mac-address multicast** *mac-address* **vlan** *vlan-id*	デフォルト：設定なし

2.4.5 IGMP last member クエリ間隔の設定

グループの IGMP group-specific クエリを受信すると、レシーバホストは参加した各マルチキャストグループのタイマを起動します。このタイマは、0 から最大応答時間（ホストは、受信した IGMP クエリの Max Response Time フィールドから最大応答時間の値を取得します）の範囲でランダムな値に初期化されます。タイマ値が経過して 0 になった場合に、ホストは対応するマルチキャストグループに IGMP report を送信します。

IGMP クエリの最大応答時間を適切に設定すると、ホストは速やかにクエリに応答できます。また、対応するタイマの期限が多数のホストで同時に切れた場合に同時に送信する

report によってネットワーク上で発生する IGMP トラフィックのバーストを回避することもできます。

I. 設定の制限とガイドライン

IGMP last member クエリの間隔を設定する場合、以下の制限とガイドラインに従ってください。

- fast-leave 処理が有効なポートから IGMP leave メッセージを受信した場合、装置は IGMP group-specific クエリを送信しません。
- IGMP-snooping view のすべての VLAN、あるいは VLAN view の VLAN でグローバルに IGMP last member クエリの間隔を設定することができます。VLAN で行った設定はグローバルで行った設定よりも優先されます。

II. グローバルでの IGMP last member クエリの間隔の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. IGMP-snooping view に移行する	**igmp-snooping**	―
3. IGMP last-member クエリの送信間隔を設定する	**last-member-query-interval** *interval*	デフォルト：1秒

III. VLAN での IGMP last member クエリの間隔の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. VLAN view に移行する	**vlan** *vlan-id*	―
3. IGMP last-member クエリの送信間隔を設定する	**igmp-snooping last-member-query-interval** *interval*	デフォルト：1秒

2.5 IGMP snoopingポート機能の設定

IGMP snooping ポート機能の設定をする前に、以下の作業を完了させてください。

- VLAN で IGMP snooping を有効にしてください。
- ダイナミックルータポートのエージングタイマを定義してください。
- ダイナミックメンバポートのエージングタイマを定義してください。
- マルチキャストグループとマルチキャスト送信元アドレスを定義してください。

2.5.1 ダイナミックポートのエージングタイマの設定

ダイナミックポートのエージングタイマを設定する場合、以下のガイドラインに従ってください。

- マルチキャストグループメンバシップが頻繁に変更される場合は、メンバポートのエージングタイマに比較的小さな値を設定します。マルチキャストグループメンバシッ

プがほとんど変更されない場合は、メンバポートのエージングタイマに比較的大きな値を設定します。

- ダイナミックルータポートが PIMv2 hello メッセージを受信した場合、ダイナミックポートのエージングタイマの時間は、hello メッセージの時間で指定されません。この場合、**router-aging-time** コマンドあるいは **igmp-snooping router-aging-time** コマンドはポートで適用されません。
- ダイナミックポートのエージングタイマの設定は、VLAN view の現在の VLAN あるいは IGMP-snooping view のすべての VLAN のどちらかに設定することができます。VLAN view と IGMP-snooping view の両方に設定がある場合、VLAN view の設定が適用されます。

I. グローバルでのダイナミックポートのエージングタイマの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. IGMP-snooping view に移行する	**igmp-snooping**	―
3. グローバルでのダイナミックルータポートのエージングタイマを設定する	**router-aging-time** *seconds*	デフォルト：260秒
4. グローバルでのダイナミックメンバポートのエージングタイマを設定する	**host-aging-time** *seconds*	デフォルト：260秒

II. VLAN でのダイナミックポートのエージングタイマの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. VLAN view に移行する	**vlan** *vlan-id*	―
3. VLAN でのダイナミックルータポートのエージングタイマを設定する	**igmp-snooping router-aging-time** *seconds*	デフォルト：260秒
4. VLAN でのダイナミックメンバポートのエージングタイマを設定する	**igmp-snooping host-aging-time** *seconds*	デフォルト：260秒

2.5.2 スタティックポートの設定

以下のタイプのスタティックポートを設定することができます。

- **スタティックメンバポート**－マルチキャストグループのスタティックメンバポートを設定する場合、ポートに接続されるすべてのホストはグループのマルチキャストデータを受信することができます。

  設定を完了あるいは取り消した場合、ポートは IGMP report や leave メッセージを送信しません。スタティックメンバポートは IGMP クエリに応答しません。

- **スタティックルータポート**－マルチキャストグループのスタティックルータポートを設定する場合、ポートで受信されたグループのすべてのマルチキャストデータは転送されます。

以下にスタティックポートの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	－
2. Layer 2 Ethernet interface view あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	－
3. ポートをスタティックポートに設定する	• ポートをスタティックメンバポートに設定する：**igmp-snooping static-group** *group-address* [**source-ip** *source-address*] **vlan** *vlan-id* • ポートをスタティックルータポートに設定する：**igmp-snooping static-router-port vlan** *vlan-id*	デフォルト：設定なし

2.5.3 シミュレーティッドメンバホストの設定

ポートでシミュレーティッドメンバホストを設定した場合、以下の方法により独立したホストと同等になります。

- 設定が完了した場合、unsolicited IGMP report を送信します。
- IGMP report として IGMP general クエリに応答します。
- 設定を削除した場合、IGMP leave メッセージを送信します。

シミュレーティッドホストの IGMP のバージョンと IGMP snooping バージョンが同一であることを確認してください。スタティックメンバポートと異なり、シミュレーティッドメンバホストとして設定されたポートはダイナミックメンバポートと同様にエージアウトします。

以下にシミュレーティッドメンバホストの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	－
2. Layer 2 Ethernet interface view あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	－
3. ポートをシミュレーティッドメンバホストとして設定する	**igmp-snooping host-join** *group-address* [**source-ip** *source-address*] **vlan** *vlan-id*	デフォルト：設定なし

2.5.4 fast-leave 処理の有効化

ポートが leave メッセージを受信する場合、装置は fast-leave 処理機能によって、IGMP leave メッセージを迅速に転送エントリからポートを削除することができます。

I. 設定の制限とガイドライン

IGMP snooping fast-leave 処理機能を設定する場合、以下の設定の制限とガイドラインに従ってください。

- 複数のホストが接続しているポートでは fast-leave 処理機能を有効にしないでください。これを行うと、同じマルチキャストグループにあるポートに接続された他のレシーバのホストはマルチキャストデータを受信することができません。
- IGMP snooping fast-leave 処理機能は、ポートあるいはグローバルのどちらかに設定することができます。ポートとグローバルの両方に設定がある場合、ポートの設定が適用されます。

II. グローバルでの IGMP snooping fast-leave 処理機能の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. IGMP-snooping view に移行する	**igmp-snooping**	—
3. グローバルで IGMP snooping fast-leave 処理機能を設定する	**fast-leave** [**vlan** *vlan-list*]	デフォルト：無効

III. ポートでの IGMP snooping fast-leave 処理機能の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. Layer 2 Ethernet interface view あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	—
3. ポートで IGMP snooping fast-leave 処理機能を設定する	**igmp-snooping fast-leave** [**vlan** *vlan-list*]	デフォルト：無効

2.6 IGMP snooping クエリの設定

この項では IGMP snooping クエリの設定方法について記載します。

2.6.1 設定要件

IGMP snooping クエリを設定する前に、以下の作業を完了してください。

- VLAN で IGMP snooping を有効にしてください。
- IGMP general クエリの送信間隔を定義してください。
- IGMP last-member クエリの送信間隔を定義してください。
- IGMP general クエリの最大応答時間を定義してください。

2.6.2 IGMP snooping クエリアの有効化

この機能は、データリンクレイヤでマルチキャスト転送エントリを確立し、維持するために、装置が IGMP general クエリを定期的に送信します。レイヤ 3 マルチキャスト装置がないネットワークで IGMP snooping クエリアを設定することができます。

IGMP snooping クエリアを有効にする場合、IGMP が動作するマルチキャストネットワークで IGMP snooping クエリアを有効にしないでください。IGMP Snooping クエリアは IGMP クエリアの選択に関与しませんが、小さい送信元 IP アドレスで IGMP general クエリを送信するので IGMP クエリアの選択に影響を与える可能性があります。

以下に VLAN で IGMP snooping クエリアを有効にする設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． VLAN view に移行する	**vlan** *vlan-id*	―
3． IGMP snooping クエリアを有効にする	**igmp-snooping querier**	デフォルト：無効

2.6.3 IGMP クエリと response のパラメータの設定

⚠ **注意**：

IGMP general クエリ間隔は IGMP general クエリの最大応答時間よりも大きいことを確認してください。マルチキャストグループメンバが誤って削除されてしまう可能性があります。

VLAN ベースのネットワークの実際の状況にもとづいて、IGMP general クエリ の送信間隔 を調整することができます。

IGMP クエリ（general クエリ または group-specific クエリ）を受信すると、レシーバホストは参加した各マルチキャストグループの report delay タイマを起動します。このタイマは、0 から最大応答時間（ホストは、受信した IGMP クエリの Max Response Time フィールドから最大応答時間の値を取得します）の範囲でランダムな値に初期化されます。タイマ値が経過して 0 になった場合に、ホストは対応するマルチキャストグループに IGMP report を送信します。

IGMP クエリの最大応答時間を適切に設定すると、ホストは速やかにクエリに応答できます。また、対応するタイマの期限が多数のホストで同時に切れた場合に同時に送信する report によってネットワーク上で発生する IGMP トラフィックのバーストを回避することもできます。

IGMP クエリと応答のパラメータは、VLAN view で現在の view あるは IGMP-snooping view ですべての VLAN で設定できます。VLAN view と IGMP-snooping view の 2 つの設定がある場合、VLAN view で設定された設定が適用されます。

I. グローバルでの IGMP クエリと response のパラメータの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． IGMP-snooping view に移行する	**igmp-snooping**	―
3． IGMP general クエリの最大応答時間を設定する	**max-response-time** *seconds*	デフォルト：10秒

II. VLAN での IGMP クエリと response のパラメータの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． VLAN view に移行する	**vlan** *vlan-id*	―
3． IGMP general クエリの送信間隔を設定する	**igmp-snooping query-interval** *interval*	デフォルト：125秒
4． IGMP general クエリの最大応答時間を設定する	**igmp-snooping max-response-time** *seconds*	デフォルト：10秒

2.7 IGMP snooping プロキシー機能の有効化

IGMP snooping プロキシーが有効になっている装置は、IGMP snooping プロキシーと呼ばれます。IGMP snooping プロキシーは、アップストリーム装置のホストとして機能します。IGMP snooping クエリアで有効になっている IGMP snooping プロキシーは、ダウンストリーム装置へのルーターとして機能し、report を受信し、アップストリーム装置に代わってメッセージを残します。ベストプラクティスとして、エッジ装置で IGMP snooping プロキシーを有効にして、過剰なパケットによる影響を軽減します。

VLAN で IGMP snooping プロキシー機能を有効にする前に、まず IGMP snooping をグローバルに有効にし、VLAN で IGMP snooping 機能を有効にしてください。

この機能は IGMP snooping クエリアで使用します。IGMP snooping クエリアの有効化の詳細は、オペレーションマニュアルのセクション 5 *マルチキャスト*“*IGMP スヌーピング*”の“*IGMP snooping クエリアの有効化*”を参照してください。

以下に VLAN で IGMP snooping プロキシー機能を有効にする設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． VLAN view に移行する	**vlan** *vlan-id*	―
3． IGMP snooping プロキシー機能を有効にする	**igmp-snooping proxy enable**	デフォルト：無効

2.8 IGMPメッセージのパラメータの設定

この章では IGMP メッセージのパラメータの設定について記載します。

2.8.1 設定要件

VLAN で IGMP メッセージのパラメータを設定する前に、以下の作業を完了してください。

- VLAN で IGMP snooping を有効にしてください。
- IGMP general クエリの送信元 IP アドレスを定義してください。
- IGMP group-specific クエリの送信元 IP アドレスを定義してください。
- IGMP report の送信元 IP アドレスを定義してください。
- IGMP leave メッセージの送信元 IP アドレスを定義してください。
- IGMP メッセージの 802.1p 優先度を定義してください。

2.8.2 IGMP メッセージの送信元 IP アドレスの設定

送信元 IP アドレスが 0.0.0.0 である IGMP クエリをポートで受信すると、装置はそのポートをダイナミックルータポートとして設定しません。これによって、マルチキャスト転送エントリがデータリンクレイヤで正しく作成されずに、最終的にマルチキャストトラフィック転送エラーが発生する可能性があります。

この問題を防ぐため、IGMP snooping クエリアの IGMP クエリの送信元 IP アドレスとしてオール 0 以外の IP アドレスを設定することができます。IGMP クエリの送信元アドレスを変更するとサブネット内の IGMP クエリアの選定に影響する可能性があります。

シミュレーティッドメンバホストあるいは IGMP snooping のプロキシーによって IGMP report あるいは IGMP leave メッセージの送信元 IP アドレスを変更することができます。

以下に VLAN での IGMP メッセージの送信元 IP アドレスの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． VLAN view に移行する	**vlan** *vlan-id*	―
3． IGMP general クエリの送信元 IP アドレスを設定する	**igmp-snooping general-query source-ip** *ip-address*	デフォルト : 現在のVLANインタフェースのIPアドレスです。 現在のVLANインタフェースにIPアドレスがない場合、0.0.0.0です。

操作	コマンド	補足
4． IGMP group-specific クエリの送信元 IP アドレスを設定する	**igmp-snooping special-query source-ip** *ip-address*	デフォルト : 以下のいずれかとなります。 ● VLANのIGMP snoopingクエリアがIGMP general クエリを受信した場合、IGMP group-specific クエリの送信元IPアドレスはIGMP general クエリの送信元IPアドレスです。 ● VLANのIGMP snoopingクエリアがIGMP general クエリを受信していない場合、IGMP group-specific クエリの送信元IPアドレスは現在のVLANインタフェースのIPアドレスです。 ● VLANのIGMP snoopingクエリアがIGMP general クエリを受信しておらず、現在のVLANインタフェースにIPアドレスが設定されていない場合、送信元IPアドレスは0.0.0.0です。
5． IGMP reports の送信元 IP アドレスを設定する	**igmp-snooping report source-ip** *ip-address*	デフォルト : 現在のVLANインタフェースのIPアドレスです。 現在のVLANインタフェースにIPアドレスがない場合、0.0.0.0です。
6． IGMP leave メッセージの送信元 IP アドレスを設定する	**igmp-snooping leave source-ip** *ip-address*	デフォルト : 現在のVLANインタフェースのIPアドレスです。 現在のVLANインタフェースにIPアドレスがない場合、0.0.0.0です。

2.8.3 IGMP メッセージの 802.1p 優先度の設定

装置の出力ポートで混雑が発生すると、802.1p 優先度が高い順から IGMP メッセージを転送します。装置によって作成あるいは転送される IGMP メッセージに高い 802.1p 優先度を割り当てることができます。

IGMP-snooping view のすべての VLAN あるいは VLAN view の現在の VLAN で IGMP メッセージの優先度を設定することができます。VLAN view での設定は IGMP-snooping view での設定よりも優先されます。

I. グローバルでの IGMP メッセージの 802.1p 優先度の設定

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

操作	コマンド	補足
2． IGMP-snooping view に移行する	**igmp-snooping**	―
3． IGMP メッセージの 802.1p 優先度を設定する	**dot1p-priority** *priority*	デフォルト：設定なし 装置によって作成される IGMPメッセージの優先度は0です。IGMPメッセージを転送する場合、優先度は変更しません。

II. VLAN での IGMP メッセージの 802.1p 優先度の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． VLAN view に移行する	**vlan** *vlan-id*	―
3． IGMP メッセージの 802.1p 優先度を設定する	**igmp-snooping dot1p-priority** *priority*	デフォルト：設定なし 装置によって作成される IGMPメッセージの優先度は0です。IGMPメッセージを転送する場合、優先度は変更しません。

2.9 IGMP snooping ポリシーの設定

IGMP snooping ポリシーの設定をする前に、以下の作業を完了させてください。

- VLAN で IGMP snooping を有効にしてください。
- マルチキャストグループポリシーに使用する ACL を定義してください。
- ポートが追加できるマルチキャストグループの最大数を定義してください。

2.9.1 マルチキャストグループポリシーの設定

マルチキャストグループを指定するACLとオプションのソースにもとづいてIGMP reportをフィルタします。受信ホストが加入するマルチキャストグループを管理するために使用されます。

I. 設定の制限とガイドライン

マルチキャストグループポリシーの設定を行う場合、以下の設定の制限とガイドラインに従ってください。

- この設定はポートがダイナミックに追加するマルチキャストグループに適用されます。
- マルチキャストグループポリシーは、ポートあるいはグローバルのどちらかに設定することができます。ポートとグローバルの両方に設定がある場合、ポートの設定が適用されます。

II. グローバルでのマルチキャストグループポリシーの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. IGMP-snooping view に移行する	**igmp-snooping**	―
3. グローバルでマルチキャストグループポリシーを設定する	**group-policy** *ipv4-acl-number* [**vlan** *vlan-list*]	デフォルト：設定なし

III. ポートでのマルチキャストグループポリシーの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Layer 2 Ethernet interface view あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	―
3. ポートでマルチキャストグループポリシーを設定する	**igmp-snooping group-policy** *ipv4-acl-number* [**vlan** *vlan-list*]	デフォルト：設定なし

2.9.2 マルチキャストソースポートフィルタの設定

この機能はすべてのマルチキャストデータパケットを廃棄し、マルチキャストプロトコルパケットを許可します。マルチキャストレシーバに接続するポートに設定します。

IGMP-snooping view で指定したポートあるいは interface view の現在のポートでマルチキャストソースポートフィルタを有効にすることができます。これらの設定は同じ優先度を持ちます。

I. グローバルでのマルチキャストソースポートフィルタの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. IGMP-snooping view に移行する	**igmp-snooping**	―
3. マルチキャストソースポートフィルタを有効にする	**source-deny port** *interface-list*	デフォルト：無効

II. ポートでのマルチキャストソースポートフィルタの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Layer 2 Ethernet interface view に移行する	**interface** *interface-type interface-number*	―

操作	コマンド	補足
3． マルチキャストソースポートフィルタを有効にする	**igmp-snooping source-deny**	デフォルト：無効

2.9.3 未知のマルチキャストデータ廃棄機能の有効化

この機能はすべての未知のマルチキャストデータを廃棄します。未知のマルチキャストデータとは、IGMP snooping 転送テーブルにエントリが存在しないマルチキャストデータのことです。装置にルータポートがない場合、未知のマルチキャストデータを廃棄します。

この機能はすべての未知のマルチキャストデータを廃棄します。この機能を無効にした場合、装置は未知のマルチキャストパケットをデータが存在する VLAN にフラッディングします。

レイヤ 3 マルチキャストパケットのマルチキャスト転送エントリの発信ポートが同じ VLAN にある場合は、VLAN の未知のマルチキャストデータの廃棄を有効にしてください。この制限により、装置が VLAN のレイヤ 3 マルチキャストパケットをフラッディングするのを防ぎます。

以下に未知のマルチキャストデータ廃棄機能の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． VLAN view に移行する	**vlan** *vlan-id*	―
3． 未知のマルチキャストデータ廃棄機能を有効にする	**igmp-snooping drop-unknown**	デフォルト：無効 未知のマルチキャストデータはフラッディングします。

2.9.4 IGMP report 抑制機能の有効化

この機能はマルチキャストグループ用に、直接接続されているレイヤ 3 装置に最初の IGMP report のみを転送します。以降の同じマルチキャストグループからの IGMP report を廃棄します。

以下に IGMP report 抑制機能を有効にする設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． IGMP-snooping view に移行する	**igmp-snooping**	―
3． IGMP report 抑制機能を有効にする	**report-aggregation**	デフォルト：有効

2.9.5 ポートで参加可能なマルチキャストグループの最大数の設定

ポートトラフィックを調整するため、ポートで参加可能なマルチキャストグループの最大数を設定することができます。

I. 設定の制限とガイドライン

ポートで参加可能なマルチキャストグループの最大数を設定する場合、以下の設定の制限とガイドラインに従ってください。

- この設定はダイナミックにマルチキャストグループに加入されたポートのみ適用します。
- ポートが参加したマルチキャストグループの数が設定されている最大数に達した場合は、そのポートに残るすべての転送エントリを IGMP snooping 転送テーブルから削除します。このポートに接続されたホストは、最大数になる前に、再度マルチキャストグループに参加することができます。

II. 設定手順

以下にポートで参加可能なマルチキャストグループの最大数の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Layer 2 Ethernet interface view あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	―
3. ポートで参加可能なマルチキャストグループの最大数を設定する	**igmp-snooping group-limit** *limit* [**vlan** *vlan-list*]	デフォルト：4294967295

2.9.6 マルチキャストグループ置き換え機能の有効化

この機能は、グループのメンバ数が上限を超えた場合、装置が既存のマルチキャストグループを新規に追加されたマルチキャストグループに置き換える機能です。この機能は一般的にチャンネルスイッチアプリケーションで使われます。この機能が無効の場合、装置は新しいグループの IGMP report を廃棄し、ユーザが新しいチャンネルに変更することができません。

I. 設定の制限とガイドライン

マルチキャストグループ置き換え機能を有効にした場合、以下の設定の制限とガイドラインに従ってください。

- この設定はダイナミックにマルチキャストグループに加入されたポートのみ適用します。
- マルチキャストグループ置き換え機能は、インタフェースあるいはグローバルのどちらかに設定することができます。インタフェースとグローバルの両方に設定がある場合、インタフェースの設定が適用されます。

II. グローバルでのマルチキャストグループ置き換え機能の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． IGMP-snooping view に移行する	**igmp-snooping**	―
3． グローバルでマルチキャストグループ置き換え機能を有効にする	**overflow-replace** [**vlan** *vlan-list*]	デフォルト：無効

III. ポートでのマルチキャストグループ置き換え機能の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． Layer 2 Ethernet interface view あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	―
3． ポートでマルチキャストグループ置き換え機能を有効にする	**igmp-snooping overflow-replace** [**vlan** *vlan-list*]	デフォルト：無効

2.10 IGMP snoopingの表示と維持

すべての view で **display** コマンドを実行でき、user view で **reset** コマンドを実行できます。

操作	コマンド
IGMP snoopingステータスを表示する	**display igmp-snooping** [**global** | **vlan** *vlan-id*]
ダイナミックIGMP snooping転送エントリの情報を表示する	**display igmp-snooping group** [*group-address* | *source-address*] * [**vlan** *vlan-id*] [**verbose**] [**slot** *slot-number*]
スタティックIGMP snooping転送エントリの情報を表示する	**display igmp-snooping static-group** [*group-address* | *source-address*] * [**vlan** *vlan-id*] [**verbose**] [**slot** *slot-number*]
ダイナミックルータポートの情報を表示する	**display igmp-snooping router-port** [**vlan** *vlan-id*] [**slot** *slot-number*]
スタティックルータポートの情報を表示する	**display igmp-snooping static-router-port** [**vlan** *vlan-id*] [**slot** *slot-number*]
IGMP snoopingによって学習されたIGMPメッセージの統計情報を表示する	**display igmp-snooping statistics**
レイヤ2 IPマルチキャストグループエントリの情報を表示する	**display l2-multicast ip forwarding** [**group** *group-address* | **source** *source-address*] * [**vlan** *vlan-id*] [**slot** *slot-number*]
レイヤ2 MACマルチキャストグループエントリの情報を表示する	**display l2-multicast mac forwarding** [*mac-address*] [**vlan** *vlan-id*] [**slot** *slot-number*]
スタティックマルチキャストMACアドレスエントリを表示する	**display mac-address** [*mac-address* [**vlan** *vlan-id*] | [**multicast**] [**vlan** *vlan-id*] [**count**]]
指定されたマルチキャストグループのダイナミックIGMP snooping転送エントリを削除する	**reset igmp-snooping group** { *group-address* [*source-address*] | **all** } [**vlan** *vlan-id*]
ダイナミックルータポートを削除する	**reset igmp-snooping router-port** { **all** | **vlan** *vlan-id*]

操作	コマンド
IGMP snoopingによって学習されたIGMPメッセージの統計情報を削除する	**reset igmp-snooping statistics**

2.11 IGMP snooping設定例

2.11.1 VLAN ベースのグループポリシーとシミュレーティッドメンバホストの設定例

I. ネットワーク要件

図 2-4に示すように、Router A は IGMPv2 を動作させ、IGMP クエリアとして機能します。Switch A は IGMPv2 snooping を動作させます。

グローバルポリシーとシミュレーティッドメンバホストを以下のように設定します。

- Host A と Host B がマルチキャストグループ 224.1.1.1 のマルチキャストデータのみ受信します。Host A と Host B がマルチキャストデータの受信に失敗しても、マルチキャストデータは連続して Switch A の GigabitEthernet1/0/3 と GigabitEthernet1/0/4 を通して転送することができます。
- Switch A は VLAN100 でフラッディングしないように未知のマルチキャストデータを廃棄します。

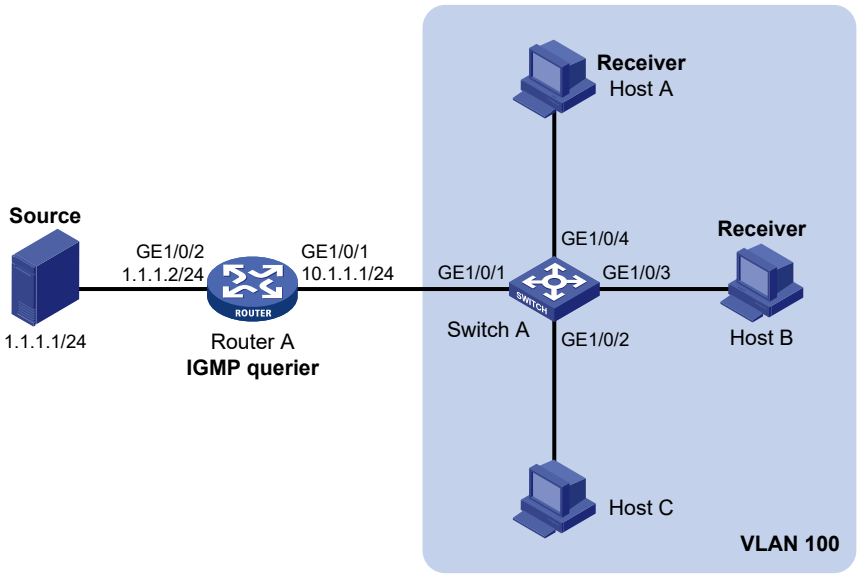


図 2-4 ネットワーク図

II. 設定手順

1) 図 2-4に対応する各インタフェースに IP アドレスとサブネットマスクを割り当てます。（詳細は省略します）

2)　Router A を設定します。

IP マルチキャストルーティングを有効にします。

```
<RouterA> system-view
[RouterA] multicast routing
[RouterA-mrib] quit
```

GigabitEthernet 1/0/1 で IGMP を有効にします。

```
[RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] igmp enable
[RouterA-GigabitEthernet1/0/1] quit
```

GigabitEthernet 1/0/2 で PIM-SM を有効にします。

```
[RouterA] interface gigabitethernet 1/0/2
[RouterA-GigabitEthernet1/0/2] pim sm
[RouterA-GigabitEthernet1/0/2] quit
```

3)　Switch A を設定します。

グローバルで IGMP snooping を有効にします。

```
<SwitchA> system-view
[SwitchA] igmp-snooping
[SwitchA-igmp-snooping] quit
```

VLAN 100 を作成し、この VLAN に GigabitEthernet 1/0/1～GigabitEthernet 1/0/4 を割り当てます。

```
[SwitchA] vlan 100
[SwitchA-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/4
```

VLAN100 で IGMP snooping を有効にし、未知のマルチキャストデータ廃棄機能を有効にします。

```
[SwitchA-vlan100] igmp-snooping enable
[SwitchA-vlan100] igmp-snooping drop-unknown
[SwitchA-vlan100] quit
```

VLAN 100 にマルチキャストグループ 224.1.1.1 だけが参加できるように、マルチキャストグループポリシーを設定します。

```
[SwitchA] acl basic 2001
[SwitchA-acl-ipv4-basic-2001] rule permit source 224.1.1.1 0
[SwitchA-acl-ipv4-basic-2001] quit
[SwitchA] igmp-snooping
[SwitchA-igmp-snooping] group-policy 2001 vlan 100
[SwitchA-igmp-snooping] quit
```

マルチキャストグループ 224.1.1.1 のシミュレーティッドメンバホストとして GigabitEthernet 1/0/3、GigabitEthernet 1/0/4 を設定します。

```
[SwitchA] interface gigabitethernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] igmp-snooping host-join 224.1.1.1 vlan 100
[SwitchA-GigabitEthernet1/0/3] quit
[SwitchA] interface gigabitethernet 1/0/4
[SwitchA-GigabitEthernet1/0/4] igmp-snooping host-join 224.1.1.1 vlan 100
[SwitchA-GigabitEthernet1/0/4] quit
```

III. 設定の確認

Host A と Host B がマルチキャストグループ 224.1.1.1、224.2.2.2 に加入するため IGMP report を受信します。（詳細は省略します）

Switch A で VLAN 100 のダイナミック IGMP snooping 転送エントリの情報を表示します。

```
[SwitchA] display igmp-snooping group vlan 100
Total 1 entries.

VLAN 100: Total 1 entries.
  (0.0.0.0, 224.1.1.1)
    Host ports (2 in total):
      GE1/0/3                                 (00:03:23)
      GE1/0/4                                 (00:04:10)
```

出力は、以下を示します。

- Switch A のメンバポート GigabitEthernet 1/0/4、GigabitEthernet 1/0/3 を通して、Host A と Host B がマルチキャストグループ 224.1.1.1 に加入しています。
- Host A と Host B がマルチキャストグループ 224.2.2.2 に加入できないことを示しています。マルチキャストグループのポリシーが適用されていることを示します。

2.11.2 VLAN ベースのスタティックポートの設定例

I. ネットワーク要件

図 2-5に示すようなネットワークを設定します。

- Router A は IGMPv2 を動作させ、IGMP クエリアとして機能し、Switch A、Switch B、Switch C は IGMPv2 snooping を動作させます。
- Host A と Host C はマルチキャストグループ 224.1.1.1 の永久的な Receiver です。

以下の要件に適用するためスタティックポートを設定します。

- マルチキャストトラフィック送信の信頼性を強化するために、Switch C の GigabitEthernet 1/0/3 と GigabitEthernet 1/0/5 をマルチキャストグループ 224.1.1.1 のスタティックメンバポートとして設定します。
- ネットワークで STP が実行されていると仮定します。データループを回避するために、Switch A から Switch C への転送パスは通常状態ではブロックされます。マルチ

キャストトラフィックは Switch A—Switch B—Switch C のパスを経由して、Switch C に接続されている Receiver に転送されます。Switch A—Switch B—Switch C のパスがブロックされた場合に、Switch A—Switch C のパスを経由してマルチキャストトラフィックがほとんど途切れずに Receiver へと転送できるように、Switch A の GigabitEthernet 1/0/3 にスタティックルータポートを設定します。STP の詳細は、オペレーションマニュアルのセクション 2 *アクセス ”STP”* を参照してください。

メモ：

スタティックルータポートが設定されていない場合、Switch A—Switch B－Switch C のパスがブロックされたのち、マルチキャストの転送が中断されます。新しいパスでマルチキャストパケットを転送する前に、少なくとも 1 回以上の IGMP クエリと IGMP 応答の交換が必要です。

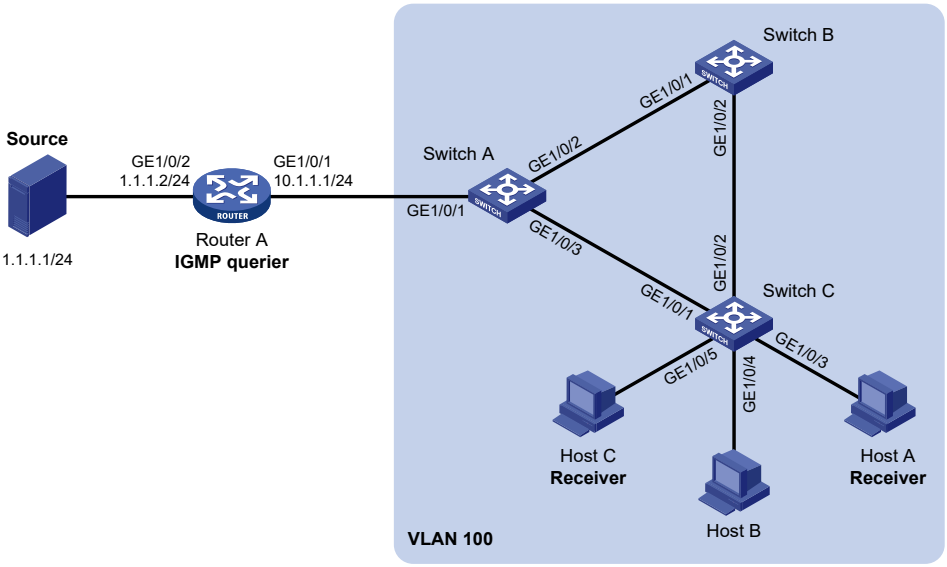


図 2-5 ネットワーク図

II. 設定手順

1) 図 2-5に対応する各インタフェースに IP アドレスとサブネットマスクを割り当てます。（詳細は省略します）
2) Router A を設定します。

IP マルチキャストルーティングを有効にします。

```
<RouterA> system-view
[RouterA] multicast routing
[RouterA-mrib] quit
```

GigabitEthernet 1/0/1 で IGMP を有効にします。

```
[RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] igmp enable
```

```
[RouterA-GigabitEthernet1/0/1] quit
```

GigabitEthernet 1/0/2 で PIM-SM を有効にします。

```
[RouterA] interface gigabitethernet 1/0/2
[RouterA-GigabitEthernet1/0/2] pim sm
[RouterA-GigabitEthernet1/0/2] quit
```

3)　Switch A を設定します。

グローバルに IGMP snooping を有効にします。

```
<SwitchA> system-view
[SwitchA] igmp-snooping
[SwitchA-igmp-snooping] quit
```

VLAN 100 を作成し、この VLAN に GigabitEthernet 1/0/1～GigabitEthernet 1/0/3 を割り当てます。

```
[SwitchA] vlan 100
[SwitchA-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/3
```

VLAN 100 で IGMP snooping を有効にします。

```
[SwitchA-vlan100] igmp-snooping enable
[SwitchA-vlan100] quit
```

スタティックルータポートとして、GigabitEthernet 1/0/3 を設定します。

```
[SwitchA] interface gigabitethernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] igmp-snooping static-router-port vlan 100
[SwitchA-GigabitEthernet1/0/3] quit
```

4)　Switch B を設定します。

グローバルに IGMP snooping を有効にします。

```
<SwitchB> system-view
[SwitchB] igmp-snooping
[SwitchB-igmp-snooping] quit
```

VLAN 100 を作成し、この VLAN に GigabitEthernet 1/0/1～GigabitEthernet 1/0/2 を割り当てます。

```
[SwitchB] vlan 100
[SwitchB-vlan100] port gigabitethernet 1/0/1 gigabitethernet 1/0/2
```

VLAN 100 で IGMP snooping を有効にします。

```
[SwitchB-vlan100] igmp-snooping enable
[SwitchB-vlan100] quit
```

5)　Switch C を設定します。

グローバルに IGMP snooping を有効にします。

```
<SwitchC> system-view
[SwitchC] igmp-snooping
[SwitchC-igmp-snooping] quit
```

VLAN 100 を作成し、この VLAN に GigabitEthernet 1/0/1～GigabitEthernet 1/0/5 を割り当てます。

```
[SwitchC] vlan 100
[SwitchC-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/5
```

VLAN100 で IGMP snooping を有効にします。

```
[SwitchC-vlan100] igmp-snooping enable
[SwitchC-vlan100] quit
```

マルチキャストグループ 224.1.1.1 のスタティックメンバポートとして GigabitEthernet 1/0/3、GigabitEthernet 1/0/5 を設定します。

```
[SwitchC] interface gigabitethernet 1/0/3
[SwitchC-GigabitEthernet1/0/3] igmp-snooping static-group 224.1.1.1 vlan 100
[SwitchC-GigabitEthernet1/0/3] quit
[SwitchC] interface gigabitethernet 1/0/5
[SwitchC-GigabitEthernet1/0/5] igmp-snooping static-group 224.1.1.1 vlan 100
[SwitchC-GigabitEthernet1/0/5] quit
```

III. 設定の確認

Switch A で VLAN 100 のスタティックルータポートの情報を表示します。

```
[SwitchA] display igmp-snooping static-router-port vlan 100
VLAN 100:
  Router ports (1 in total):
    GE1/0/3
```

出力は、Switch A の GigabitEthernet 1/0/3 がスタティックルータポートになっていることを示します。

Switch C で VLAN 100 のスタティック IGMP snooping 転送エントリの情報を表示します。

```
[SwitchC] display igmp-snooping static-group vlan 100
Total 1 entries.

VLAN 100: Total 1 entries.
  (0.0.0.0, 224.1.1.1)
    Host ports (2 in total):
      GE1/0/3
      GE1/0/5
```

出力は、Switch C の GigabitEthernet 1/0/3 と GigabitEthernet 1/0/5 がマルチキャストグループ 224.1.1.1 のスタティックメンバポートになっていることを示します。

2.11.3 VLAN ベースの IGMP snooping クエリアの設定例

I. ネットワーク要件

図 2-6に示すようなネットワークを設定します。

- ネットワークはレイヤ 2 のみのネットワークです。
- Source 1、Source 2 はそれぞれマルチキャストグループ 224.1.1.1、225.1.1.1 にマルチキャストデータを送信します。
- Host A、Host C はマルチキャストグループ 224.1.1.1 の Receiver で、Host B、Host D はマルチキャストグループ 225.1.1.1 の Receiver です。
- すべての Receiver ホストは IGMPv2 が動作し、すべての装置は IGMPv2 snooping が動作します。Switch A（マルチキャストソースにもっとも近い）は IGMP snooping クエリアとして動作します。

以下の要件に適合するように Switch を設定します。

- VLAN で未知のパケットをフラッディングしないように、すべての Switch で未知のマルチキャストパケットの廃棄機能を有効にします。
- レイヤ 2 転送エントリを確立するため、オール 0 以外の IP アドレスとして IGMP クエリの送信元 IP アドレスを設定します。

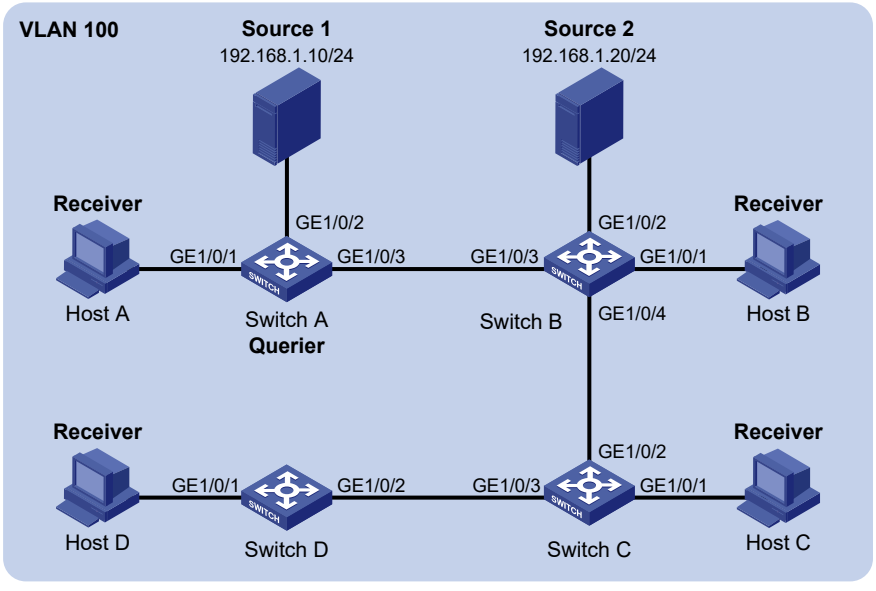


図 2-6 ネットワーク図

II. 設定手順

1)　Switch A を設定します。

グローバルに IGMP snooping を有効にします。

```
<SwitchA> system-view
[SwitchA] igmp-snooping
[SwitchA-igmp-snooping] quit
```

VLAN 100 を作成し、この VLAN に GigabitEthernet 1/0/1～GigabitEthernet 1/0/3 を割り当てます。

```
[SwitchA] vlan 100
[SwitchA-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/3
```

VLAN 100 で IGMP Snooping を有効にし、未知のマルチキャストデータ廃棄機能を有効にします。

```
[SwitchA-vlan100] igmp-snooping enable
[SwitchA-vlan100] igmp-snooping drop-unknown
```

VLAN 100 で IGMP Snooping クエリア機能を有効にします。

```
[SwitchA-vlan100] igmp-snooping querier
[SwitchA-vlan100] quit
```

VLAN 100 で IGMP general クエリの送信元 IP アドレスを 192.168.1.1 に設定します。

```
[SwitchA-vlan100] igmp-snooping general-query source-ip 192.168.1.1
```

VLAN 100 で IGMP group-specific クエリの送信元 IP アドレスを 192.168.1.1 に設定します。

```
[SwitchA-vlan100] igmp-snooping special-query source-ip 192.168.1.1
[SwitchA-vlan100] quit
```

2)　Switch B を設定します。

グローバルに IGMP snooping を有効にします。

```
<SwitchB> system-view
[SwitchB] igmp-snooping
[SwitchB-igmp-snooping] quit
```

VLAN 100 を作成し、この VLAN に GigabitEthernet 1/0/1～GigabitEthernet 1/0/4 を割り当てます。

```
[SwitchB] vlan 100
[SwitchB-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/4
```

VLAN 100 で IGMP Snooping を有効にし、未知のマルチキャストデータ廃棄機能を有効にします。

```
[SwitchB-vlan100] igmp-snooping enable
[SwitchB-vlan100] igmp-snooping drop-unknown
[SwitchB-vlan100] quit
```

3)　Switch C を設定します。

グローバルに IGMP snooping を有効にします。

```
<SwitchC> system-view
[SwitchC] igmp-snooping
[SwitchC-igmp-snooping] quit
```

VLAN 100 を作成し、この VLAN に GigabitEthernet 1/0/1～GigabitEthernet 1/0/3 を割り当てます。

```
[SwitchC] vlan 100
[SwitchC-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/3
```

VLAN 100 で IGMP Snooping を有効にし、未知のマルチキャストデータ廃棄機能を有効にします。

```
[SwitchC-vlan100] igmp-snooping enable
[SwitchC-vlan100] igmp-snooping drop-unknown
[SwitchC-vlan100] quit
```

4)　Switch D を設定します。

グローバルに IGMP snooping を有効にします。

```
<SwitchD> system-view
[SwitchD] igmp-snooping
[SwitchD-igmp-snooping] quit
```

VLAN 100 を作成し、この VLAN に GigabitEthernet 1/0/1～GigabitEthernet 1/0/2 を割り当てます。

```
[SwitchD] vlan 100
[SwitchD-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/2
```

VLAN 100 で IGMP Snooping を有効にし、未知のマルチキャストデータ廃棄機能を有効にします。

```
[SwitchD-vlan100] igmp-snooping enable
[SwitchD-vlan100] igmp-snooping drop-unknown
[SwitchD-vlan100] quit
```

III. 設定の確認

Switch B で IGMP snooping を通して学習した IGMP メッセージと PIMv2 メッセージの統計情報を表示します。

```
[SwitchB] display igmp-snooping statistics
Received IGMP general queries:  3
Received IGMPv1 reports:  0
Received IGMPv2 reports:  12
Received IGMP leaves:  0
Received IGMPv2 specific queries:  0
Sent     IGMPv2 specific queries:  0
Received IGMPv3 reports:  0
Received IGMPv3 reports with right and wrong records:  0
Received IGMPv3 specific queries:  0
Received IGMPv3 specific sg queries:  0
Sent     IGMPv3 specific queries:  0
Sent     IGMPv3 specific sg queries:  0
Received PIMv2 hello:  0
Received error IGMP messages:  0
```

出力は、Switch A が IGMP snooping クエリアとして動作したのち、Switch A を除くすべての Switch が IGMP general クエリを受信することができます。

2.11.4 VLAN ベースの IGMP snooping プロキシー機能の設定例

I. ネットワーク要件

図 2-7に示すように、Router A は IGMPv2 を動作させ、IGMP クエリアとして動作します。Switch A は IGMPv2 snooping を動作させます。Switch A が以下の動作を行うため、IGMP snooping プロキシー機能の設定を行います。

- IGMP report、IGMP leave メッセージを Router A に転送します。
- Router A に送信された IGMP クエリに応答し、下流のホストにクエリを転送します。

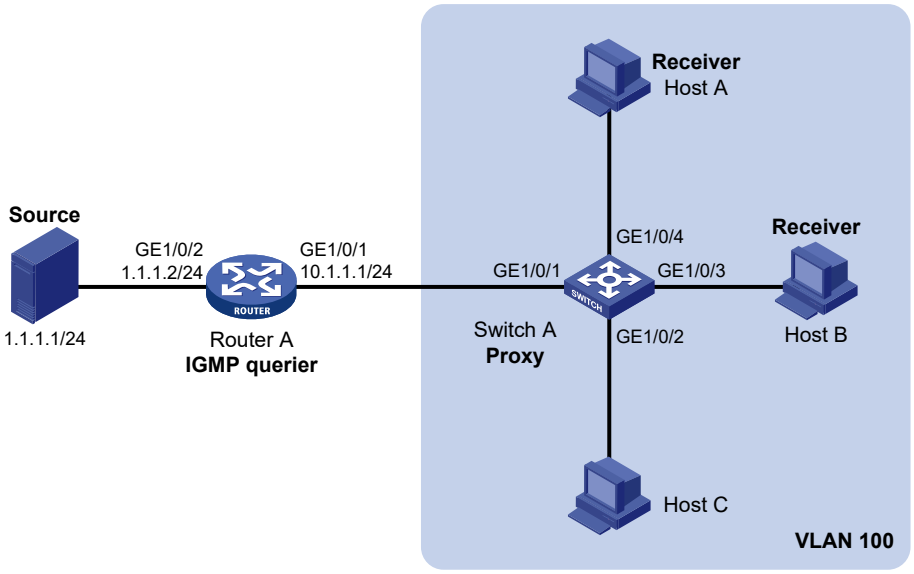


図 2-7 ネットワーク図

II. 設定手順

1) 図 2-7に対応する各インタフェースに IP アドレスとサブネットマスクを割り当てます。（詳細は省略します）
2) Router A を設定します。

IP マルチキャストルーティングを有効にします。

```
<RouterA> system-view
[RouterA] multicast routing
[RouterA-mrib] quit
```

GigabitEthernet 1/0/1 で IGMP を有効にし、PIM-SM を有効にします。

```
[RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] igmp enable
[RouterA-GigabitEthernet1/0/1] pim sm
```

```
[RouterA-GigabitEthernet1/0/1] quit
```

GigabitEthernet 1/0/2 で PIM-SM を有効にします。

```
[RouterA] interface gigabitethernet 1/0/2
[RouterA-GigabitEthernet1/0/2] pim sm
[RouterA-GigabitEthernet1/0/2] quit
```

3)　Switch A を設定します。

グローバルに IGMP snooping を有効にします。

```
<SwitchA> system-view
[SwitchA] igmp-snooping
[SwitchA-igmp-snooping] quit
```

VLAN 100 を作成し、この VLAN に GigabitEthernet 1/0/1～GigabitEthernet 1/0/4 を割り当てます。

```
[SwitchA] vlan 100
[SwitchA-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/4
```

VLAN 100 で IGMP snooping、IGMP snooping プロキシー機能を有効にします。

```
[SwitchA-vlan100] igmp-snooping enable
[SwitchA-vlan100] igmp-snooping proxy enable
[SwitchA-vlan100] quit
```

III. 設定の確認

Host A と Host B からマルチキャストグループ 224.1.1.1 に加入するため、IGMP report を送信します。（詳細は省略します。）

Switch A でダイナミック IGMP snooping グループエントリの情報を表示します。

```
[SwitchA] display igmp-snooping group
 Total 1 entries.

VLAN 100: Total 1 entries.
  (0.0.0.0, 224.1.1.1)
    Host ports (2 in total):
      GE1/0/3                                  (00:04:00)
      GE1/0/4                                  (00:04:04)
```

出力は、Switch C の GigabitEthernet 1/0/3 と GigabitEthernet 1/0/4 がマルチキャストグループ 224.1.1.1 のメンバポートになっていることを示します。Host A と Host B はグループのマルチキャストデータを受信することができます。

Router A の IGMP グループエントリの情報を表示します。

```
[RouterA] display igmp group
IGMP groups in total: 1
 GigabitEthernet1/0/1(10.1.1.1):
  IGMP groups reported in total: 1
   Group address   Last reporter   Uptime      Expires
   224.1.1.1       0.0.0.0         00:00:31    00:02:03
```

Host A からマルチキャストグループ 224.1.1.1 から削除するため、IGMP leave メッセージを送信します。（詳細は省略します。）

Switch A で IGMP snooping グループメンバシップの情報を表示します。

```
[SwitchA] display igmp-snooping group
Total 1 entries.

VLAN 100: Total 1 entries.
  (0.0.0.0, 224.1.1.1)
    Host ports (1 in total):
      GE1/0/3                                  ( 00:01:23 )
```

出力では、GigabitEthernet 1/0/3（Host A に接続されています）はマルチキャストグループ 224.1.1.1 のエントリから削除されていることを示します。

2.12 IGMP snoopingのトラブルシューティング

2.12.1 レイヤ 2 マルチキャスト転送ができない

I. 症状

装置でレイヤ 2 マルチキャスト転送ができません。

II. 分析

IGMP snooping が有効になっていません。

III. 解決策

1) IGMP snooping 情報を表示するため **display igmp-snooping** コマンドを使用します。
2) IGMP snooping が有効になっていない場合、グローバルで **igmp-snooping** コマンドを使用して IGMP snooping を有効にし、VLAN view で **igmp-snooping enable** コマンドを使用して IGMP snooping を有効にしてください。
3) グローバルで IGMP snooping が有効で、対応する VLAN で IGMP snooping が無効になっている場合、対応する VLAN の VLAN view 上で **igmp-snooping enable** コマンドを使用して IGMP snooping を有効にしてください。
4) 問題が解決しない場合、NEC に問い合わせてください。

2.12.2 マルチキャストグループポリシーが動作しない

I. 症状

マルチキャストポリシーによって許可されていないマルチキャストグループから、ホストがマルチキャストデータを受信できません。

II. 分析

- ACL ルールの設定が間違っています。

- マルチキャストグループポリシーが正しく適用されていません 。
- 未知のマルチキャストデータ廃棄機能が無効で、マルチキャストデータがフラッディングしています。

III. 解決策

1) **display acl** コマンドで ACL ルールの設定を確認してください。実行するマルチキャストグループポリシーに ACL ルールが一致していることを確認してください。
2) **display this** コマンドを IGMP snooping view または対応するポートの interface view で使用して、マルチキャストグループポリシーが正しく適用されているかどうかを確認してください。適用されていない場合、**group-policy** または **igmp-snooping group-policy** コマンドでマルチキャストグループポリシーを正しく適用してください。
3) **display igmp-snooping** コマンドを使用して、未知のマルチキャストデータ廃棄機能が有効になっているかどうか確認してください。有効になっていない場合、**igmp-snooping drop-unknown** コマンドを使用して未知のマルチキャストデータ廃棄機能を有効にしてください。
4) 問題が解決しない場合、NEC に問い合わせてください。

目次

このセクションのページは**5-x-x** です。

3 章 MLD スヌーピング 3-1
3.1 概要 3-1
3.1.1 MLD snooping のポート 3-1
3.1.2 MLD snooping の動作 3-3
3.1.3 MLD snooping プロキシー機能 3-5
3.2 プロトコルと標準 3-6
3.3 VLAN ベースの MLD snooping 設定作業リスト 3-6
3.4 MLD snooping の基本機能の設定 3-7
3.4.1 MLD snooping の有効化 3-7
3.4.2 MLD snooping のバージョンの設定 3-8
3.4.3 MLD snooping 転送エントリの最大数の設定 3-8
3.4.4 MLD last listener クエリ間隔の設定 3-9
3.5 MLD snooping のポート機能の設定 3-10
3.5.1 ダイナミックポートのエージングタイマの設定 3-10
3.5.2 スタティックポートの設定 3-11
3.5.3 シミュレーティッドメンバホストのポート設定 3-11
3.5.4 fast-leave 処理の有効化 3-12
3.6 MLD snooping クエリアの設定 3-13
3.6.1 設定要件 3-13
3.6.2 MLD snooping クエリアの有効化 3-13
3.6.3 MLD general クエリと response のパラメータの設定 3-13
3.7 MLD メッセージのパラメータの設定 3-14
3.7.1 設定要件 3-14
3.7.2 MLD メッセージの送信元 IPv6 アドレスの設定 3-15
3.7.3 MLD メッセージの 802.1p 優先度の設定 3-16
3.8 MLD snooping ポリシーの設定 3-17
3.8.1 IPv6 マルチキャストグループポリシーの設定 3-17
3.8.2 IPv6 マルチキャストソースポートフィルタの有効化 3-18
3.8.3 未知の IPv6 マルチキャストデータ廃棄機能の有効化 3-18
3.8.4 MLD report 抑制機能の有効化 3-19
3.8.5 ポートの IPv6 マルチキャストグループの最大数の設定 3-19
3.8.6 IPv6 マルチキャストグループ置き換え機能の有効化 3-20
3.9 MLD snooping の表示と維持 3-21
3.10 MLD snooping 設定例 3-22
3.10.1 VLAN ベースの IPv6 グループポリシーとシミュレーティッドメンバホスト設定例 3-22
3.10.2 VLAN ベースのスタティックポート設定例 3-24
3.10.3 VLAN ベースの MLD snooping クエリア設定例 3-28
3.11 MLD snooping のトラブルシューティング 3-31
3.11.1 レイヤ 2 マルチキャスト転送ができない 3-31
3.11.2 IPv6 マルチキャストグループポリシーが動作しない 3-31

3章 MLD スヌーピング

3.1 概要

MLD snooping は IPv6 マルチキャスト転送時のネットワークへの負荷を軽減するためのメカニズムです。

図 3-1に示すように MLD snooping を有効にしない場合、IPv6 マルチキャストパケットはすべてのホストにフラッディングされます。MLD snooping を有効にする場合、装置は既知の IPv6 マルチキャストグループからのマルチキャストパケットを Receiver のみに転送します。MLD snooping を有効にすることで、不要なマルチキャストトラフィックのフラッディングを抑止し、ネットワークを効率的に利用することができます。

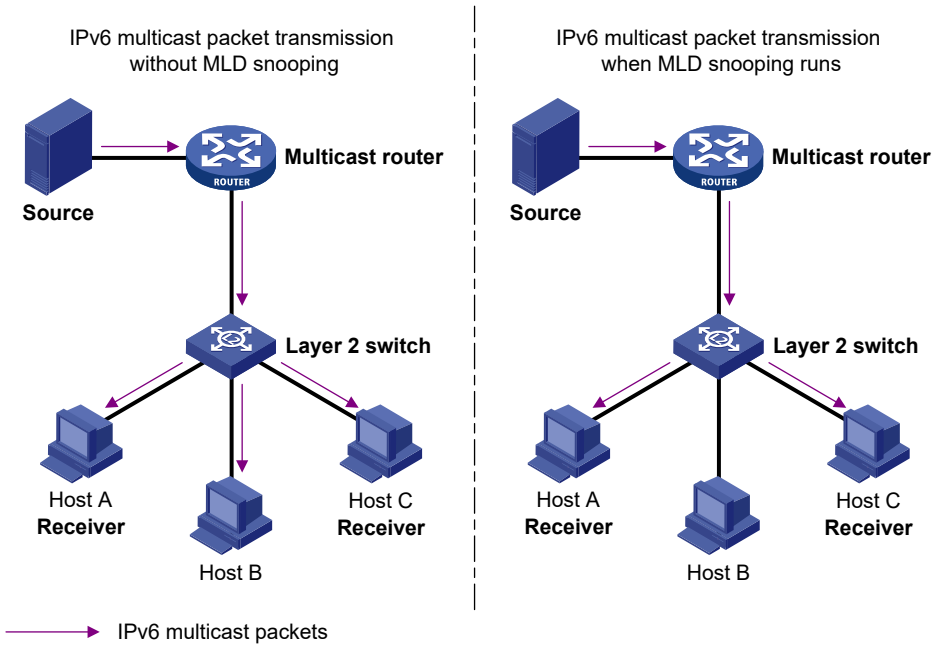


図 3-1 MLD snooping が無効な場合と有効にした場合のマルチキャストパケットの転送処理

3.1.1 MLD snooping のポート

図 3-2に示すように、MLD snooping は Switch A と Switch B で動作します。Host A と Host C は IPv6 マルチキャストグループ内のレシーバホストです。MLD snooping のポートはメンバポートとルータポートに分類されます。

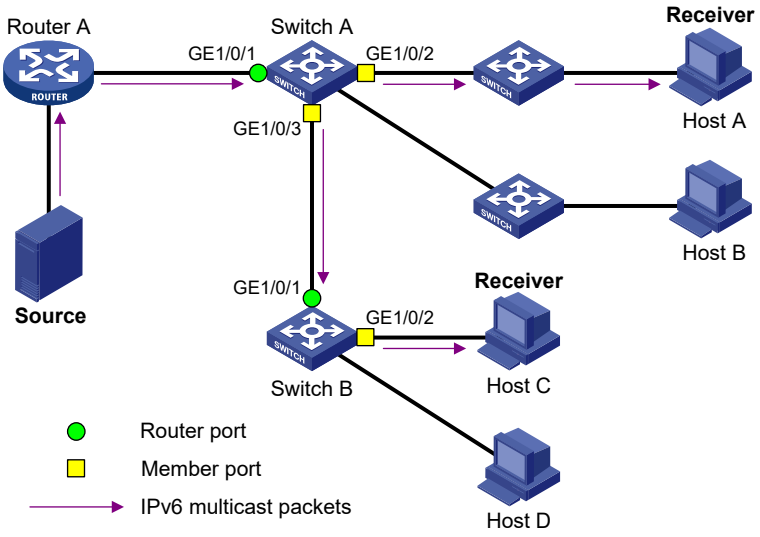


図 3-2 MLD snooping 関連ポート

I. ルータポート

MLD snooping のレイヤ 2 装置で、レイヤ 3 マルチキャストへのポートはルータポートと呼ばれます。図 3-2では、Switch A の GigabitEthernet 1/0/1 と Switch B の GigabitEthernet 1/0/1 がルータポートです。

ルータポートは以下のタイプがあります。

- **ダイナミックルータポート**－ポートで 0::0 以外の送信元アドレスの MLD general クエリあるいは IPv6 PIM Hello メッセージを受信した場合、ダイナミックルータポートリストにポートを追加します。同時にポートのタイマを開始します。タイマが満了する前にメッセージを受信しない場合、ポートはダイナミックルータポートリストからポートを削除します。
- **スタティックルータポート**－ポートがルータポートとしてスタティックに設定された場合、スタティックルータポートリストにポートを追加します。スタティックルータポートはエージアウトしません。手動でのみ削除することができます。

MLD snooping のルータポートをレイヤ 3 インタフェースのルーテッドインタフェースと混同しないでください。MLD snooping のルータポートはレイヤ 2 インタフェースです。

II. メンバポート

MLD snooping のレイヤ 2 装置で、マルチキャストレシーバへのポートはメンバポートと呼ばれます。図 3-2では、Switch A の GigabitEthernet 1/0/2 と GigabitEthernet 1/0/3、Switch B の GigabitEthernet 1/0/2 がメンバポートです。

メンバポートは以下のタイプがあります。

- **ダイナミックメンバポート**－ポートが MLD report をした場合、出力インタフェースとして関連づけられたダイナミック MLD snooping 転送エントリに追加されます。同時にポートのタイマを開始します。タイマが満了する前にメッセージを受信しない場合、ポートはダイナミック転送エントリからからポートを削除します。

- **スタティックメンバポート**－ポートがメンバポートとしてスタティックに設定された場合、出力インタフェースとして関連づけられたスタティック MLD snooping 転送エントリに追加されます。スタティックメンバポートはエージアウトしません。手動でのみ削除することができます。

特に指定しない限り、この章のルータポート、メンバポートはダイナミック、スタティックの両方を示します。

3.1.2 MLD snooping の動作

この章のポートはダイナミックポートです。スタティックポートの設定、削除方法については、オペレーションマニュアルのセクション 5 *マルチキャスト”MLD スヌーピング*”の”*スタティックポートの設定*”を参照してください。

MLD メッセージのタイプは、general クエリ、MLD report、done メッセージを含みます。MLD snooping が有効なレイヤ 2 装置は、受信した MLD メッセージによってそれぞれ異なる動作をします。

I. General クエリ

MLD クエリアは、IPv6 マルチキャストグループメンバが存在するかどうかを調べるために、ローカルサブネット上のすべてのホストとルータへ MLD general クエリを定期的に送信します。

MLD general クエリを受信すると、装置は受信したポート以外の VLAN 内のすべてのポートへクエリメッセージを転送します。装置は以下のアクションの 1 つを実行します。

- 受信ポートがルータポートリストに存在するルータポートの場合、装置はこのルータポートのエージングタイマを再起動します。
- 受信ポートがルータポートリストに存在しない場合、装置はその受信ポートをルータポートリストに追加し、このルータポートのエージングタイマを開始します。

II. MLD report

ホストは以下の目的により MLD report を MLD クエリアへ送信します。

- ホストが IPv6 マルチキャストグループメンバである場合、クエリに応答します。
- IPv6 マルチキャスト membership を適用します。

ホストから MLD report を受信すると、装置は VLAN 内のすべてのルータポートから report を転送し、報告された IPv6 マルチキャストグループの IPv6 アドレスを解決します。そして、エントリに一致するかどうか転送テーブルを検索します。

- 転送テーブルエントリが存在しない場合、装置はエントリを作成して、受信したポートを転送エントリにダイナミックメンバポートとして追加します。そして、そのポートでメンバポートエージングタイマを起動します。
- 転送テーブルエントリは存在するが、そのグループの発信ポートリストにポートが含まれていない場合、装置はポートをダイナミックメンバポートとして転送エントリに追加し、そのポートのメンバポートエージングタイマを起動します。
- 転送テーブルエントリが存在し、転送エントリに受信ポートが含まれている、つまりこの受信ポートが既にメンバポートである場合、装置はそのポートのメンバポートエージングタイマを再起動します。

MLD snooping が有効な装置で IPv6 マルチキャストグループポリシーの設定がある状況で、ユーザが IPv6 マルチキャストプログラムをリクエストした場合、ユーザのホストは MLD report を初期化します。このレポートを受信した後、装置はレポートの IPv6 マルチキャストグループアドレスを解決し、ポートの ACL フィルタリングを実行します。MLD report が ACL フィルタリングにパスした場合、装置は出力インタフェースが受信ポートの IPv6 マルチキャストグループの MLD snooping 転送エントリを作成します。MLD report が ACL フィルタリングにパスしない場合、装置は MLD report メッセージを廃棄します。Receiver が IPv6 マルチキャストグループに加入できず、ユーザはグループアドレス解決を行うことができません。

装置は、MLD report 抑制メカニズムによって MLD report を非ルータポートから転送することはありません。

III. Done メッセージ

ホストが IPv6 マルチキャストグループを離脱する場合、ホストは IPv6 マルチキャストルータに MLD done メッセージを送信します。装置がダイナミックメンバポートで MLD done メッセージを受信した場合、装置は最初にメッセージの IPv6 マルチキャストグループアドレスに一致する転送エントリが存在するかどうかを確認します。

- 転送テーブルエントリが存在しない場合、装置は MLD done メッセージを廃棄します。
- 転送テーブルエントリに存在するが、受信ポートが転送エントリに含まれていない場合、装置は MLD done メッセージを廃棄します。
- 転送テーブルエントリが存在し、受信ポートが唯一の転送エントリの出力インタフェースでない場合、以下の処理を行います。
  - MLD done メッセージを廃棄します。
  - グループに受信ポートに接続されたアクティブな Receiver があるかどうかを確認するため、MLD multicast-address-specific クエリを送信します
  - 受信ポートのエージングタイマを MLD last member クエリ間隔の 2 倍に設定します。
- 転送テーブルエントリが存在し、受信ポートが唯一の転送エントリの出力インタフェースである場合、以下の処理を行います。
  - VLAN のすべてのルータポートに MLD done メッセージを転送します。
  - グループに受信ポートに接続されたアクティブな Receiver があるかどうかを確認するため、MLD multicast-address-specific クエリを送信します。
  - 受信ポートのエージングタイマを MLD last member クエリ間隔の 2 倍に設定します。

ポートで MLD done メッセージを受信すると、MLD クエリアはメッセージの IPv6 マルチキャストグループのアドレスを解決します。そして、受信ポートを通して IPv6 マルチキャストグループに MLD multicast-address-specific クエリを送信します。

MLD multicast-address-specific クエリを受信したのち、装置は VLAN のグループのすべてのルータポートとメンバポートを通して、クエリを転送します。直接接続されているホストから MLD report の応答を待ちます。done メッセージを受信したダイナミックメンバポートは以下のアクションの 1 つを実行します。

- エージングタイマが満了する前にポートが MLD report を受信した場合、装置はポートのエージングタイマをリセットします。
- エージングタイマが満了しても MLD report を受信しない場合、装置は IPv6 マルチキャストグループの転送エントリからポートを削除します。

3.1.3 MLD snooping プロキシー機能

図 3-3に示すように、上流装置で受信される MLD report メッセージ、MLD done メッセージの数を削減する場合、エッジ装置で MLD snooping プロキシー機能を有効にします。MLD snooping プロキシー機能を有効にした場合、MLD report メッセージ、MLD done メッセージを Router A に送信するため、上流の MLD snooping クエリアのエッジ装置はホストとして動作します。エッジ装置でホスト MLD report の抑制メカニズムは適用しません。

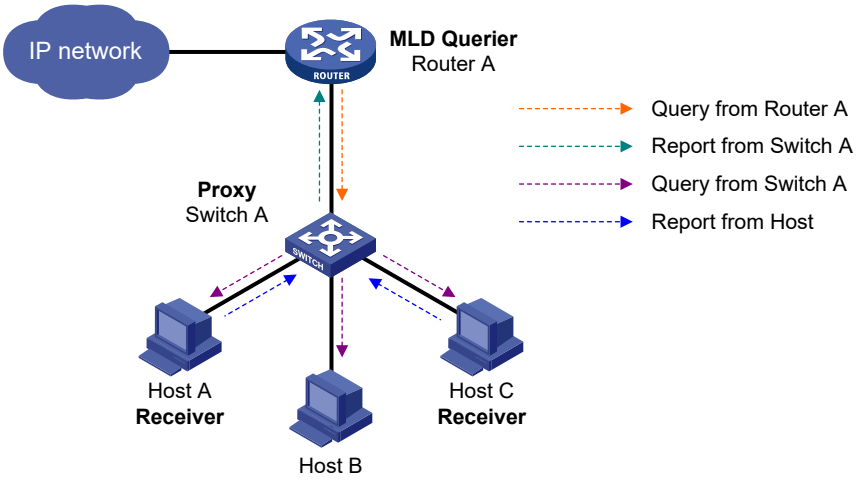


図 3-3 MLD snooping プロキシー機能

MLD snooping プロキシー機能が有効な装置は異なる MLD メッセージを処理します。

- General クエリ

MLD general クエリを受信したのち、装置は受信ポートを除く VLAN のすべてのポートにクエリを転送します。装置はローカルメンバシップ情報をもとにして MLD report を作成し、すべてのルータポートに送信します。

- Group-specific クエリあるいは group-and-source-specific クエリ

MLD group-specific クエリ あるいは MLD group-and-source-specific クエリを受信したのち、装置は受信ポートを除く VLAN のすべてのポートにクエリを転送します。転送エントリにメンバポートがある場合、装置は VLAN のすべてのルータポートに report を送信します。

- Report

ホストから MLD report を受信したのち、装置は以下のように一致するエントリを転送テーブルから検索します。

  - エントリが一致し、転送エントリに受信ポートを含んでいる場合、装置はポートのエージングタイマをリセットします。
  - エントリが一致するが、転送エントリに受信ポートが含まれない場合、装置は出力インタフェースリストに受信ポートを追加します。そして受信ポートをダイナミックメンバポートとしてマーキングし、ポートのエージングタイマを開始します。
  - エントリが一致しない場合、装置は出力インタフェースを受信ポートとして転送エントリを作成します。受信ポートをダイナミックメンバポートとしてマーキン

グし、ポートのエージングタイマを開始します。そしてすべてのルータポートに report を送信します。

- Done メッセージ

ポートで MLD done メッセージを受信したのち、装置は受信ポートを通して MLD multicast-address-specific を送信します。last メンバポートが転送エントリから削除された場合のみ、すべてのルータポートに MLD done メッセージを送信します。

3.2 プロトコルと標準

RFC 4541, *Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches*

3.3 VLANベースのMLD snooping設定作業リスト

作業リスト
MLD snoopingの基本機能の設定： ● （必須設定項目） MLD snoopingの有効化 ● （オプション設定項目） MLD snoopingのバージョンの設定 ● （オプション設定項目） MLD snooping転送エントリの最大数の設定 ● （オプション設定項目）MLD last listener クエリ間隔の設定
MLD snoopingのポート機能の設定： ● （オプション設定項目） ダイナミックポートのエージングタイマの設定 ● （オプション設定項目） スタティックポートの設定 ● （オプション設定項目） シミュレーティッドメンバホストのポート設定 ● （オプション設定項目） fast-leave処理の有効化
MLD snoopingクエリアの設定： ● （オプション設定項目） MLD snoopingクエリアの有効化 ● （オプション設定項目） MLD クエリとresponseのパラメータの設定
MLDメッセージのパラメータの設定： ● （オプション設定項目） MLDメッセージの送信元IPv6アドレスの設定 ● （オプション設定項目） MLDメッセージの802.1p優先度の設定
MLD snoopingポリシーの設定： ● （オプション設定項目） IPv6マルチキャストグループポリシーの設定 ● （オプション設定項目） IPv6マルチキャストソースポートフィルタの有効化 ● （オプション設定項目） 未知のIPv6マルチキャストデータ廃棄機能の有効化 ● （オプション設定項目） MLD report 抑制機能の有効化 ● （オプション設定項目） ポートのIPv6マルチキャストグループの最大数の設定 ● （オプション設定項目） IPv6マルチキャストグループ置き換え機能の有効化

レイヤ 2 アグリゲートインタフェースで設定された MLD snooping の設定は、メンバポートの設定に影響しません。また、アグリゲーションの計算にも参加しません。アグリゲー

トグループのメンバポートでの設定は、アグリゲートグループから離脱するまで有効になりません。

3.4 MLD snoopingの基本機能の設定

MLD snooping の基本機能の設定をする前に、以下の作業を完了させてください。

- 対応する VLAN を設定してください。
- MLD snooping のバージョンを定義してください。
- MLD last-member クエリの間隔を定義してください。
- MLD クエリの最大応答時間を定義してください。

3.4.1 MLD snooping の有効化

MLD snooping を有効にする場合、以下のガイドラインに従ってください。

- VLAN で MLD snooping を有効にする前に、グローバルで有効にしてください。
- VLAN 用の MLD snooping は、VLAN のメンバポートでのみ動作します。
- MLD snooping は MLD-snooping view あるいは VLAN view のどちらかで設定することができます。MLD-snooping view での設定と VLAN view での設定は同じ優先度を持ちます。

I. MLD-snooping view での VLAN の MLD snooping の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. MLD snooping をグローバルで有効にし、MLD-snooping view に移行する	**mld-snooping**	デフォルト：無効
3. 指定した VLAN で MLD snooping を有効にする	**enable vlan** *vlan-list*	デフォルト：無効

II. VLAN view での VLAN の MLD snooping の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. MLD snooping をグローバルで有効にし、MLD-snooping view に移行する	**mld-snooping**	デフォルト：無効
3. system view に戻る	**quit**	―
4. VLAN view に移行する	**vlan** *vlan-id*	―
5. VLAN での MLD snooping を有効にする	**mld-snooping enable**	デフォルト：無効

3.4.2 MLD snooping のバージョンの設定

MLD snooping のバージョンが異なると、異なるバージョンの MLD メッセージの処理を行います。

- MLDv1 snooping は、MLDv1 メッセージと MLDv2 クエリを処理できますが、MLDv2 report を処理する代わりに VLAN 内でフラッディングします。
- MLDv2 snooping は MLDv1 および MLDv2 メッセージを処理することができます。

MLDv2 snooping を MLDv1 snooping に変更する場合、装置は以下のことを行います。

- ダイナミックに作成されたすべての MLD snooping 転送エントリを削除します。
- MLDv2 snooping スタティック（* , G）の転送エントリは維持します。
- MLDv2 snooping スタティック（S , G）の転送エントリは削除します。MLD snooping が MLDv2 snooping に切り替わった場合復元されます。

スタティック MLD snooping 転送エントリの詳細は、オペレーションマニュアルのセクション 5 *マルチキャスト”MLD スヌーピング”の”スタティックポートの設定”*を参照してください。

MLD snooping のバージョンは MLD-snooping view あるいは VLAN view のどちらかで設定することができます。MLD-snooping view での設定と VLAN view での設定は同じ優先度を持ちます。

以下に MLD-snooping view での MLD snooping のバージョンの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. MLD snooping をグローバルで有効にし、MLD-snooping view に移行する.	**mld-snooping**	―
3. 指定した VLAN で MLD snooping のバージョンを指定する	**version** *version-number* **vlan** *vlan-list*	デフォルト：1

以下に VLAN view での MLD snooping のバージョンの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. VLAN view に移行する	**vlan** *vlan-id*	―
3. VLAN で MLD snooping のバージョンを指定する	**mld-snooping version** *version-number*	デフォルト：1

3.4.3 MLD snooping 転送エントリの最大数の設定

MLD snooping 転送エントリの最大数を変更することができます。転送エントリはダイナミックエントリとスタティックエントリの両方が含まれます。装置の転送エントリ数が上限に達すると、装置はいくつかのエントリがタイムアウトするか、手動で削除されるまで転送エントリを作成することができません。この場合、手動でエントリを削除することを推奨します。

以下に MLD snooping 転送エントリの最大数の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． MLD-snooping view に移行する	**mld-snooping**	―
3． MLD snooping 転送エントリの最大数を設定する	**entry-limit** *limit*	デフォルト：4294967295

3.4.4 MLD last listener クエリ間隔の設定

IPv6 マルチキャストグループの MLD multicast-address-specific クエリを受信すると、レシーバホストは参加した各 IPv6 マルチキャストグループのタイマを起動します。このタイマは、0 から最大応答時間の範囲でランダムな値に初期化されます。タイマ値が経過して 0 になった場合に、ホストは対応する IPv6 マルチキャストグループに MLD report を送信します。

MLD last listener クエリ間隔は、MLD multicast-address-specific クエリの配信された最大応答時間を定義します。MLD last listener クエリの時間を適切に設定すると、ホストは速やかに MLD multicast-address-specific クエリに応答できます。また、対応するタイマの期限が多数のホストで同時に切れた場合に同時に送信する report によってネットワーク上で発生する MLD report トラフィックのバーストを回避することもできます。

I. 設定の制限とガイドライン

MLD last listener クエリ間隔を設定する場合、以下の制限とガイドラインに従ってください。

- fast-leave 処理が有効なポートから MLD done メッセージを受信した場合、装置は MLD multicast-address-specific クエリを送信しません。
- MLD-snooping view のすべての VLAN、あるいは VLAN view の VLAN でグローバルに MLD last listener クエリの間隔を設定することができます。VLAN で行った設定はグローバルで行った設定よりも優先されます。

II. グローバルでの MLD クエリと response のパラメータの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． MLD-snooping view に移行する	**mld-snooping**	―
3． MLD last listener クエリ間隔を設定する	**last-listener-query-interval** *interval*	デフォルト：1秒

III. VLAN での MLD クエリと response のパラメータの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． MLD-snooping view に移行する	**mld-snooping**	―
3． MLD last listener クエリ間隔を設定する	**mld-snooping** **last-listener-query-interval** *interval*	デフォルト：1秒

3.5 MLD snoopingのポート機能の設定

MLD snooping のポート機能の設定をする前に、以下の作業を完了させてください。

- VLAN で MLD snooping を有効にしてください。
- ダイナミックルータポートのエージングタイマを定義してください。
- ダイナミックメンバポートのエージングタイマを定義してください。
- IPv6 マルチキャストグループと IPv6 マルチキャストソースのアドレスを定義してください。

3.5.1 ダイナミックポートのエージングタイマの設定

ダイナミックポートのエージングタイマを設定する場合、以下の制限とガイドラインに従ってください。

- IPv6 マルチキャストグループメンバシップが頻繁に変更される場合は、メンバポートのエージングタイマに比較的小さな値を設定します。IPv6 マルチキャストグループメンバシップがほとんど変更されない場合は、メンバポートのエージングタイマに比較的大きな値を設定します。
- ダイナミックルータポートが IPv6 PIMv2 hello メッセージを受信した場合、ダイナミックポートのエージングタイマの時間は、hello メッセージで指定された時間となります。**mld-snooping router-aging-time** コマンドの設定は適用されません。
- 装置が開始した MLD multicast-address-specific クエリによってダイナミックメンバポートのエージングタイマの調整を行います。ダイナミックメンバポートがクエリを受信した場合、エージングタイマは MLD last listener クエリ間隔の 2 倍に設定されます。
- ダイナミックポートのエージングタイマの設定は、VLAN view あるいは MLD-snooping view のどちらかに設定することができます。VLAN view と MLD-snooping view の両方に設定がある場合、VLAN view の設定が適用されます。

I. グローバルでのダイナミックポートのエージングタイマの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. MLD-snooping view に移行する	**mld-snooping**	—
3. グローバルでのダイナミックルータポートのエージングタイマを設定する	**router-aging-time** *seconds*	デフォルト：260秒
4. グローバルでのダイナミックメンバポートのエージングタイマを設定する	**host-aging-time** *seconds*	デフォルト：260秒

II. VLAN でのダイナミックポートのエージングタイマの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. VLAN view に移行する	**vlan** *vlan-id*	―
3. VLAN でのダイナミックルータポートのエージングタイマを設定する	**mld-snooping router-aging-time** *seconds*	デフォルト：260秒
4. VLAN でのダイナミックメンバポートのエージングタイマを設定する	**mld-snooping host-aging-time** *seconds*	デフォルト：260秒

3.5.2 スタティックポートの設定

以下のタイプのスタティックポートを設定することができます。

- **スタティックメンバポート**－IPv6 マルチキャストグループのスタティックメンバポートとしてポートを設定する場合、ポートに所属されたすべてのホストはグループの IPv6 マルチキャストデータを受信します。

  スタティックメンバポートは MLD クエリに応答しません。設定あるいは設定を取り消す場合、ポートは unsolicited MLD report や done メッセージを送信しません。
- **スタティックルータポート**－IPv6 マルチキャストグループのスタティックルータポートとしてポートを設定する場合、ポートで受信されたグループのすべての IPv6 マルチキャストデータは転送されます。

以下にスタティックポートの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Ethernet interface view あるいは aggregate interface view に移行する.	**interface** *interface-type interface-number*	―
3. ポートをスタティックポートに設定する	• ポートをスタティックメンバポートに設定する：**mld-snooping static-group** *ipv6-group-address* [**source-ip** *ipv6-source-address*] **vlan** *vlan-id* • ポートをスタティックルータポートに設定する：**mld-snooping static-router-port vlan** *vlan-id*	デフォルト：設定なし

3.5.3 シミュレーティッドメンバホストのポート設定

ポートがシミュレーティッドメンバホストとして設定される場合、以下に示す独立したホストと同等になります。

- 設定が完了した場合、unsolicited MLD report を送信します。
- MLD report の MLD general クエリに応答します。

- 設定を削除した場合、MLD done メッセージを送信します。

この操作を実行する場合､シミュレーティッドホストの MLD バージョンと MLD snooping バージョンが同一であることを確認してください。スタティックメンバポートと異なり、シミュレーティッドメンバホストとして設定されたポートはダイナミックメンバポートと同様にエージアウトします。

以下にシミュレーティッドメンバホストの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． Layer 2 Ethernet interface view あるいは aggregate interface view に移行する.	**interface** *interface-type interface-number*	―
3． シミュレーティッドメンバホストとしてポートを設定する	**mld-snooping host-join** *ipv6-group-address* [**source-ip** *ipv6-source-address*] **vlan** *vlan-id*	デフォルト：設定なし

3.5.4 fast-leave 処理の有効化

fast-leave 処理を有効にすることで、ポートが done メッセージを受信すると、IPv6 マルチキャストグループの転送エントリからポートをすぐに削除することができます。

I. 設定の制限とガイドライン

fast-leave 処理を有効にする場合、以下の制限とガイドラインに従ってください。

- VLAN に所属した複数のレシーバホストが接続されているポートでは有効にしないでください。これを行うと、同じ IPv6 マルチキャストグループにあるポートに接続された他のレシーバのホストは IPv6 マルチキャストデータを受信することができません。
- interface view での現在のポート、あるいはグローバルでのすべてのポートで fast-leave 処理を有効にすることができます。interface view と MLD-snooping view の両方に設定がある場合、interface view の設定が適用されます。

II. グローバルでの fast-leave 処理の有効化

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． MLD-snooping view に移行する	**mld-snooping**	―
3． グローバルで fast-leave 処理を有効にする	**fast-leave** [**vlan** *vlan-list*]	デフォルト：無効

III. ポートでの fast-leave 処理の有効化

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． Ethernet interface view あるいは aggregate interface view に移行する.	**interface** *interface-type interface-number*	―

操作	コマンド	補足
3． ポートで fast-leave 処理を有効にする	**mld-snooping fast-leave** [**vlan** *vlan-list*]	デフォルト：無効

3.6 MLD snoopingクエリアの設定

この項では MLD snooping クエリアを設定する方法を記載します。

3.6.1 設定要件

VLAN の MLD snooping クエリアを設定する前に、以下の作業を完了してください。

- VLAN で MLD snooping を有効にしてください。
- MLD general クエリの間隔を定義してください。
- MLD general クエリの最大応答時間を定義してください。

3.6.2 MLD snooping クエリアの有効化

この機能は、データリンクレイヤで IPv6 マルチキャスト転送エントリを確立、維持するために、装置が MLD general クエリを定期的に送信します。レイヤ 3 マルチキャスト装置がないネットワークで MLD snooping クエリアを設定することができます。

MLD が動作する IPv6 マルチキャストネットワークで MLD snooping クエリアを有効にしないでください。MLD snooping クエリアは、MLD クエリアの選択に関与しませんが、小さい送信元 IPv6 アドレスで MLD general クエリを送信する場合、MLD クエリアの選択に影響する可能性があります。

以下に VLAN で MLD snooping クエリアを有効にする設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． VLAN view に移行する	**vlan** *vlan-id*	―
3． MLD snooping クエリアを有効にする	**mld-snooping querier**	デフォルト：無効

3.6.3 MLD general クエリと response のパラメータの設定

注意：

MLD general クエリの間隔は、MLD general クエリの最大応答時間よりも大きいことを確認してください。IPv6 マルチキャストグループメンバが誤って削除される可能性があります。

MLD general クエリの間隔を実際のネットワークの状況にもとづいて変更することができます。

MLD general クエリを受信すると、レシーバホストは参加した各 IPv6 マルチキャストグループのタイマを開始します。このタイマは、0 から最大応答時間の範囲でランダムな値に初期化されます。タイマ値が経過して 0 になった場合、ホストは IPv6 マルチキャストグループに MLD report を送信します。

MLD クエリの最大応答時間を適切に設定すると、ホストは速やかにクエリに応答できます。また、対応するタイマの期限が多数のホストで同時に切れた場合に同時に送信する report によってネットワーク上で発生する MLD トラフィックのバーストを回避することもできます。

MLD クエリと応答のパラメータは、VLAN view で現在の view あるは MLD-snooping view ですべての VLAN で設定できます。VLAN view と MLD-snooping view の両方に設定がある場合、VLAN view の設定が適用されます。

I. グローバルでの MLD クエリと response のパラメータの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. MLD-snooping view に移行する	**mld-snooping**	―
3. MLD general クエリの最大応答時間を設定する	**max-response-time** *seconds*	デフォルト：10秒

II. VLAN での MLD クエリと response のパラメータの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. VLAN view に移行する	**vlan** *vlan-id*	―
3. MLD general クエリの送信間隔を設定する	**mld-snooping query-interval** *interval*	デフォルト：125秒
4. MLD general クエリの最大応答時間を設定する	**mld-snooping max-response-time** *seconds*	デフォルト：10秒

3.7 MLDメッセージのパラメータの設定

この章では MLD メッセージのパラメータの設定方法について記載します。

3.7.1 設定要件

VLAN で MLD メッセージのパラメータを設定する前に、以下の作業を完了してください。

- VLAN で MLD snooping を有効にしてください。
- MLD general クエリの送信元 IPv6 アドレスを定義してください。
- MLD multicast-address-specific クエリの送信元 IPv6 アドレスを定義してください。
- MLD report の送信元 IPv6 アドレスを定義してください。

- MLD done メッセージの送信元 IPv6 アドレスを定義してください。
- MLD メッセージの 802.1p 優先度を定義してください。

3.7.2 MLD メッセージの送信元 IPv6 アドレスの設定

MLD snooping クエリアによって送信された MLD クエリの送信元 IPv6 アドレスを変更することができます。この設定はサブネット内の MLD クエリアの選択に影響する可能性があります。

シミュレーティッドメンバホストによって MLD report あるいは MLD done メッセージの送信元 IPv6 アドレスを変更することができます。

以下に VLAN の MLD メッセージの送信元 IPv6 アドレスの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. VLAN view に移行する	**vlan** *vlan-id*	ー
3. MLD general クエリの送信元 IPv6 アドレスを設定する	**mld-snooping general-query source-ip** *ipv6-address*	デフォルト : 現在のVLANインタフェースのIPv6リンクローカルアドレスです。 現在のVLANインタフェースがIPv6リンクローカルアドレスを持っていない場合、送信元IPv6アドレスはFE80::02FF:FFFF:FE00:0001です。
4. MLD multicast-address-specific クエリの送信元 IPv6 アドレスを設定する	**mld-snooping special-query source-ip** *ipv6-address*	デフォルト : 送信元IPv6アドレスは以下のいずれかとなります。 ● MLD snoopingクエリアがMLD general クエリを受信した場合、MLD multicast-address-specific クエリの送信元IPv6アドレスはMLD general クエリのIPv6アドレスです。 ● MLD snoopingクエリアがMLD general クエリを受信しない場合、送信元IPv6アドレスは現在のVLANインタフェースのIPv6リンクローカルアドレスです。 ● 現在のVLANインタフェースにIPv6リンクローカルアドレスが設定されていない場合、送信元IPv6アドレスはFE80::02FF:FFFF:FE00:0001です。

操作	コマンド	補足
5． MLD report の送信元 IPv6 アドレスを設定する	**mld-snooping report source-ip** *ipv6-address*	デフォルト： 現在のVLANインタフェースのIPv6リンクローカルアドレスです。現在のVLANインタフェースがIPv6リンクローカルアドレスを持っていない場合、送信元IPv6アドレスはFE80::02FF:FFFF:FE00:0001です。
6． MLD done メッセージの送信元 IPv6 アドレスを設定する	**mld-snooping done source-ip** *ipv6-address*	デフォルト： 現在のVLANインタフェースのIPv6リンクローカルアドレスです。現在のVLANインタフェースがIPv6リンクローカルアドレスを持っていない場合、送信元IPv6アドレスはFE80::02FF:FFFF:FE00:0001です。

3.7.3 MLD メッセージの 802.1p 優先度の設定

装置の出力ポートで混雑が発生した場合、802.1p 優先度が高い順から MLD メッセージを転送します。装置で作成あるいは転送された MLD メッセージに高い 802.1p 優先度を割り当てることができます。

MLD メッセージの 802.1p 優先度は、MLD-snooping view ですべての VLAN あるいは VLAN view で現在の VLAN で設定できます。VLAN view と MLD-snooping view の両方に設定がある場合、VLAN view の設定が適用されます。

I. グローバルでの MLD メッセージの 802.1p 優先度の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． MLD-snooping view に移行する	**mld-snooping**	―
3． MLD メッセージの 802.1p 優先度を設定する	**dot1p-priority** *priority*	デフォルト：MLDメッセージの802.1p優先度はデフォルトで設定されていません。装置によって作成されるMLDメッセージの優先度は0です。

II. VLAN での MLD メッセージの 802.1p 優先度の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． VLAN view に移行する	**vlan** *vlan-id*	―

操作	コマンド	補足
3． MLD メッセージの 802.1p 優先度を設定する	**mld-snooping dot1p-priority** *priority*	デフォルト：MLDメッセージの802.1p優先度はデフォルトで設定されていません。装置によって作成されるMLDメッセージの優先度は0です。

3.8 MLD snoopingポリシーの設定

MLD snooping ポリシーを設定する前に、以下の作業を完了してください。

- VLAN で MLD snooping を有効にしてください。
- IPv6 マルチキャストグループポリシーとして使用される ACL を定義してください。
- ポートが加入できる IPv6 マルチキャストグループの最大数を定義してください。

3.8.1 IPv6 マルチキャストグループポリシーの設定

この機能は IPv6 マルチキャストグループとオプションソースを指定した ACL をもとにして MLD report をフィルタする装置を有効にします。レシーバホストが加入できる IPv6 マルチキャストグループを管理することに使用されます。

I. 設定の制限とガイドライン

IPv6 マルチキャストグループポリシーを設定する場合に、以下の設定の制限とガイドラインに従ってください。

- 設定はダイナミックにポートが加入する IPv6 マルチキャストグループにのみ適用されます。
- IPv6 マルチキャストポリシーの設定は MLD-snooping view ですべてのポート、あるいは interface view で現在のポートで行うことができます。interface view と MLD-snooping view の両方に設定がある場合、interface view の設定が適用されます。

II. グローバルでの IPv6 マルチキャストグループポリシーの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． MLD-snooping view に移行する	**mld-snooping**	—
3． グローバルで IPv6 マルチキャストグループポリシーを設定する	**group-policy** *ipv6-acl-number* [**vlan** *vlan-list*]	デフォルト：設定なし

III. ポートでの IPv6 マルチキャストグループポリシーの設定

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

操作	コマンド	補足
2． Ethernet interface view あるいは aggregate interface view に移行する.	**interface** *interface-type interface-number*	―
3． ポートで IPv6 マルチキャストグループポリシーを設定する	**mld-snooping group-policy** *ipv6-acl-number* [**vlan** *vlan-list*]	デフォルト：設定なし

3.8.2 IPv6 マルチキャストソースポートフィルタの有効化

この機能は、すべての IPv6 マルチキャストデータパケットの廃棄および IPv6 マルチプロトコルパケットの許可を、装置で設定することができます。IPv6 マルチキャストレシーバに接続されたポートのみ機能を有効にすることができます。

MLD-snooping view で指定されたポートあるいは interface view で現在のポートの IPv6 マルチキャストソースポートフィルタリングを有効にすることができます。MLD-snooping view での設定と interface view での設定の優先度は同一です。

I. グローバルでの IPv6 マルチキャストソースポートフィルタリングの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． MLD-snooping view に移行する	**mld-snooping**	―
3． IPv6 マルチキャストソースポートフィルタリングを有効にする	**source-deny port** *interface-list*	デフォルト：無効

II. ポートでの IPv6 マルチキャストソースポートフィルタリングの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． interface view に移行する	**interface** *interface-type interface-number*	―
3． IPv6 マルチキャストソースポートフィルタリングを有効にする	**mld-snooping source-deny**	デフォルト：無効

3.8.3 未知の IPv6 マルチキャストデータ廃棄機能の有効化

未知の IPv6 マルチキャストデータとは、MLD snooping 転送テーブルにエントリが存在しない IPv6 マルチキャストデータのことです。この機能はすべての未知の IPv6 マルチキャストデータを廃棄します。

この機能が無効である場合、未知の IPv6 マルチキャストデータが所属している VLAN にフラッディングされます。

レイヤ 3 IPv6 マルチキャストパケットの IPv6 マルチキャスト転送エントリの発信ポートが同じ VLAN にある場合、ベストプラクティスとして、VLAN の未知の IPv6 マルチキャストデータの廃棄を有効にします。この制限により、装置が VLAN のレイヤ 3 IPv6 マルチキャストパケットをフラッディングするのを防ぎます。

以下に未知の IPv6 マルチキャストデータ廃棄機能の有効化の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． VLAN view に移行する	**vlan** *vlan-id*	ー
3． 未知の IPv6 マルチキャストデータ廃棄機能を有効にする	**mld-snooping drop-unknown**	デフォルト：無効 未知のIPv6マルチキャストデータはフラッディングします。

3.8.4 MLD report 抑制機能の有効化

この機能を有効にすることで、装置は直接接続されたレイヤ 3 装置に IPv6 マルチキャストグループの最初の MLD report のみ転送します。同じクエリ間隔内の同じグループの他の MLD report は廃棄されます。

以下に MLD report 抑制機能の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． MLD-snooping view に移行する	**mld-snooping**	ー
3． MLD report 抑制を有効にする	**report-aggregation**	デフォルト：有効

3.8.5 ポートの IPv6 マルチキャストグループの最大数の設定

ポートトラフィックを調整するため、ポートでの IPv6 マルチキャストグループの最大数を設定することができます。

I. 設定の制限とガイドライン

ポートの IPv6 マルチキャストグループの最大数を設定する場合、以下の設定の制限とガイドラインに従ってください。

- この設定はダイナミックに IPv6 マルチキャストグループに加入されたポートのみ適用します。
- ポートが参加した IPv6 マルチキャストグループの数が設定されている上限に達した場合、そのポートに残るすべての転送エントリを MLD snooping 転送テーブルから削除します。このポートに接続されたレシーバホストは、上限になる前に、再度 IPv6 マルチキャストグループに参加することができます。

II. 設定手順

以下にポートの IPv6 マルチキャストグループの最大数の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Ethernet interface view あるいは aggregate interface view に移行する.	**interface** *interface-type interface-number*	―
3. ポートの IPv6 マルチキャストグループの最大数を設定する	**mld-snooping group-limit** *limit* [**vlan** *vlan-list*]	デフォルト：4294967295

3.8.6 IPv6 マルチキャストグループ置き換え機能の有効化

この機能は IPv6 マルチキャストグループが上限を超えた場合、装置が既存の IPv6 マルチキャストグループを新規に追加されたグループに置き換えることができます。この機能は一般的にチャンネルスイッチングアプリケーションで使用されます。この機能が無効である場合、装置が新しいグループの MLD report を廃棄し、ユーザが新しいチャンネルに変更することができません。

I. 設定の制限とガイドライン

IPv6 マルチキャストグループ置き換え機能を有効にする場合、以下の設定の制限とガイドラインに従ってください。

- この設定はダイナミックに IPv6 マルチキャストグループに加入されたポートのみ適用します。
- IPv6 マルチキャストグループ置き換え機能は、ポートあるいはグローバルのどちらかに設定することができます。ポートとグローバルの両方に設定がある場合、ポートの設定が適用されます。

II. グローバルでの IPv6 マルチキャストグループ置き換え機能の有効化の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. MLD-snooping view に移行する	**mld-snooping**	―
3. グローバルで IPv6 マルチキャストグループ置き換え機能を有効にする	**overflow-replace** [**vlan** *vlan-list*]	デフォルト：無効

III. ポートでの IPv6 マルチキャストグループ置き換え機能の有効化の設定

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

操作	コマンド	補足
2． Ethernet interface view あるいは aggregate interface view に移行する.	**interface** *interface-type interface-number*	―
3． ポートで IPv6 マルチキャストグループ置き換え機能を有効にする	**mld-snooping overflow-replace** [**vlan** *vlan-list*]	デフォルト：無効

3.9 MLD snoopingの表示と維持

すべての view で **display** コマンドを実行でき、user view で **reset** コマンドを実行できます。

操作	コマンド
レイヤ2 IPv6マルチキャストグループエントリの情報を表示する	**display ipv6 l2-multicast ip forwarding** [**group** *ipv6-group-address* | **source** *ipv6-source-address*] * [**vlan** *vlan-id*] [**slot** *slot-number*]
レイヤ2 IPv6 MACマルチキャストグループエントリの情報を表示する	**display ipv6 l2-multicast mac forwarding** [*mac-address*] [**vlan** *vlan-id*] [**slot** *slot-number*]
MLD snoopingのステータスを表示する	**display mld-snooping** [**global** | **vlan** *vlan-id*]
ダイナミックMLD snooping転送エントリの情報を表示する	**display mld-snooping group** [*ipv6-group-address* | *ipv6-source-address*] * [**vlan** *vlan-id*] [**verbose**] [**slot** *slot-number*]
スタティックMLD snooping転送エントリの情報を表示する	**display mld-snooping static-group** [*ipv6-group-address* | *ipv6-source-address*] * [**vlan** *vlan-id*] [**verbose**] [**slot** *slot-number*]
ダイナミックルータポートの情報を表示する	**display mld-snooping router-port** [**vlan** *vlan-id*] [**slot** *slot-number*]
スタティックルータポートの情報を表示する	**display mld-snooping static-router-port** [**vlan** *vlan-id*] [**slot** *slot-number*]
MLD snoopingによって学習されたMLDメッセージの統計情報を表示する	**display mld-snooping statistics**
IPv6マルチキャストグループのダイナミックMLD snooping転送エントリを削除する	**reset mld-snooping group** { *ipv6-group-address* [*ipv6-source-address*] | **all** } [**vlan** *vlan-id*]
ダイナミックルータポートを削除する	**reset mld-snooping router-port** { **all** | **vlan** *vlan-id* }
MLD snoopingによって学習されたMLDメッセージの統計情報を削除する	**reset mld-snooping statistics**

3.10 MLD snooping設定例

3.10.1 VLAN ベースの IPv6 グループポリシーとシミュレーティッドメンバホスト設定例

I. ネットワーク要件

図 3-4に示すように Router A は MLDv1 を動作させ、MLD クエリアとして機能し、Switch A は MLDv1 snooping を動作させます。

以下が成り立つようにグループポリシーを設定します。

- Host A と Host B は宛先が IPv6 マルチキャストグループ FF1E::101 の IPv6 マルチキャストデータのみ受信します。
- VLAN100 でフラッディングしないように Switch A で未知の IPv6 マルチキャストデータ廃棄機能を有効にします。

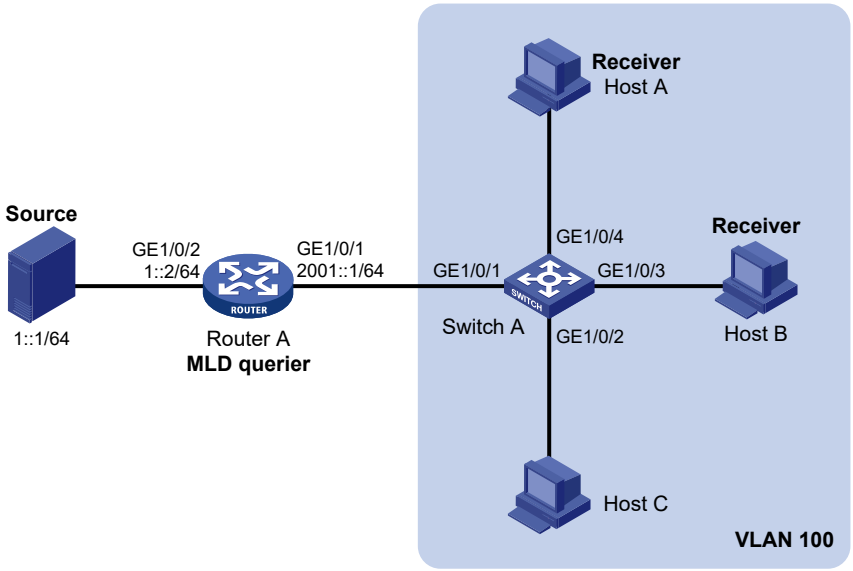


図 3-4 ネットワーク図

II. 設定手順

1) 図 3-4に対応する各インタフェースに IPv6 アドレスとプレフィックス長を割り当てます。（詳細は省略します）
2) Router A を設定します。

IPv6 マルチキャストルーティングを有効にします。

```
<RouterA> system-view
[RouterA] ipv6 multicast routing
[RouterA-mrib6] quit
```

GigabitEthernet 1/0/1 で MLD を有効にします。

```
[RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] mld enable
[RouterA-GigabitEthernet1/0/1] quit
```

GigabitEthernet 1/0/2 で IPv6 PIM-SM を有効にします。

```
[RouterA] interface gigabitethernet 1/0/2
[RouterA-GigabitEthernet1/0/2] ipv6 pim sm
[RouterA-GigabitEthernet1/0/2] quit
```

3)　Switch A を設定します。

グローバルで MLD snooping を有効にします。

```
<SwitchA> system-view
[SwitchA] mld-snooping
[SwitchA-mld-snooping] quit
```

VLAN 100 を作成し、この VLAN に GigabitEthernet 1/0/1～GigabitEthernet 1/0/4 を割り当てます。

```
[SwitchA] vlan 100
[SwitchA-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/4
```

VLAN100 で未知の IPv6 マルチキャストデータ廃棄機能を有効にします。

```
[SwitchA-vlan100] mld-snooping enable
[SwitchA-vlan100] mld-snooping drop-unknown
[SwitchA-vlan100] quit
```

VLAN 100 のホストが IPv6 マルチキャストグループ FF1E::101 のみ参加できるように、IPv6 マルチキャストグループポリシーを設定します。

```
[SwitchA] acl ipv6 basic 2001
[SwitchA-acl-ipv6-basic-2001] rule permit source ff1e::101 128
[SwitchA-acl-ipv6-basic-2001] quit
[SwitchA] mld-snooping
[SwitchA–mld-snooping] group-policy 2001 vlan 100
[SwitchA–mld-snooping] quit
```

IPv6 マルチキャストグループ FF1E::101 のシミュレーティッドメンバホストとして GigabitEthernet 1/0/3、GigabitEthernet 1/0/4 を設定します。

```
[SwitchA] interface gigabitethernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] mld-snooping host-join ff1e::101 vlan 100
[SwitchA-GigabitEthernet1/0/3] quit
[SwitchA] interface gigabitethernet 1/0/4
```

```
[SwitchA-GigabitEthernet1/0/4] mld-snooping host-join ff1e::101 vlan 100
[SwitchA-GigabitEthernet1/0/4] quit
```

III. 設定の確認

IPv6 マルチキャストグループ FF1E::101、FF1E::202 に加入するため Host A と Host B から MLD report を送信します。（詳細は省略します）

Switch A の VLAN 100 のダイナミック MLD snooping 転送エントリの情報を表示します。

```
[SwitchA] display mld-snooping group vlan 100
Total 1 entries.

VLAN 100: Total 1 entries.
  (::, FF1E::101)
    Host ports (2 in total):
      GE1/0/3                                 (00:03:23)
      GE1/0/4                                 (00:04:10)
```

出力は以下の情報を表示します。

- Host A と Host B は IPv6 マルチキャストグループ FF1E::101 に加入しています。（それぞれ Switch A の GigabitEthernet 1/0/4 と GigabitEthernet 1/0/3 のメンバポートを通して加入しています）
- Host A と Host B は IPv6 マルチキャストグループ FF1E::202 に加入できません。

3.10.2 VLAN ベースのスタティックポート設定例

I. ネットワーク要件

図 3-5に示すように設定します。

- Router A は MLDv1 を動作させ、MLD クエリアとして機能し、Switch A、Switch B、Switch C は MLDv1 snooping を動作させます。
- Host A と Host C は IPv6 マルチキャストグループ FF1E::101 の永久的な Receiver です。

スタティックポートを以下の要件に従って設定します。

- IPv6 マルチキャストトラフィック送信の信頼性を強化するために、Switch C の GigabitEthernet 1/0/3 と GigabitEthernet 1/0/5 を IPv6 マルチキャストグループ FF1E::101 のスタティックメンバポートとして設定します。
- ネットワークで STP が実行されていると仮定します。データループを回避するために、Switch A から Switch C への転送パスは通常状態ではブロックされます。IPv6 マルチキャストトラフィックは Switch A—Switch B—Switch C のパスを経由して、Switch C に接続されている Receiver に転送されます。Switch A—Switch B—Switch C のパスがブロックされた場合に、Switch A—Switch C のパスを経由して IPv6 マルチキャストトラフィックがほとんど途切れずに Receiver へと転送できるように、Switch A の GigabitEthernet 1/0/3 にスタティックルータポートを設定します。STP の詳細は、オペレーションマニュアルのセクション 2 *アクセス ”STP*”を参照してください。

メモ：

スタティックルータポートが設定されていない場合、Switch A—Switch B－Switch C のパスがブロックされたのち、IPv6 マルチキャストの転送が中断されます。新しいパスで IPv6 マルチキャストパケットを転送する前に、少なくとも 1 回以上の MLD クエリ、MLD 応答の交換が必要です。

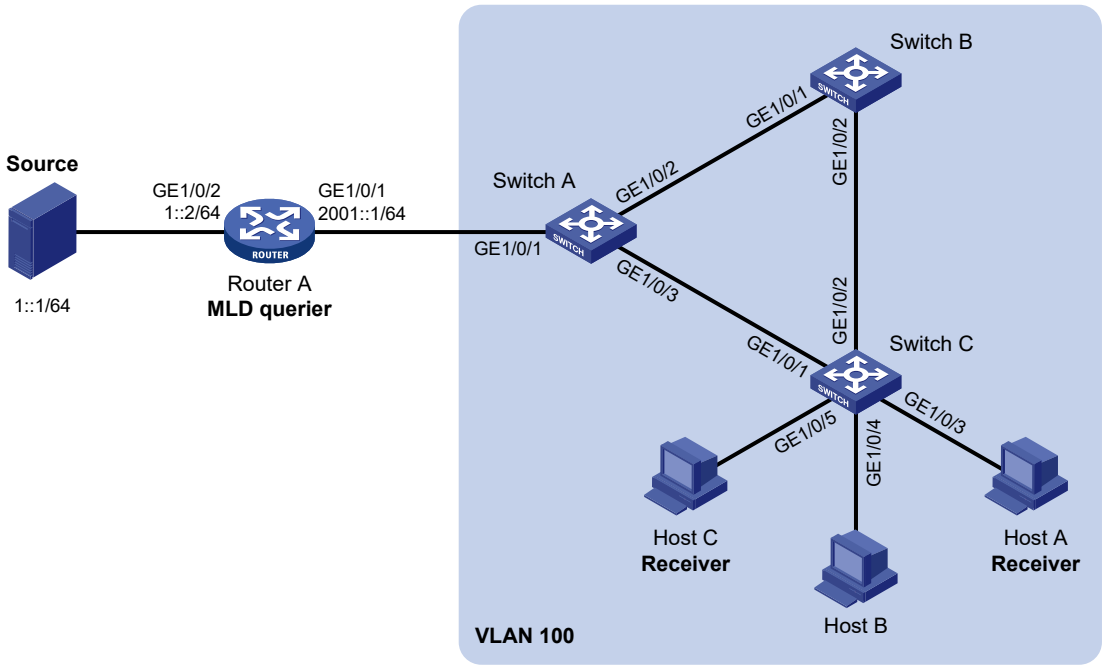


図 3-5 ネットワーク図

II. 設定手順

1) 図 3-5に対応する各インタフェースに IPv6 アドレスとプレフィックス長を割り当てます。（詳細は省略します）
2) Router A を設定します。

IPv6 マルチキャストルーティングを有効にします。

```
<RouterA> system-view
[RouterA] ipv6 multicast routing
[RouterA-mrib6] quit
```

GigabitEthernet 1/0/1 で MLD を有効にします。

```
[RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] mld enable
[RouterA-GigabitEthernet1/0/1] quit
```

GigabitEthernet 1/0/2 で IPv6 PIM-SM を有効にします。

```
[RouterA] interface gigabitethernet 1/0/2
[RouterA-GigabitEthernet1/0/2] ipv6 pim sm
[RouterA-GigabitEthernet1/0/2] quit
```

3)　Switch A を設定します。

グローバルで MLD snooping を有効にします。

```
<SwitchA> system-view
[SwitchA] mld-snooping
[SwitchA-mld-snooping] quit
```

VLAN 100 を作成し、この VLAN に GigabitEthernet 1/0/1～GigabitEthernet 1/0/3 を割り当てます。

```
[SwitchA] vlan 100
[SwitchA-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/3
```

VLAN 100 で MLD snooping を有効にします。

```
[SwitchA-vlan100] mld-snooping enable
[SwitchA-vlan100] quit
```

スタティックルータポートとして GigabitEthernet 1/0/3 を設定します。

```
[SwitchA] interface gigabitethernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] mld-snooping static-router-port vlan 100
[SwitchA-GigabitEthernet1/0/3] quit
```

4)　Switch B を設定します。

グローバルで MLD snooping を有効にします。

```
<SwitchB> system-view
[SwitchB] mld-snooping
[SwitchB-mld-snooping] quit
```

VLAN 100 を作成し、この VLAN に GigabitEthernet 1/0/1～GigabitEthernet 1/0/2 を割り当てます。

```
[SwitchB] vlan 100
[SwitchB-vlan100] port gigabitethernet 1/0/1 gigabitethernet 1/0/2
```

VLAN 100 で MLD snooping を有効にします。

```
[SwitchB-vlan100] mld-snooping enable
[SwitchB-vlan100] quit
```

5)　Switch C を設定します。

グローバルで MLD snooping を有効にします。

```
<SwitchC> system-view
[SwitchC] mld-snooping
```

```
[SwitchC-mld-snooping] quit
```

VLAN 100 を作成し、この VLAN に GigabitEthernet 1/0/1～GigabitEthernet 1/0/5 を割り当てます。

```
[SwitchC] vlan 100
[SwitchC-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/5
```

VLAN 100 で MLD snooping を有効にします。

```
[SwitchC-vlan100] mld-snooping enable
[SwitchC-vlan100] quit
```

IPv6 マルチキャストグループ FF1E::101 のスタティックメンバポートとして GigabitEthernet 1/0/3、GigabitEthernet 1/0/5 を設定します。

```
[SwitchC] interface gigabitethernet 1/0/3
[SwitchC-GigabitEthernet1/0/3] mld-snooping static-group ff1e::101 vlan 100
[SwitchC-GigabitEthernet1/0/3] quit
[SwitchC] interface gigabitethernet 1/0/5
[SwitchC-GigabitEthernet1/0/5] mld-snooping static-group ff1e::101 vlan 100
[SwitchC-GigabitEthernet1/0/5] quit
```

III. 設定の確認

Switch A で VLAN 100 のスタティックルータポートの情報を表示します。

```
[SwitchA] display mld-snooping static-router-port vlan 100
VLAN 100:
  Router ports (1 in total):
    GE1/0/3
```

出力は、Switch A の GigabitEthernet 1/0/3 がスタティックルータポートになっていることを示します。

Switch C で VLAN 100 のスタティック MLD snooping 転送エントリの情報を表示します。

```
[SwitchC] display mld-snooping static-group vlan 100
Total 1 entries).

VLAN 100: Total 1 entries).
  (::, FF1E::101)
    Host ports (2 in total):
      GE1/0/3
      GE1/0/5
```

出力は、Switch C の GigabitEthernet 1/0/3 と GigabitEthernet 1/0/5 が IPv6 マルチキャストグループ FF1E::101 のスタティックメンバポートになっていることを示します。

3.10.3 VLAN ベースの MLD snooping クエリア設定例

I. ネットワーク要件

図 3-6に示すように設定します。

- ネットワークはレイヤ 2 ネットワークです。
- Source1、Source2 はそれぞれ IPv6 マルチキャストグループ FF1E::101、FF1E::102 に IPv6 マルチキャストデータを送信します。
- Host A、Host C は IPv6 マルチキャストグループ FF1E::101 の Receiver です。Host B、Host D は IPv6 マルチキャストグループ FF1E::102 の Receiver です。
- すべてのレシーバホストで MLDv1 が動作し、すべての Switch で MLDv1 snooping が動作します。Switch A（IPv6 マルチキャストソースにもっとも近い Switch です）は MLD snooping クエリアとして動作します。
- VLAN に IPv6 パケットをフラッディングしないようにすべての Switch で未知の IPv6 マルチキャストデータ廃棄機能を有効にします。

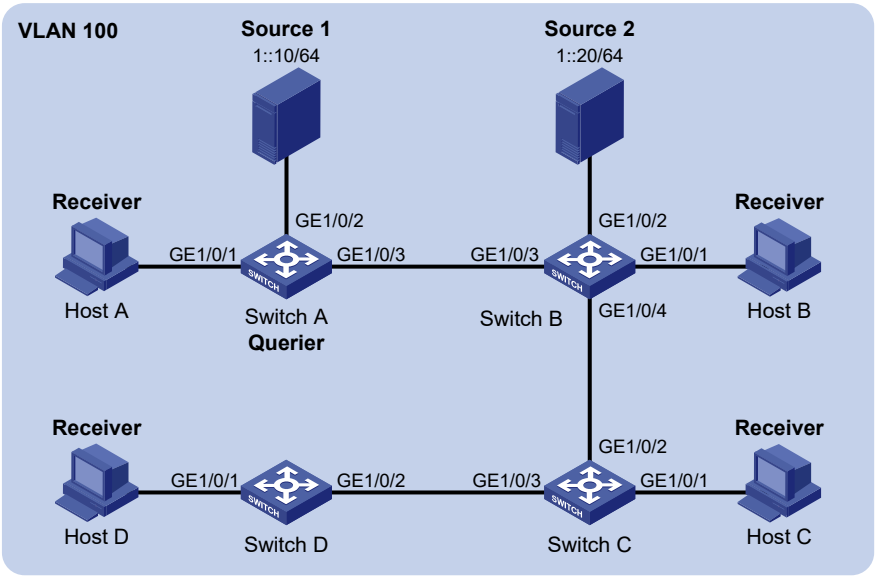


図 3-6 ネットワーク図

II. 設定手順

1)　Switch A を設定します。

グローバルで MLD snooping を有効にします。

```
<SwitchA> system-view
[SwitchA] mld-snooping
[SwitchA-mld-snooping] quit
```

VLAN 100 を作成し、この VLAN に GigabitEthernet 1/0/1～GigabitEthernet 1/0/3 を割り当てます。

```
[SwitchA] vlan 100
```

```
[SwitchA-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/3
```

VLAN 100 で MLD snooping を有効にし、未知の IPv6 マルチキャストデータ廃棄機能を有効にします。

```
[SwitchA-vlan100] mld-snooping enable
[SwitchA-vlan100] mld-snooping drop-unknown
```

VLAN 100 で MLD snooping クエリアを有効にします。

```
[SwitchA-vlan100] MLD-snooping querier
[SwitchA-vlan100] quit
```

2)　Switch B を設定します。

グローバルで MLD snooping を有効にします。

```
<SwitchB> system-view
[SwitchB] mld-snooping
[SwitchB-mld-snooping] quit
```

VLAN 100 を作成し、この VLAN に GigabitEthernet 1/0/1～GigabitEthernet 1/0/4 を割り当てます。

```
[SwitchB] vlan 100
[SwitchB-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/4
```

VLAN100 で MLD snooping を有効にし、未知の IPv6 マルチキャストデータ廃棄機能を有効にします。

```
[SwitchB-vlan100] mld-snooping enable
[SwitchB-vlan100] mld-snooping drop-unknown
[SwitchB-vlan100] quit
```

3)　Switch C を設定します。

グローバルで MLD snooping を有効にします。

```
<SwitchC> system-view
[SwitchC] mld-snooping
[SwitchC-mld-snooping] quit
```

VLAN 100 を作成し、この VLAN に GigabitEthernet 1/0/1～GigabitEthernet 1/0/3 を割り当てます。

```
[SwitchC] vlan 100
[SwitchC-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/3
```

VLAN 100 で MLD snooping を有効にし、未知の IPv6 マルチキャストデータ廃棄機能を有効にします。

```
[SwitchC-vlan100] mld-snooping enable
[SwitchC-vlan100] mld-snooping drop-unknown
[SwitchC-vlan100] quit
```

4)　Switch D を設定します。

グローバルで MLD snooping を有効にします。

```
<SwitchD> system-view
[SwitchD] mld-snooping
[SwitchD-mld-snooping] quit
```

VLAN 100 を作成し、この VLAN に GigabitEthernet 1/0/1～GigabitEthernet 1/0/2 を割り当てます。

```
[SwitchD] vlan 100
[SwitchD-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/2
```

VLAN 100 で MLD snooping を有効にし、未知の IPv6 マルチキャストデータ廃棄機能を有効にします。

```
[SwitchD-vlan100] mld-snooping enable
[SwitchD-vlan100] mld-snooping drop-unknown
[SwitchD-vlan100] quit
```

III. 設定の確認

Switch B の MLD snooping を通して学習した MLD メッセージ、IPv6 PIM hello メッセージの統計情報を表示します。

```
[SwitchB] display mld-snooping statistics
Received MLD general queries:  3
Received MLDv1 specific queries:  0
Received MLDv1 reports:  12
Received MLD dones:  0
Sent     MLDv1 specific queries:  0
Received MLDv2 reports:  0
Received MLDv2 reports with right and wrong records:  0
Received MLDv2 specific queries:  0
Received MLDv2 specific sg queries:  0
Sent     MLDv2 specific queries:  0
Sent     MLDv2 specific sg queries:  0
Received IPv6 PIM hello:  0
Received error MLD messages:  0
```

出力は、Switch A が MLD snooping クエリアとして動作した後、Switch A を除くすべての Switch が MLD general クエリを受信できることを示します。

3.11 MLD snoopingのトラブルシューティング

3.11.1 レイヤ 2 マルチキャスト転送ができない

I. 症状

MLD snooping を通してレイヤ 2 マルチキャスト転送ができません。

II. 分析

MLD snooping が有効になっていません。

III. 解決策

1) **display mld-snooping** コマンドを使用し、MLD snooping の情報を表示します。
2) MLD snooping が有効になっていない場合、system view でグローバルに **mld-snooping** コマンドを使用して MLD snooping を有効にしてください。VLAN view で **mld-snooping enable** コマンドを使用して MLD snooping を有効にしてください。
3) 対応する VLAN でのみ MLD snooping が無効になっている場合、対応する VLAN の VLAN view 上で **mld-snooping enable** コマンドを使用して MLD snooping を有効にしてください。
4) 問題が解決しない場合、NEC に問い合わせてください。

3.11.2 IPv6 マルチキャストグループポリシーが動作しない

I. 症状

ホストは IPv6 マルチキャストグループポリシーで許可されていない IPv6 マルチキャストグループから IPv6 マルチキャストデータを受信することができます。

II. 分析

- IPv6 ACL ルールの設定が間違っています。
- IPv6 マルチキャストグループポリシーが正しく適用されていません 。
- 未知の IPv6 マルチキャストデータ廃棄機能が無効で、IPv6 マルチキャストデータがフラッディングしています。

III. 解決策

1) **display acl ipv6** コマンドで IPv6 ACL ルールの設定を確認してください。実行する IPv6 マルチキャストグループポリシーに IPv6 ACL ルールが一致していることを確認してください。
2) **display this** コマンドを MLD snooping view または対応する interface view で使用して、IPv6 マルチキャストグループポリシーが正しく適用されているかどうかを確認してください。適用されていない場合、**group-policy** コマンドまたは **mld-snooping group-policy** コマンドで IPv6 マルチキャストグループポリシーを正しく適用してください。

3) **display mld-snooping** コマンドを使用して、未知の IPv6 マルチキャストデータ廃棄機能が有効になっているかどうか確認してください。有効になっていない場合、**mld-snooping drop-unknown** コマンドを使用して未知の IPv6 マルチキャストデータ廃棄機能を有効にしてください。
4) 問題が解決しない場合、NEC に問い合わせてください。

QX-S1100G シリーズ Ethernet スイッチ

オペレーションマニュアル

6.ACL and QoS

本マニュアルは以下に示す章で構成されています。

01-ACL
02-QoS の概要
03-QoS ポリシー
04-プライオリティマッピング
05-ラインレート
06-輻輳制御
07-トラフィックフィルタリング
08-プライオリティマーキング
09-ネスティング
10-トラフィックリダイレクティング
11-クラスベースアカウンティング
12-タイムレンジ
13-データバッファ
14-付録

目次

このセクションのページは**6-x-x** です。

1章 ACL 1-1
1.1 概要 1-1
1.1.1 ACLタイプ 1-1
1.1.2 ACLの番号づけと命名 1-1
1.1.3 走査順 1-2
1.1.4 ルールナンバリング 1-3
1.1.5 ACLでのフラグメントフィルタリング 1-4
1.2 設定作業リスト 1-4
1.3 標準ACLの設定 1-5
1.3.1 標準IPv4 ACLの設定 1-5
1.3.2 標準IPv6 ACLの設定 1-5
1.4 拡張ACLの設定 1-6
1.4.1 拡張IPv4 ACLの設定 1-6
1.4.2 拡張IPv6 ACLの設定 1-7
1.5 L2 ACLの設定 1-8
1.6 ACLのコピー 1-9
1.7 ACLへのパケットフィルタの設定 1-10
1.7.1 パケットフィルタリングのためのインタフェースへのACLの適用 1-10
1.7.2 フィルタリングのログ作成と出力間隔の設定 1-11
1.8 ACLの表示と維持 1-11
1.9 ACL設定例 1-11
1.9.1 ネットワーク要件 1-11
1.9.2 設定手順 1-12
1.9.3 設定の確認 1-13

1章 ACL

1.1 概要

ACL（Access Control List）は、ルール（許可または拒否ステートメント）の設定で、送信元 IP アドレス、宛先 IP アドレス、ポート番号などにマッチするルールに従って、どのパケット処理するかを決定します。

ACL は､設定されたマッチするルールに従ってパケットをフィルタすることによく使用されます。パケットフィルタ機能の章で例を示します。ACL は QoS、セキュリティ、ルーティング、その他の機能でトラフィックの設定に使用できます。ACL を使用して、モジュールにおけるパケットの廃棄、転送を決定します。

⚠ **注意：**

ACL の処理には、「interface > vlan > global」の優先順位があります。ACL は、高優先の処理を実行すると低優先の処理を実行しません。つまり、interface に設定された ACL の処理が実行された場合、vlan や global に設定された ACL の処理は実行されません。

1.1.1 ACL タイプ

タイプ	ACL 番号	IP バージョン	マッチング基準
標準ACL	2000～2999	IPv4	送信元IPアドレス
		IPv6	送信元IPv6アドレス
拡張ACL	3000～3999	IPv4	送信元IPv4アドレス、宛先IPv4アドレス、パケットプライオリティ、プロトコル番号、その他のレイヤ3、またはレイヤ4のプロトコルヘッダ情報
		IPv6	送信元IPv6アドレス、宛先IPv6アドレス、パケットプライオリティ、プロトコル番号、その他のレイヤ3、またはレイヤ4のプロトコルヘッダ情報
L2 ACL	4000～4999	IPv4、IPv6	送信元MACアドレス、宛先MACアドレス、802.1pプライオリティ、リンクレイヤプロトコルタイプなどの、レイヤ2プロトコルヘッダフィールド

1.1.2 ACL の番号づけと命名

各 ACL のタイプには、ACL 番号の固有な範囲があります。ACL を作成するとき、固有の ACL 番号あるいは名前を付ける必要があります。識別を簡略化するために ACL の名前を割り当てることができます。ACL を作成した後、設定した名前を変更、削除することもできません。

標準 IPv4 ACL と拡張 IPv4 ACL では、IPv4 で固有の ACL 番号と名前を使用する必要があります。

標準 IPv6 ACL と拡張 IPv6 ACL では、IPv6 で固有の ACL 番号と名前を使用する必要があります。

L2 ACL では、固有の ACL 番号と名前を使用する必要があります。

1.1.3 走査順

ACL のルールは指定された順序で探索されます。パケットが、あるルールにマッチした時点で探索動作を終了します。ACL が重複や矛盾したルールを含んでいる場合、探索結果や動作は探索順序に依存します。

IPv4 ACL の走査順には、以下の 2 つ方法があります。

- **config**：ルール ID を昇順で探索します。大きいルール ID よりも先に小さいルール ID にマッチします。この方法を使用する場合、ルールの内容と順序に注意してください。
- **auto**：depth-first により ACL の探索を行います。depth-first ルールでの走査順は、ACL のタイプによって表 1-1の定義に従って決定されます。

表 1-1 ACL の depth-first 走査順

ACL 種別	走査順
標準IPv4 ACL	1. 送信元 IPv4 アドレスのワイルドカードの 0 が多い順（0 が多いと IPv4 アドレスのワイルドカードの範囲が狭いことを示します。） 2. ルールが作成された順
拡張IPv4 ACL	1. プロトコルタイプが IP よりも高いレイヤかどうか 2. 送信元 IP アドレスのワイルドカードマスクの 0 が多い順 3. 宛先 IP アドレスのワイルドカードマスクの 0 が多い順 4. TCP/UDP のポート番号の範囲が小さい順 5. ルールが作成された順
標準IPv6 ACL	1. 送信元 IPv6 アドレスのプレフィックスの長い順（0 が多いと IPv6 アドレスのワイルドカードの範囲が狭いことを示します。） 2. ルーが作成された順
拡張IPv6 ACL	1. プロトコルタイプが IP よりも高いレイヤかどうか 2. 送信元 IPv6 アドレスのプレフィックスの長い順 3. 宛先 IPv6 アドレスのプレフィックスの長い順 4. TCP/UDP のポート番号の範囲が小さい順 5. ルールが作成された順
L2 ACL	1. 送信元 MAC アドレスのマスクの 1 が多い順（1 が多いと MAC アドレスが小さいことを示します。） 2. 宛先 MAC アドレスのマスクの 1 が多い順 3. ルールが作成された順

インバースマスク（inverse mask）と呼ばれるワイルドカードマスクは、10 進数表示のドット表示で

表される 32 ビットバイナリです。ネットマスクの 0 は“一致する（do care）”ビットと表現され、

1 は“無視する（don’t care)”ビットと表現されます。サブネットマスクの 0 と 1 を反転したものとは異なります。IP アドレスが“do care”ビットである場合、一致させ、“無視する（don’t care)”

ビットである場合、無視されます。ワイルドマスクが 0.255.255.255、ネットマスクが 192.168.1.1 の

場合、最初の 0 は”一致する（do care）"ビットで、2 番目以降が“無視する（don’t care)”ビットであるため、192.0.0.0 のネットワークに一致する ACL となります。ワイルドカードマスクの 0 と 1 は非連続にすることができます。たとえば 0.255.0.255 は有効なワイルドマスクです。

🕮 **メモ：**

- 標準 IPv4 ACL、拡張 IPv4 ACL のマスク値は、インバースマスクとなります。0 は "一致する(do care)" ビット、1 は "無視する(don’t care)" ビットとなります。
- 標準 IPv6 ACL、拡張 IPv6 ACL、L2 ACL のマスク値は、インバースマスクではありません。1 は "一致する(do care)" ビット、0 は "無視する(don’t care)" ビットとなります。

1.1.4 ルールナンバリング

ACL ルールは手動ナンバリングあるいは自動ナンバリングを選択できます。本セクションでは自動ナンバリングの動作を説明します。

I. ルールナンバリングのステップ

作成したルールに ID を割り当てない場合、システムは ACL ルールにルール ID を自動的に割り当てます。ステップのナンバリングルールは、システムが自動的にルールの番号づけを行う増加分を設定します。たとえば、デフォルトの ACL ルールのナンバリングステップは 5 です。ルールに ID を割り当てない場合、ルールには 0、5、10、15･･･の順で自動的に番号が振られます。広いナンバリングのステップの場合、2 つのルールの間に、さらにルールを挿入することができます。

隣接したナンバリングルールより、ルールの間に隙間を導入することによって、新規にルールを挿入するように、ACL に柔軟性を持たせることができます。この機能は config-order ACL にとって重要です。config-order ACL の ACL ルールはルール ID の昇順でマッチされています。

II. 自動ルールナンバリングと再ナンバリング

システムは、現在の最大のステップ番号よりも大きなステップの最小倍数を新しく定義されたルールに割り当てます。これは 0 から始まります。

たとえば、ナンバリングのステップを 5 に設定し、ACL ルールに 0、5、9、10、12 を設定した場合、新しく定義されたルールには 15 が割り当てられます。ACL にルールが 1 つも定義されていない場合、最初に定義されるルールの番号は 0 です。

ルールのステップを変更したとき、ルールは再ナンバリングされ、0 から始まります。たとえば、ルールの番号 5、10、13、15 があるとします。ステップを 5 から 2 に変更すると、ルールの番号は 0、2、4、6 となります。

一致順序が **auto** の ACL の場合、ルールは深さ優先順でソートされ、一致順序に基づいて番号が付け直されます。 たとえば、ルールは 0、10、5 の一致順序にあります。番号付けステップを 2 に変更すると、ルール 0、10、5（0、5、10 ではない）がルール 0、2、4 として再番号付けされます。

1.1.5 ACL でのフラグメントフィルタリング

通常のパケットフィルタリングはパケットの最初のフラグメントのみマッチし、後続のフラグメントはパスします。攻撃者はネットワークを攻撃するため、最初でないフラグメントを偽造することができます。

このリスクを防ぐため、以下の ACL を使用します。

- デフォルトで、最初のフラグメント以外のパケットを含むすべてのフラグメントをフィルタします。
- マッチ条件の変更を行います。たとえば、最初のフラグメント以外のパケットのみをフィルタします。

1.2 設定作業リスト

作業リスト
（必須設定項目） 少なくとも1つの作業を行ってください。 • 標準ACLの設定   • 標準IPv4 ACLの設定   • 標準IPv6 ACLの設定 • 拡張ACLの設定   • 拡張IPv4 ACLの設定   • 拡張IPv6 ACLの設定 • L2 ACLの設定
（オプション設定項目） ACLのコピー
（オプション設定項目） ACLへのパケットフィルタの設定

🕮 **メモ：**

- ACL は設定したルールの最終行に暗黙のルールが自動的に適用されます。暗黙のルールは ACL を使用する機能によって、すべて破棄する暗黙の deny とすべて許可する暗黙の permit に分かれます。
- QoS,や packet-filter などインタフェースに設定するハードウェアベースの ACL は暗黙の permit で動作します。
- telnet や snmp など、**telnet server** コマンドや **snmp-agent community** コマンドなどのように、機能に ACL を設定するソフトウェアベースの ACL は暗黙の deny で動作します。

1.3 標準ACLの設定

この章では、IPv4 および IPv6 での標準 ACL の設定方法について説明します。

1.3.1 標準 IPv4 ACL の設定

標準 IPv4 ACL は送信元 IP アドレスにもとづいたパケットにのみマッチします。

以下に標準 IPv4 ACL の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. 標準 IPv4 ACL を作成し、その view に移行する	**acl basic** { *acl-number* | **name** *acl-name* } [**match-order** { **auto** | **config** }] **number**コマンドの場合： **acl number** *acl-number* [**match-order** { **auto** | **config** }]	デフォルト：設定なし 設定範囲は2000～2999です。 IPv4 ACLの番号を指定する場合、**acl basic** *acl-number*コマンドを使用した後でviewに移行することができます。 IPv4 ACLの名前を指定する場合、**acl basic name** *acl-name* コマンドを使用した後でviewに移行することができます。
3. （オプション設定項目）標準 IPv4 ACL の説明を設定する	**description** *text*	デフォルト：設定なし
4. （オプション設定項目）ルールの番号づけステップを設定する	**step** *step-value*	デフォルト：5
5. ルールを作成/修正する	**rule** [*rule-id*] { **deny** | **permit** } [**counting** | **fragment** | **logging** | **source** { *source-address source-wildcard* | **any** } | **time-range** *time-range-name*] *	デフォルト：設定なし **logging**キーワードはモジュール（パケットフィルタリングなど）がサポートしている場合のみ機能します。
6. （オプション設定項目）ルールの説明を設定する	**rule** *rule-id* **comment** *text*	デフォルト：設定なし

1.3.2 標準 IPv6 ACL の設定

標準 IPv6 ACL は送信元 IP アドレスにもとづいたパケットにのみマッチします。

以下に標準 IPv6 ACL の設定を示します。

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

操作	コマンド	補足
2. 標準 IPv6 ACL を作成し、その view に移行する	**acl ipv6 basic** { *acl-number* | **name** *acl-name* } [**match-order** { **auto** | **config** }] **number**コマンドの場合： **acl ipv6 number** *acl-number* [**match-order** { **auto** | **config** }]	デフォルト：設定なし 設定範囲は2000～2999です。 IPv6 ACLの番号を指定する場合、**acl ipv6 basic** *acl-number*コマンドを使用した後でviewに移行することができます。 IPv6 ACLの名前を指定する場合、**acl ipv6 basic name** *acl-name*コマンドを使用した後でviewに移行することができます。
3. （オプション設定項目）標準 IPv6 ACL の説明を設定する	**description** *text*	デフォルト：設定なし
4. （オプション設定項目）ルールの番号付けステップを設定する	**step** *step-value*	デフォルト：5
5. ルールを作成/修正する	**rule** [*rule-id*] { **deny** | **permit** } [**counting** | **fragment** | **logging** | **routing** [**type** *routing-type*] | **source** { *source-address source-prefix* | *source-address/source-prefix* | **any** } | **time-range** *time-range-name*] *	デフォルト：設定なし **logging**キーワードはモジュール（たとえばパケットフィルタリング）がサポートしている場合のみ機能します。
6. （オプション設定項目）ルールの説明を設定する	**rule** *rule-id* **comment** *text*	デフォルト：設定なし

1.4 拡張ACLの設定

この章では、IPv4 および IPv6 での拡張 ACL の設定方法について説明します。

1.4.1 拡張 IPv4 ACL の設定

拡張 IPv4 ACL では、以下の情報にもとづいてマッチングを行うことができます。

- 送信元 IP アドレス
- 送信先 IP アドレス
- パケットのプライオリティ
- プロトコル番号
- TCP/UDP の送信元/送信先ポート番号、TCP フラグ、ICMP メッセージタイプ、ICMP メッセージコードなどの他のプロトコルヘッダ情報

標準 IPv4 ACL と比較すると、拡張 IPv4 ACL では柔軟で正確なフィルタリングを行うことができます。

以下に拡張 IPv4 ACL の設定を示します。

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

操作	コマンド	補足
2. 拡張 IPv4 ACL を作成し、その view に移行する	**acl advanced** { *acl-number* | **name** *acl-name* } [**match-order** { **auto** | **config** }] **number**コマンドの場合： **acl number** *acl-number* [**match-order** { **auto** | **config** }]	デフォルト：設定なし 設定範囲は3000～3999です。 IPv4 ACLの番号を指定する場合、**acl advanced** *acl-number*コマンドを使用した後でviewに移行することができます。 IPv4 ACLの名前を指定する場合、**acl advanced name** *acl-name*コマンドを使用した後でviewに移行することができます。
3. （オプション設定項目）拡張 IPv4 ACL の説明を設定する	**description** *text*	デフォルト：設定なし
4. （オプション設定項目）ルールの番号付けステップを設定する	**step** *step-value*	デフォルト：5
5. ルールを作成/修正する	**rule** [*rule-id*] { **deny** | **permit** } *protocol* [{ { **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn** *syn-value* | **urg** *urg-value* } * | **established** } | **counting** | **destination** { *dest-address dest-wildcard* | **any** } | **destination-port** *operator port* | { **dscp** *dscp* | { **precedence** *precedence* | **tos** *tos* } * } | **fragment** | **icmp-type** { *icmp-type* [*icmp-code*] | *icmp-message* } | **logging** | **source** { *source-address source-wildcard* | **any** } | **source-port** *operator port* | **time-range** *time-range-name*] *	デフォルト：設定なし **logging**キーワードはモジュール（たとえばパケットフィルタリング）がサポートしている場合のみ機能します。
6. （オプション設定項目）ルールの説明を設定する	**rule** *rule-id* **comment** *text*	デフォルト：設定なし

1.4.2 拡張 IPv6 ACL の設定

🕮 **ポイント**：

IPv6 アドレスのフィルタについて、destination の場合は、フィルタできるアドレスに条件があります。
inbound フィルタ の場合は、アドレスの先頭 1 バイトと末尾 2 バイトをフィルタします。
outbound フィルタの場合は、アドレスの先頭 1 バイトのみをフィルタします。
詳細はコマンドマニュアルのセクション 6 ACL and QoS ”rule (IPv6 advanced ACL view)”を参照してください。

拡張 IPv6ACL では、以下の情報にもとづいてマッチングを行うことができます。

- 送信元 IPv6 アドレス
- 送信先 IPv6 アドレス
- パケットのプライオリティ

- プロトコル番号
- TCP/UDP の送信元/送信先ポート番号、TCP フラグ、ICMP メッセージタイプ、ICMP メッセージコードなどの他のプロトコルヘッダ情報

標準 IPv6 ACL と比較すると、拡張 IPv6 ACL では柔軟で正確なフィルタリングを行うことができます。

以下に拡張 IPv6 ACL の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. 拡張 IPv6 ACL を作成し、その view に移行する	**acl ipv6 advanced** { *acl-number* | **name** *acl-name* } [**match-order** { **auto** | **config** }] **number**コマンドの場合： **acl ipv6 number** *acl-number* [**match-order** { **auto** | **config** }]	デフォルト：設定なし 設定範囲は3000～3999です。 IPv6 ACLの番号を指定する場合、**acl ipv6 advanced** *acl-number*コマンドを使用した後でviewに移行することができます。 IPv6 ACLの名前を指定する場合、**acl ipv6 advanced name** *acl-name* コマンドを使用した後でviewに移行することができます。
3. （オプション設定項目）拡張 IPv6 ACL の説明を設定する	**description** *text*	デフォルト：設定なし
4. （オプション設定項目）ルールの番号付けステップを設定する	**step** *step-value*	デフォルト：5
5. ルールを作成/修正する	**rule** [*rule-id*] { **deny** | **permit** } *protocol* [{ { **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn** *syn-value* | **urg** *urg-value* } * | **established** } | **counting** | **destination** { *dest-address dest-prefix* | *dest-address/dest-prefix* | **any** } | **destination-port** *operator port* | **dscp** *dscp* | **flow-label** *flow-label-value* | **fragment** | **icmp6-type** { *icmp6-type icmp6-code* | *icmp6-message* } | **logging** | **routing** [**type** *routing-type*] | **source** { *source-address source-prefix* | *source-address/source-prefix* | **any** } | **source-port** *operator port* | **time-range** *time-range-name*] *	デフォルト：設定なし **logging**キーワードはモジュール（たとえばパケットフィルタリング）がサポートしている場合のみ機能します。
6. （オプション設定項目）ルールの説明を設定する	**rule** *rule-id* **comment** *text*	デフォルト：設定なし

1.5 L2 ACLの設定

イーサネットフレームのヘッダを使用した ACL は“L2 ACL”と呼ばれます。L2 ACL では以下のレイヤ 2 のプロトコルヘッダにもとづいてマッチングを行います。

- 送信元 MAC アドレス
- 送信先 MAC アドレス
- 802.1p 優先順位（VLAN プライオリティ）
- リンクレイヤのプロトコルタイプ
- カプセル化タイプ
- 内部送信元 MAC アドレス
- 内部宛先 MAC アドレス
- 内部リンクレイヤのプロトコルタイプ

以下に L2 ACL の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. L2 ACL を作成し、その view に移行する	**acl mac** { *acl-number* | **name** *acl-name* } [**match-order** { **auto** | **config** }] **number**コマンドの場合： **acl number** *acl-number* [**match-order** { **auto** | **config** }]	デフォルト：設定なし 設定範囲は4000～4999です。 L2 ACLの番号を指定する場合、**acl mac** *acl-number*コマンドを使用した後でviewに移行することができます。 L2 ACLの名前を指定する場合、**acl mac name** *acl-name* コマンドを使用した後でviewに移行することができます。
3. （オプション設定項目）L2 ACL の説明を設定する	**description** *text*	デフォルト：設定なし
4. （オプション設定項目）ルールの番号付けステップを設定する	**step** *step-value*	デフォルト：5
5. ルールを作成/修正する	**rule** [*rule-id*] { **deny** | **permit** } [**cos** *dot1p* | **counting** | **dest-mac** *dest-address dest-mask* | { **lsap** *lsap-type lsap-type-mask* | **type** *protocol-type protocol-type-mask* } | **source-mac** *source-address source-mask* | **time-range** *time-range-name*] *	デフォルト：設定なし
6. （オプション設定項目）ルールの説明を設定する	**rule** *rule-id* **comment** *text*	デフォルト：設定なし

1.6 ACLのコピー

既存の ACL（送信元 ACL）をコピーして、ACL（宛先 ACL）を新しく作成することができます。新しい ACL（宛先 ACL）は送信元 ACL と同じタイプ、内容を持ちます。ただし同じ ACL 番号、ACL 名ではありません。

ACL のコピーを行うため、以下のことを確認してください。

- 送信元の ACL と宛先 ACL は同じタイプである必要があります。
- コピーを実行する前に、送信元の ACL が存在し、宛先 ACL は存在しないことを確認してください。

以下に ACL のコピーの設定を示します。

操作	コマンド
1． system view に移行する	**system-view**
2． 既存の ACL をコピーし、新しく ACL を作成する	**acl** [**ipv6** | **mac**] **copy** { *source-acl-number* | **name** *source-acl-name* } **to** { *dest-acl-number* | **name** *dest-acl-name* }

1.7 ACLへのパケットフィルタの設定

この章では指定したインタフェースの受信、出力パケットをフィルタする手順を示します。

メモ：
パケットフィルタはイーサネットインタフェース、VLAN インタフェースで有効にすることが可能です。

1.7.1 パケットフィルタリングのためのインタフェースへの ACL の適用

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． interface view に移行する	**interface** *interface-type interface-number*	―
3． パケットをフィルタするために ACL をインタフェースに適用する	**packet-filter** [**ipv6** | **mac**] { *acl-number* | **name** *acl-name* } { **inbound** | **outbound** } [**hardware-count**]	デフォルト：設定なし インタフェースに同一方向の設定は最大3つまで設定できます。標準IPv4 ACL、標準IPv6 ACL、L2 ACLそれぞれ1つずつ設定することができます。 インタフェースで送信されるパケットをフィルタすることはできません。 VLANインタフェースでフィルタリングを設定した場合、別のVLANインタフェースに転送される場合にのみフィルタされます。

メモ：
VLAN インタフェースには同じ方向のパケットフィルタを設定できません。設定がある場合は、先に元の設定を削除してください。
同じ方向のパケットフィルタを設定してエラーが表示された場合は、**display packet-filter verbose** コマンドで正常に適用されていない ACL を確認できます。

1.7.2 フィルタリングのログ作成と出力間隔の設定

出力間隔を設定したのち、装置は information center にパケットフィルタリングのログを定期的に出力することができます。ログにはパケットにマッチする数、マッチした ACL ルールが含まれます。information center の詳細は、オペレーションマニュアルのセクション 9 *システム管理”Information Center”*を参照してください。

以下にフィルタリングログの出力設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. フィルタリングのログ出力を設定し、出力間隔を設定する	**acl logging interval** *interval*	デフォルト：0分 0分を設定した場合、ログを出力しません。

1.8 ACLの表示と維持

すべての view で **display** コマンドを実行でき、user view で **reset** コマンドを実行できます。

操作	コマンド
ACLの設定とマッチした統計情報を表示する	**display acl** [**ipv6** | **mac**] { *acl-number* | **all** | **name** *acl-name* }
インタフェースに適用したACLが正常に動作したかどうかパケットフィルタの状態を表示する	**display packet-filter** { **interface** [*interface-type interface-number*] [**inbound** | **outbound**] | **interface** *vlan-interface vlan-interface-number* [**inbound** | **outbound**] [**slot** *slot-number*] }
パケットフィルタの統計情報を表示する	**display packet-filter statistics interface** *interface-type interface-number* { **inbound** | **outbound** } [[**ipv6** | **mac**] { *acl-number* | **name** *acl-name* }] [**brief**]
パケットフィルタの累積統計情報を表示する	**display packet-filter statistics sum** { **inbound** | **outbound** } [**ipv6** | **mac**] { *acl-number* | **name** *acl-name* } [**brief**]
パケットフィルタの詳細情報を表示する	**display packet-filter verbose interface** *interface-type interface-number* { **inbound** | **outbound** } [[**ipv6** | **mac**] { *acl-number* | **name** *acl-name* }] [**slot** *slot-number*]
QoSおよびACLリソースの使用率を表示する	**display qos-acl resource** [**slot** *slot-number*]
ACLの統計情報を削除する	**reset acl** [**ipv6** | **mac**] **counter** { *acl-number* | **all** | **name** *acl-name* }
パケットフィルタの累積統計を含む統計情報を削除する	**reset packet-filter statistics interface** [*interface-type interface-number*] { **inbound** | **outbound** } [[**ipv6** | **mac**] { *acl-number* | **name** *acl-name* }]

1.9 ACL設定例

1.9.1 ネットワーク要件

会社は Device を通して Department が相互に通信します。ACL を以下のように設定します。

- 社長室からの経理データベースへのアクセスを常時許可します。

- 経理部門からの経理データベースへのアクセス許可を平日 8:00～18:00 までに制限します。
- 上記 2 部門以外からの経理データベースへのアクセスを常時拒否します。

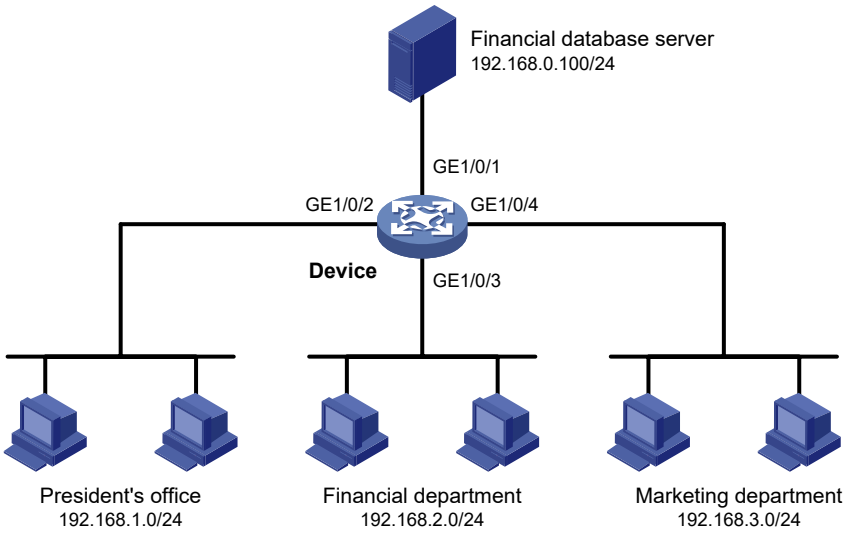


図 1-1 ネットワーク図

1.9.2 設定手順

勤務時間を平日 8:00～18:00 として設定します。

```
<Device> system-view
[Device] time-range work 08:0 to 18:00 working-day
```

拡張 IPv4 ACL 3000 を作成します。

```
[Device] acl advanced 3000
```

社長室から経理データベースサーバへのアクセスを許可するルールを作成します。

```
[Device-acl-ipv4-adv-3000] rule permit ip source 192.168.1.0 0.0.0.255 destination 192.168.0.100 0
```

経理部門から経理データベースサーバへの平日の勤務時間内でのアクセスを許可するルールを作成します。

```
[Device-acl-ipv4-adv-3000] rule permit ip source 192.168.2.0 0.0.0.255 destination 192.168.0.100 0 time-range work
```

他部門からの経理データベースサーバへのアクセスを拒否するルールを作成します。

```
[Device-acl-ipv4-adv-3000] rule deny ip source any destination 192.168.0.100 0
[Device-acl-ipv4-adv-3000] quit
```

GigabitEthernet 1/0/1 の出力パケットについて拡張 IPv4 ACL 3000 を適用します。

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] packet-filter 3000 outbound
[Device-GigabitEthernet1/0/1] quit
```

1.9.3 設定の確認

平日の勤務時間において、経理部門の PC から経理データベースサーバへ ping を実行します。（この例では、PC はすべて Windows 2000 以上を使用しています）

```
C:\> ping 192.168.0.100

Pinging 192.168.0.100 with 32 bytes of data:

Reply from 192.168.0.100: bytes=32 time=1ms TTL=255
Reply from 192.168.0.100: bytes=32 time<1ms TTL=255
Reply from 192.168.0.100: bytes=32 time<1ms TTL=255
Reply from 192.168.0.100: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.0.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

平日の勤務時間において、マーケティング部門から経理データベースサーバへ ping を実行します。

```
C:\> ping 192.168.0.100

Pinging 192.168.0.100 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.0.100:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

平日の勤務時間中の Device A での拡張 IPv4 ACL 3000 の統計情報および設定情報を表示します。

```
[Device] display acl 3000
Advanced IPv4 ACL 3000, 3 rules,
ACL's step is 5
 rule 0 permit ip source 192.168.1.0 0.0.0.255 destination 192.168.0.100 0
 rule 5 permit ip source 192.168.2.0 0.0.0.255 destination 192.168.0.100 0
time-range work (Active)
 rule 10 deny ip destination 192.168.0.100 0
```

出力は、ルール 5 がアクティブであることを示します。

目次

このセクションのページは**6-x-x** です。

2 章 QoS の概要 2-1
2.1 QoS サービスモデル 2-1
2.1.1 ベストエフォートサービスモデル 2-1
2.1.2 IntServ モデル 2-1
2.1.3 DiffServ モデル 2-2
2.2 QoS 技術の概要 2-2
2.2.1 ネットワークの QoS 技術の展開 2-2
2.2.2 装置の QoS 処理フロー 2-3

2章 QoS の概要

QoS（Quality of Service）は、ネットワークトラフィックのフォワーディングプロセスで帯域幅、遅延、パケットロスに関与します。帯域の保証や、遅延、ジッタ、パケットロス率等の低減を行うことによって、QoS の向上ができます。

QoS でトラフィックの優先度付けを行い、各トラフィックに対するネットワークリソースの割り当てを考慮する必要があります。

本章では、QoS サービスモデルと広く使用される QoS の技術を紹介します。

2.1 QoSサービスモデル

この章では一般的な QoS サービスモデルについて説明します。

2.1.1 ベストエフォートサービスモデル

ベストエフォートモデルは、単独のサービスモデルです。最も簡単なサービスモデルです。ベストエフォートサービスモデルは、他のモデルに比べて信頼性は低くなり、遅延や信頼性などの保証はしません。

ベストエフォートサービスモデルは、インターネットでのデフォルトのモデルです。ほとんどのネットワークアプリケーションに適用され、FIFO（First In First Out）キューイングとして実装されます。

2.1.2 IntServ モデル

IntServ（integrated service）は、複数の多様な QoS 要件に適用できる多重サービスモデルです。このモデルは、各データフローに QoS を保証、識別することができ、きめ細かく差別化された QoS を提供します。

IntServ モデルでは、データを送信する前にアプリケーション上で、特定の種類のサービスを使用できるようにネットワークへ要求する必要があります。IntServ の要求は、RSVP シグナリングによって行われます。RSVP は、送信元から宛先までの装置で動作し、データフローがあらかじめ要求/予約したリソースより多くのリソースを使わないよう、各アプリケーションフローをモニタします。

IntServ は装置の高い処理能力が必要となります。IntServ モデルはネットワークへの大量のデータトラフィックが、ストレージデバイスの処理能力に非常に大きな負担がかかります。したがって多くのデータフローが流れるコアインターネット網や何百万のフローが流れるネットワークなどの大規模のネットワークでは利用されず、IntServ モデルは中小規模のネットワークで利用されます。

2.1.3 DiffServ モデル

DiffServ（differentiated service）は、多様な QoS 要件を満たせる多重サービスモデルです。IntServ とは異なり、DiffServ はデータを送信する前に、アプリケーションからネットワークに信号に出す必要がありません。DiffServ は、実行や拡張が容易に行えます。

2.2 QoS技術の概要

QoS 技術には以下の機能があります。

- トラフィックの分類
- トラフィックポリシー
- トラフィックシェーピング
- レートリミット
- 輻輳管理
- 輻輳回避

このマニュアルに記載するすべての QoS 技術は、DiffServ モデルにもとづいています。

🕮 **メモ：**

QX-S1100G シリーズは輻輳回避をサポートしていません。

2.2.1 ネットワークの QoS 技術の展開

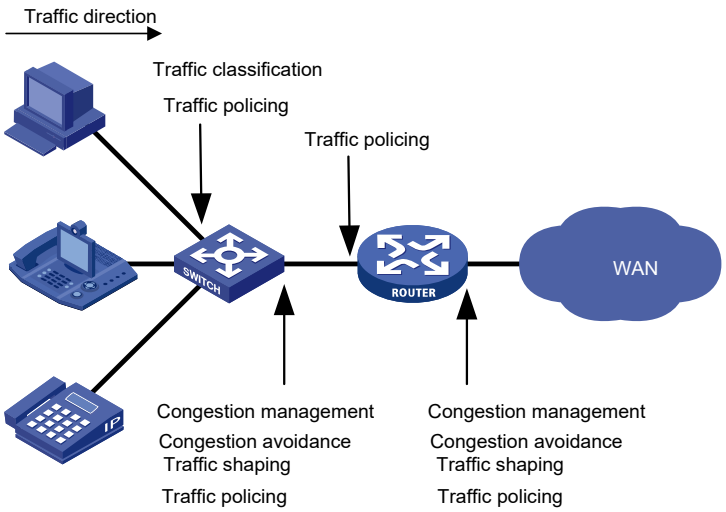


図 2-1 ネットワークの QoS 技術の位置

図 2-1に示すように、以下にトラフィックの分類、トラフィックシェーピング、トラフィックポリシー、輻輳管理、輻輳回避の主要な機能を実装します。

- **トラフィックの分類**－異なった特性、異なったクラスのパケットを組織化するために、ある評価基準を使用します。トラフィックの分類にもとづいて、差別化されたサービスを提供することができます。
- **トラフィックポリシー**－トラフィックが設定したしきい値を超えたとき、ネットワークリソースの過剰使用を防ぐため、フローの制限等の対策を施行できます。トラフィックポリシーは、ポートの入力トラフィック、出力トラフィックの双方向に適用できます。
- **トラフィックシェーピング**－下流の装置向けのトラフィックに適用することで、パケット廃棄と輻輳回避のため、トラフィック出力レートを調整できます。トラフィックシェーピングは、ポートの出力トラフィックに適用します。
- **輻輳管理**－パケットの輻輳が発生した際の転送順序を定義し、リソースのスケジューリングポリシーを提供します。輻輳管理は、ポートの出力トラフィックに適用します。
- **輻輳回避**－ネットワークリソースの使用状態をモニタし、パケットの輻輳が発生すると、パケットを廃棄してキューのトラフィック量を減らすことができます。輻輳回避は、ポートの出力トラフィックに適用します。

2.2.2 装置の QoS 処理フロー

図 2-2に示すように QoS モジュールはトラフィックの処理を行います。

1) トラフィックの分類処理は、後続の QoS アクションを行うため、トラフィックを識別し、分類します。
2) QoS モジュールはトラフィック処理プロセスフェーズとネットワークの状態に従い、分類されたトラフィックでさまざまな QoS アクションを行います。たとえば、以下の処理を行うように QoS モジュールを設定することができます。

- 入力トラフィックのトラフィックポリシー
- 出力トラフィックのトラフィックシェーピング
- 衝突が発生したときに衝突制御を行います。

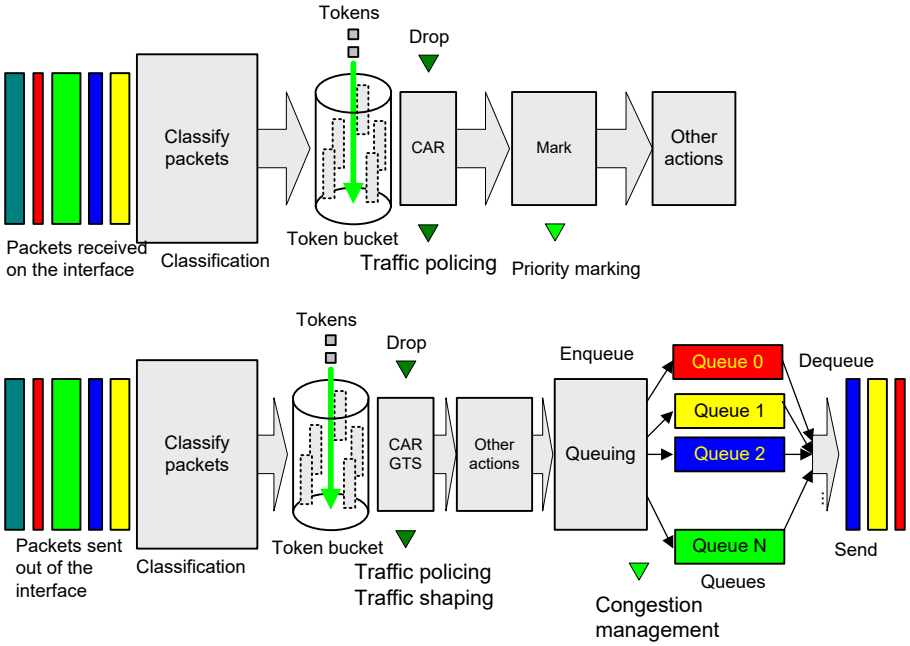


図 2-2 QoS 処理フロー

目次

このセクションのページは**6-x-x** です。

3 章 QoS ポリシー 3-1
3.1 非ポリシーベースのアプローチ 3-1
3.2 ポリシーベースのアプローチ 3-1
3.3 QoS ポリシーの設定手順 3-1
3.4 トラフィッククラスの定義 3-2
3.5 トラフィック動作の定義 3-2
3.6 QoS ポリシーの定義 3-3
3.7 QoS ポリシーの適用 3-3
3.7.1 インタフェースへの QoS ポリシーの適用 3-4
3.7.2 VLAN への QoS ポリシーの適用 3-4
3.7.3 グローバルへの QoS ポリシーの適用 3-4
3.8 QoS ポリシーの情報表示と維持 3-5

3章 QoS ポリシー

QoS 設定は、ポリシーベースあるいは非ポリシーベースの 2 つのアプローチが利用可能です。

3.1 非ポリシーベースのアプローチ

インタフェースに直接レートリミットを設定する等、QoS ポリシーを使用せずに QoS サービスパラメータを使用する設定を非ポリシーベースと呼びます。

3.2 ポリシーベースのアプローチ

QoS ポリシーによる QoS サービスパラメータを使用して設定する設定をポリシーベース MQC（Modular QoS Configuration）と呼びます。ポリシーベースは、トラフィックの異なるクラスに対応するため、トラフィックポリシーやほかの QoS アクションを定義します。

トラフィッククラスはトラフィックを特定するための条件を定義し、論理積（AND）または論理和（OR）の演算子（オペレータ）を使用します。

- オペレータが AND である場合、パケットはトラフィッククラスの一致条件すべてにマッチする必要があります。
- オペレータが OR である場合、パケットはトラフィッククラスの一致条件のいずれかにマッチします。

トラフィック動作（traffic behavior）でパケットの優先順位のマーキングとトラフィックのリダイレクト等の QoS アクションを定義します。

QoS ポリシーでトラフィッククラスとトラフィック動作を関連づけます。トラフィッククラスで定義した条件で特定されたトラフィックをトラフィック動作で定義した QoS アクションで処理させることができます。

3.3 QoSポリシーの設定手順

図 3-1に QoS ポリシーの設定手順を示します。

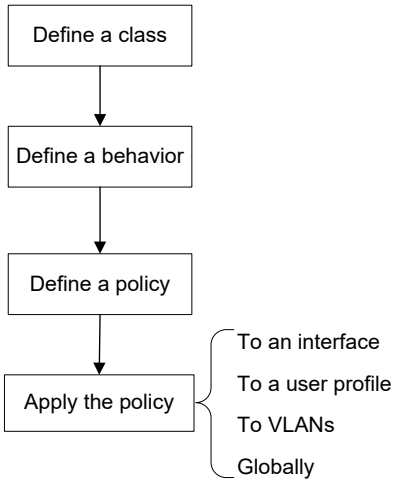


図 3-1 QoS ポリシーの設定手順

3.4 トラフィッククラスの定義

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． トラフィッククラスを作成し、演算子を定義して class view に移行する	**traffic classifier** *classifier-name* [**operator** { **and** | **or** }]	デフォルト：設定なし
3． 一致条件を設定する	**if-match** *match-criteria*	デフォルト：設定なし **if-match**コマンドの詳細は、コマンドマニュアルのセクション6 *ACL and QoS*”*QoSポリシー*”を参照してください。

3.5 トラフィック動作の定義

トラフィック動作でトラフィックフィルタリング、トラフィックポリシー、プライオリティマーキング等の QoS の動作を定義します。

以下にトラフィック動作の設定手順を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． トラフィック動作を作成し traffic behavior view に移行する	**traffic behavior** *behavior-name*	デフォルト：設定なし

操作	コマンド	補足
3． QoS の動作を定義する	トラフィックポリシー、トラフィックフィルタリング、プライオリティマーキング、クラスベースアカウンティングなどのトラフィック動作の目的に応じて、オペレーションマニュアルのセクション6 *ACL and QoS* を参照してください。	デフォルト：設定なし

3.6 QoSポリシーの定義

トラフィック動作を QoS ポリシーのトラフィッククラスに関連づけます。トラフィック動作は、クラスの一致条件にマッチしたパケットに実行されます。

トラフィッククラス定義のために QoS ポリシーによって ACL が参照された場合は、ACL のアクション（許可あるいは拒否）は無視されます。アクションはトラフィック動作に関連づけられたものが使われます。

クラスとトラフィック動作の関連づけ手順を以下に示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． QoS ポリシーを作成し、qos policy view に移行する	**qos policy** *policy-name*	デフォルト：設定なし
3． トラフィッククラスとトラフィック動作を関連づける	**classifier** *classifier-name* **behavior** *behavior-name* [**insert-before** *before-classifier-name*]	デフォルト：設定なし 複数、作成する場合、コマンドを繰り返してください。

3.7 QoSポリシーの適用

QoS ポリシーは以下の種類に適用できます。

- **インタフェース**－QoS ポリシーはインタフェースで送受信したトラフィックに適用します。
- **VLAN**－QoS ポリシーは VLAN のすべてのポートで送受信したトラフィックに適用します。
- **グローバル**－QoS ポリシーはすべてのポートで送受信したトラフィックに適用します。

QoS ポリシーを適用している場合、QoS ポリシーを適用した後でも QoS ポリシーのトラフィッククラス、トラフィック動作、トラフィッククラスとトラフィッククラスの関連づけの設定を修正できます。トラフィッククラスがトラフィックの分類の ACL を参照する場合、ACL を削除あるいは修正できます。（たとえば、ACL のルールへの追加、削除、修正です）

3.7.1 インタフェースへの QoS ポリシーの適用

1 つの QoS ポリシーを複数のインタフェースに適用できますが、インタフェースの 1 つの方向（インバウンド/アウトバウンド）に適用できる QoS ポリシーは 1 つのみです。

インタフェースの出力トラフィックに適用された QoS ポリシーはローカルパケットに適用されません。ローカルパケットは、装置の正常動作を維持するためのパケットです。一般的なローカルパケットはリンクのメンテナンスパケットやルーティング､LDP パケット、RSVP パケット、SSH パケットがあります。

以下にインタフェースへの QoS ポリシーの適用手順を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． interface view に移行する	**interface** *interface-type interface-number*	―
3． QoS ポリシーを適用する	**qos apply policy** *policy-name* { **inbound** | **outbound** }	デフォルト：設定なし

3.7.2 VLAN への QoS ポリシーの適用

QoS ポリシーを VLAN に対してトラフィック制御のために適用できます。

I. 設定の制限とガイドライン

QoS ポリシーは、GVRP によって作成された VLAN を含むダイナミック VLAN には適用できません。

II. 設定手順

VLAN への QoS ポリシーの適用手順を以下に示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． QoS ポリシーを適用する	**qos vlan-policy** *policy-name* **vlan** *vlan-id-list* { **inbound** | **outbound** }	デフォルト：設定なし

3.7.3 グローバルへの QoS ポリシーの適用

すべてのポートのインバウンド/アウトバウンド方向に QoS ポリシーを適用できます。

グローバルへの QoS ポリシーの適用手順を以下に示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． QoS ポリシーを適用する	**qos apply policy** *policy-name* **global** { **inbound** | **outbound** }	デフォルト：設定なし

3.8 QoSポリシーの情報表示と維持

すべての view で **display** コマンドを実行でき、user view で **reset** コマンドを実行できます。

操作	コマンド
トラフィッククラスの設定情報を表示する	**display traffic classifier user-defined** [*classifier-name*] [**slot** *slot-number*]
トラフィック動作についての情報を表示する	**display traffic behavior user-defined** [*behavior-name*] [**slot** *slot-number*]
QoSポリシーの設定を表示する	**display qos policy user-defined** [*policy-name* [**classifier** *classifier-name*]] [**slot** *slot-number*]
指定したinterface、あるいはすべてのinterfaceのQoSポリシーの設定を表示する	**display qos policy interface** [*interface-type interface-number*] [**inbound** | **outbound**]
VLANに適用されたQoSポリシーについての情報を表示する	**display qos vlan-policy** { **name** *policy-name* | **vlan** [*vlan-id*] } [**slot** *slot-number*] [**inbound** | **outbound**]
グローバルに適用されたQoSポリシーについての情報を表示する	**display qos policy global** [**slot** *slot-number*] [**inbound** | **outbound**]
VLANに適用されたQoSポリシーの統計情報を削除する	**reset qos vlan-policy** [**vlan** *vlan-id*] [**inbound** | **outbound**]
グローバルに適用されたQoSポリシーの統計情報を削除トする	**reset qos policy global** [**inbound** | **outbound**]

目次

このセクションのページは**6-x-x** です。

4 章 プライオリティマッピング 4-1
4.1 概要 4-1
4.1.1 プライオリティの導入 4-1
4.1.2 プライオリティマッピング 4-1
4.2 プライオリティマッピングの設定作業リスト 4-2
4.3 プライオリティマッピングの設定 4-2
4.4 プライオリティマッピングのパケットプライオリティを信用するインタフェースの設定4-3
4.5 インタフェースのポートプライオリティの変更 4-3
4.6 プライオリティマッピングの表示と維持 4-4
4.7 プライオリティマッピングの設定例 4-4
4.7.1 トラステッドモードの設定例 4-4
4.7.2 プライオリティマッピングテーブルとプライオリティマーキングの設定例 4-5

4章 プライオリティマッピング

4.1 概要

パケットを受信すると、装置は以下のどちらかのプライオリティにもとづいて QoS プライオリティのパラメータをパケットに割り当てます。

- パケットに含まれているプライオリティのフィールドの値
- 入力ポートのポートプライオリティ

このプロセスはプライオリティマッピングと呼ばれます。このプロセスの間、装置はプライオリティマッピングのルールに従ってパケットのプライオリティを修正することができます。QoS プライオリティのパラメータはパケットのスケジュールプライオリティとフォワーディングプライオリティを決めます。

プライオリティマッピングはプライオリティマッピングテーブルに実装され、以下のプライオリティを決定します。

- 802.1p プライオリティ
- DSCP
- IP プレシーデンス
- ローカルプレシーデンス

4.1.1 プライオリティの導入

プライオリティは、ローカルプライオリティとパケットに含まれているプライオリティと、スケジューリング用にローカルに割り当てられるプライオリティがあります。

パケットに含まれているプライオリティは、802.1p プライオリティ、DSCP プレシーデンス、IP プレシーデンスがあります。パケットに含まれるプライオリティは、他の装置でも使用されるため、ネットワークに影響します。プライオリティの詳細は、オペレーションマニュアルのセクション 6 *ACL and QoS ”付録”* を参照してください。

ローカルプライオリティは装置内でのみ使用されるため、ネットワークに影響しません。ローカルプライオリティは、ローカルプレシーデンスと呼ばれ、キューのスケジューリング用に使用されます。ローカルプレシーデンスの値は出力キューに対応します。ローカルプレシーデンスの値が高いパケットが高い出力キューに割り当てられます。

4.1.2 プライオリティマッピング

装置はさまざまなプライオリティマッピングのタイプを提供します。プライオリティマッピングは、プライオリティマッピングテーブルを参照し、その後のパケットを処理するため、パケットに割り当てるプライオリティを決定します。

デフォルトのプライオリティマップ（オペレーションマニュアルのセクション 6 *ACL and QoS ”付録”の”デフォルトプライオリティ”* を参照してください）はプライオリティマッピングに利用できます。デフォルトのマップは、ほとんどの場合において通常に使用

することができます。デフォルトのプライオリティマップでは要件を満たすことができない場合、必要に応じてプライオリティのマッピングを変更することができます。

4.2 プライオリティマッピングの設定作業リスト

以下の方法を使用してプライオリティマッピングを設定することができます。

プライオリティマッピングテーブル、ポートのプライオリティのトラステッドモード、ポートプライオリティを変更することによって、プライオリティマッピングを変更することができます。

- **プライオリティのトラステッドモードの設定**－プライオリティマッピングで運ばれた受信パケットのトラステッドプライオリティタイプ（たとえば、802.1p）を検索するために使用するプライオリティを設定することができます。システムはターゲットのプライオリティのタイプと値にトラステッドプライオリティの値をマッピングします。
- **ポートプライオリティの変更**－パケットのプライオリティを信用しない場合、受信パケットのポートプライオリティが使用されます。ポートのポートプライオリティを変更することによって、ポートで受信するパケットのプライオリティを変更します。

プライオリティマッピングを設定するには、以下の手順を実施してください。

作業リスト
（オプション設定項目）プライオリティマッピングの設定
（必須設定項目）いずれか1つを設定してください。 • プライオリティマッピングのパケットプライオリティを信用するインタフェースの設定 • インタフェースのポートプライオリティの変更

4.3 プライオリティマッピングの設定

装置は以下のタイプのプライオリティマッピングを提供します。

プライオリティマッピング	説明
dot1p-lp	802.1p-ローカルプライオリティマッピングテーブルです。
dscp-dot1p	DSCP-802.1pプライオリティマッピングテーブルです。
dscp-dscp	DSCP-DSCPプライオリティマッピングテーブルです。

以下にプライオリティマッピングの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	－
2. priority map view に移行する	**qos map-table** { **dot1p-lp** | **dscp-dot1p** | **dscp-dscp** }	－

操作	コマンド	補足
3. プライオリティマッピングを設定する	**import** *import-value-list* **export** *export-value*	デフォルト : デフォルトのプライオリティマップ 詳細はオペレーションマニュアルのセクション6 *ACL and QoS ”付録”* を参照してください。 新規の設定は、既存に上書きします。

4.4 プライオリティマッピングのパケットプライオリティを信用するインタフェースの設定

インタフェースのプライオリティマッピングのパケットで運ばれた特定のプライオリティフィールドを信用するように装置を設定できます。

インタフェース上で信用できるパケットのプライオリティタイプを設定する場合は、以下の内で使用可能なキーワードを使用します。

- **dot1p**: マッピングのため受信したパケットの 802.1p プライオリティを使用します。
- **dscp**: マッピングのため受信した IP パケットの DSCP プレシーデンスを使用します。

プライオリティトラステッドモードの設定手順を以下に示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. interface view に移行する	**interface** *interface-type interface-number*	―
3. パケットプライオリティタイプの信用を設定する	**qos trust** { **dot1p** | **dscp** }	デフォルト：信用しない

4.5 インタフェースのポートプライオリティの変更

インタフェースがパケットのプライオリティを信用しない設定の場合、装置は受信したパケットのプライオリティパラメータセットを探すために、自身のポートプライオリティを使用します。ポートプライオリティを変更することで、異なるインタフェースで受信されたトラフィックに優先順位を付けることができます。

ポートプライオリティの変更手順を以下に示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. interface view に移行する	**interface** *interface-type interface-number*	―
3. ポートプライオリティを設定する	**qos priority** *priority-value*	デフォルト：0

4.6 プライオリティマッピングの表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
プライオリティマッピングの設定を表示する	**display qos map-table** [**dot1p-lp** | **dscp-dot1p** | **dscp-dscp**]
ポートに設定されているトラステッドプレシーデンスを表示する	**display qos trust interface** [*interface-type interface-number*]

4.7 プライオリティマッピングの設定例

4.7.1 トラステッドモードの設定例

I. ネットワーク要件

図 4-1に示すように設定します。

- Device A から Device C へのトラフィックの IP プレシーデンスは 3 です。
- Device B から Device C へのトラフィックの IP プレシーデンスは 1 です。

Device C の GigabitEthernet 1/0/3 でパケットが輻輳した場合、Device C は Device A からサーバへのパケットを優先します。

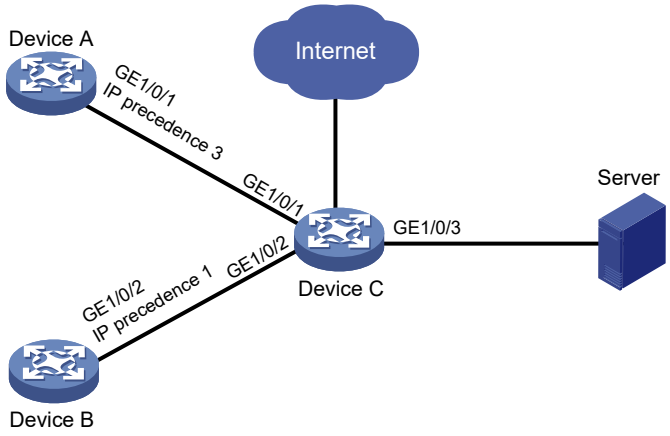


図 4-1 ネットワーク図

II. 設定手順

GigabitEthernet 1/0/1、GigabitEthernet 1/0/2 にポートプライオリティを設定します。GigabitEthernet 1/0/1 のプライオリティは GigabitEthernet 1/0/2 のプライオリティよりも高いことを確認してください。

```
<DeviceC> system-view
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] qos priority 3
[DeviceC-GigabitEthernet1/0/1] quit
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] qos priority 1
[DeviceC-GigabitEthernet1/0/2] quit
```

4.7.2 プライオリティマッピングテーブルとプライオリティマーキングの設定例

I. ネットワーク要件

図 4-2に示すように、プライオリティマッピングテーブルとプライオリティマーキングを設定します。

- 営業部は装置の GigabitEthernet 1/0/1 に接続し、営業部からのトラフィックの 802.1p プライオリティを 3 に設定します。
- 研究開発部は装置の GigabitEthernet 1/0/2 に接続し、研究開発部からのトラフィックの 802.1p プライオリティを 4 に設定します。
- 管理部は装置の GigabitEthernet 1/0/3 に接続し、管理部からのトラフィックの 802.1p プライオリティを 5 に設定します。

表 4-1に示すようにポートプライオリティ、802.1p-local プライオリティマッピングテーブル、プライオリティマーキングを設定します。

表 4-1 設定計画

トラフィック先	トラフィックプライオリティの順番	キューイング計画		
		送信元	送信キュー	キュープライオリティ
Public servers	研究開発部>管理部>営業部	研究開発部	6	High
		管理部	4	Medium
		営業部	2	Low
Internet	管理部>営業部>研究開発部	研究開発部	2	Low
		管理部	6	High
		営業部	4	Medium

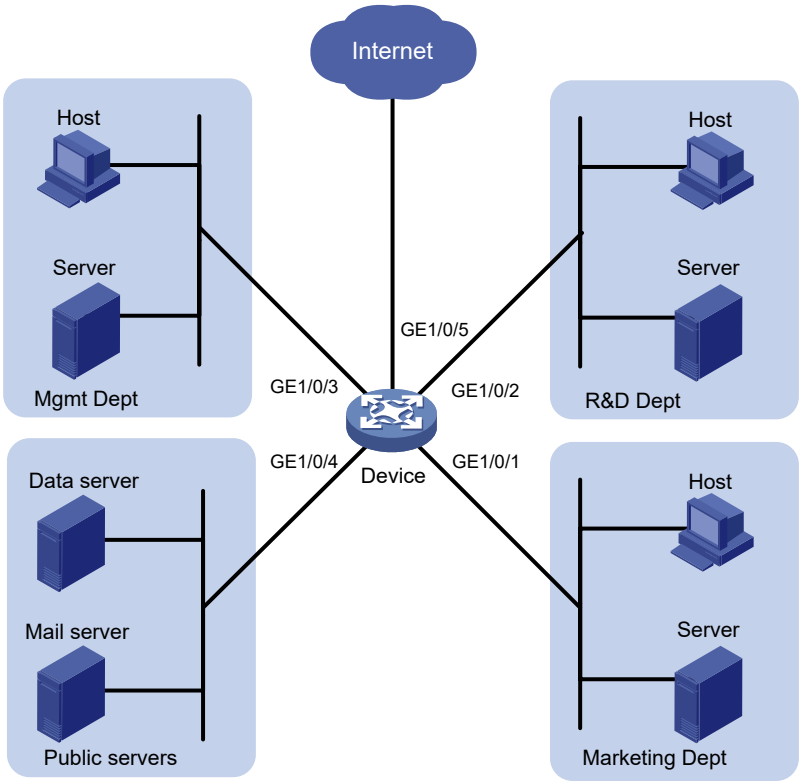


図 4-2 ネットワーク図

II. 設定手順

1)　ポートプライオリティを設定します。

GigabitEthernet 1/0/1 のポートプライオリティを 3 に設定します。

```
<Device> system-view
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] qos priority 3
[Device-GigabitEthernet1/0/1] quit
```

GigabitEthernet 1/0/2 のポートプライオリティを 4 に設定します。

```
[Device] interface gigabitethernet 1/0/2
[Device-GigabitEthernet1/0/2] qos priority 4
[Device-GigabitEthernet1/0/2] quit
```

GigabitEthernet 1/0/3 のポートプライオリティを 5 に設定します。

```
[Device] interface gigabitethernet 1/0/3
[Device-GigabitEthernet1/0/3] qos priority 5
[Device-GigabitEthernet1/0/3] quit
```

2)　プライオリティマッピングテーブルを設定します。802.1p-ローカルプライオリティのマッピングテーブルを 802.1p プライオリティの値 3、4、5 をローカルプライオリティの 2、6、4 にマップします。

研究開発部、管理部、営業部は public server にアクセスするため、プライオリティを低くします。

```
[Device] qos map-table dot1p-lp
[Device-maptbl-dot1p-lp] import 3 export 2
[Device-maptbl-dot1p-lp] import 4 export 6
[Device-maptbl-dot1p-lp] import 5 export 4
[Device-maptbl-dot1p-lp] quit
```

3)　プライオリティマーキングを設定します。

ACL 3000 を作成します。HTTP のトラフィックに一致するようにルールを設定します。

```
[Device] acl advance 3000
[Device-acl-adv-3000] rule permit tcp destination-port eq 80
[Device-acl-adv-3000] quit
```

トラフィッククラス **http** を作成し、ACL 3000 を一致条件に設定します。

```
[Device] traffic classifier http
[Device-classifier-http] if-match acl 3000
[Device-classifier-http] quit
```

トラフィック動作 **admin** を作成し、管理部向けのマーキングアクションを設定します。

```
[Device] traffic behavior admin
[Device-behavior-admin] remark dot1p 4
[Device-behavior-admin] quit
```

QoS ポリシー**admin** を作成し、トラフィッククラス **http** とトラフィック動作 **admin** を関連づけます。

```
[Device] qos policy admin
[Device-qospolicy-admin] classifier http behavior admin
[Device-qospolicy-admin] quit
```

GigabitEthernet 1/0/3 の入力トラフィックに QoS ポリシー**admin** を適用します。

```
[Device] interface gigabitethernet 1/0/3
[Device-GigabitEthernet1/0/3] qos apply policy admin inbound
```

トラフィック動作 **market** を作成し、営業部向けのマーキングアクションを設定します。

```
[Device] traffic behavior market
[Device-behavior-market] remark dot1p 5
[Device-behavior-market] quit
```

QoS ポリシー**market** を作成し、トラフィッククラス **http** とトラフィック動作 **admin** を関連づけます。

```
[Device] qos policy market
[Device-qospolicy-market] classifier http behavior market
[Device-qospolicy-market] quit
```

GigabitEthernet 1/0/1 の入力トラフィックに QoS ポリシー**market** を適用します。

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] qos apply policy market inbound
```

トラフィック動作 **rd** を作成し、研究開発部向けのマーキングアクションを設定します。

```
[Device] traffic behavior rd
[Device-behavior-rd] remark dot1p 3
[Device-behavior-rd] quit
```

QoS ポリシー**rd** を作成し、トラフィッククラス **http** とトラフィック動作 **rd** を関連づけます。

```
[Device] qos policy rd
[Device-qospolicy-rd] classifier http behavior rd
[Device-qospolicy-rd] quit
```

GigabitEthernet 1/0/2 の入力トラフィックに QoS ポリシー**rd** を適用します。

```
[Device] interface gigabitethernet 1/0/2
[Device-GigabitEthernet1/0/2] qos apply policy rd inbound
```

目次

このセクションのページは**6-x-x** です。

5 章 ラインレート.....5-1
5.1 概要.....5-1
5.1.1 トラフィックレートの検証とトークンバケット.....5-1
5.1.2 ラインレート.....5-1
5.2 インタフェースのラインレートの設定.....5-2
5.3 ラインレートの表示と維持.....5-3

5章 ラインレート

5.1 概要

トラフィックポリシングはネットワークリソース（帯域幅を含みます）の割り当てを手助けし、ネットワーク性能を向上させます。たとえば、特定のパケット転送に使用する帯域幅を制限することで、バーストトラフィックに起因するネットワークの輻輳を回避したりすることができます。

ラインレート(レートリミット)は、トラフィックの仕様に従ってトラフィックレートとリソース使用量を制御します。トークンバケットを使用して、トラフィックの仕様を評価できます。

5.1.1 トラフィックレートの検証とトークンバケット

I. トークンバケットの機能

トークンバケットは、トークンを保持するための一定の容量を持つ容器と見なすことができます。システムは、設定されたレートでトークンをバケットに入れます。トークンバケットが一杯になると、トークンがバケットからあふれます。

II. トークンバケットを使用したトラフィックレートの検証

トラフィックは、バケット内のトークンの数を見て検証します。パケット転送に対して、バケット内のトークンの数に余裕がある場合、以下のように対応します。

- トラフィックは仕様に対応します。（適合トラフィックと呼ばれます）
- 対応するトークンがバケットから取り外されます。

そうでない場合、トラフィックは仕様に対応しません。（余剰トラフィックと呼ばれます）

トークンバケットは以下の設定可能なパラメータがあります。

- トークンが許可されたトラフィック平均レートによってバケットに入るレートです。通常 CIR（Committed Information Rate）によって設定されます。
- バーストサイズあるいはトークンバケットの容量です。各バーストで許可された最大トラフィックサイズです。通常 CBS（Committed Burst Size）によって設定されます。設定されたバーストサイズは最大パケットサイズよりも大きくする必要があります。

各パケットが到着するたびに検証されます。

5.1.2 ラインレート

ラインレート（レートリミット）は、入出力トラフィックのレートを管理します。たとえば出力トラフィックについて説明します。

物理インタフェースのラインレートは、パケット（クリティカルパケットを除く）の最大転送レートを指定します。

ラインレートも、トラフィックを管理するためにトークンバケットを使用します。ラインレートがインタフェースで設定されるとき、トークンバケットはインタフェースを通してすべてのパケットが送信されます。もしトークンバケットに十分なトークンがある場合、パケットを転送することができます。そうでなければ、パケットは輻輳制御のため QoS キューに入ります。このように物理インタフェースを通したトラフィックが管理されます。

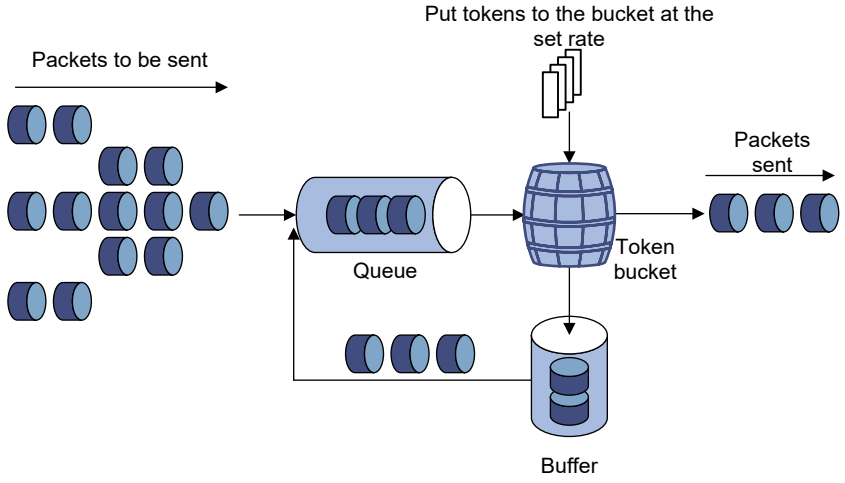


図 5-1 ラインレートの実装

トークンバケットメカニズムは、バーストデータを適応させるときに、トラフィックレートを制限します。十分なトークンが有効である場合、バーストトラフィックは転送されます。トークンが不十分である場合、効率的なトークンがトークバケットで作成されるまでパケットは転送できません。トラフィックレートを、トークン作成用のレートに制限します。

ラインレートは物理インタフェースのすべてのパケットの全レートを管理します。物理インタフェースの全トラフィックレートを管理するトラフィックポリシングよりも簡単に利用できます。

5.2 インタフェースのラインレートの設定

物理インタフェースのラインレート（レートリミット）は、受信または送信パケットの最大レートで設定します。

ラインレートの設定手順を以下に示します。

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

操作	コマンド	補足
2． interface view に移行する	**interface** *interface-type interface-number*	―
3． ラインレートを設定する	**qos lr** { **inbound** | **outbound** } **cir** *committed-information-rate* [**cbs** *committed-burst-size*]	デフォルト：設定なし

5.3 ラインレートの表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
インタフェースのラインレートの設定と統計情報を表示する	**display qos lr interface** [*interface-type interface-number*]

目次

このセクションのページは**6-x-x** です。

6 章 輻輳制御 6-1
6.1 概要 6-1
6.1.1 SP キューイング 6-1
6.1.2 WRR キューイング 6-2
6.2 設定作業リスト 6-4
6.3 キューごとの輻輳制御の設定 6-4
6.3.1 SP キューイングの設定 6-4
6.3.2 WRR キューイングの設定 6-4
6.3.3 SP+WRR キューイングの設定 6-4
6.4 輻輳制御の表示と維持 6-6

6章 輻輳制御

6.1 概要

輻輳は、トラフィックサイズがリンクあるいはノードの処理容量を超えるとき、リンクあるいはノードで発生します。これは、統計多重化ネットワークで起こる輻輳の典型であり、その他にも、リンク障害、リソース不足、その他 様々な原因によって発生します。

図 6-1に 2 つの典型的な輻輳のシナリオを示します。

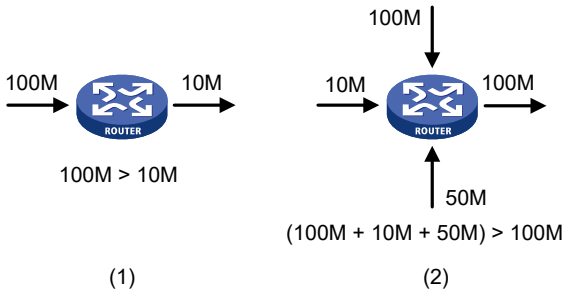


図 6-1 トラフィックの輻輳のシナリオ

輻輳は、以下のような悪影響をもたらします。

- パケット伝送の遅延およびジッタの増加
- ネットワークのスループットおよびリソースの使用効率の減少
- ネットワークリソース（特にメモリ）の枯渇やシステムの故障

輻輳は、スイッチネットワークとマルチユーザーアプリケーション環境では避けられません。ネットワークサービスのパフォーマンスを向上させるために、輻輳に対処する適切な措置の管理と制御を行う必要があります。

輻輳管理の鍵は、パケットを送信する順序を定めたポリシーのリソースを設定することです。

輻輳管理はポートを除外するトラフィックを区分けし、分類するためにキューイングとスケジューリングアルゴリズムを使用します。

装置は以下のキューースケジューリングメカニズムをサポートします。

6.1.1 SP キューイング

SP キューイングは、輻輳が発生するときに応答遅延を減らすように、優先的なサービスが要求されるミッションクリティカルなアプリケーションのために設計されています。

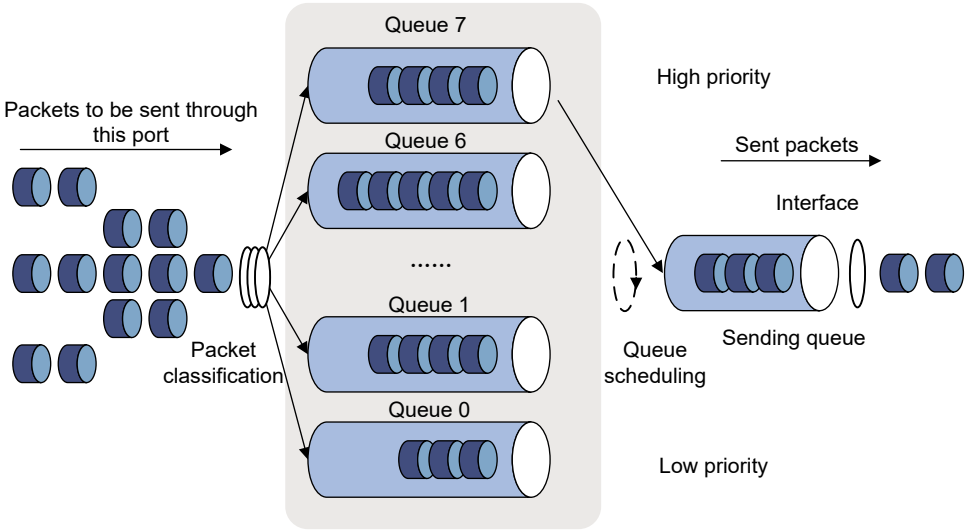


図 6-2 SP キューイング

図 6-2に示すように、SP キューイングはポートに 8 つにクラス分けしたキューを割り当てます。キューの番号 7 から 0 の順に優先順位は低くなります。

SP キューイングは、優先順位が高い方から低い方へ順番に従って 8 つのキューを厳格にスケジューリングします。最初にキューの中のもっとも優先順位が高いパケットを送信します。もっとも高いプライオリティのキューが空のとき、キューの中でその次に優先度の高いプライオリティのパケットが送信されます。ミッションクリティカルなパケットを高いプライオリティキューに割り当てることで、常に最初に処理されるようにし、一般サービスパケットは低いプライオリティに順番付けすることにより、高いプライオリティキューが空のときに送信するようになります。
SP キューの欠点は、より高い優先度のキューにパケットがある場合、低い優先度のキューのパケットは転送できないということです。これは、低い優先度トラフィックの通信停止を引き起こします。

6.1.2 WRR キューイング

図 6-3に示すように、WRR キューイングでは、すべてのキューが一定時間処理されるように、すべてのキューを順番にスケジュールします。

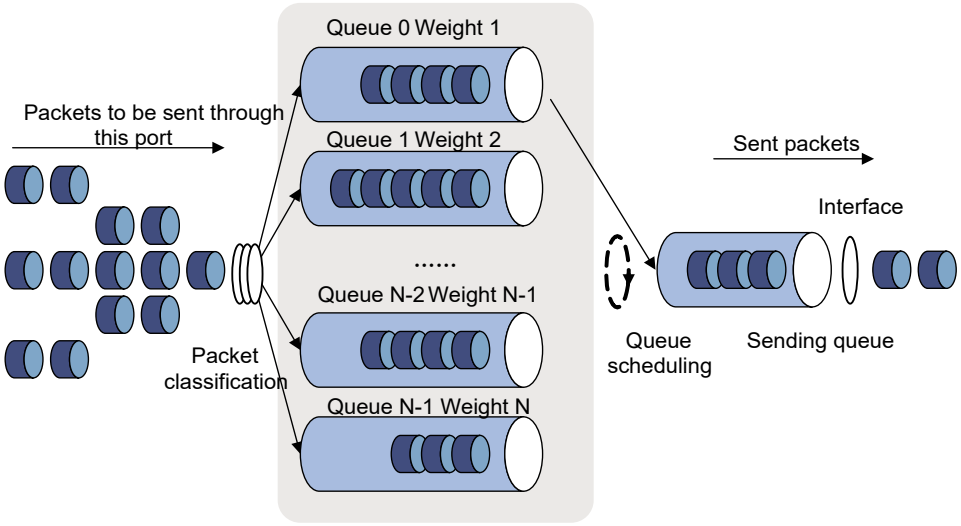


図 6-3 WRR キューイング

ポートに 8 つの出力キューがあると仮定します。WRR は、各キューへリソース割り当てを決めるため、w7、w6、w5、w4、w3、w2、w1、w0 と示される 8 つの重み付けを割り当てます。キューの重みづけはキューに割り当てられたリソースの割合を決定します。100Mbps のポートでは、重みづけの値を 50、30、10、10、50、30、10、10（それぞれ w7、w6、w5、w4、w3、w2、w1、w0 に対応します）に設定できます。このように、最低優先度のキューも、少なくとも 5Mbps（100Mbps ×（最低優先度の重み 10/重みづけの合計 200））の帯域幅が確保できます。こうして、低優先度のキューがなかなか転送されない可能性がある SP キューイングの欠点を回避できます。

WRR キューイングのもう 1 つの利点は、キューが順番にスケジュールされるときに、各キューの処理時間が固定されないことです。キューが空の場合、次のキューはすぐにスケジュールされます。これにより、帯域幅の リソース 使用効率が向上します。

WRR キューイングは以下のタイプがあります。

- **基本 WRR キューイング**– 複数のキューが含まれます。各キューの重みを設定することができます。WRR は総当たりでユーザ定義のパラメータにもとづいてキューをスケジュールすることができます。
- **グループベース WRR キューイング**– すべてのキューが WRR によってスケジューリングされます。出力キューを WRR プライオリティキューグループ 1、WRR プライオリティキューグループ 2 に分割することができます。総当たりのキュースケジューリングは最初にグループ 1 を実行します。グループ 1 が空きの場合、グループ 2 が実行されます。

グループベース WRR キューイングが有効なインタフェースでは、SP グループにキューを割り当てることができます。SP グループのキューは SP にスケジューリングされます。SP グループは WRR グループよりも高いプライオリティを持ちます。

🕮 **メモ：**

基本 WRR キューイングはサポートしていません。WRR プライオリティキューグループはグループ 1 のみサポートします。

6.2 設定作業リスト

作業リスト
（必須設定項目）キューごとの輻輳制御を設定するため、以下のどちらかを設定してください。 ● SPキューイングの設定 ● WRRキューイングの設定 ● SP+WRRキューイングの設定

6.3 キューごとの輻輳制御の設定

ポートにもとづいてキューごとのトラフィックの輻輳を制御します。

6.3.1 SP キューイングの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． interface *view に移行する*	**interface** *interface-type interface-number*	―
3． SP キュースケジューリングアルゴリズムを設定する	**qos sp**	デフォルト: パケット単位の WRRキューイング

6.3.2 WRR キューイングの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． interface view に移行する	**interface** *interface-type interface-number*	―
3． パケット単位の WRR キューイングを有効にする	**qos wrr weight**	デフォルト: パケット単位の WRRキューイング
4． WRR グループにキューを割り当て、キューのスケジュールパラメータを設定する	**qos wrr** *queue-id* **group 1 weight** *schedule-value*	デフォルト : WRRが有効なすべてのキューはWRRグループ1にあります。キュー0～キュー7の重みは、それぞれ1、2、3、4、5、9、13、15です。

6.3.3 SP+WRR キューイングの設定

スケジューリングの重みを設定するには、WRR キューイングを有効にするときに指定したものと同じスケジューリング単位を指定する必要があります。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． interface view に移行する	**interface** *interface-type interface-number*	ー
3． パケット単位の WRR キューイングを有効にする	**qos wrr weight**	デフォルト: パケット単位の WRRキューイング
4． SP キュースケジュールグループにキューを割り当てる	**qos wrr** *queue-id* **group sp**	デフォルト : WRRキューが有効なポートはWRRグループ1です キューがインタフェースのトラフィックの負荷でもっとも低いプライオリティを持つ場合、SPグループのキューはスケジューリングされません。
5． WRR グループにキューを割り当て、キューのスケジュールパラメータを設定する	**qos wrr** *queue-id* **group 1 weight** *schedule-value*	デフォルト : WRRが有効なすべてのキューはWRRグループ1にあります。キュー0～キュー7の重みは、それぞれ1、2、3、4、5、9、13、15です。

I. 設定例

1)　ネットワーク要件

- □　GigabitEthernet 1/0/1 で SP+WRR キューイングを設定します。
- □　GigabitEthernet 1/0/1 のキュー4、5、6、7 に SP グループを割り当てます。
- □　GigabitEthernet 1/0/1 のキュー0、1、2、3 に WRR グループ 1 を割り当てます。それぞれ重みづけ 1、2、1、3 を設定します。

2)　設定手順

system view に移行します。

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

GigabitEthernet11/0/1 に SP+WRR キューイングを設定します。

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] qos wrr weight
[Switch-GigabitEthernet1/0/1] qos wrr 4 group sp
[Switch-GigabitEthernet1/0/1] qos wrr 5 group sp
[Switch-GigabitEthernet1/0/1] qos wrr 6 group sp
[Switch-GigabitEthernet1/0/1] qos wrr 7 group sp
[Switch-GigabitEthernet1/0/1] qos wrr 0 group 1 weight 1
[Switch-GigabitEthernet1/0/1] qos wrr 1 group 1 weight 2
[Switch-GigabitEthernet1/0/1] qos wrr 2 group 1 weight 1
[Switch-GigabitEthernet1/0/1] qos wrr 3 group 1 weight 3
```

6.4 輻輳制御の表示と維持

すべての view で **display** コマンドが実行できます。

操作	コマンド
SPキューイングの情報を表示する	**display qos queue sp interface** [*interface-type interface-number*]
WRRキューイングの情報を表示する	**display qos queue wrr interface** [*interface-type interface-number*]
キューベースの出力トラフィックの統計情報を表示する	**display qos queue-statistics interface** [*interface-type interface-number*] **outbound**
インタフェースの統計情報を削除する	**reset counters interface** [*interface-type interface-number*]

目次

このセクションのページは**6-x-x** です。

7 章 トラフィックフィルタリング 7-1
7.1 設定手順 7-1
7.2 設定例 7-2
7.2.1 ネットワーク要件 7-2
7.2.2 設定手順 7-2

7章 トラフィックフィルタリング

トラフィックフィルタリングは、設定したアクションとクラスを組み合わせることにより受信/送信トラフィックをフィルタします。たとえば、ネットワークの状態にしたがって指定した送信元 IP アドレスのパケットをフィルタすることができます。

7.1 設定手順

以下にトラフィックフィルタリングの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． トラフィッククラスを作成し、traffic class view に移行する	**traffic classifier** *classifier-name* [**operator** { **and** | **or** }]	デフォルト：設定なし
3． マッチ条件を設定する	**if-match** *match-criteria*	デフォルト：設定なし
4． system view に戻る	**quit**	―
5． トラフィック動作を作成し、traffic behavior view に移行する	**traffic behavior** *behavior-name*	デフォルト：設定なし
6． トラフィックフィルタリングアクションを設定する	**filter** { **deny** | **permit** }	デフォルト：設定なし
7． system view に戻る	**quit**	―
8． QoS ポリシーを作成し、QoS policy view に移行する	**qos policy** *policy-name*	デフォルト：設定なし
9． トラフィッククラスと QoS ポリシーのトラフィック動作を関連づける	**classifier** *classifier-name* **behavior** *behavior-name*	デフォルト：設定なし
10．system view に戻る	**quit**	―
11．QoS ポリシーを適用する	● VLANにQoSポリシーを適用する ● インタフェースにQoSポリシーを適用する ● グローバルにQoSポリシーを適用する	必要とされるアプリケーションの宛先の1つを選択してください。 デフォルト：設定なし
12．(オプション設定項目) トラフィックフィルタリングの設定を表示する	**display traffic behavior user-defined** [*behavior-name*]	すべてのviewで実行できます。

7.2 設定例

7.2.1 ネットワーク要件

図 7-1に示すように、GigabitEthernet 1/0/1 で受信し、送信元ポート番号 21 で、パケットをフィルタするためにトラフィックフィルタリングを設定します。

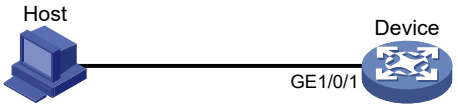


図 7-1 ネットワーク図

7.2.2 設定手順

拡張 ACL 3000 を作成し、送信元ポートが 21 のパケットにマッチするルールを設定します。

```
<Device> system-view
[Device] acl advanced 3000
[Device-acl-ipv4-adv-3000] rule 0 permit tcp source-port eq 21
[Device-acl-ipv4-adv-3000] quit
```

トラフィッククラス **classifier_1** を作成し、トラフィッククラスにマッチする条件として ACL 3000 を参照するように設定します。

```
[Device] traffic classifier classifier_1
[Device-classifier-classifier_1] if-match acl 3000
[Device-classifier-classifier_1] quit
```

#トラフィック動作 **behavior_1** を作成し、パケットを廃棄するトラフィックフィルタリングのアクションを設定します。

```
[Device] traffic behavior behavior_1
[Device-behavior-behavior_1] filter deny
[Device-behavior-behavior_1] quit
```

QoS ポリシー**policy** を作成し、トラフィッククラス **classifier_1** とトラフィック動作 **behavior_1** を関連づけます。

```
[Device] qos policy policy
[Device-qospolicy-policy] classifier classifier_1 behavior behavior_1
[Device-qospolicy-policy] quit
```

GigabitEthernet 1/0/1 の入力トラフィックに QoS ポリシー **policy** を適用します。

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] qos apply policy policy inbound
```

目次

このセクションのページは**6-x-x** です。

8章 プライオリティマーキング 8-1
8.1 概要 8-1
8.2 設定手順 8-1
8.3 プライオリティマーキングの設定例 8-3
8.3.1 ネットワーク要件 8-3
8.3.2 設定手順 8-3

8章 プライオリティマーキング

8.1 概要

プライオリティマーキングは、トラフィックのプライオリティを変更するためにパケットのプライオリティフィールドまたはフラグビットを設定します。たとえば、パケットを転送するプライオリティを変更する場合、トラフィッククラスの IP プレシーデンスまたは DSCP を設定するプライオリティマーキングを用います。

プライオリティマーキングを設定するために、パケットクラスのプライオリティフィールドあるいはフラグビットを以下のように設定します。

1)　トラフィック動作をプライオリティマーキングアクションに設定します。
2)　トラフィッククラスをトラフィック動作に関連づけます。

プライオリティマーキングの設定は、プライオリティマッピングと同時に設定することができます。詳細はオペレーションマニュアルのセクション 6 *ACL and QoS ” プライオリティマッピング*”を参照してください。

8.2 設定手順

以下にプライオリティマーキングの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． トラフィッククラスを作成し、traffic class view に移行する	**traffic classifier** *classifier-name* [**operator** { **and** | **or** }]	デフォルト：設定なし
3． マッチ条件を設定する	**if-match** *match-criteria*	デフォルト：設定なし **if-match**コマンドの詳細は、コマンドマニュアルのセクション6 *ACL and QoS ” QoSポリシー*”を参照してください。
4． system view に戻る	**quit**	ー
5． トラフィック動作を作成し、traffic behavior view に移行する	**traffic behavior** *behavior-name*	デフォルト：設定なし

操作	コマンド	補足
6. プライオリティマーキングアクションを設定する	• DSCP値を設定する：**remark** [**green** | **red** | **yellow**] **dscp** *dscp-value* • 802.1pプライオリティを設定する、あるいは内部-外部タグのプライオリティのコピー機能を設定する： • **remark** [**green** | **red** | **yellow**] **dot1p** *dot1p-value* • **remark dot1p customer-dot1p-trust** • DSCP マーキングアクションを設定する：**remark** [**green** | **red** | **yellow**] **dscp** *dscp-value* • ローカルプレシーデンスを設定する：**remark local-precedence** *local-precedence-value* • 外部VLAN IDを設定する：**remark service-vlan-id** *vlan-id*	1つ以上のいずれかのコマンドを設定します。 デフォルト：設定なし
7. system view に戻る	**quit**	ー
8. QoS ポリシーを作成し、QoS policy view に移行する	**qos policy** *policy-name*	デフォルト：設定なし
9. トラフィッククラスにQoS ポリシーのトラフィック動作を関連付け得る	**classifier** *classifier-name* **behavior** *behavior-name*	デフォルト：設定なし
10. system view に戻る.	**quit**	ー
11. QoS ポリシーを適用する	• インタフェースにQoSポリシーを適用する • VLANにQoSポリシーを適用する • グローバルにQoSポリシーを適用する	必要とされるアプリケーションの宛先の1つを選択してください。 デフォルト：設定なし
12. （オプション設定項目）プライオリティマーキングの設定を表示する	**display traffic behavior user-defined** [*behavior-name*]	すべてのviewで実行できます。

8.3 プライオリティマーキングの設定例

8.3.1 ネットワーク要件

図 8-1に示すように、以下の要件を満足するようにプライオリティマーキングを設定します。

送信元	宛先	プライオリティ
Host A, B	Data server	High
Host A, B	Mail server	Medium
Host A, B	File server	Low

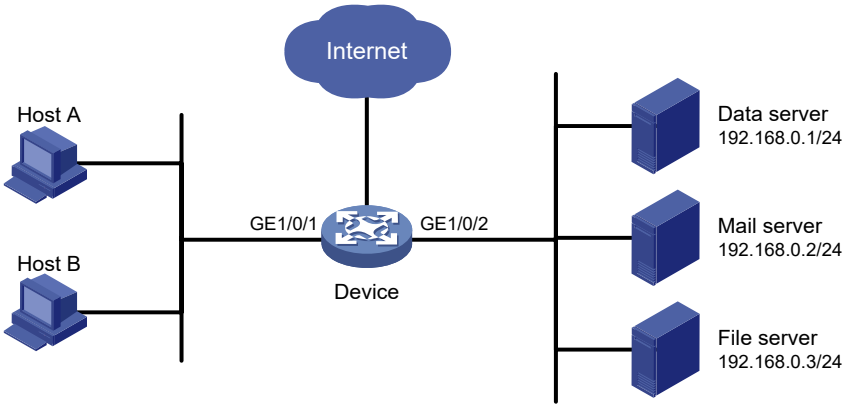


図 8-1 ネットワーク図

8.3.2 設定手順

拡張 ACL 3000 を作成し、宛先 IP アドレス 192.168.0.1 にパケットがマッチするルールを設定します。

```
<Device> system-view
[Device] acl advanced 3000
[Device-acl-ipv4-adv-3000] rule permit ip destination 192.168.0.1 0
[Device-acl-ipv4-adv-3000] quit
```

拡張 ACL 3001 を作成し、宛先 IP アドレス 192.168.0.2 にパケットがマッチするルールを設定します。

```
[Device] acl advanced 3001
[Device-acl-ipv4-adv-3001] rule permit ip destination 192.168.0.2 0
[Device-acl-ipv4-adv-3001] quit
```

拡張 ACL 3002 を作成し、宛先 IP アドレス 192.168.0.3 にパケットがマッチするルールを設定します。

```
[Device] acl advanced 3002
[Device-acl-ipv4-adv-3002] rule permit ip destination 192.168.0.3 0
[Device-acl-ipv4-adv-3002] quit
```

トラフィッククラス **classifier_dbserver** を作成し、トラフィッククラスのマッチ条件に ACL 3000 を適用します。

```
[Device] traffic classifier classifier_dbserver
[Device-classifier-classifier_dbserver] if-match acl 3000
[Device-classifier-classifier_dbserver] quit
```

トラフィッククラス **classifier_mserver** を作成し、トラフィッククラスのマッチ条件に ACL 3001 を適用します。

```
[Device] traffic classifier classifier_mserver
[Device-classifier-classifier_mserver] if-match acl 3001
[Device-classifier-classifier_mserver] quit
```

トラフィッククラス **classifier_fserver** を作成し、トラフィッククラスのマッチ条件に ACL 3002 を適用します。

```
[Device] traffic classifier classifier_fserver
[Device-classifier-classifier_fserver] if-match acl 3002
[Device-classifier-classifier_fserver] quit
```

トラフィック動作 **behavior_dbserver** を作成し、ローカルプレシーデンスの値を 4 としたアクションを設定します。

```
[Device] traffic behavior behavior_dbserver
[Device-behavior-behavior_dbserver] remark local-precedence 4
[Device-behavior-behavior_dbserver] quit
```

トラフィック動作 **behavior_mserver** を作成し、ローカルプレシーデンスの値を 3 としたアクションを設定します。

```
[Device] traffic behavior behavior_mserver
[Device-behavior-behavior_mserver] remark local-precedence 3
[Device-behavior-behavior_mserver] quit
```

トラフィック動作 **behavior_fserver** を作成し、ローカルプレシーデンスの値を 2 としたアクションを設定します。

```
[Device] traffic behavior behavior_fserver
[Device-behavior-behavior_fserver] remark local-precedence 2
[Device-behavior-behavior_fserver] quit
```

QoS ポリシー**policy_server** を作成し、トラフィッククラスを QoS ポリシーのトラフィック動作に関連づけます。

```
[Device] qos policy policy_server
[Device-qospolicy-policy_server] classifier classifier_dbserver behavior behavior_dbserver
[Device-qospolicy-policy_server] classifier classifier_mserver behavior behavior_mserver
[Device-qospolicy-policy_server] classifier classifier_fserver behavior behavior_fserver
[Device-qospolicy-policy_server] quit
```

GigabitEthernet 1/0/1 の入力トラフィックに QoS ポリシー**policy_server** を適用します。

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] qos apply policy policy_server inbound
[Device-GigabitEthernet1/0/1] quit
```

目次

このセクションのページは**6-x-x** です。

9 章 ネスティング..... 9-1
9.1 設定手順..... 9-1
9.2 設定例 9-2
9.2.1 ネットワーク要件..... 9-2
9.2.2 設定手順 9-2

9章 ネスティング

ネスティングはマッチするパケットに VLAN タグを追加します。対応する VLAN によって、VLAN タグ付けされているパケットを許可するようにします。たとえば、カスタマネットワークからサービスプロバイダネットワークのパケットに外部 VLAN タグを追加します。サービスプロバイダによって割り当てられた VLAN タグをパケットにつけることによってサービスプロバイダネットワークを通過できるようにします。

9.1 設定手順

以下にネスティングの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． トラフィッククラスを作成し、traffic class view に移行する	**traffic classifier** *classifier-name* [**operator** { **and** | **or** }]	デフォルト：設定なし
3． マッチ条件を設定する	**if-match** *match-criteria*	デフォルト：設定なし **if-match**コマンドの詳細は、コマンドマニュアルのセクション6 *ACL and QoS*”*QoSポリシー*”を参照してください。
4． system view に戻る	**quit**	―
5． トラフィック動作を作成し、traffic behavior view に移行する	**traffic behavior** *behavior-name*	デフォルト：設定なし
6． VLAN タグの追加アクションを設定する	**nest top-most vlan** *vlan-id*	デフォルト：設定なし
7． system view に戻る	**quit**	―
8． QoS ポリシーを作成し、QoS policy view に移行する	**qos policy** *policy-name*	デフォルト：設定なし
9． トラフィッククラスを QoS ポリシーのトラフィック動作に関連づける	**classifier** *classifier-name* **behavior** *behavior-name*	デフォルト：設定なし
10．system view に戻る	**quit**	―
11．QoS ポリシーを適用する	● インタフェースにQoSポリシーを適用する ● VLANにQoSポリシーを適用する ● グローバルにQoSポリシーを適用する	必要とされるアプリケーションの宛先の1つを選択してください。 デフォルト：設定なし

9.2 設定例

9.2.1 ネットワーク要件

図 9-1に示すように、VPN A の Site1 と Site2 は、company の 2 つの支社で、トラフィックを転送するのに、VLAN 5 を使用します。Site1 と Site2 は異なるエリアにあるため、2 つの Site はサービスプロバイダの VPN アクセスサービスを使用します。サービスプロバイダは 2 つの Site に VLAN 100 を割り当てます。

2 つの支社がサービスプロバイダネットワークを通して通信できるように、ネスティングを設定します。

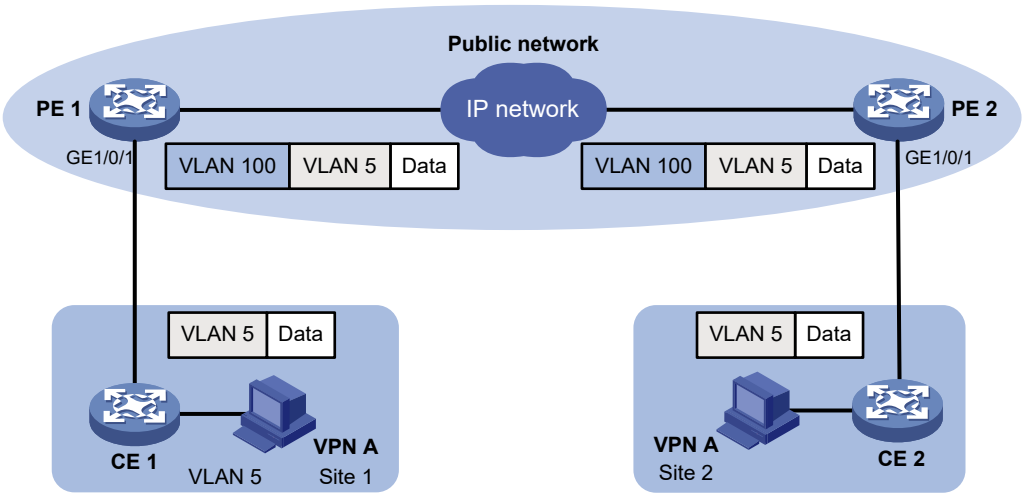


図 9-1 ネットワーク図

9.2.2 設定手順

1)　PE 1 を設定します。

VLAN ID 5 にトラフィックをマッチさせるクラス **test** を作成します。

```
<PE1> system-view
[PE1] traffic classifier test
[PE1-classifier-test] if-match service-vlan-id 5
[PE1-classifier-test] quit
```

トラフィック動作 **test** に外部 VLAN タグ 100 を追加するアクションを設定します。

```
[PE1] traffic behavior test
[PE1-behavior-test] nest top-most vlan 100
[PE1-behavior-test] quit
```

QoS ポリシー**test** を作成し、トラフィッククラス **test** と QoS ポリシーのトラフィック動作 **test** を関連づけます。

```
[PE1] qos policy test
[PE1-qospolicy-test] classifier test behavior test
[PE1-qospolicy-test] quit
```

ハイブリッドポートとして下流ポート GigabitEthernet 1/0/1 を設定し、タグ付けされていないメンバとして VLAN 100 にポートを割り当てます。

```
[PE1] interface gigabitethernet 1/0/1
[PE1-GigabitEthernet1/0/1] port link-type hybrid
[PE1-GigabitEthernet1/0/1] port hybrid vlan 100 untagged
```

QoS ポリシー**test** に下流ポート GigabitEthernet 1/0/1 の入力トラフィックを適用します。

```
[PE1-GigabitEthernet1/0/1] qos apply policy test inbound
[PE1-GigabitEthernet1/0/1] quit
```

トランクポートとして上流ポート GigabitEthernet 1/0/2 を設定し、VLAN 100 に割り当てます。

```
[PE1] interface gigabitethernet 1/0/2
[PE1-GigabitEthernet1/0/2] port link-type trunk
[PE1-GigabitEthernet1/0/2] port trunk permit vlan 100
[PE1-GigabitEthernet1/0/2] quit
```

2)　PE 2 を設定します。

PE1 の設定と同様に PE2 の設定を行います。

目次

このセクションのページは**6-x-x** です。

10 章 トラフィックリダイレクティング 10-1
10.1 設定手順 10-1
10.2 設定例 10-2
10.2.1 ネットワーク要件 10-2
10.2.2 設定手順 10-3

10章 トラフィックリダイレクティング

トラフィックリダイレクトは、指定した条件でパケットをリダイレクトさせます。CPU あるいはインタフェースへのリダイレクトアクションをサポートしています。

10.1 設定手順

以下にトラフィックリダイレクティングの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． トラフィッククラスを作成し、traffic class view に移行する	**traffic classifier** *classifier-name* [**operator** { **and** | **or** }]	デフォルト：設定なし
3． マッチ条件を設定する	**if-match** *match-criteria*	デフォルト：設定なし **if-match**コマンドの詳細は、コマンドマニュアルのセクション6 *ACL and QoS*”*QoSポリシー*”を参照してください。
4． system view に戻る	**quit**	―
5． トラフィック動作を作成し、traffic behavior view に移行する	**traffic behavior** *behavior-name*	デフォルト：設定なし
6． トラフィックリダイレクティングアクションを設定する	**redirect** { **cpu** | **interface** *interface-type interface-number* }	デフォルト：設定なし CPUへのトラフィックリダイレクティングとインタフェースへのリダイレクティングは同じtraffic 動作で同時に使用することはできません。最後に設定したリダイレクティングアクションが適用されます。
7． system view に戻る	**quit**	―
8． QoS ポリシーを作成し、QoS policy view に移行する	**qos policy** *policy-name*	デフォルト：設定なし
9． トラフィッククラスを QoS ポリシーのトラフィック動作に関連づける	**classifier** *classifier-name* **behavior** *behavior-name*	デフォルト：設定なし
10．system view に戻る	**quit**	―

操作	コマンド	補足
11．QoS ポリシーを適用する	• インタフェースにQoSポリシーを適用する • VLANにQoSポリシーを適用する • グローバルにQoSポリシーを適用する	必要とされるアプリケーションの宛先の1つを選択してください。 デフォルト：設定なし QoSポリシーは入力方向に適用されたときのみトラフィックリダイレクティングが適用されます。
12．（オプション設定項目）トラフィックリダイレクティングの設定情報を表示する	**display traffic behavior user-defined** [*behavior-name*]	すべてのviewで実行できます。

10.2 設定例

10.2.1 ネットワーク要件

図 10-1に示すように設定します。

- Device A は 2 つのリンクを通して Device B に接続します。互いに他の装置と同時に通信可能です。
- Device A の GigabitEthernet 1/0/2 と Device B の GigabitEthernet 1/0/2 は VLAN 200 に属しています。
- Device A の GigabitEthernet 1/0/3 と Device B の GigabitEthernet 1/0/3 は VLAN 201 に属しています。
- Device A の VLAN インタフェース 200 の IP アドレスは 200.1.1.1/24 で、VLAN インタフェース 201 の IP アドレスは 201.1.1.1/24 です。
- Device B の VLAN インタフェース 200 の IP アドレスは 200.1.1.2/24 で、VLAN インタフェース 201 の IP アドレスは 201.1.1.2/24 です。

インタフェースにトラフィックリダイレクティングアクションを設定します。

- Device A の GigabitEthernet 1/0/1 で受信した送信元 IP アドレス 2.1.1.1 のパケットは GigabitEthernet 1/0/2 に転送されます。
- Device A の GigabitEthernet 1/0/1 で受信した送信元 IP アドレス 2.1.1.2 のパケットは GigabitEthernet 1/0/3 に転送されます。
- Device A の GigabitEthernet 1/0/1 で受信した他のパケットは、ルーティングテーブルに従って転送されます。

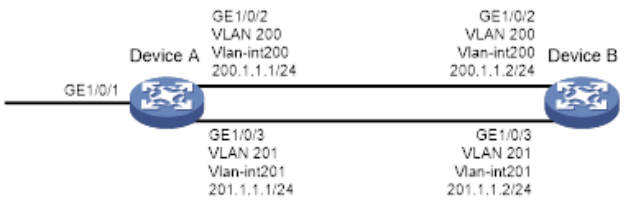


図 10-1 ネットワーク図

10.2.2 設定手順

標準 ACL 2000 を作成し、送信元 IP アドレス 2.1.1.1 のパケットにマッチするルールを設定します。

```
<DeviceA> system-view
[DeviceA] acl basic 2000
[DeviceA-acl-ipv4-basic-2000] rule permit source 2.1.1.1 0
[DeviceA-acl-ipv4-basic-2000] quit
```

標準 ACL 2001 を作成し、送信元 IP アドレス 2.1.1.2 のパケットにマッチするルールを設定します。

```
[DeviceA] acl basic 2001
[DeviceA-acl-ipv4-basic-2001] rule permit source 2.1.1.2 0
[DeviceA-acl-ipv4-basic-2001] quit
```

トラフィッククラス **classifier_1** を作成し、トラフィッククラスのマッチ条件として ACL 2000 を使用します。

```
[DeviceA] traffic classifier classifier_1
[DeviceA-classifier-classifier_1] if-match acl 2000
[DeviceA-classifier-classifier_1] quit
```

トラフィッククラス **classifier_2** を作成し、トラフィッククラスのマッチ条件として ACL 2001 を使用します。

```
[DeviceA] traffic classifier classifier_2
[DeviceA-classifier-classifier_2] if-match acl 2001
[DeviceA-classifier-classifier_2] quit
```

トラフィック動作 **behavior_1** を作成し、GigabitEthernet 1/0/2 にトラフィックリダイレクティングアクションを設定します。

```
[DeviceA] traffic behavior behavior_1
[DeviceA-behavior-behavior_1] redirect interface gigabitethernet 1/0/2
[DeviceA-behavior-behavior_1] quit
```

トラフィック動作 **behavior_2** を作成し、GigabitEthernet 1/0/3 にトラフィックリダイレクティングアクションを設定します。

```
[DeviceA] traffic behavior behavior_2
[DeviceA-behavior-behavior_2] redirect interface gigabitethernet 1/0/3
[DeviceA-behavior-behavior_2] quit
```

QoS ポリシー**policy** を作成します。

```
[DeviceA] qos policy policy
```

トラフィッククラス **classifier_1** を QoS ポリシーのトラフィック動作 **behavior_1** に関連づけます。

```
[DeviceA-qospolicy-policy] classifier classifier_1 behavior behavior_1
```

トラフィッククラス **classifier_2** を QoS ポリシーのトラフィック動作 **behavior_2** に関連づけます。

```
[DeviceA-qospolicy-policy] classifier classifier_2 behavior behavior_2
[DeviceA-qospolicy-policy] quit
```

QoS ポリシー**policy** を GigabitEthernet 1/0/1 の入力トラフィックに適用します。

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] qos apply policy policy inbound
```

目次

このセクションのページは**6-x-x** です。

11 章 クラスベースアカウンティング..... 11-1
11.1 設定手順..... 11-1
11.2 設定例 11-2
11.2.1 ネットワーク要件..... 11-2
11.2.2 設定手順 11-2

11章 クラスベースアカウンティング

クラスベースアカウンティングは、クラスにもとづいてトラフィック毎の統計情報（パケット毎あるいはバイト毎）を収集します。たとえば、特定の IP アドレスからのトラフィック情報を収集できます。統計情報を分析することにより、例外動作があるかを確認でき、適切な措置をとることが可能になります。

11.1 設定手順

以下にクラスベースアカウンティングの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． トラフィッククラスを作成し、traffic class view に移行する	**traffic classifier** *classifier-name* [**operator** { **and** | **or** }]	デフォルト：設定なし
3． マッチ条件を設定する	**if-match** *match-criteria*	デフォルト：設定なし **if-match**コマンドの詳細は、コマンドマニュアルのセクション6 *ACL and QoS ”QoSポリシー”* を参照してください。
4． system view に戻る	**quit**	―
5． トラフィック動作を作成し、traffic behavior view に移行する	**traffic behavior** *behavior-name*	デフォルト：設定なし
6． アカウンティングアクションを設定する	**accounting** { **byte** | **packet** }	デフォルト：設定なし
7． system view に戻る	**quit**	―
8． QoS ポリシーを作成し、QoS policy view に移行する	**qos policy** *policy-name*	デフォルト：設定なし
9． トラフィッククラスを QoS ポリシーのトラフィック動作に関連づける	**classifier** *classifier-name* **behavior** *behavior-name*	デフォルト：設定なし
10．system view に戻る	**quit**	―
11．QoS ポリシーを適用する	● インタフェースにQoSポリシーを適用する ● VLANにQoSポリシーを適用する ● グローバルにQoSポリシーを適用する	必要とされるアプリケーションの宛先の1つを選択してください。 デフォルト：設定なし

操作	コマンド	補足
12．（オプション設定項目）トラフィックアカウンティングの設定情報を表示する	• **display qos policy interface** [*interface-type interface-number*] [**inbound** | **outbound**] • **display qos vlan-policy** { **name** *policy-name* | **vlan** [*vlan-id*] } [**slot** *slot-number*] [**inbound** | **outbound**]	すべてのviewで実行できます。

11.2 設定例

11.2.1 ネットワーク要件

図 11-1に示すように、GigabitEthernet 1/0/1 で受信する送信元 IP アドレスが 1.1.1.1/24 のトラフィックを、クラスベースアカウンティングで収集するように設定します。

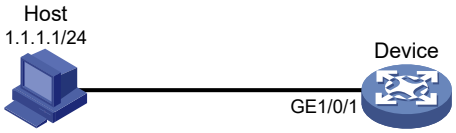


図 11-1 ネットワーク図

11.2.2 設定手順

標準 ACL 2000 を作成し、送信元 IP アドレス 1.1.1.1 のパケットにマッチするルールを設定します。

```
<Device> system-view
[Device] acl basic 2000
[Device-acl-ipv4-basic-2000] rule permit source 1.1.1.1 0
[Device-acl-ipv4-basic-2000] quit
```

トラフィッククラス **classifier_1** を作成し、トラフィッククラスにマッチする条件として ACL 2000 を使用します。

```
[Device] traffic classifier classifier_1
[Device-classifier-classifier_1] if-match acl 2000
[Device-classifier-classifier_1] quit
```

トラフィック動作 **behavior_1** を設定し、クラスベースアカウンティングアクションを設定します。

```
[Device] traffic behavior behavior_1
[Device-behavior-behavior_1] accounting packet
[Device-behavior-behavior_1] quit
```

QoS ポリシー**policy** を作成し、トラフィッククラス **classifier_1** を QoS ポリシーのトラフィック動作 **behavior_1** に関連づけます。

```
[Device] qos policy policy
[Device-qospolicy-policy] classifier classifier_1 behavior behavior_1
[Device-qospolicy-policy] quit
```

GigabitEthernet 1/0/1 の入力トラフィックに QoS ポリシー**policy** を適用させます。

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] qos apply policy policy inbound
[Device-GigabitEthernet1/0/1] quit
```

設定を確認するために、トラフィックの統計情報を表示します。

```
[Device] display qos policy interface gigabitethernet 1/0/1

Interface: GigabitEthernet1/0/1

  Direction: Inbound

  Policy: policy
   Classifier: classifier_1
     Operator: AND
     Rule(s) :
      If-match acl 2000
     Behavior: behavior_1
      Accounting enable:
        28529 (Packets)
```

目次

このセクションのページは**6-x-x** です。

12 章 タイムレンジ..... 12-1
12.1 設定手順..... 12-1
12.2 タイムレンジの表示と維持..... 12-1
12.3 タイムレンジの設定例..... 12-2
12.3.1 ネットワーク要件..... 12-2
12.3.2 設定手順..... 12-2
12.3.3 設定の確認..... 12-3

12章 タイムレンジ

タイムレンジを適用することで、日時をもとにしたサービスを提供することができます。このタイムレンジは指定した期間のみ適用されます。たとえばタイムレンジを設定し、日時を指定した ACL を設定することができます。もしタイムレンジが存在しない場合、サービスは適用されません。

タイムレンジは以下のタイプがあります。

- **周期的タイムレンジ** － 一週間のある曜日、または複数の曜日で周期的に繰り返します。
- **絶対的タイムレンジ** － 一定期間内のみ有効になり、繰り返しません。

タイムレンジはタイムレンジ名によって一意に決められます。最大 1024 のタイムレンジを設定することができますが、各タイムレンジは、32 の周期的な記述と 12 の絶対的な記述まで設定することができます。

1) すべての周期的タイムレンジを組み合わせます。
2) すべての絶対的タイムレンジを組み合わせます。
3) タイムレンジのアクティブな期間として 2 つの記述の AND を行います。

12.1 設定手順

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． タイムレンジを作成あるいは修正する	**time-range** *time-range-name* { *start-time* **to** *end-time days* [**from** *time1 date1*] [**to** *time2 date2*] | **from** *time1 date1* [**to** *time2 date2*] | **to** *time2 date2* }	デフォルト：設定なし

12.2 タイムレンジの表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
タイムレンジの設定と状態を表示する	**display time-range** { *time-range-name* | **all** }

12.3 タイムレンジの設定例

12.3.1 ネットワーク要件

図 12-1に示すように、Host A が Server に 2015 年 6 月 1 日から 2015 年 12 月 31 日の、営業時間 8:00 から 18:00 のみアクセスできるように、Device A に ACL を設定します。

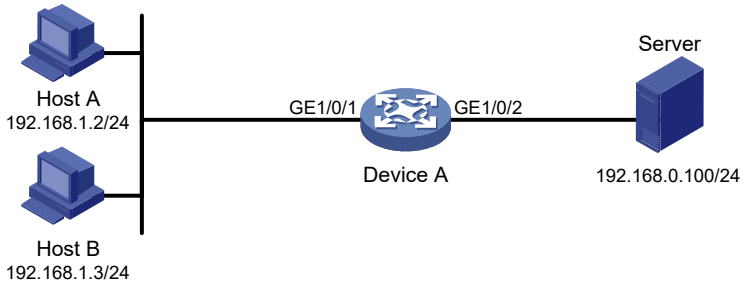


図 12-1 ネットワーク図

12.3.2 設定手順

2015 年 6 月 1 日から 2015 年 12 月 31 日の、営業時間 8:00 から 18:00 の周期的タイムレンジを作成します。

```
<DeviceA> system-view
[DeviceA] time-range work 8:0 to 18:0 working-day from 0:0 6/1/2015 to 24:00 12/31/2015
```

IPv4 標準 ACL 2001 を作成し、タイムレンジ **work** の間、192.168.1.2/32 からのパケットのみ許可するようにルールを設定します。

```
[DeviceA] acl basic 2001
[DeviceA-acl-ipv4-basic-2001] rule permit source 192.168.1.2 0 time-range work
[DeviceA-acl-ipv4-basic-2001] rule deny source any time-range work
[DeviceA-acl-ipv4-basic-2001] quit
```

GigabitEthernet 1/0/2 の出力パケットをフィルタするため、IPv4 標準 ACL 2001 を適用します。

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] packet-filter 2001 outbound
[DeviceA-GigabitEthernet1/0/2] quit
```

12.3.3 設定の確認

Device A でタイムレンジの設定と状態を表示します。

```
[DeviceA] display time-range all
Current time is 13:58:35 6/29/2015 Friday

Time-range : work ( Active )
 08:00 to 18:00 working-day
 from 00:00 6/1/2015 to 00:00 1/1/2016
```

目次

このセクションのページは**6-x-x** です。

13 章 データバッファ 13-1
13.1 設定作業リスト 13-2
13.2 データバッファ機能の有効化 13-2
13.3 設定例 13-3
13.3.1 ネットワーク要件 13-3
13.3.2 設定手順 13-4

13章 データバッファ

データバッファは輻輳を引き起こすバーストデータにより、パケットロスを避けるため、一時的にパケットを記録（バッファ）します。図 13-1にデータバッファの構造を示します。装置は、衝突が発生したとき、出力バッファにパケットを送信するパケットをバッファします。CPU がビジー状態のとき、入力バッファのパケットを記録します。

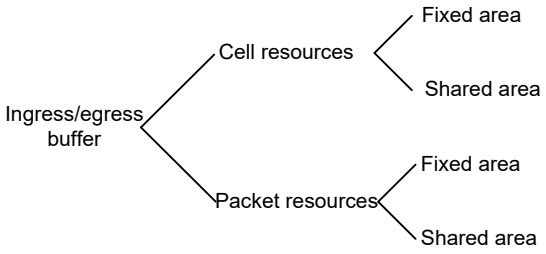


図 13-1 データバッファ構造

インタフェースは、衝突が発生したとき、出力バッファに送信するパケットを記録します。

出力バッファは以下のリソースタイプを使用します。

- **セルリソース** – パケットを記録します。バッファはパケットのサイズにもとづいて、208 バイトのセルリソースを提供します。1 つのセルリソースに 128 バイトのパケットを割り当て、2 つのセルリソースに 300 バイトのパケットを割り当てます。
- **パケットリソース** – パケットの保存場所を記録します。パケットをセルリソースに割り当てた場所を示します。バッファは、各送受信パケットに 1 つのパケットリソースを使用します。

🕮 **メモ：**

装置がブロードキャストあるいはマルチキャストパケットを受信するとき、装置は複数のパケットのコピーを転送します。この場合、セルリソースとパケットリソースは以下のように割り当てられます。

- パケット共有セルリソースのコピーを転送するすべてのインタフェースはパケットを適応させるセルリソースを共有します。
- パケットを転送する各インタフェースは1つのパケットリソースが割り当てられます。

リソースの各タイプには、専用（固定）エリアと共有エリアがあります。

- **専用エリア** – 図 13-2に示すように、すべてのインタフェースに均等に割り当てられ分割されたキューです。衝突が発生したとき以下のように動作します。

a) インタフェースはパケットをバッファするため、最初に専用エリアの関連するキューを使用します。

b) キューが一杯になったとき、インタフェースは共有エリアの対応するキューを使用し

ます。

c) 共有エリアが一杯になったとき、インタフェースは後続のパケットを廃棄します。

システムはユーザによって指定されたキューで共有エリアを割り当てます。キューが一杯でない場合でも、他のキューを使用することはできません。同様にインタフェースのキューに空きがあったとしても、キューを共有することはできません。

- **共有エリア** – 図 13-2に示すように、すべてのインタフェースに不均等に割り当てられ分割されたキューです。システムはキューが一杯でない場合、他のキューを使用することができます。

  システムはすべてのインタフェースで受信されたパケットを到着順にキューに格納します。キューが一杯のとき、後続のパケットを廃棄します。

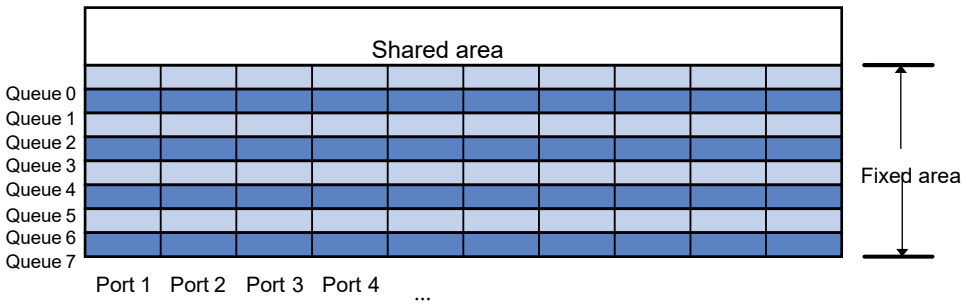


図 13-2 専用（固定）エリアと共有エリア

13.1 設定作業リスト

データバッファを自動で設定することができます。

作業リスト
データバッファ機能の有効化

13.2 データバッファ機能の有効化

データバッファ機能はセルリソースとパケットリソースを自動的に割り当てます。データバッファ機能は以下の状態のパケットバッファを最適化します。

- ブロードキャストあるいはマルチキャストトラフィックが密集して、トラフィックのバーストサイズが大きくなった状態にパケットバッファを最適化します。
- トラフィックが以下の状態にパケットバッファを最適化します。
  - 低速インタフェースから転送された高速トラフィックに転送されている状態にパケットバッファを最適化します。
  - 同一速度の複数ポートから受信されたトラフィックが、同一速度で一つのポートに転送されている状態にパケットバッファを最適化します。
- 装置の高速インタフェースから低速インタフェースにトラフィックが転送されます。
- 複数の同一レートのインタフェースから同一レートでインタフェースにトラフィックが転送されます。

バースト機能が無効の場合、セルリソースとパケットリソースは表 13-1に示すような割合で割り当てられます。

表 13-1 パケットバッファの割り当て（バースト機能が無効の場合）

リソースタイプ	キューの専用（固定）エリアの割合	ポートあるいはキューごとに使用できる共有エリアの割合の最大	共有エリア全体の割合
セル	12%	10%	50%
パケット	12%	10%	52%

バースト機能が有効の場合、セルリソースとパケットリソースは表 13-2に示すような割合で割り当てられます。

表 13-2 パケットバッファの割り当て（バースト機能が有効の場合）

リソースタイプ	キューの専用（固定）エリアの割合	ポートあるいはキューごとに使用できる共有エリアの割合の最大	共有エリア全体の割合
セル	12%	90%	72%
パケット	12%	90%	74%

以下にデータバッファ機能の有効化の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． データバッファ機能を有効にする	**burst-mode enable**	デフォルト：無効 データバッファ機能は既知のユニキャストパケットのみ適用します。 データバッファ機能を無効にすると、PFC機能が長時間動作し、正常に動作しない可能性があります。

13.3 設定例

13.3.1 ネットワーク要件

図 13-3に示すように、Server は 1000Mbps の Ethernet インタフェースを通して装置に接続します。サーバは不規則に大量のブロードキャストあるいはマルチキャストトラフィッ

クを Host に送信します。各 Host は 100Mbps のネットワークアダプタを通して装置に接続します。

サーバからホストにパケットを送信することを保証し、装置が大量のトラフィックを処理できるように設定します。

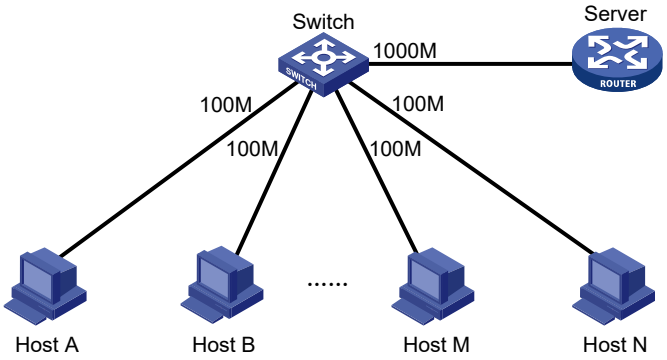


図 13-3 ネットワーク図

13.3.2 設定手順

system view に移行します。

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

データバッファ機能を有効にします。

```
[Switch] burst-mode enable
```

目次

このセクションのページは**6-x-x** です。

14 章 付録 14-1
14.1 付録 A 頭字語 14-1
14.2 付録 B デフォルトプライオリティマップ 14-1
14.3 付録 C パケットプレシーデンスの概要 14-2
14.3.1 IP プレシーデンスと DSCP フィールドの値 14-2
14.3.2 802.1p プライオリティ 14-3

14章 付録

14.1 付録A 頭字語

頭字語	フルスペル
BE	Best Effort
CAR	Committed Access Rate
CBS	Committed Burst Size
CE	Congestion Experienced
CIR	Committed Information Rate
DiffServ	Differentiated Service
DSCP	Differentiated Services Code Point
EBS	Excess Burst Size
FIFO	First in First out
FQ	Fair Queuing
GTS	Generic Traffic Shaping
IntServ	Integrated Service
ISP	Internet Service Provider
MPLS	Multiprotocol Label Switching
PE	Provider Edge
PIR	Peak Information Rate
QoS	Quality of Service
RED	Random Early Detection
RSVP	Resource Reservation Protocol
RTP	Real-Time Transport Protocol
SP	Strict Priority
ToS	Type of Service
VoIP	Voice over IP
VPN	Virtual Private Network
WFQ	Weighted Fair Queuing
WRED	Weighted Random Early Detection
WRR	Weighted Round Robin

14.2 付録B デフォルトプライオリティマップ

デフォルトの dscp-dscp プライオリティマップでは、入力した値と出力の値が同一となります。

表 14-1 デフォルトの dot1p-lp プライオリティマップ

プライオリティの入力値	dot1p-lp マッピング
dot1p	lp
0	2
1	0
2	1
3	3
4	4
5	5
6	6
7	7

表 14-2 デフォルトの dscp-dot1p プライオリティマップ

プライオリティの入力値	dscp-dot1p マッピング
dscp	dot1p
0 ～ 7	0
8 ～ 15	1
16 ～ 23	2
24 ～ 31	3
32 ～ 39	4
40 ～ 47	5
48 ～ 55	6
56 ～ 63	7

14.3 付録C パケットプレシーデンスの概要

14.3.1 IP プレシーデンスと DSCP フィールドの値

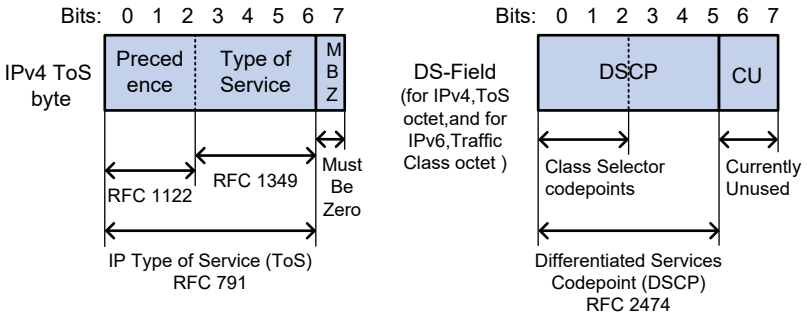


図 14-1 ToS、DS フィールド

図 14-1に示すように、IP ヘッダの ToS フィールドは 8 ビットが含まれます。最初の 3 ビット(0～2)は、0～7 までの IP プレシーデンスを示します。RFC2474 に従い、ToS フィールドは、右側の DS(Differentiated Services)フィールドとして再定義されます。ここで最初の 6 ビット(0～5)は DSCP を表し、0～63 までの値となります。残りの 2 ビット(6、7)は予約された値として使われません。

表 14-3 IP プレシーデンス

IP プレシーデンス(10 進表示)	IP プレシーデンス(2 進表示)	説明
0	000	Routine
1	001	priority
2	010	immediate
3	011	flash
4	100	flash-override
5	101	critical
6	110	internet
7	111	network

表 14-4 DSCP 値

DSCP 値(10 進表示)	DSCP 値(2 進表示)	説明
46	101110	ef
10	001010	af11
12	001100	af12
14	001110	af13
18	010010	af21
20	010100	af22
22	010110	af23
26	011010	af31
28	011100	af32
30	011110	af33
34	100010	af41
36	100100	af42
38	100110	af43
8	001000	cs1
16	010000	cs2
24	011000	cs3
32	100000	cs4
40	101000	cs5
48	110000	cs6
56	111000	cs7
0	000000	be (default)

14.3.2 802.1p プライオリティ

802.1p プライオリティは、レイヤ 2 ヘッダにありレイヤ 3 ヘッダを解析する必要がなく、QoS がレイヤ 2 で必要となるところで使用されます。

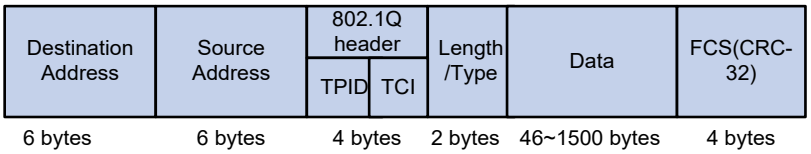


図 14-2 802.1Q タグヘッダの Ethernet フレーム

図 14-2に示すように、4 バイトの 802.1Q タグヘッダはタグプロトコル識別子(TPID、2 バイト長)とタグ管理情報(TCI、2 バイト長)から構成されます。TPID の値は 0x8100 です。図 14-3は、802.1Q ヘッダのフォーマットを示します。802.1Q タグヘッダのプライオリティフィールドは、IEEE802.1p で定義され、802.1p プライオリティと呼ばれます。表 14-5 に 802.1p プライオリティの値を示します。

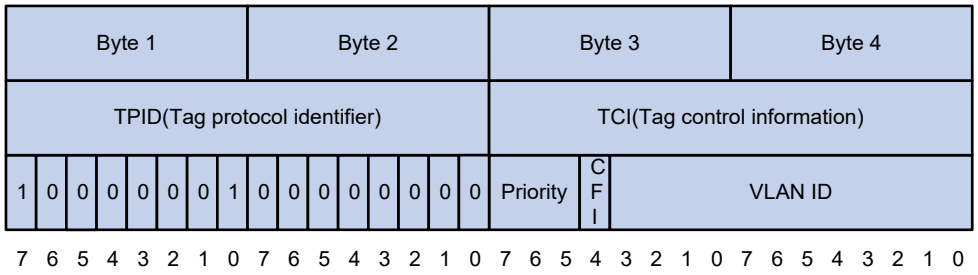


図 14-3 802.1Q タグヘッダ

表 14-5 802.1p プライオリティの説明

802.1p プライオリティ(10 進表示)	802.1p プライオリティ(2 進表示)	説明
0	000	best-effort
1	001	background
2	010	spare
3	011	excellent-effort
4	100	controlled-load
5	101	video
6	110	voice
7	111	network-management

QX-S1100G シリーズ Ethernet スイッチ

オペレーションマニュアル

7. セキュリティ

本マニュアルは以下に示す章で構成されています。

01-AAA
02-802.1X の概要
03-802.1X
04-MAC アドレス認証
05-ポートセキュリティ
06-公開鍵
07-SSH
08-IP ソースガード
09-ARP アタックプロテクション
10-TCP フラグメントアタックプロテクション
11-パスワード管理

目次

このセクションのページは **7-x-x** です。

1 章 AAA 1-1
1.1 概要 1-1
1.1.1 RADIUS 1-2
1.1.2 装置の AAA 実装 1-7
1.1.3 プロトコルと標準 1-9
1.1.4 RADIUS 属性 1-9
1.2 AAA 設定要件と設定作業リスト 1-11
1.3 AAA スキームの設定 1-12
1.3.1 ローカルユーザの設定 1-13
1.3.2 RADIUS スキームの設定 1-16
1.4 ISP ドメインの AAA 方式の設定 1-25
1.4.1 設定要件 1-25
1.4.2 ISP ドメインの作成 1-25
1.4.3 ISP ドメインの属性の設定 1-26
1.4.4 ISP ドメインの認証方式の設定 1-27
1.4.5 ISP ドメインの許可方式の設定 1-28
1.4.6 ISP ドメインのアカウンティング方式の設定 1-28
1.4.7 同時ログインユーザの最大数の設定 1-29
1.5 AAA の表示と維持 1-30
1.6 SSH ユーザのローカル認証、RADIUS アカウンティングの設定例 1-30
1.6.1 ネットワーク要件 1-30
1.6.2 設定手順 1-30
1.6.3 設定の確認 1-31
1.7 RADIUS のトラブルシューティング 1-32
1.7.1 RADIUS 認証の失敗 1-32
1.7.2 RADIUS パケットが到達不能 1-32
1.7.3 RADIUS アカウンティングエラー 1-33

1章 AAA

1.1 概要

AAA は認証（Authentication）、許可（Authorization）、アカウンティング（Accounting）の 3 つのセキュリティ機能の総称です。実用的なネットワークアクセス管理を行うためのフレームワークを提供します。それぞれの以下のセキュリティを提供します。

- **認証** － リモートユーザを特定し、有効なユーザか否かを判断します。
- **許可（認可）** － 認証に成功したユーザに対して提供する権限を制限します。
- **アカウンティング（課金）** － サービスタイプ、開始/終了の時間、トラフィックを含む、認証に成功したユーザのネットワークサービスの使用情報を取得します。これにより、アカウンティング機能は、時間ベースおよびトラフィックベースで、ネットワークセキュリティの監視にも使用することができます。

通常、AAA ではクライアント/サーバモデルを使用します。クライアントは NAS（Network Access Server）上で動作し、サーバで集中的にユーザ情報を管理します。AAA ネットワークにおいて、図 1-1に示すように、NAS はユーザのためのサーバですが、AAA サーバのためのクライアントでもあります。

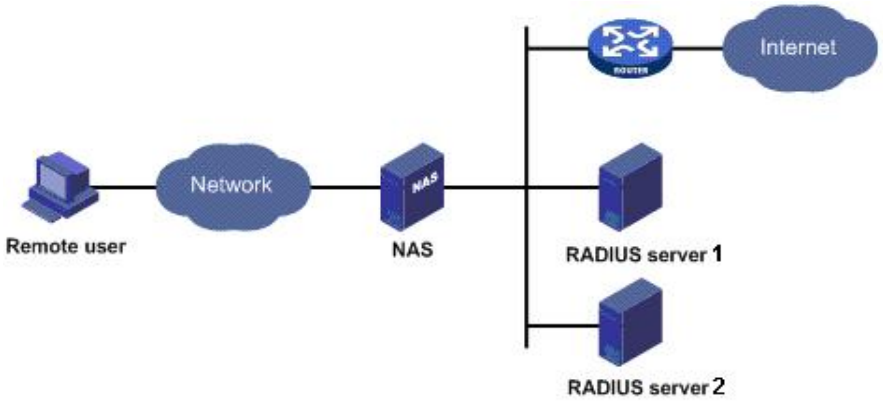


図 1-1 AAA のネットワーク構成

ユーザが NAS への接続を確立し、ほかのネットワーク、またはいくつかのネットワークリソースにアクセスするための権利を取得しようとする場合、NAS は、ユーザ、または対応する接続を認証します。NAS はユーザの AAA 情報をサーバ（RADIUS サーバ）に透過的に通すことができます。その結果 NAS はアクセス要求を許可/禁止するか決定します。

AAA を実現する方法として、最も使用されるものとして RADIUS があります。

図 1-1に示すように、RADIUS サーバ 1 と RADIUS サーバ 2 があります。この場合、必要に応じて、認証、許可、アカウンティングの役割を決めることができます。たとえば、RADIUS サーバ 2 を認証と許可に使用し、RADIUS サーバ 1 をアカウンティングサーバにすることができます。

必要に応じて、AAA を使用してセキュリティ機能を選択することができます。たとえば、会社の従業員が指定のリソースにアクセスする前に、認証を行いたい場合、認証サーバのみを設定することで実行可能です。ネットワークの使用情報を登録したい場合、アカウンティングサーバも設定することで実行可能になります。

装置は、ダイナミックにパスワードの認証を行うことができます。

1.1.1 RADIUS

RADIUS（Remote Authentication Dial-In User Service）は、クライアント/サーバモデルにおける分散情報交換プロトコルの 1 つです。RADIUS は非許可ユーザのアクセスからネットワークを保護することから、高いセキュリティとリモートユーザアクセスの両方が必要な環境でよく使用されます。

RADIUS 許可は、RADIUS 認証と組み合わせて使用されます。ユーザ許可情報は、認証のレスポンスによって運ばれます。RADIUS はトランスポートプロトコルとして UDP を使用します。RADIUS は認証に UDP ポート 1812 を、アカウンティングに UDP ポート 1813 を使用します。

RADIUS は、元々ダイヤルインユーザアクセスのために定義されました。RADIUS は、イーサネットアクセス、ADSL アクセスのようなより多くのアクセス方式をサポートするために拡張されました。

I. クライアント／サーバモデル

RADIUS クライアントは、ネットワーク中に配置された NAS（Network Attached Storage）上で動作します。NAS は指定されたサーバにユーザ情報を転送し、そのレスポンス（たとえば、ユーザのアクセスリクエストを許可/拒否する）によって動作します。

RADIUS サーバは、ネットワークセンターのコンピュータ、またはワークステーションで動作し、ユーザ認証とネットワークアクセスサービスに関連した情報を管理します。

RADIUS サーバは以下のプロセスを実行します。

1) RADIUS クライアントから認証、許可、アカウンティングの要求を受信します。
2) ユーザ認証、許可、アカウンティングを実行します。
3) ユーザアクセスコントロール情報（たとえば、ユーザのアクセスリクエストを許可/拒否する）をクライアントに送信します。

加えて RADIUS サーバは、認証プロキシのサービスを提供する別の RADIUS サーバのクライアントによって実行することができます。

通常、RADIUS サーバは、Users、Clients、Dictionary の 3 つのデータベースを管理します。

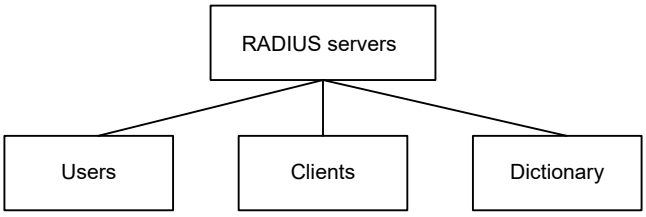


図 1-2 RADIUS サーバデータベース

- **Users** － ユーザ名、パスワード、適用プロトコル、IP アドレスのようなユーザ情報を収容します。
- **Clients** － 共有鍵や IP アドレスのような RADIUS クライアントについての情報を収容します。
- **Dictionary** － RADIUS のプロトコル属性とその値を把握するための情報を収容します。

II. 情報交換セキュリティメカニズム

RADIUS クライアントとサーバは、あらかじめ設定された共有鍵を用いて、情報の交換を行います。RADIUS パケットは Authenticator と呼ばれる 16 バイトフィールドがあります。このフィールドは、MD5 アルゴリズム、共有鍵、ほかのいくつかの情報を使用して作成されたシグネチャを送信します。パケットの受信者はシグネチャを確認し、シグネチャが正しい場合のみパケットを受信します。このメカニズムは RADIUS クライアントとサーバ間の情報交換のセキュリティを保証することができます。

共有鍵は RADIUS パケットにあるユーザのパスワードを暗号化するのに使われます。

III. ユーザ認証メカニズム

RADIUS サーバは、PAP、CHAP、EAP のような複数のユーザ認証方式をサポートします。

IV. RADIUS の標準的なパケット交換プロセス

図 1-3にユーザホスト、RADIUS クライアント、RADIUS サーバ間の情報交換について示します。

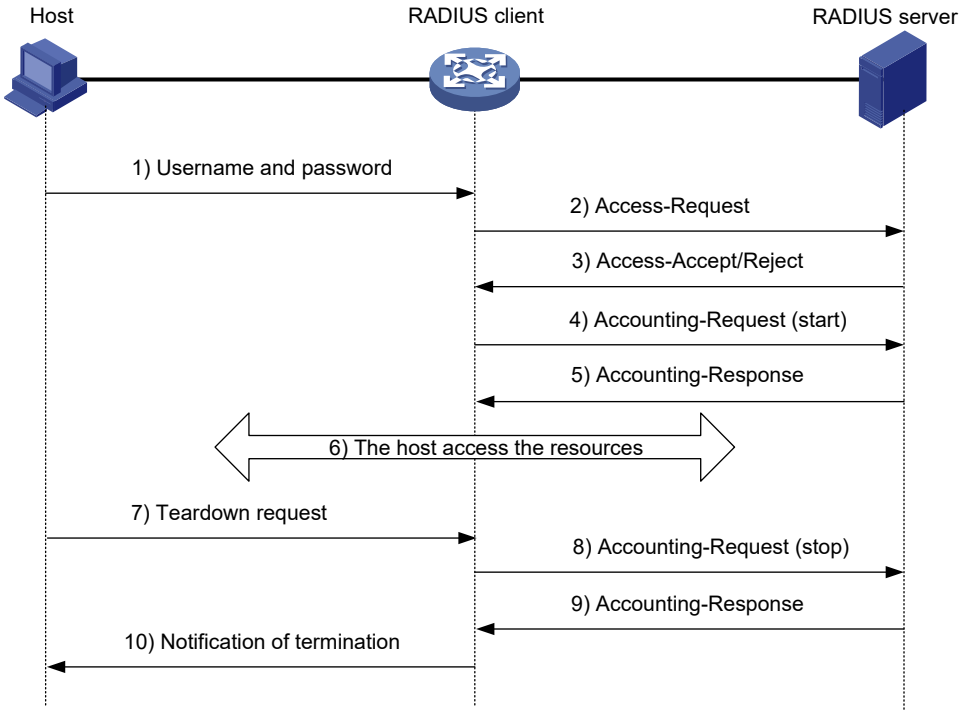


図 1-3 RADIUS の標準的なパケット交換プロセス

RADIUS は以下のように動作します。

1) ホストは、RADIUS クライアントにユーザ名とパスワードを転送し、接続リクエストを送信し始めます。
2) ユーザ名とパスワードを受信した後、RADIUS クライアントは MD5（Message-Digest5）アルゴリズムを使用して暗号化されたユーザパスワードと共有鍵を持つ認証要求（Access-Request）パケットを RADIUS サーバに送信します。
3) RADIUS サーバはユーザ名とパスワードを認証します。認証が成功した場合、ユーザの許可情報を含む Access-Accept message パケットを送り返します。認証に失敗した場合、Access-Reject message パケットを送り返します。
4) RADIUS クライアントは、返された認証結果に従ってユーザを許可、または拒否します。ユーザを許可した場合、クライアントは RADIUS サーバにアカウンティング開始要求（Accounting-Request）パケットを送信します。
5) RADIUS サーバはアカウンティング開始応答（Accounting-Response）パケットを返し、アカウンティングし始めます。
6) ユーザはネットワークリソースにアクセスすることができるようになります。
7) ホストが RADIUS クライアントに接続切断要求を行います。
8) RADIUS クライアントは RADIUS サーバにアカウンティング停止要求（Accounting-Request）パケットを送信します
9) RADIUS サーバは、ユーザのアカウンティングを停止するためにアカウンティング停止応答（Accounting-Response）パケットをクライアントに送り返します。
10) ユーザのネットワークリソースへのアクセスが停止します。

V. RADIUS パケットフォーマット

RADIUS は転送メッセージに UDP を使用します。転送メッセージは、時間管理メカニズム、再送メカニズム、バックアップサーバメカニズムを含む一連のメカニズムによって RADIUS サーバとクライアント間でのスムーズなメッセージ交換を確実にします。図 1-4 に RADIUS パケットのフォーマットを示します。

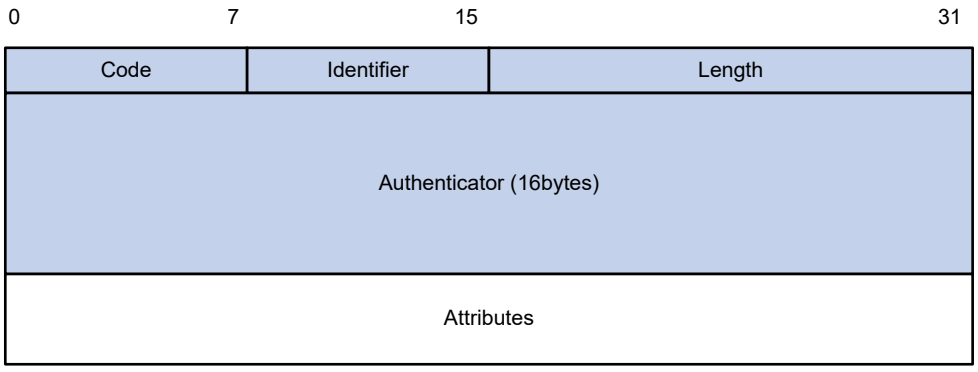


図 1-4 RADIUS パケットフォーマット

以下にフィールドの説明について記載します。

- Code フィールド（1 バイト長）は RADIUS パケットのタイプを表します。表 1-1にコードフィールドと主な値について説明します。

表 1-1 コードフィールドの主な値

Code	パケットタイプ	説明
1	Access-Request	クライアントからサーバに送信されるパケットです。このタイプのパケットは、ユーザを認証するためにサーバにユーザ情報を運ぶために使用されます。このパケットはユーザ名属性を含む必要があり、オプションとしてNAS-IPアドレス、ユーザパスワード、NAS-ポートの属性を含むことができます。
2	Access-Accept	サーバからクライアントに送信されるパケットです。Access-Requestで運ばれるすべての属性値を許可できる場合、つまり、認証が成功する場合、サーバはAccess-Accept応答パケットを送信します。
3	Access-Reject	サーバからクライアントに送信されるパケットです。Access-Requestで運ばれる情報を許可できない場合、サーバはユーザを拒否し、Access-Reject応答パケットを送信します。
4	Accounting-Request	クライアントからサーバに送信されるパケットです。このタイプのパケットはユーザのアカウンティングを開始/停止するためにサーバにユーザ情報を運ぶために使用されます。このパケットは、サーバがアカウンティングの開始/停止するための応答を示すAcct-Status-Type属性を含みます。
5	Accounting-Response	サーバからクライアントに送信されるパケットです。サーバからクライアントに送信するこのタイプのパケットは、Accounting-Requestを受信し、正確にアカウンティング情報を記録し始めたことを通知します。

- Identifier フィールド（1 バイト長）は、要求パケットと応答パケットをマッチングして、再送済みの要求パケットを検出するために使用されます。（認証あるいはアカウンティングのような）同じタイプの要求/応答パケットは同じ identifier を持ちます。
- Length フィールド（2 バイト長）は、Code、Identifier、Length、Authenticator、Attribute フィールドを含む全パケット長を示します。このフィールドの値の範囲は 20～4096 です。この範囲よりも大きい値は、不要なものとみなされ、パケットを受信されても無視します。受信パケットの長さが Length フィールドの範囲よりも小さな値の場合、そのパケットは破棄されます。
- Authenticator フィールド（16 バイト長）は、RADIUS サーバからの応答パケットを認証するために使用され、アルゴリズムを隠すパスワードにも使用されます。要求 Authenticator と応答 Authenticator の 2 種類の Authenticator があります。
- Attribute フィールド（可変長）は、要求、または応答の詳細設定を定義するために指定の認証、許可、アカウンティング情報を運びます。このフィールドは Type、Length、Value の 3 つのサブフィールドが含まれます。
  - **Type** － 属性のタイプを示します。
  - **Length** － Type、Length、Value フィールドを含む属性の長さを示します。
  - **Value** － 属性の値を示します。フォーマットと内容はサブフィールドに依存します。

一般的に使用される RADIUS 属性は、RFC2865、RFC2866、RFC2867、RFC2868 で定義されています。詳細はオペレーションマニュアルのセクション 7 *セキュリティ”AAA”の”一般的に使われる標準 RADIUS 属性*”を参照してください。

表 1-2 一般的に使用される RADIUS 属性

No.	属性	No.	属性
1	User-Name	45	Acct-Authentic
2	User-Password	46	Acct-Session-Time
3	CHAP-Password	47	Acct-Input-Packets
4	NAS-IP-Address	48	Acct-Output-Packets

No.	属性	No.	属性
5	NAS-Port	49	Acct-Terminate-Cause
6	Service-Type	50	Acct-Multi-Session-Id
7	Framed-Protocol	51	Acct-Link-Count
8	Framed-IP-Address	52	Acct-Input-Gigawords
9	Framed-IP-Netmask	53	Acct-Output-Gigawords
10	Framed-Routing	54	(unassigned)
11	Filter-ID	55	Event-Timestamp
12	Framed-MTU	56-59	(unassigned)
13	Framed-Compression	60	CHAP-Challenge
14	Login-IP-Host	61	NAS-Port-Type
15	Login-Service	62	Port-Limit
16	Login-TCP-Port	63	Login-LAT-Port
17	(unassigned)	64	Tunnel-Type
18	Reply-Message	65	Tunnel-Medium-Type
19	Callback-Number	66	Tunnel-Client-Endpoint
20	Callback-ID	67	Tunnel-Server-Endpoint
21	(unassigned)	68	Acct-Tunnel-Connection
22	Framed-Route	69	Tunnel-Password
23	Framed-IPX-Network	70	ARAP-Password
24	State	71	ARAP-Features
25	Class	72	ARAP-Zone-Access
26	Vendor-Specific	73	ARAP-Security
27	Session-Timeout	74	ARAP-Security-Data
28	Idle-Timeout	75	Password-Retry
29	Termination-Action	76	Prompt
30	Called-Station-Id	77	Connect-Info
31	Calling-Station-Id	78	Configuration-Token
32	NAS-Identifier	79	EAP-Message
33	Proxy-State	80	Message-Authenticator
34	Login-LAT-Service	81	Tunnel-Private-Group-id
35	Login-LAT-Node	82	Tunnel-Assignment-id
36	Login-LAT-Group	83	Tunnel-Preference
37	Framed-AppleTalk-Link	84	ARAP-Challenge-Response
38	Framed-AppleTalk-Network	85	Acct-Interim-Interval
39	Framed-AppleTalk-Zone	86	Acct-Tunnel-Packets-Lost
40	Acct-Status-Type	87	NAS-Port-Id
41	Acct-Delay-Time	88	Framed-Pool
42	Acct-Input-Octets	89	(unassigned)
43	Acct-Output-Octets	90	Tunnel-Client-Auth-id
44	Acct-Session-Id	91	Tunnel-Server-Auth-id

VI. 拡張 RADIUS 属性

RADIUS プロトコルは優れた拡張性を持ちます。RFC 2865 で定義されている属性番号 26（Vender-Specific）は、標準 RADIUS プロトコルが提供しない機能をベンダが実装するために拡張属性を定義することができます。

ベンダはアプリケーションを拡張するために、RADIUS パケットの複数の TLV（type-length-value）のサブ属性をカプセル化することができます。図 1-5に示すように、属性番号 26 でカプセル化されるサブ属性は、以下の 4 つで構成されます。

- **Vendor-ID** – ベンダ ID を示します。最上位のバイト値は 0 で、ほかの 3 つのバイト値には RFC1700 に準拠したコードが入ります。
- **Vendor-Type** – サブ属性のタイプを示します。
- **Vendor-Length** – サブ属性の長さを示します。
- **Vendor-Data** – サブ属性の内容を示します。

RADIUS サブ属性は 25506 のベンダ ID をサポートします。拡張 RADIUS 属性の詳細については、オペレーションマニュアルのセクション 7 *セキュリティ”AAA”の”QX シリーズ用 RADIUS 属性*”を参照してください。

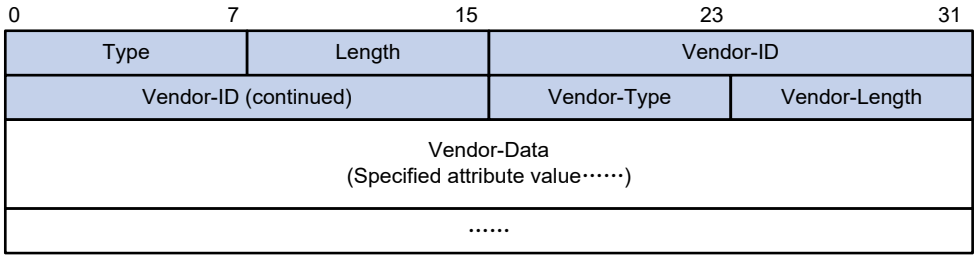


図 1-5 属性番号 26 の拡張 RADIUS 属性フォーマット

1.1.2 装置の AAA 実装

この章は AAA のユーザ管理と方法について記載します。

I. ISP ドメインにもとづくユーザ管理とユーザアクセスタイプ

AAA は ISP ドメインとアクセスタイプにもとづいてユーザを管理します。

NAS で各ユーザは 1 つの ISP ドメインに属しています。通常、NAS はユーザがログインするために使用するユーザ名によって、ISP ドメインを決定します。

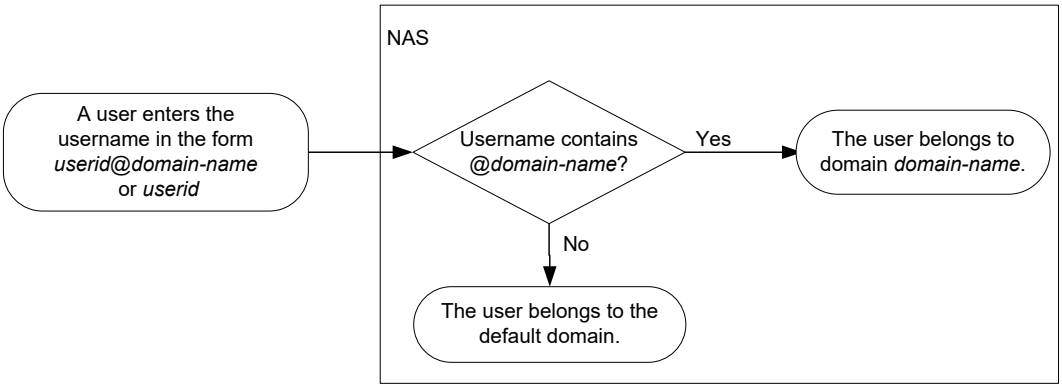


図 1-6 ユーザ名を用いた ISP ドメインの決定

AAA はアクセスタイプにもとづいて、同じ ISP ドメインのユーザを管理します。装置は以下のユーザアクセスタイプをサポートします。

- **LAN**－802.1X 認証あるいは MAC アドレス認証にパスした LAN ユーザを含みます。
- **Login**－SSH、Telnet、FTP、装置にログインしている端末のユーザを含みます。端末のユーザはコンソールポートを通してアクセスすることができます。

- **Web**－HTTP、HTTPS を用いて Web インタフェースにログインしている Web ユーザを含みます。

🕮 **メモ：**

ユーザ認証の管理ポリシーに対応するため、装置は 802.1X のような認証モジュールを提供します。認証モジュールを設定した場合、アクセスタイプのユーザの ISP ドメインは認証モジュールの設定に依存します。

II. AAA 認証方式

AAA は ISP ドメインの異なるタイプのユーザのため、異なる認証、許可、アカウンティング方式を設定することができます。NAS はユーザの ISP ドメインとアクセスタイプを決定し、ユーザのアクセスを管理するため、設定された認証方式を使用します。

AAA は ISP ドメインのデフォルト方式の設定をサポートします。デフォルト方式は、特定の AAA 方式が設定されていないユーザに使われます。

装置は、以下の認証方式をサポートします。

- **認証なし** － すべてのユーザが信頼され、認証が実施されません。通常、この方式はセキュリティ目的で使われません。
- **ローカル認証** － 認証は、ユーザ名、パスワード、属性を含むユーザ情報の設定された NAS によって実行されます。ローカル認証は、高速かつ低コストですが、収容できる情報量は、記憶容量に依存します。
- **リモート認証** － アクセス装置は、ユーザを認証するために RADIUS サーバを利用します。RADIUS に関して、装置はユーザ認証を実行するために、標準的な RADIUS プロトコルを使用することができます。リモート認証の特徴は、集中した情報管理、高い能力、高い信頼性、複数の装置のための集中した認証が挙げられます。また、リモート認証サーバが有効でない場合のバックアップ方式としてローカル認証を設定することができます。

装置は、以下の許可方式をサポートします。

- **許可なし** － NAS は許可を実行しません。認証にパスするとネットワークに以下のデフォルト許可情報を適用します。
  - □ ログインユーザはネットワークにアクセスできません。
  - □ ログインユーザはレベル 0 ユーザロールを獲得します。レベル 0 ユーザロールの詳細は、オペレーションマニュアルのセクション 1 *はじめに*”*RBAC*”を参照してください。
  - □ FTP、SFTP ユーザが認証にパスした場合、作業ディレクトリが NAS のルートディレクトリになりますが、アクセスすることはできません。
- **ローカル許可** － ユーザは、ユーザのために設定された属性に従って、NAS によって許可されます。
- **リモート許可** － NAS はユーザを許可するため、RADIUS サーバと協力します。RADIUS 許可は RADIUS 認証と結び付けられます。RADIUS 許可は、RADIUS 認証が成功した後のみ動作し、許可情報は Access-Accept で運ばれます。リモートサーバが有効でない場合は、バックアップ方式としてローカル許可、または許可なしを設定することができます。

装置は、以下のアカウンティング方式をサポートします。

- **アカウンティングなし** － NAS はユーザのアカウンティングを実行しません。

- **ローカルアカウンティング** － ローカルアカウンティング方式は NAS 上で実行されます。ユーザ数の統計情報を収集し、ローカルユーザ接続の数を制御します。ローカルアカウンティング方式は、ユーザ管理のための統計情報を提供しません。
- **リモートアカウンティング** － NAS は、ユーザアカウンティングのために、RADIUS サーバと連携します。リモートサーバが利用できない場合に備えて、バックアップ方法としてローカルアカウンティング方式を設定することができます。

加えて、装置は、セキュリティを向上させるために、以下のサービスを提供します。

- **ユーザロール切り替え認証** － ログアウトや切断を行うことなしで、一時的なユーザロールを使用してユーザを認証します。一時的なユーザロールの許可の詳細は、オペレーションマニュアルのセクション 1 *はじめに*”*RBAC*”を参照してください。

1.1.3 プロトコルと標準

以下に AAA、RADIUS に関連したプロトコルと標準を示します。

- RFC 2865, *Remote Authentication Dial In User Service (RADIUS)*
- RFC 2866, *RADIUS Accounting*
- RFC 2867, *RADIUS Accounting Modifications for Tunnel Protocol Support*
- RFC 2868, *RADIUS Attributes for Tunnel Protocol Support*
- RFC 2869, *RADIUS Extensions*

1.1.4 RADIUS 属性

I. 一般的に使われる標準 RADIUS 属性

番号	属性	説明
1	User-Name	認証されるユーザ名です。
2	User-Password	PAP認証のユーザパスワードです。PAP認証モードでAccess-Requestパケットでのみ存在します。
3	CHAP-Password	CHAP認証のユーザパスワードです。CHAP認証モードでAccess-Requestパケットでのみ存在します。
4	NAS-IP-Address	サーバがクライアントを認識するIPアドレスです。通常、クライアントはNASのアクセスインタフェースで識別され、NASのIPアドレスと呼ばれます。Access-Requestパケットでのみ存在します。
5	NAS-Port	ユーザがアクセスするNASの物理ポートです。
6	Service-Type	ユーザが要求したあるいは提供されたType of serviceです。
7	Framed-Protocol	フレーム化されるカプセル化プロトコルです。
8	Framed-IP-Address	ユーザに割り当てられるIPアドレスです。
11	Filter-ID	フィルタリスト名です。
12	Framed-MTU	ユーザとNAS間のデータリンクの最大転送ユニット（MTU）です。たとえば802.1X EAP認証です。NASはこの属性を使用してEAPパケットのMTUサイズが超過しないようにサーバに知らせます。
14	Login-IP-Host	ユーザアクセスを行うNASインタフェースのIPアドレスです。
15	Login-Service	ユーザがログインするためのサービスタイプです。
18	Reply-Message	ユーザに表示されるテキストです。認証失敗などでサーバがユーザに通知するために使われます。

番号	属性	説明
26	Vendor-Specific	ベンダ仕様属性です。パケットはベンダ属性のような1つ以上の属性を含めることができます。それは1つ以上のサブ属性を含みます。
27	Session-Timeout	セッションが終了する前に提供されるサービスの最大継続時間です。
28	Idle-Timeout	セッションが終了する前に許可される最大Idle時間です。
31	Calling-Station-Id	NASがサーバに送信したユーザ識別子です。QXシリーズの装置によって提供されるLANアクセスサービスとして、この属性は、ユーザのHHHH-HHHH-HHHH形式のMACアドレスを保持します。
32	NAS-Identifier	NASがRADIUSサーバを識別するために使用する識別子です。
40	Acct-Status-Type	Accounting-Requestパケットタイプです。 ● **1** – Start ● **2** – Stop ● **3** – Interim-Update ● **4** – Reset-Charge ● **7** – Accounting-On （第3世代（3G）移動体通信システムの標準化プロジェクト）で定義。） ● **8** – Accounting-Off （第3世代（3G）移動体通信システムの標準化プロジェクト）で定義。） ● **9 ～ 14**– トンネルアカウンティング用に予約 ● **15** – 故障用に予約
45	Acct-Authentic	ユーザによって使われる認証方式です。 ● **1** – RADIUS ● **2** – Local ● **3** – Remote
60	CHAP-Challenge	NASは、CHAP認証の間、MD5を計算するためにCHAPチャレンジを作成します。
61	NAS-Port-Type	ユーザによって、認証されているNASの物理ポートタイプです。 ● **15** – Ethernet ● **16** – ADSLのすべてのタイプ ● **17** – ケーブル （ケーブルTV用） ● **19** – WLAN-IEEE 802.11 ● **201** – VLAN ● **202** – ATM ポートがATMやEthernetで、VLANがそのポートに実装された場合、この属性の値は201です。
79	EAP-Message	NASが、EAPを経由して、カプセル化しているEAPパケットを許可するために使われます。
80	Message-Authenticator	偽のAccess-Requestを防ぐため、認証し、認証パケットをチェックするのに使われます。この属性は、RADIUSがEAP認証をサポートする場合に使われます。
87	NAS-Port-Id	ユーザを認証しているNASのポートです。

II. QX シリーズ用 RADIUS 属性

番号	属性	説明
1	Input-Peak-Rate	ユーザからNASへの最大レート（bps）です。
2	Input-Average-Rate	ユーザからNASへの平均レート（bps）です。
3	Input-Basic-Rate	ユーザからNASへの基本レート（bps）です。
4	Output-Peak-Rate	NASからユーザへの最大レート（bps）です。
5	Output-Average-Rate	NASからユーザへの平均レート（bps）です。
6	Output-Basic-Rate	NASからユーザへの基本レート（bps）です。
15	Remanent_Volume	異なるサーバタイプのため、異なるユニットの存在している有効な接続のトータルトラフィックです。
20	Command	セッション管理で使われるセッション処理です。 ● **1**– Trigger-Request ● **2**– Terminate-Request ● **3**– SetPolicy ● **4**– Result ● **5**– PortalClear
25	Result_Code	Trigger-RequestあるいはSetPolicy動作の戻り値です。値が0の場合、動作が成功し、他の値の場合、動作は失敗しています。
26	Connect_ID	ユーザ接続のインデックスです。
28	Ftp_Directory	FTPユーザの作業ディレクトリです。FTPユーザのため、RADIUSクライアントがFTPサーバとして動作する場合、この属性はRADIUSクライアントのFTPディレクトリを設定するのに使われます。
29	Exec_Privilege	実行ユーザの優先度です。
59	NAS_Startup_Timestamp	NASの開始時間です。1970 年1月1日0時0分0秒（UTC時間）からの経過時間を示しています。
60	Ip_Host_Addr	認証とアカウンティング要求で使われるユーザのIPアドレス、MACアドレスです。IPアドレスA.B.C.DとMACアドレスhh:hh:hh:hh:hh:hhの間には空白が必要です。
61	User_Notify	サーバからクライアントに透過的に送信する必要がある情報です。
62	User_HeartBeat	802.1Xユーザが認証をパスした後、32バイト長で割り当てられるハッシュ値です。この属性は、装置のユーザリストに記録され、802.1Xユーザからハンドシェイクメッセージをチェックするために使われます。この属性はAccess-AcceptパケットとAccounting-Requestパケットでのみ存在します。
140	User_Group	ユーザが認証にパスした後に割り当てられるユーザグループです。 通常、ユーザは1つのユーザグループにのみ属することができます。
255	Product_ID	装置名です。

1.2 AAA設定要件と設定作業リスト

AAA を設定するため、NAS で以下の作業を完了している必要があります。

1)　必要な AAA スキームの設定

- **ローカル認証** – ユーザのユーザ名、パスワードを含む、認証するために必要なローカルユーザと、属性を設定します。

□ **リモート認証** – 必要な RADIUS スキームを設定し、サーバに従ってユーザ属性を設定します

2) ユーザの ISP ドメインの AAA 方式を設定します。リモート AAA 方式は ISP domain view で設定された RADIUS スキームを参照します。

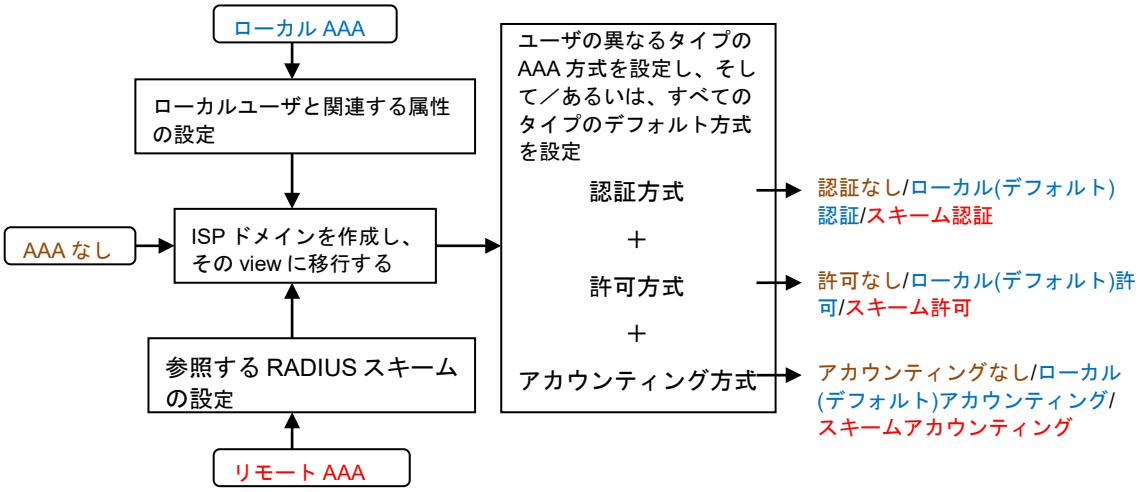


図 1-7 AAA 設定手順

以下に AAA 認証の設定作業リストを示します。

作業リスト
（必須設定項目） ローカルユーザあるいはAAAスキームの設定で、いずれか1つを実行します。 • ローカルユーザの設定 • RADIUSスキームの設定
（必須設定項目） ISPドメインのAAA方式の設定 1. （必須設定項目） ISP ドメインの作成 2. （オプション設定項目） ISP ドメインの属性の設定 3. （必須設定項目）ISP ドメインの AAA 認証、許可、アカウンティングの設定で、少なくとも 1 つを実行します。 • ISPドメインの認証方式の設定 • ISPドメインの許可方式の設定 • ISPドメインのアカウンティング方式の設定
（オプション設定項目）同時ログインユーザの最大数の設定

1.3 AAAスキームの設定

この章はローカルユーザ、RADIUS スキームの設定について記載します。

1.3.1 ローカルユーザの設定

ローカルユーザ認証、許可、アカウンティングを実装するため、装置でローカルユーザを作成し、ユーザの属性の設定を行う必要があります。ローカルユーザと属性は装置のローカルユーザデータベースに記録されます。ローカルユーザはユーザ名とユーザタイプの組み合わせで一意に識別されます。

ローカルユーザは以下のタイプに分類されます。

- **装置管理ユーザ**－装置にログインする装置管理ユーザをサポートします。
- **ネットワークアクセスユーザ**－装置を通してネットワークリソースにアクセスするユーザをサポートします。

設定可能なローカルユーザ属性を以下に示します。

- **サービスタイプ**－ユーザが使用できるサービスタイプです。ローカル認証はローカルユーザのサービスタイプをチェックします。サービスタイプが有効でない場合、ユーザは認証にパスできません。

  サービスタイプは FTP、LAN アクセス、SSH、Telnet、ターミナルがあります。
- **ユーザ状態**－ローカルユーザがネットワークサービスをリクエストできるかどうかを示します。active と blocked の 2 つの状態があります。active 状態のユーザはネットワークサービスをリクエストできますが、blocked のユーザはリクエストできません。
- **同一ユーザ名を使用する同時ログインユーザの上限**－同一ユーザ名を使用して同時に装置にアクセスすることができるユーザの最大の数です。同一ユーザ名を使用するローカルユーザの数が上限に達する場合、ローカルユーザは、そのユーザ名を使用して装置にアクセスすることができません。
- **ユーザグループ**－各ローカルユーザはローカルユーザグループと、許可属性のようなグループのすべての属性を運んでいます。ローカルユーザグループの詳細は、オペレーションマニュアルのセクション *7 セキュリティ ”AAA”の”ユーザグループ属性の設定*”を参照してください。
- **許可属性**－許可属性は、ローカル認証をパスした後、ユーザの権利を示します。許可属性は ACL、アイドルカット機能、ユーザロール、VLAN、FTP/SFTP 作業ディレクトリを含みます。許可属性の詳細は、オペレーションマニュアルのセクション *7 セキュリティ ”AAA”の”ローカルユーザ属性の設定*”を参照してください。

  ローカルユーザのサービスタイプにもとづいて許可属性を設定します。

  user group view ですべてのローカルユーザに適用される属性、local user view でローカルユーザのみに適用される属性となるように、許可属性を設定することができます。local user view で設定した許可属性の設定は、user group view で設定した許可属性よりも優先されます。

  - □ user group view で設定した属性はユーザグループのすべてのローカルユーザに適用します。
  - □ local user view で設定した属性はローカルユーザのみ適用します。

I. ローカルユーザ設定作業リスト

作業リスト
（必須設定項目） ローカルユーザ属性の設定
（オプション設定項目） ユーザグループ属性の設定
（オプション設定項目） ローカルユーザとローカルユーザグループの表示と維持

II. ローカルユーザ属性の設定

ローカルユーザ属性の設定を行う場合、以下のガイドラインに従ってください。

- 許可属性はアプリケーションの環境と目的に従って設定してください。ユーザのサービスタイプにもとづいて許可属性をサポートします。
  - LAN ユーザは acl、user-profile、vlan の許可属性をサポートします。
  - telnet、端末ユーザは idle-cut、user-role の許可属性をサポートします。
  - http ユーザは user-role の許可属性をサポートします。
  - ssh ユーザは idle-cut、user-role、work-directory の許可属性をサポートします。
  - ftp ユーザは user-role、work-directory の許可属性をサポートします。
  - ほかのユーザは許可属性をサポートしません。

以下にローカルユーザ属性の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. ローカルユーザ（装置管理ユーザ）を追加し、local user view に移行する	**local-user** *user-name* [**class** { **manage** | **network** }]	デフォルト：設定なし
3. （オプション設定項目）ローカルユーザのパスワードを設定する	**password** [{ **hash** | **simple** } *string*]	装置管理ユーザパスワードはハッシュアルゴリズムで暗号化され、cipherで保存されます。 パスワードの設定を行わないローカルユーザは正しいローカルユーザ名と属性のチェックにパスした後、認証をパスすることができます。セキュリティを確保するため、各ローカルユーザにパスワードを設定してください。
4. ローカルユーザのサービスタイプを指定する	● ネットワークアクセスユーザ： **service-type lan-access** ● 装置管理ユーザ： **service-type** { **ftp** | { **ssh** | **telnet** | **terminal** } * }	デフォルト：設定なし
5. （オプション設定項目）ローカルユーザを active あるいは blocked に設定する	**state** { **active** | **block** }	デフォルト：**active** ネットワークサービスを要求することができます。
6. （オプション設定項目）同時にログインするローカルユーザの上限を設定する	**access-limit** *max-user-number*	デフォルト：制限なし ローカルユーザの設定のみ適用され、アカウンティングをサポートしていないFTPユーザには適用しません。
7. （オプション設定項目）ローカルユーザのインタフェースバインディング属性を設定する	**bind-attribute location interface** *interface-type interface-number*	デフォルト：設定なし

操作	コマンド	補足
8.　（オプション設定項目）ローカルユーザの許可属性を設定する	**authorization-attribute** { **acl** *acl-number* | **idle-cut** *minute* | **user-profile** profile-name | **user-role** *role-name* | **vlan** *vlan-id* | **work-directory** *directory-name* } *	デフォルト：以下に示します。 ● FTPまたはSFTPユーザはNASのルートディレクトリがありますが、アクセス許可がありません。 ● network-operatorユーザロールは、network-adminまたはレベル15ユーザによって作成されるローカルユーザに割り当てられます。
9.　（オプション設定項目）ローカルユーザのユーザグループを指定する	**group** *group-name*	デフォルト：ローカルユーザはデフォルトユーザグループのsystemに属しています。

III. ユーザグループ属性の設定

ユーザグループはローカルユーザの設定と管理を簡略化します。ユーザグループはローカルユーザのグループから構成され、ローカルユーザ属性の構成があります。グループ内のローカルユーザを集中化してユーザ属性の管理を行うため、ユーザグループ用のローカルユーザ属性を設定することができます。許可属性を含んだユーザ属性を設定できます。

デフォルトでは、新しく追加された各ローカルユーザは、システムデフォルトユーザグループ system に属し、グループのすべての属性に対応します。ローカルユーザが属しているユーザグループを割り当てる場合、local user view で **group** コマンドを使用します。

以下にユーザグループ属性の設定を示します。

操作	コマンド	補足
1.　system view に移行する	**system-view**	ー
2.　ユーザグループを作成し、その view に移行する	**user-group** *group-name*	デフォルト：デフォルトユーザグループとしてsystemがあります
3.　ユーザグループの許可属性を設定する	**authorization-attribute** { **acl** *acl-number* | **idle-cut** *minute* | **user-profile** *profile-name* | **vlan** *vlan-id* | **work-directory** *directory-name* } *	デフォルト：設定なし

IV. ローカルユーザとローカルユーザグループの表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
ローカルユーザの設定とオンラインユーザに関する統計情報を表示する	**display local-user** [**class** { **manage** | **network** } | **idle-cut** { **disable** | **enable** } | **service-type** { **ftp** | **lan-access** | **ssh** | **telnet** | **terminal** } | **state** { **active** | **block** } | **user-name** *user-name* **class** { **manage** | **network** } | **vlan** *vlan-id*]
ユーザグループの設定を表示する	**display user-group** { **all** | **name** *group-name* }

1.3.2 RADIUS スキームの設定

RADIUS スキームは、装置と一緒に動作する RADIUS サーバを指定し、RADIUS サーバの情報を交換するのに使われるパラメータを定義します。パラメータは、サーバの IP アドレス、UDP ポート番号、共有鍵、サーバタイプを含んでいます。

I. 設定作業リスト

作業リスト
（必須設定項目） RADIUSスキームの作成
（必須設定項目） RADIUS認証サーバの指定
（オプション設定項目） RADIUSアカウンティングサーバと関連パラメータの指定
（オプション設定項目） セキュアなRADIUS通信を行うための共有鍵の指定
（オプション設定項目） ユーザ名フォーマットとトラフィック統計情報ユニットの設定
（オプション設定項目） RADIUS要求の再送信の最大試行回数の設定
（オプション設定項目） RADIUSサーバのステータスの設定
（オプション設定項目） 出力するRADIUSパケットの送信元IPアドレスの指定
（オプション設定項目） RADIUSサーバのタイマ機能の設定
（オプション設定項目） RADIUSアカウンティング機能の設定
（オプション設定項目） RADIUSパケットのDSCP値の設定
（オプション設定項目） 再認証を行う際のRADIUSサーバの選択モードの選択
（オプション設定項目） RADIUSの表示と維持

II. RADIUS スキームの作成

ほかの RADIUS 設定を行う前に、RADIUS スキームを作成してください。RADIUS スキームを 16 まで作成することができます。RADIUS スキームは複数の ISP ドメインから参照することができます。

以下に RADIUS スキームの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． RADIUS スキームを作成し、その view に移行する	**radius scheme** *radius-scheme-name*	デフォルト : 起動するコンフィグレーションのタイプに依存します。 ● 初期設定で起動する場合、RADIUSスキームはありません。 ● デフォルトコンフィグレーションファイルで起動する場合、RADIUSスキーム名が**system**のRADIUSスキームが定義されます。 起動時の設定の詳細は、オペレーションマニュアルのセクション1 *はじめに”コンフィグレーションファイル管理”*を参照してください。

III. RADIUS 認証サーバの指定

許可情報は認証の応答パケットに含めて RADIUS クライアントに送信されるため、RADIUS 認証サーバは、認証、許可を一緒に扱います。

1 つのプライマリ認証サーバと 16 のセカンダリ認証/許可サーバを指定することができます。プライマリサーバが有効でない場合、装置は順番に設定されたセカンダリサーバと通信を行い、**active** 状態の最初のセカンダリサーバと通信を行います。

冗長性を必要としない場合、プライマリサーバのみ指定します。RADIUS 認証サーバは同時に、1 つのスキーム用にプライマリ認証サーバとして機能させ、ほかのスキーム用にセカンダリ認証サーバとして機能させることができます。

以下に RADIUS スキームの RADIUS 認証サーバの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． RADIUS scheme view に移行する	**radius scheme** *radius-scheme-name*	—
3． RADIUS 認証サーバを指定する	• プライマリRADIUS認証サーバを指定する：**primary authentication** { *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** { **cipher** | **simple** } *string*] * • セカンダリRADIUS認証サーバを指定する：**secondary authentication** { *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** { **cipher** | **simple** } *string*] *	少なくとも1つのコマンドを設定してください。 デフォルト：指定なし プライマリ認証サーバとセカンダリ認証サーバで、同一のIPアドレス、ポート番号を設定することはできません。

IV. RADIUS アカウンティングサーバと関連パラメータの指定

RADIUS スキームに、1 つのプライマリアカウンティングサーバと 16 のセカンダリアカウンティングサーバを指定することができます。プライマリサーバが有効でない場合、装置は順番に設定されたセカンダリサーバと通信を行い、**active** 状態の最初のセカンダリサーバと通信を行います。

冗長性を必要としない場合、プライマリサーバのみ指定します。RADIUS アカウンティングサーバは同時に、1 つのスキーム用にプライマリアカウンティングサーバとして機能させ、ほかのスキーム用にセカンダリアカウンティングサーバとして機能させることができます。

装置は以下の状況でアカウンティングサーバにアカウンティング停止要求（stop-accounting request）を送信します。

- ホストから接続切断要求を受信します。
- 管理者から接続切断通知を受信します。

アカウンティング要求に対して、指定した試行回数の上限に達しても応答がない場合、ユーザを切断します。

RADIUS は FTP、SFTP ユーザのアカウンティングをサポートしていません。

以下に RADIUS スキームのアカウンティングサーバと関連パラメータの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. RADIUS scheme view に移行する	**radius scheme** *radius-scheme-name*	―
3. RADIUS アカウンティングサーバを指定する	● プライマリRADIUSアカウンティングサーバを指定する： **primary accounting** { *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** { **cipher** | **simple** } *string*] * ● セカンダリRADIUSアカウンティングサーバを指定する： **secondary accounting** { *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** { **cipher** | **simple** } *string*] *	少なくとも1つのコマンドを設定してください。 デフォルト：指定なし プライマリアカウンティングサーバとセカンダリアカウンティングサーバで、同一のIPアドレス、ポート番号を設定することはできません。
4. （オプション設定項目）アカウンティング要求の最大試行回数を設定する	**retry realtime-accounting** *retry-times*	デフォルト：5
5. （オプション設定項目）応答のない RADIUS ストップアカウンティング要求のバッファを有効にする	**stop-accounting-buffer enable**	デフォルト：有効
6. （オプション設定項目）RADIUS ストップアカウンティング要求の最大試行回数を設定する	**retry stop-accounting** *retries*	デフォルト：500

V. セキュアな RADIUS 通信を行うための共有鍵の指定

RADIUS クライアントと RADIUS サーバは、パケット認証とユーザパスワードの暗号化を行うため、MD5 アルゴリズムを使用して、クライアントとサーバ間で交換するパケットと共有鍵を暗号化し、パケットの検証を行います。同じ共有鍵が使用される場合のみ、パケットを適切に受信し、応答を返すことができます。

スキームで同じタイプ（アカウンティングあるいは認証）のすべてのサーバで、共有鍵が設定されます。RADIUS サーバ用に個別に設定された共有鍵よりも優先度は低くなります。

以下にセキュアな RADIUS 通信を行うための共有鍵の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. RADIUS scheme view に移行する	**radius scheme** *radius-scheme-name*	―

操作	コマンド	補足
3． セキュアな RADIUS 通信を行うための共有鍵を指定する	**key** { **accounting** | **authentication** } { **cipher** | **simple** } *string*	デフォルト：指定なし 装置とRADIUSサーバで必ず同じ共有鍵を設定するようにしてください。

VI. ユーザ名フォーマットとトラフィック統計情報ユニットの設定

ユーザ名は、一般的に *userid@isp-name* のフォーマットで表されます。*isp-name* はユーザが属している ISP ドメイン名で、ユーザがどこの ISP ドメインに属しているか装置が認識するのに使われます。しかし初期の RADIUS サーバは ISP ドメイン名が含まれていないユーザ名を認識することはできません。この場合、ユーザ名を送信する前に各ユーザ名のドメイン名を削除する必要があります。

同一 RADIUS スキームを参照するために 2 つ以上の ISP ドメインを使用する場合、ドメインを識別するため、ユーザ名の中の ISP ドメイン名を削除しないでください。

装置は、アカウンティングパケットのオンラインユーザのトラフィックの統計情報を RADIUS アカウンティングサーバに周期的に通知します。正しいトラフィック統計情報を行うため、装置でのデータフローのユニットとパケットのユニットが、RADIUS サーバのユニットと同一になっていることを確認してください。

以下にユーザ名フォーマットとトラフィック統計情報ユニットの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． RADIUS scheme view に移行する	**radius scheme** *radius-scheme-name*	―
3． RADIUS サーバに送信されるユーザ名の形式を指定する	**user-name-format** { **keep-original** | **with-domain** | **without-domain** }	デフォルト：**with-domain** 起動時の設定の詳細については、オペレーションマニュアルのセクション1 *はじめに”コンフィグレーションファイル管理”* を参照してください。
4． （オプション設定項目）RADIUS サーバへ送信されるデータフロー、またはパケットの単位を指定する	**data-flow-format** { **data** { **byte** | **giga-byte** | **kilo-byte** | **mega-byte** } | **packet** { **giga-packet** | **kilo-packet** | **mega-packet** | **one-packet** } }*	データフロー：**byte** パケット：**one-packet**

VII. RADIUS 要求の再送信の最大試行回数の設定

RADIUS はデータ送信に UDP を使用します。UDP を使用しているため、RADIUS は信頼性を向上させるため、再送信メカニズムを使用します。応答タイムアウト時間（**timer response-timeout** コマンドで設定されます。）が切れる前に RADIUS サーバから応答がなかった場合、NAS は RADIUS リクエストを再送します。RADIUS サーバ応答タイムアウト時間についての詳細は、オペレーションマニュアルのセクション 7 *セキュリティ ”AAA”の”RADIUS サーバのタイマ機能の設定”* を参照してください。

再送の試行回数が上限に達しても、RADIUS サーバから応答がない場合、**active** 状態の他の RADIUS サーバと通信を試みます。**active** 状態の他の RADIUS サーバから応答がない場合、装置は認証あるいはアカウンティングが失敗したとみなします。

以下に RADIUS 要求の再送信の最大試行回数の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． RADIUS scheme view に移行する	**radius scheme** *radius-scheme-name*	―
3． RADIUS 要求の再送信の最大試行回数を設定する	**retry** *retry-times*	デフォルト：3

VIII. RADIUS サーバのステータスの設定

RADIUS サーバのステータスを blocked 状態あるいは active 状態に設定することで、装置と通信を行う現在のサーバが有効でなくなった場合に、接続先の制御ができます。実際には、1 つのプライマリ RADIUS サーバと、プライマリサーバのバックアップとして動作する複数のセカンダリ RADIUS サーバを指定することができます。一般的に装置は、以下のルールにもとづいてサーバを選択します。

- プライマリサーバが active 状態の場合、装置はプライマリサーバと通信します。
- プライマリサーバが故障した場合装置は以下の処理を行います。
  - サーバのステータスを blocked 状態に変更します。
  - サーバの quiet タイマを開始します。
  - active 状態のセカンダリサーバと通信を行います。（最初に設定されたセカンダリサーバが高い優先度を持ちます）
- セカンダリサーバが有効でなくなった場合、装置は以下の処理を行います。
  - サーバのステータスを blocked 状態に変更します。
  - サーバの quiet タイマを開始します。
  - active 状態の次のセカンダリサーバのチェックを行います。このプロセスは、装置が有効なセカンダリサーバを見つける、あるいは active 状態のすべてのセカンダリサーバのチェックを完了するまで行います。
- quiet タイマの時間が経過した場合あるいは手動で active 状態に設定した場合、サーバは active 状態になります。しかし装置は認証あるいはアカウンティングプロセスの間、サーバを再度チェックしません。

  1 回の検索プロセスで通信可能なサーバが見つからない場合、認証あるいはアカウンティングの試みが失敗したと認識します。
- 使用している認証あるいはアカウンティングサーバが削除された場合、サーバと装置の通信はタイムアウトとなります。装置は active 状態のサーバを検索します。最初にプライマリサーバ（ある場合）をチェックし、次にセカンダリサーバをチェックする順番で確認します。
- プライマリとセカンダリサーバの両方が blocked 状態の場合、装置はすべてのサーバと通信しません。
- 1 つのサーバが active 状態で、ほかのすべてのサーバが blocked 状態の場合、装置は、たとえサーバが有効でない場合でも active 状態のサーバのみと通信します。
- RADIUS サーバの状態が自動的に変更する場合、装置はすべての RADIUS スキームに従いサーバの状態を変更します。

デフォルトでは、すべての RADIUS サーバの状態は active となります。必要に応じて、サーバの状態を変更できます。たとえば、サーバが故障している場合、サーバとの通信を防ぐために blocked となっているサーバの状態を変更することができます。

以下に RADIUS サーバのステータスの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． RADIUS scheme view に移行する	**radius scheme** *radius-scheme-name*	―
3． RADIUS サーバのステータスを設定する	• プライマリRADIUS認証サーバのステータスを設定する： **state primary authentication** { **active** | **block** } • プライマリRADIUSアカウンティングサーバのステータスを設定する： **state primary accounting** { **active** | **block** } • セカンダリRADIUS認証サーバのステータスを設定する： **state secondary authentication** [{ *ipv4-address* | **ipv6** *ipv6-address* } [*port-number*]] { **active** | **block** } • セカンダリRADIUSアカウンティングサーバのステータスを設定する： **state secondary accounting** [{ *ipv4-address* | **ipv6** *ipv6-address* } [*port-number*]] { **active** | **block** }	少なくとも1つのコマンドを設定します。 デフォルト : RADIUSスキームに指定されたサーバはactive状態です。 設定されたサーバのステータスは設定ファイルに保存することができません。**display radius scheme**コマンドを使用して表示することのみ可能です。 装置の再起動後、すべてのサーバはactive状態に戻ります。 RADIUSサーバの負荷分散機能が無効になっている場合、装置は、このセクションのサーバ選択ルールに従って、新しいユーザの認証またはアカウンティングのために到達可能なサーバを選択します。

IX. 出力する RADIUS パケットの送信元 IP アドレスの指定

NAS が送信した RADIUS パケットの送信元 IP アドレスは、RADIUS サーバで設定された NAS の IP アドレスとマッチする必要があります。RADIUS パケットを受信する際、RADIUS サーバはパケットの送信元 IP アドレスを確認します。

- パケットの送信元 IP アドレスが管理された NAS の IP アドレスとマッチしている場合、サーバは処理を行います。
- パケットの送信元 IP アドレスが管理された NAS の IP アドレスとマッチしていない場合、パケットを廃棄します。

一般的に、RADIUS パケットの送信元アドレスは NAS のいずれかの出力インタフェースの IP アドレスです。ある状況においては、送信元 IP アドレスを変更する必要があります。

RADIUS scheme view、または system view で出力する RADIUS パケットの送信元 IP アドレスを指定することができます。

- RADIUS scheme view で指定された IP アドレスは、1 つの RADIUS scheme のみに適用されます。

- system view で指定された IP アドレスは、すべての RADIUS scheme に適用されます。

RADIUS パケットを送信する前に、NAS は以下の順番で送信元 IP アドレスを選択します。

1) RADIUS スキーム用に指定された送信元 IP アドレス
2) system view で指定された送信元 IP アドレス
3) ルートで指定された出力インタフェースの IP アドレス

出力する RADIUS パケットの送信元 IP アドレスを直接指定するか、出力インタフェースを指定して、出力する RADIUS パケットの送信元 IP アドレスを提供できます。送信元インタフェースの設定と送信元 IP アドレスの設定は互いに上書きします。

以下にすべての RADIUS スキームの送信元インタフェースまたは送信元 IP アドレスの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. 出力する RADIUS パケットの送信元インタフェースまたは送信元 IP アドレスを指定する	**radius nas-ip** { **interface** *interface-type interface-number* | { *ipv4-address* | **ipv6** *ipv6-address* } }	デフォルト : 出力するRADIUSパケットの送信元IPアドレスは、出力インタフェースのIPv4アドレスまたはIPv6アドレスです。

以下に指定された RADIUS スキームの送信元インタフェースまたは送信元 IP アドレスの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. RADIUS scheme view に移行する	**radius scheme** *radius-scheme-name*	―
3. 出力する RADIUS パケットの送信元インタフェースまたは送信元 IP アドレスを指定する	**nas-ip** { *ipv4-address* | **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }	デフォルト：system view で **radius nas-ip**コマンドが設定されたIPアドレスが使用されます。**radius nas-ip**コマンドが設定されていない場合、送信元IPアドレスは送信するインタフェースのIPアドレスです。

X. RADIUS サーバのタイマ機能の設定

装置は、RADIUS サーバとの通信を管理するため、以下のタイマを使用します。

- **RADIUS サーバの応答タイムアウトタイマ**（**response-timeout**） － RADIUS リクエスト再送信間隔です。このタイマは RADIUS リクエストが送信された後、すぐに開始します。装置はタイマが満了する前に RADIUS サーバから応答を受信しない場合、リクエストを再送します。
- **サーバ停止タイマ**（**quiet**） － block 状態にある到達不能のサーバを保持する時間です。1 つのサーバが到達不能である場合、装置はサーバのステータスを blocked 状態に変更し、サーバ停止タイマを開始します。active 状態の別のサーバと通信しようとします。サーバ停止タイマが満了した後、装置はサーバの状態を active に戻します。

- **リアルタイムのアカウンティング間隔**（**realtime-accounting**） – ユーザのリアルタイムアカウンティングを実行する間隔を定義します。このタイマが設定されると、装置は指定された間隔で、オンラインユーザのアカウンティング情報を RADIUS サーバに送信します。装置がサーバからの応答を受信しない場合、ユーザの接続が強制的に切断されます。

RADIUS サーバのタイマを設定する場合、以下のガイドラインに従ってください。

- RADIUS パケットの再送信の最大試行回数の設定と RADIUS サーバ応答タイムアウトタイマの設定を行う場合、セカンダリサーバの数を考慮してください。再送プロセスに十分な時間がない場合、Telnet のようなアクセスモジュールのクライアント接続では、有効なサーバを検索しようとしている間にタイムアウトしてしまう可能性があります。
- セカンダリサーバ数が設定された場合、たとえパケット転送試行制限とサーバ応答タイムアウト期間が小さい値で設定されている場合でも、クライアント接続タイムアウトの時間を短く設定している、アクセスモジュールのクライアント接続は、初期認証あるいはアカウンティングの間にタイムアウトしてしまう可能性があります。この場合、装置はブロックする到達不能サーバの状態と短くした到達可能サーバを検索する時間を設定しているため、次の認証あるいはアカウンティングの試行は成功します。
- サーバ停止タイマは、適切に設定してください。短すぎると、サーバは active 状態の到達不能なサーバの通信を繰り返し試みる必要があるため、頻繁に認証あるいはアカウンティングが失敗します。タイマの時間を長くすると、タイマの期間が満了する間に blocked 状態になるため、一時的に故障から回復した到達可能なサーバをブロックする可能性があります。
- リアルタイムのアカウンティング間隔の設定は、NAS と RADIUS サーバの性能によって代わります。短い間隔にすると、より正確なアカウンティングを行うことができますが、高い性能が必要となります。ユーザの最大数が多い（1000 以上）場合、間隔を長くしてください。

以下に RADIUS サーバのタイマ機能の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	–
2. RADIUS scheme view に移行する	**radius scheme** *radius-scheme-name*	–
3. RADIUS サーバの応答タイムアウトタイマを設定する	**timer response-timeout** *seconds*	デフォルト：3秒
4. サーバの停止タイマを設定する	**timer quiet** *minutes*	デフォルト：5分
5. リアルタイムアカウンティング間隔を設定する	**timer realtime-accounting** *interval*	デフォルト：12分

XI. RADIUS アカウンティング機能の設定

アカウンティング機能を有効にした場合、装置は再起動した後に RADIUS サーバに accounting-on パケットを自動的に送信します。accounting-on パケットを受信すると、RADIUS サーバは装置に対して再ログインできるように全オンラインユーザをログアウトします。この機能を使用しない場合、RAIUS サーバはユーザがオンライン中と見なしているため再起動後にユーザが再ログインすることができません。

装置が accounting-on パケットを再送するために待機する間隔と最大試行回数を設定できます。

以下に RADIUS スキームのアカウンティング機能設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. RADIUS scheme view に移行する	**radius scheme** *radius-scheme-name*	—
3. RADIUS サーバの応答タイムアウトタイマを設定する	**accounting-on enable** [**interval** *interval* | **send** *send-times*] *	デフォルト：無効

XII. RADIUS パケットの DSCP 値の設定

ToS フィールドの DSCP 値は、パケットの優先度レベルを指定し、パケットの優先度に影響します。値が大きいほど、優先度は高くなります。

以下に RADIUS パケットの DSCP 値の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. RADIUS パケットの DSCP 値を設定する	**radius** [**ipv6**] **dscp** *dscp-value*	—

XIII. 再認証を行う際の RADIUS サーバの選択モードの選択

この機能を使用して、再認証時の RADIUS サーバ選択メカニズムを設定します。次の RADIUS サーバ選択モードを使用できます。

- **Inherit**—装置は、ユーザの認証を実行した RADIUS サーバを使用して、そのユーザの再認証を実行します。このモードでは、再認証に使用される時間が短縮されます。ただし、RADIUS サーバに到達できない場合、再認証は失敗します。
- **Reselect**—装置は、ユーザの再認証を実行するために到達可能な RADIUS サーバを検索します。このモードは、inherit モードよりも時間がかかります。ただし、このモードでは、装置が再認証に最適な到達可能な RADIUS サーバを見つけることができます。RADIUS サーバの選択には、次の要因が影響します。
  - 設定順を含む RADIUS スキームのサーバ設定。
  - RADIUS サーバのロードシェアリング機能の有効化状態。
  - RADIUS スキーム内の RADIUS サーバの状態。

以下に再認証を行う際の RADIUS サーバの選択モードの選択の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. RADIUS scheme view に移行する	**radius scheme** *radius-scheme-name*	—
3. 再認証を行う際の RADIUS サーバの選択モードを設定する	**reauthentication server-select** { **inherit** | **reselect** }	デフォルト：**inherit**

XIV. RADIUS の表示と維持

すべての view で **display** コマンドを実行でき、user view で **reset** コマンドを実行できます。

操作	コマンド
RADIUSスキームの設定を表示する	**display radius scheme** [*radius-scheme-name*]
RADIUSパケットの統計情報を表示する	**display radius statistics**
応答がなくバッファされたRADIUSストップアカウンティング要求の統計情報を表示する	**display stop-accounting-buffer** { **radius-scheme** *radius-scheme-name* | **session-id** *session-id* | **time-range** *start-time end-time* | **user-name** *user-name* }
RADIUSパケットの統計情報をクリアする	**reset radius statistics**
応答がなくバッファされたRADIUSストップアカウンティング要求の統計情報をクリアする	**reset stop-accounting-buffer** { **radius-scheme** *radius-scheme-name* | **session-id** *session-id* | **time-range** *start-time end-time* | **user-name** *user-name* }

1.4 ISPドメインのAAA方式の設定

ISP domain view で設定された AAA スキームを使用して、ISP ドメインの AAA 方式を設定することができます。各 ISP ドメインは、ローカル認証、ローカル許可、ローカルアカウンティングのシステム定義の AAA 方式があります。ISP ドメインの AAA 方式を設定しない場合、装置はシステム定義の AAA 方式を使用します。

1.4.1 設定要件

ISP ドメインでユーザのローカル認証を使用する場合、最初に装置でローカルユーザのアカウントを設定してください。詳細はオペレーションマニュアルのセクション 7 *セキュリティ”AAA”の”ローカルユーザ属性の設定”*を参照してください。

リモート認証、許可、アカウンティングを使用する場合、要求される RADIUS スキームを作成してください。RADIUS スキームについては、オペレーションマニュアルのセクション 7 *セキュリティ”AAA”の”RADIUS スキームの設定”*を参照してください。

1.4.2 ISP ドメインの作成

複数の ISP を持つネットワークシナリオでは、装置に各 ISP のユーザを接続する可能性があります。各 ISP ユーザはそれぞれのユーザ属性（たとえば、ユーザ名、パスワードの構成、サービスタイプ、権限）を持ち、ユーザを識別するために ISP ドメインを設定する必要がある可能性があります。そして ISP ドメインのために AAA 方式を含む各属性を設定する必要があります。

ドメインはあらかじめ定義されているデフォルト ISP ドメイン system を含む最大 16 の ISP ドメインを設定することができます。デフォルトのドメインとして ISP ドメインを指定することができます。ISP ドメインの設定を修正することができますが、削除することはできません。

装置では、各ユーザは ISP ドメインに属します。ユーザがログインする場合、ISP ドメイン名がない場合、装置はデフォルト ISP ドメインに属していると認識します。

装置は以下の順にそれぞれのユーザの認証ドメインを選択します。

1) アクセスモジュールを指定された認証ドメイン
2) ユーザ名の ISP ドメイン
3) 装置のデフォルト ISP ドメイン

選択されたドメインが装置に存在しない場合、装置は存在しないドメインに割り当てられるユーザを収容する ISP ドメインを検索します。そのような ISP ドメインが設定されていない場合、ユーザ認証は失敗します。

ISP ドメインの設定をする場合、以下の制限とガイドラインに従ってください

- デフォルトの ISP ドメインを削除することはできません。**undo domain** コマンドを使用する前に **undo domain default enable** コマンドを使用して、デフォルト以外の ISP ドメインに変更してください。
- ISP ドメイン **system** の設定変更はできますが、ドメインを削除することはできません。
- RADIUS の認証、承認、またはアカウンティングの失敗を回避するには、短いドメイン名を使用して、ドメイン名を含むユーザ名が 253 文字を超えないようにします。

以下に ISP ドメインの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. ISP ドメインを作成し、ISP domain view に移行する	**domain** *isp-name*	―
3. system view に戻る	**quit**	―
4. （オプション設定項目）デフォルト ISP ドメインを指定する	**domain default enable** *isp-name*	デフォルト：system

1.4.3 ISP ドメインの属性の設定

ISP ドメインで以下の属性を設定することができます。

- **ドメイン状態**－ISP ドメインを active あるいは blocked 状態にすることによって、ユーザからのネットワークサービス要求の許可あるいは拒否することができます。

ISP ドメインの属性はドメインのすべてのユーザに適用します。

以下に ISP ドメインの属性の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. ISP domain view に移行する	**domain** *isp-name*	―

操作	コマンド	補足
3． ISP ドメインを **active** あるいは **blocked** 状態に設定する	**state** { **active** | **block** }	デフォルト：**active** ドメインのユーザはネットワークサービスをリクエストすることができます。

1.4.4 ISP ドメインの認証方式の設定

I. 設定要件

認証方式を設定する前に、以下の作業を行ってください。

1) 設定するアクセスタイプ、またはサービスタイプを定義してください。AAA では、各アクセスタイプとサービスタイプのために認証方式を設定することができます。
2) すべてのアクセスタイプとサービスタイプでデフォルトの認証方式を設定するかどうか定義してください。デフォルト認証方式はすべてのアクセスユーザに適用しますが、指定された認証方式よりもプライオリティは低くなります。

II. 設定ガイドライン

認証方式を設定する場合、以下のガイドラインに従ってください。

- 認証方式が RADIUS スキームを使用し、許可方式が RADIUS スキームを使用しない場合、AAA は RADIUS サーバから認証結果のみを受け取ります。RADIUS サーバからの Access-Accept メッセージは許可情報を含みますが、装置は許可情報を無視します。
- ユーザロール認証のスキームを指定する場合、ユーザロールが level-*n* のフォーマットにあることを確認してください。RADIUS スキームを指定する場合、装置はロール認証の RADIUS サーバのユーザ名$**enab***n*$を使います。ここで *n* はユーザロール level-*n* の *n* と同一です。

III. 設定手順

以下に ISP ドメインの認証方式の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． ISP domain view に移行する	**domain** *isp-name*	―
3． ユーザのすべてのタイプのためのデフォルト認証方式を指定する	**authentication default** { **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }	デフォルト：**local**
4． ログインユーザのための認証方式を指定する	**authentication login** { **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }	デフォルト：デフォルト認証方式が使用されます。

1.4.5 ISP ドメインの許可方式の設定

I. 設定要件

許可方式を設定する前に、以下の作業を行ってください。

1) 設定されるアクセスタイプあるいはサービスタイプを定義してください。AAA では各アクセスタイプとサービスタイプに許可スキームを設定することができます。
2) すべてのアクセスタイプとサービスタイプでデフォルトの許可方式を設定するかどうか定義してください。デフォルト許可方式はすべてのアクセスユーザに適用しますが、指定された許可方式よりもプライオリティは低くなります。

II. 設定ガイドライン

RADIUS 許可を設定するため、RADIUS 認証を設定し、RADIUS 認証と許可で同じ RADIUS スキームを参照してください。RADIUS 許可の設定に間違いがある場合や RADIUS 許可に失敗する場合は、RADIUS 認証も失敗します。

III. 設定手順

以下に ISP ドメインの許可方式の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. ISP domain view に移行する	**domain** *isp-name*	―
3. すべてのタイプのユーザのためにデフォルト許可方式を指定する	**authorization default** { **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }	デフォルト：**local**
4. コマンド許可方式を指定する	**authorization command** { **local** [**none**] | **none** }	デフォルト：デフォルト許可方式が使用されます。
5. LAN ユーザの許可方式を指定する	**authorization lan-access** { **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }	デフォルト：デフォルト許可方式が使用されます。
6. ログインユーザのために許可方式を指定する	**authorization login** { **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }	デフォルト：デフォルト許可方式が使用されます。

1.4.6 ISP ドメインのアカウンティング方式の設定

I. 設定要件

アカウンティング方式を設定する前に、以下の作業を行ってください。

1) 設定されるアクセスタイプあるいはサービスタイプを定義してください。AAA では各アクセスタイプとサービスタイプにアカウンティング方式を設定することができます。
2) すべてのアクセスタイプとサービスタイプでデフォルトのアカウンティング方式を設定するかどうか定義してください。デフォルトアカウンティング方式はすべてのア

クセスユーザに適用しますが、指定されたアカウンティング方式よりもプライオリティは低くなります。

II. 設定ガイドライン

アカウンティング方式を設定する場合、以下のガイドラインに従ってください。

- FTP、SFTP サービスを使用するログインユーザはアカウンティングをサポートしていません。
- ローカルアカウンティングは、アカウンティングの統計情報を提供しません。同じローカルユーザアカウントを使用するユーザ数のカウントと管理を行います。しきい値は **access-limit** コマンドによって設定されます。

III. 設定手順

以下に ISP ドメインのアカウンティング方式の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. ISP domain view に移行する	**domain** *isp-name*	―
3. すべてのタイプのユーザに使用するデフォルトアカウンティング方式を指定する	**accounting default** { **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }	デフォルト：**local**
4. LAN ユーザにアカウンティング方式を指定する	**accounting lan-access** { **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }	デフォルト：デフォルトアカウンティング方式が使用されます。
5. ログインユーザに使用するアカウンティング方式を指定する	**accounting login** { **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }	デフォルト：デフォルトアカウンティング方式が使用されます。
6. （オプション設定項目）アカウンティング開始に失敗したユーザのアクセス制御を設定する	**accounting start-fail** { **offline** | **online** }	デフォルト：**online**
7. （オプション設定項目）すべてのアカウンティング更新の試行に失敗したユーザのアクセス制御を設定する	**accounting update-fail** { [**max-times** *max-times*] **offline** | **online** }	デフォルト：**online**

1.4.7 同時ログインユーザの最大数の設定

認証方法に関わらず、FTP、SSH、Telnet プロトコルを使用して、装置にログインできる最大ユーザ数を設定することができます。

以下に同時ログインユーザの最大数の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. 同時ログインユーザの最大数を設定する	**aaa session-limit** { **ftp** | **ssh** | **telnet** } *max-sessions*	デフォルト：32

1.5 AAAの表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
ISP ドメインの設定を表示する	**display domain** [*isp-name*]

1.6 SSHユーザのローカル認証、RADIUSアカウンティングの設定例

1.6.1 ネットワーク要件

図 1-8に示すように、SSH サーバ用にローカル認証を実行するように設定します。SSH ユーザ許可、アカウンティングを行うため、RADIUS サーバを使用します。そして認証にパスした後、SSH ユーザにデフォルトユーザロール network-operator を割り当てます。

SSH ユーザにユーザ名 **hello** のアカウントを設定します。RADIUS サーバとセキュアな通信を行うため、共有鍵 **expert** を設定します。ユーザ名からドメイン名を削除してサーバに送信するように設定します。

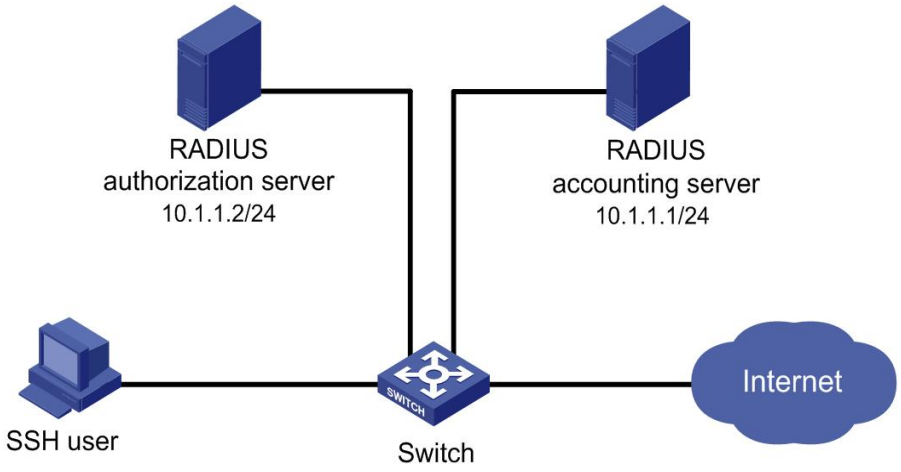


図 1-8 ネットワーク図

1.6.2 設定手順

1) RADIUS サーバを設定します。（詳細は省略します）
2) Switch を設定します。

インタフェースに IP アドレスを割り当てます。（詳細は省略します）

ローカル RSA 鍵ペアを作成します。

```
<Switch> system-view
[Switch] public-key local create rsa
```

SSH サービスを有効にします。

```
[Switch] ssh server enable
```

ユーザロール VTY0～63 のスキーム認証を有効にします。

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

RADIUS スキームを設定します。

```
[Switch] radius scheme rd
[Switch-radius-rd] primary accounting 10.1.1.1 1813
[Switch-radius-rd] key accounting simple expert
[Switch-radius-rd] user-name-format without-domain
[Switch-radius-rd] quit
```

装置管理ユーザを作成します。

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

ローカルユーザの SSH サービスを割り当てます。

```
[Switch-luser-manage-hello] service-type ssh
```

ローカルユーザのパスワードをプレーンテキストで **hello** に設定します。

```
[Switch-luser-manage-hello] password simple hello
[Switch-luser-manage-hello] quit
```

ISP ドメイン **bbb** を作成し、ログインユーザの AAA 方式を設定します。

```
[Switch] domain bbb
[Switch-isp-bbb] authentication login local
[Switch-isp-bbb] accounting login radius-scheme rd
[Switch-isp-bbb] quit
```

認証にパスした後、SSH ユーザがデフォルトユーザロール network-operator を取得できるようにデフォルトユーザロール許可機能を有効にします。

```
[Switch] role default-role enable
```

1.6.3 設定の確認

ユーザが、Switch への SSH 接続を開始し、ユーザ名 **hello@bbb** と正しいパスワードを入力した場合、ユーザが正常にログインし、network-operator ユーザロールでコマンドを使用することができます。

1.7 RADIUSのトラブルシューティング

1.7.1 RADIUS 認証の失敗

I. 症状

認証が常に失敗します。

II. 分析

可能性のある理由を以下に示します。

- NAS と RADIUS サーバ間で通信障害が存在します。
- ユーザ名が *userid@isp-name* のフォーマットではありません、あるいは NAS で ISP ドメインが正しく設定されていません。
- ユーザが RADIUS サーバで設定されていません。
- ユーザで入力したパスワードが間違っています。
- RADIUS サーバと NAS が異なる共有鍵で設定されています。

III. 解決策

以下を確認してください。

- NAS と RADIUS サーバがお互いに ping できることを確認してください。
- ユーザ名が *userid@isp-name* のフォーマットで、NAS で ISP ドメインが正しく設定されていることを確認してください。
- ユーザが RADIUS サーバで設定されていることを確認してください。
- 正しいパスワードを入力してください。
- RADIUS サーバと NAS の両方で同じ共有鍵が設定されていることを確認してください。

1.7.2 RADIUS パケットが到達不能

I. 症状

RADIUS パケットが RADIUS サーバに到達できません。

II. 分析

可能性のある理由を以下に示します。

- NAS と RADIUS サーバ間で通信障害が存在します。
- NAS に RADIUS サーバの IP アドレスが設定されていません。
- NAS の認証、アカウンティングの UDP ポートが正しくありません。
- RADIUS サーバの認証、アカウンティングのためのポート番号がほかのアプリケーションで使用されています。

III. 解決策

以下を確認してください。

- NAS と RADIUS サーバ間のリンクが物理レイヤ、データリンクレイヤの両方で正しく動作することを確認してください。
- RADIUS サーバの IP アドレスが NAS で正しく設定されていることを確認してください。
- NAS で設定された認証、アカウンティングの UDP ポートが RADIUS サーバで設定されているものと同じであることを確認してください。
- RADIUS サーバの認証、アカウンティングのためのポート番号が使用可能であることを確認してください。

1.7.3 RADIUS アカウンティングエラー

I. 症状

ユーザは認証と許可されましたが、アカウンティングが正常ではありません。

II. 分析

NAS のアカウンティングサーバの設定が間違っています。可能性のある理由を以下に示します。

- NAS で設定されたアカウンティングのためのポート番号が間違っています。
- NAS で設定されたアカウンティングサーバの IP アドレスが間違っています。たとえば、NAS が認証、許可、アカウンティングサービスを提供するために、1 つのサーバを使用するように設定されていますが、実際のサービスは異なるサーバによって提供されています。

III. 解決策

以下を確認してください。

- アカウンティングのためのポート番号が正しく設定されていることを確認してください。
- アカウンティングサーバの IP アドレスが NAS で正しく設定されていることを確認してください。

目次

このセクションのページは **7-x-x** です。

2 章 802.1X の概要 2-1
2.1 802.1X の構成 2-1
2.2 制御/非制御ポートとポート許可状態 2-1
2.3 802.1X 関連プロトコル 2-2
2.3.1 パケットフォーマット 2-2
2.3.2 EAP over RADIUS 2-4
2.4 802.1X 認証の開始 2-4
2.4.1 802.1X クライアントからの認証開始 2-5
2.4.2 アクセス装置からの認証開始 2-5
2.5 802.1X の認証プロセス 2-5
2.5.1 EAP relay と EAP termination の比較 2-6
2.5.2 EAP relay 2-6
2.5.3 EAP termination 2-8

2章 802.1X の概要

802.1X はポートベースのネットワークアクセス制御プロトコルです。

802.1X が有効な LAN ポートに接続された装置を、認証サーバ(RADIUS サーバなど)による認証をすることでネットワークを保護します。

2.1 802.1Xの構成

802.1X は、クライアント/サーバモデルで動作します。図 2-1に示すように 802.1X 認証は以下の構成要素があります。

- **クライアント（サプリカント）**－クライアントは、LAN へアクセスしようとするユーザの端末です。端末はネットワークアクセス装置を認証する 802.1X ソフトウェアが必要です。
- **アクセス装置（オーセンティケータ）**－ネットワークアクセス装置は、クライアントを認証し、LAN へのアクセスを制御します。通常の 802.1X 環境では、ネットワークアクセス装置は、認証サーバを使用して認証を実行します。
- **認証サーバ**－認証サーバは、ネットワークアクセス装置の認証サービスを提供するエンティティです。ネットワークアクセス装置から送信されたデータを使用して 802.1X クライアントを認証し、ネットワークアクセス装置がアクセスするための認証結果を返します。認証サーバは通常、RADIUS（Remote Authentication Dial-in User Service）サーバです。小規模な LAN では、認証サーバとしてネットワークアクセス装置を使用することもできます。

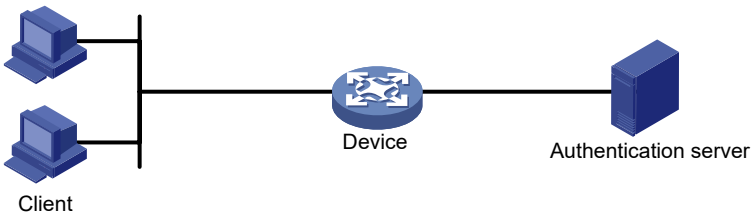


図 2-1 802.1X の構成

2.2 制御/非制御ポートとポート許可状態

802.1X は、ネットワークのアクセスポートのために、制御ポート(Controlled port)と非制御ポート(Uncontrolled port)の 2 つの論理ポートを定義しています。ネットワークのアクセスポートに受信するパケットはすべて、両方の論理ポートに表示されます。

- **非制御ポート**－非制御ポートは常にオープン状態で、認証パケットを送信します。
- **制御ポート**－ポートの状態に依存してパケットをフィルタします。
  - **許可状態**－クライアントが認証にパスした場合、ポートは authorized 状態になります。このポートはトラフィックを通過させることができます。

- **非許可状態**－クライアントが認証にパスしない場合、ポートは unauthorized 状態になります。以下の方法の 1 つによってトラフィックを制御します。
  - クライアントへのトラフィックとクライアントからのトラフィックを拒否するように、双方向のトラフィックを制御します。
  - クライアントからのトラフィックを拒否するように、片方向のトラフィックを制御します。本装置は片方向のトラフィック制御のみをサポートしています。

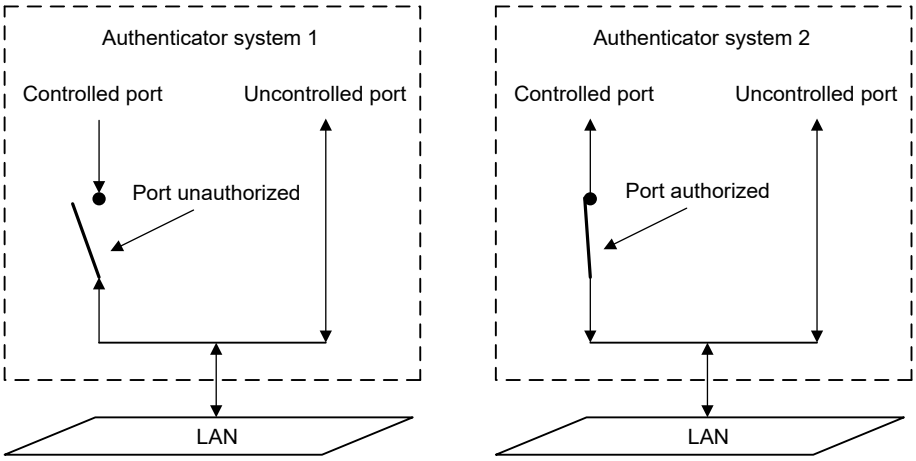


図 2-2 制御ポートの許可/非許可状態

2.3 802.1X関連プロトコル

802.1X は、クライアント、ネットワークアクセス装置、認証サーバの認証情報を転送するために EAP（Extensible Authentication Protocol）を使用しています。 EAP は、クライアント/サーバモデルを使用する認証フレームワークです。MD5-Challenge、EAP-TLS（EAP-Transport Layer Security）、PEAP（Protected EAP）を含む様々な認証方式をサポートしています。

802.1X は、有線または無線 LAN 経由で、クライアントとアクセス装置間で EAPOL（EAP over LAN）を定義します。アクセス装置と認証サーバとの間で、802.1X は、次のいずれかの方法で認証情報を提供します。

- **EAP relay**：EAPOR（EAP over RADIUS）を使用して、RADIUS で EAP パケットをカプセル化します。
- **EAP termination**：EAP パケットから認証情報を抽出し、標準的な RADIUS パケット内の情報をカプセル化します。

2.3.1 パケットフォーマット

I. EAP パケットのフォーマット

図 2-3に EAP パケットのフォーマットを示します。

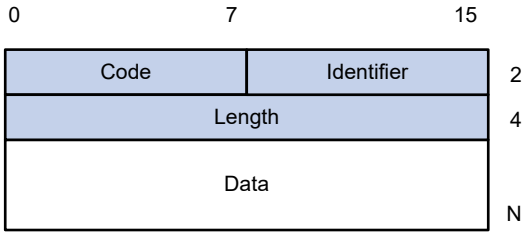


図 2-3 EAP パケットのフォーマット

- **Code**－EAP パケットのタイプです。Request(1)、Response(2)、Success(3)、Failure(4)があります。
- **Identifier**－リクエストとレスポンスを対応づけます。
- **Length**－EAP パケット長（byte）です。Code、Identifier、Length、Data フィールドの合計です。
- **Data**－EAP パケットの中身です。このフィールドは、リクエストまたはレスポンス EAP パケットにのみあります。リクエストタイプ（またはレスポンスタイプ）とタイプデータで構成されています。タイプ 1（Identify）とタイプ 4（MD5-Challenge）はタイプフィールドの 2 つの例です。

II. EAPOL パケットのフォーマット

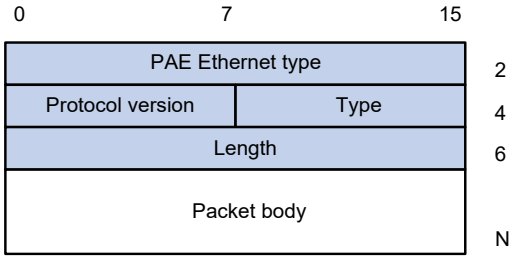


図 2-4 に EAPOL パケットのフォーマットを示します。

- **PAE Ethernet type**－プロトコルタイプです。EAPOL の値は 0x888E です。
- **Protocol version**－EAPOL パケットの送信元がサポートする EAPOL プロトコルのバージョンです。
- **Type**－EAPOL パケットのタイプです。表 2-1に装置がサポートする EAPOL パケットのタイプを示します。

表 2-1 EAPOL パケットのタイプ

値	タイプ	説明
0x00	EAP-Packet	クライアントとネットワークアクセス装置は、認証情報を運ぶためにEAP-Packetを使用します。
0x01	EAPOL-Start	クライアントは、801.1X認証を開始させるために、ネットワークアクセス装置にEAPOL-Startメッセージを送ります。
0x02	EAPOL-Logoff	クライアントは、ログオフを通知するために、アクセス装置にEAPOL-Logoffメッセージを送ります。

- **Length**－データ長（byte）です。Packet body フィールド長を示します。パケットタイプが EAPOL-Start か EAPOL-Logoff の場合、このフィールドに 0 がセットされ、Packet body フィールドは存在しません。
- **Packet body**－パケットの中身です。EAPOL パケットタイプが EAP-Packet の時、Packet body フィールドが EAP パケットの中身です。

2.3.2 EAP over RADIUS

RADIUS は EAP 認証をサポートするため、EAP-Message と Message-Authenticator の 2 つの属性を追加します。RADIUS パケットのフォーマットについての詳細は、オペレーションマニュアルのセクション 7 *セキュリティ* "*AAA*"を参照してください。

I. EAP-Message

図 2-5に示すように RADIUS は、EAP-Message 属性に EAP パケットをカプセル化します。このパケットの Type フィールドの値は 79 です。String フィールドには最大 253 バイトまで入ります。EAP パケット長が 253 バイト以上である場合、複数の EAP-Message 属性にカプセル化されます。

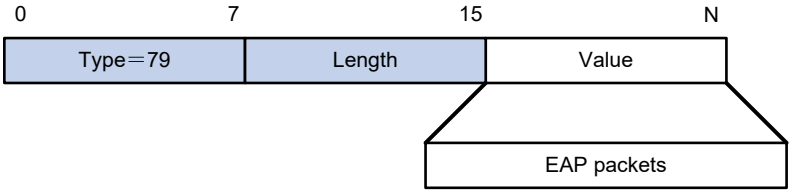


図 2-5 EAP-Message の属性フォーマット

II. Message-Authenticator

RADIUS は、整合性をチェックするため EAP-Message 属性を持つすべてのパケットに Message-Authenticator 属性を含めます。

計算されたパケットの整合性チェックサムが Message-Authenticator 属性の値と異なる場合、パケットの受信者はパケットを廃棄します。Message-Authenticator は、EAP 認証中に EAP 認証パケットが改ざんされることを防ぎます。

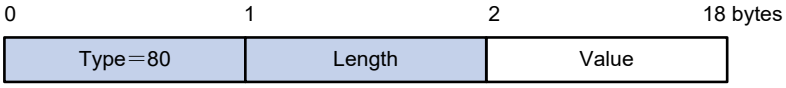


図 2-6 Message-Authenticator の属性フォーマット

2.4 802.1X認証の開始

802.1X 認証は、802.1X クライアントと装置のどちらからでも開始させることができます。

2.4.1 802.1X クライアントからの認証開始

クライアントは、アクセス装置に EAPOL-Start パケットを送信することで、802.1X 認証を開始します。このパケットの宛先 MAC アドレスは、IEEE 802.1X で指定されたマルチキャストアドレス 01-80-C2-00-00-03 またはブロードキャスト MAC アドレスです。クライアントと認証サーバ間のすべての中間装置がマルチキャストアドレスをサポートしていない場合、ブロードキャスト EAPOL-Start パケットを送信できる 802.1X クライアントを使用する必要があります。

2.4.2 アクセス装置からの認証開始

クライアントが EAPOL-Start パケットを送信できない場合、アクセス装置が認証を開始するよう設定します。たとえば 802.1X クライアントは Windows XP で使用できます。

アクセス装置は、以下のモードをサポートしています。

- **マルチキャストトリガモード**－アクセス装置が、定期的に（デフォルトでは 30 秒ごと）EAP-Request/Identity パケットをマルチキャスト送信することで、802.1X 認証を開始します。
- **ユニキャストトリガモード**－MAC アドレステーブルにない送信元 MAC アドレスのフレームを受信した場合、アクセス装置は受信ポートから未知の MAC アドレスへ EAP-Request/Identity パケットを送信します。応答を一定時間内に受信しない場合、パケットを再送します。

2.5 802.1Xの認証プロセス

802.1X 認証には、EAP relay と EAP termination の 2 つのアプローチがあります。EAP パケットと EAP 認証方式のために RADIUS サーバのサポートに応じていずれかのモードを選択してください。

- EAP relay モード

EAP relay は、IEEE802.1X で定義されています。このモードでは、ネットワーク装置は、図 2-7に示すように、RADIUS サーバに認証情報を送信するために EAPOR パケットを使用します。

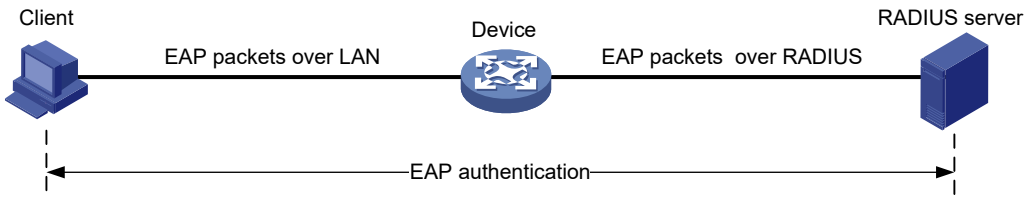


図 2-7 EAP relay

EAP relay モードでは、クライアントは RADIUS サーバと同じ認証方式を用いる必要があります。ネットワークアクセスを行う装置上では、EAP relay で利用するために **dot1x authentication-method eap** コマンドのみが必要です。

- EAP termination モード

図 2-8に示すように、アクセス装置は EAP termination モードで以下の動作を行います。

a)　クライアントから受信したEAPパケットを終端します。

b)　標準RADIUSパケットにクライアント認証情報をカプセル化します。

c)　RADIUSサーバに認証するため、PAPあるいはCHAPを使用します。

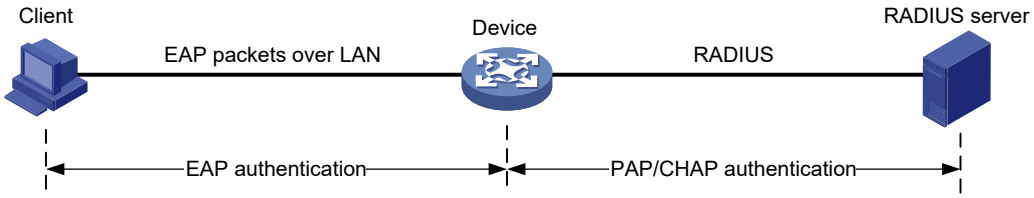


図 2-8 EAP termination

2.5.1 EAP relay と EAP termination の比較

パケット交換方式	利点	制限
EAP relay	• 様々なEAP認証方法をサポートしています。 • アクセス装置上の設定と処理が簡単です。	RADIUSサーバはEAP-MessageとMessage-Authenticator属性と、クライアントに使用されるEAP認証方式をサポートする必要があります。
EAP termination	PAPまたはCHAP認証をサポートしている任意のRADIUSサーバと連携して動作します。	• 以下のEAP認証方式のみをサポートします。 • MD5-Challenge EAP認証 • ユーザ名とパスワードのEAP認証 • アクセス装置上の処理が複雑です。

2.5.2 EAP relay

図 2-9に EAP-MD5 を使用した、EAP relay モードでの基本的な 802.1X 認証プロセスを示します。

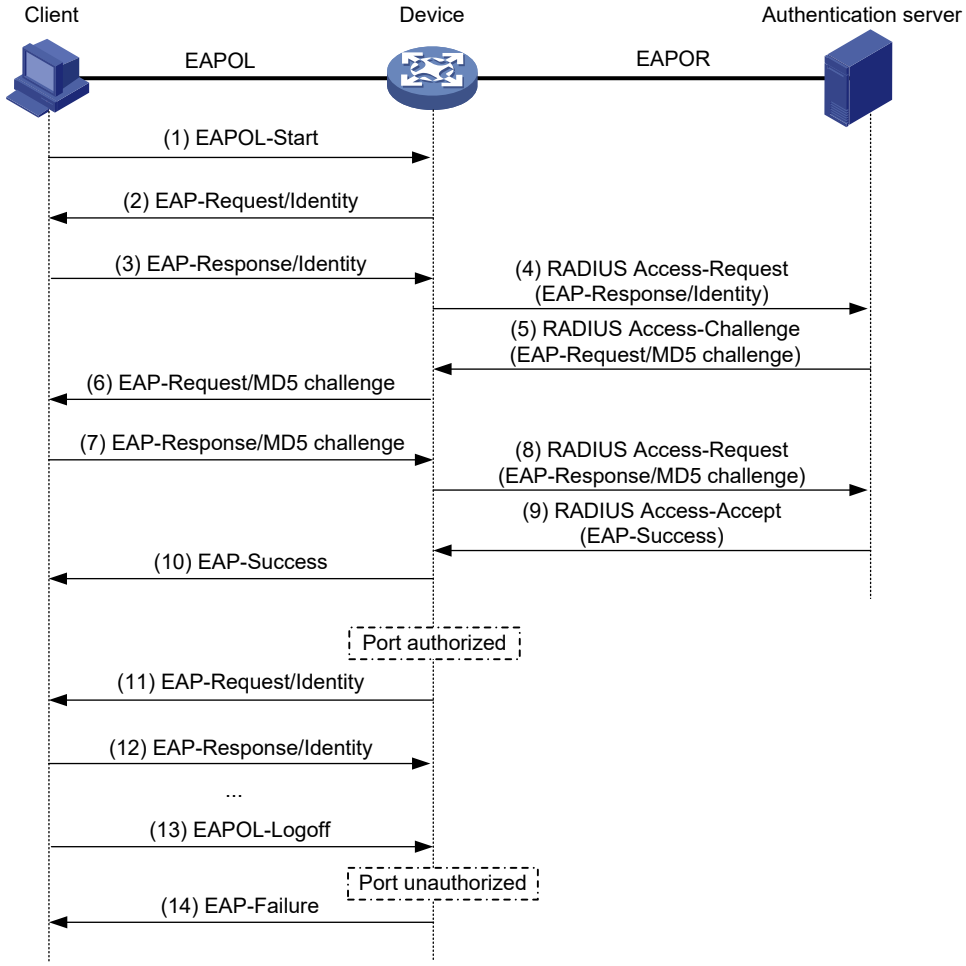


図 2-9 EAP relay モードでの 802.1X 認証プロセス

以下に 802.1X 認証プロセスを記載します。

1) ユーザが、802.1X クライアントを起動し、登録されたユーザ名とパスワードを入力すると、802.1X クライアントは、アクセス装置に EAPOL-Start パケットを送信します。
2) アクセス装置は、応答としてクライアントのユーザ名を要求するために EAP-Request/Identity パケットを送信します。
3) EAP-Request/Identity パケットの応答として、クライアントは EAP-Request/Identity パケットの中にユーザ名を入れて、アクセス装置に送信します。
4) アクセス装置は、RADIUS Access-Request パケットの EAP-Request/Identity パケットを認証サーバに伝搬します。
5) 認証サーバは、ユーザのデータベースを検索するため、RADIUS Access-Request パケットの identify 情報を使用します。一致するエントリが見つかった場合、サーバはランダムに生成されるチャレンジ（EAP-Request/MD5 challenge）を使用してパスワード情報を暗号化し、RADIUS Access-Challenge パケットを通してネットワークアクセス装置にチャレンジ情報を送信します。
6) アクセス装置は、EAP-Request/MD5 Challenge パケットをクライアントに送信します。

7) クライアントは、受信したチャレンジ情報を使用してパスワードを暗号化します。そして EAP-Response/MD5 Challenge パケットの暗号化したパスワードをアクセス装置に送信します。
8) アクセス装置は、RADIUS Access-Request パケットの EAP-Response/MD5 Challenge パケットを認証サーバに伝搬します。
9) 認証サーバは、受信したパスワード情報と、5)で自身が生成したパスワード情報を比較します。2 つのパスワード情報が一致する場合、認証サーバはクライアントが有効であるとみなし、アクセス装置に RADIUS Access-Accept パケットを送信します。
10) RADIUS Access-Accept パケットを受信すると、アクセス装置は、以下の動作を行います。

a) クライアントにEAP-Successパケットを送ります。

b) 制御ポートをauthorized状態に設定します。

クライアントはネットワークにアクセスできます。

11) クライアントがオンラインになった後、クライアントがまだオンラインであるかどうかを確認するために、アクセス装置は定期的にハンドシェイク要求を送信します。デフォルトでは、2 回連続してハンドシェイクが失敗すると、装置はクライアントをログオフします。
12) ハンドシェイク要求を受け取ると、クライアントは応答を返します。クライアントが特定の回数（デフォルトで 2 回）連続してハンドシェイク応答に失敗した場合、アクセス装置は、クライアントをログオフします。このハンドシェイクメカニズムにより、異常にオフラインになった 802.1X ユーザによって使用されるネットワークリソースをタイムリーにリリースすることが可能になります。
13) クライアントは、アクセス装置にログオフを依頼する EAPOL-Logoff パケットを送信することもできます。
14) EAPOL-Logoff パケットに応答して、アクセス装置は、制御ポートの状態を authorized から unauthorized に変更し、クライアントへ EAP-Failure パケットを送信します。

2.5.3 EAP termination

図 2-10に CHAP 認証を使用した、EAP termination モードでの基本的な 802.1X 認証プロセスを示します。

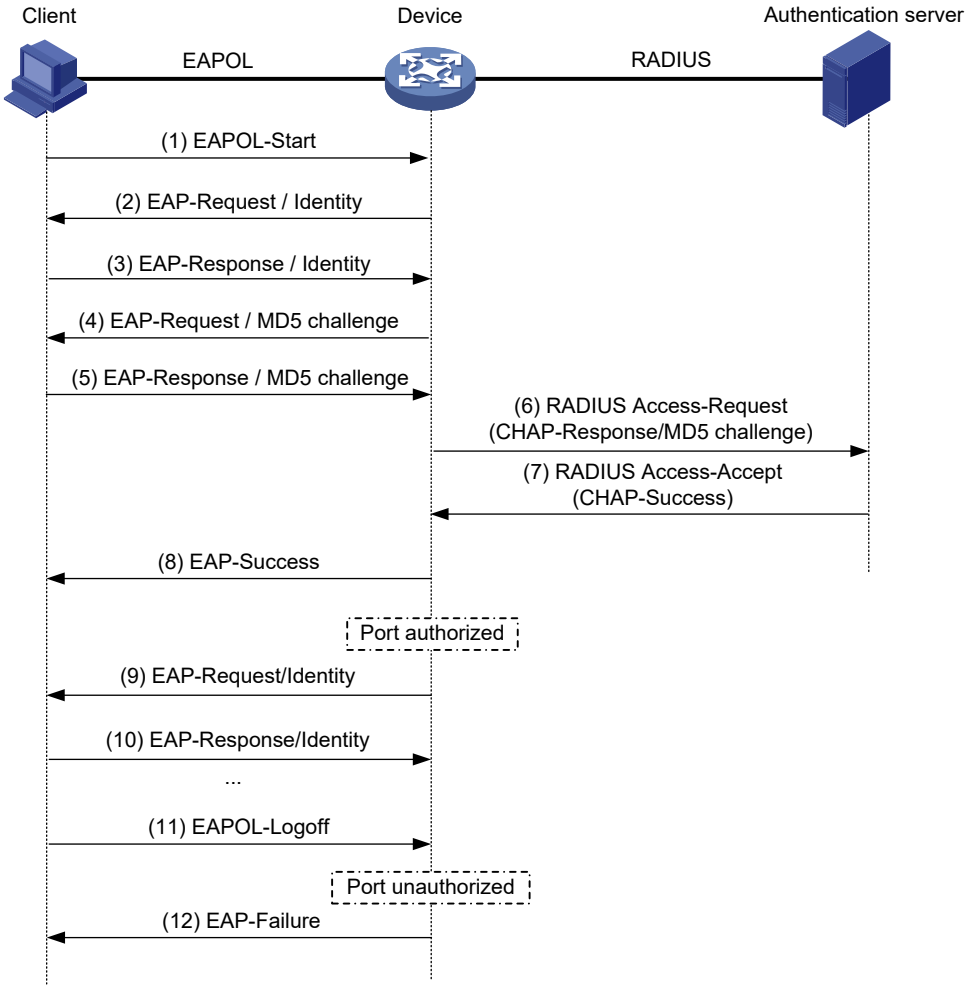


図 2-10 EAP termination での 802.1X 認証プロセス

EAP termination モードでは、パスワードを暗号化するために MD5 challenge を生成するのは認証サーバでなく、アクセス装置です。アクセス装置は次に、MD5 challenge をユーザ名と暗号化されたパスワードと一緒に標準の RADIUS パケットに入れて RADIUS サーバへ送信します。

目次

このセクションのページは**7-x-x**です。

3 章 802.1X.....3-1
3.1 アクセス制御方式.....3-1
3.2 802.1X の VLAN 操作.....3-1
3.2.1 許可 VLAN.....3-1
3.2.2 ゲスト VLAN.....3-4
3.2.3 制限 VLAN.....3-6
3.3 他の機能を用いた 802.1X 認証.....3-7
3.3.1 ACL の割り当て.....3-7
3.4 802.1X 設定制限とガイドライン.....3-7
3.4.1 設定要件.....3-7
3.5 802.1X 設定作業リスト.....3-8
3.6 802.1X 認証の有効化.....3-8
3.7 EAP relay または EAP termination の有効化.....3-8
3.8 ポート許可状態の設定.....3-9
3.9 アクセス制御方式の指定.....3-10
3.10 ポートの 802.1X ユーザの最大同時接続数の設定.....3-10
3.11 認証リクエストの最大送信数の設定.....3-10
3.12 802.1X 認証タイムアウトタイマの設定.....3-11
3.13 オンラインユーザハンドシェイク機能の設定.....3-11
3.13.1 設定ガイドライン.....3-12
3.13.2 設定手順.....3-12
3.14 認証トリガ機能の設定.....3-12
3.14.1 設定ガイドライン.....3-12
3.14.2 設定手順.....3-12
3.15 ポートでの強制認証ドメインの設定.....3-13
3.16 quiet タイマの設定.....3-13
3.17 802.1X 再認証の設定.....3-14
3.17.1 概要.....3-14
3.17.2 設定ガイドライン.....3-14
3.17.3 802.1X 定期的な再認証の設定.....3-14
3.18 802.1X ゲスト VLAN の設定.....3-15
3.18.1 設定ガイドライン.....3-15
3.18.2 設定要件.....3-16
3.18.3 設定手順.....3-16
3.19 802.1X ゲスト VLAN 割り当て遅延の有効化.....3-16
3.19.1 設定ガイドライン.....3-16
3.20 802.1X 制限 VLAN の設定.....3-17
3.20.1 設定ガイドライン.....3-17
3.20.2 設定要件.....3-17
3.20.3 設定手順.....3-18
3.21 MAC アドレス移動機能の有効化.....3-18
3.22 802.1 X ユニキャストトリガーサイレント機能.....3-19
3.23 802.1X の表示と維持.....3-19
3.24 802.1X 認証の設定例.....3-20

3.24.1 基本的な 802.1X 認証の設定例 3-20
3.24.2 802.1X ゲスト VLAN と許可 VLAN の設定例.....3-23
3.24.3 ACL の割り当てによる 802.1X の設定例.....3-26

3章 802.1X

この章は、装置上で 802.1X を設定する方法について説明します。802.1X を実行時に、ポートセキュリティ機能を設定することもできます。ポートセキュリティは 802.1X と MAC アドレス認証を組み合わせて拡張します。ポート上でユーザごとに異なる認証方法を必要とするネットワークに適用します。ポートセキュリティの詳細は、オペレーションマニュアルのセクション 7 *セキュリティ*”*ポートセキュリティ*”を参照してください。

3.1 アクセス制御方式

802.1X プロトコルで定義されたポートベースのアクセス制御を実装しており、MAC ベースのアクセス制御をサポートするためにプロトコルを拡張します。

- **ポートベースアクセス制御**－一度 802.1X ユーザがポート上で認証を通過すると、後続のユーザは、認証なしでポートを介してネットワークにアクセスできます。認証されたユーザがログオフすると、他のすべてのユーザはログオフされます。
- **MAC ベースアクセス制御**－各ユーザは個別にポート上で認証されます。ユーザがログオフしても、他のオンラインのユーザは影響を受けません。

3.2 802.1XのVLAN操作

3.2.1 許可 VLAN

802.1X ユーザが許可されたネットワークリソースへのアクセスを制御するため、許可 VLAN を指定することができます。802.1X ユーザが認証にパスしたのち、認証サーバは許可 VLAN あるいは VLAN グループをユーザに割り当てます。

I. サポートされる VLAN タイプと形式

VLAN タイプと形式は許可タイプに依存してサポートされます。

- ローカル VLAN 許可

  アクセス装置で user view あるいは user group view で VLAN ID によって 1 つの許可 VLAN のみを指定することができます。ローカルユーザの詳細は、オペレーションマニュアルのセクション 7 *セキュリティ*”*AAA*”を参照してください。

- リモート VLAN 許可

  802.1X ユーザの AAA サーバで VLAN あるいは VLAN グループを指定することができます。アクセス装置は以下の形式の VLAN をサポートします。

  - □ VLAN ID
  - □ VLAN 名

  VLAN 名はアクセス装置で VLAN の特徴を示します。

  - □ VLAN ID と VLAN 名の組み合わせ

  文字列で、ある VLAN は VLAN ID で示し、ある VLAN は VLAN 名で示します。

  - □ VLAN グループ名

VLAN グループの詳細は、オペレーションマニュアルのセクション 2 *アクセス ” VLAN*”を参照してください。

□　サフィックスを持つ VLAN ID

サフィックスは、t あるいは u が使用できます。VLAN がタグづけされるポートかどうかを示します。たとえば、2u は VLAN2 がタグづけされていないメンバに割り当てられていることを示します。

🕮 **メモ：**

アクセス装置は、VLAN の割り当てを行う前に、VLAN 名と VLAN グループ名を VLAN ID に置き換えます。

II. サポートされない VLAN タイプ

VLAN 許可では以下のタイプを指定することができません。アクセス装置は、802.1X ユーザに VLAN を割り当てることができません。

- ダイナミックに学習された VLAN
- 予約された VLAN

III. VLAN の選択と割り当て

サーバが VLAN のグループを割り当てる場合、アクセス装置は VLAN ID のフォーマットに従って VLAN を選択し、割り当てます。表 3-1に許可 VLAN のグループの選択と割り当てルールを記載します。

表 3-1 許可 VLAN のグループの VLAN の選択と割り当て

許可 VLAN のタイプ	VLAN の選択と割り当てルール
• VLAN ID • VLAN名 • VLANグループ名	選択される許可VLANは、ポートに他のオンラインユーザがいるかどうかに依存します。 • 他のオンラインユーザがいない場合、装置はVLANのグループからもっとも小さいIDのVLANを選択します。 • 他のオンラインユーザがいる場合、以下の処理によってVLANを選択します。 1． 装置はオンラインユーザから一番遠い番号を持つ VLAN を選択します。 2． 2 つの VLAN がオンライン 802.1X ユーザと同じ番号を持っている場合、装置はもっとも小さい ID の VLAN を選択します。

許可 VLAN のタイプ	VLAN の選択と割り当てルール
サフィックスを持つVLAN ID	1． 装置はサフィックスを除いた一番左の VLAN ID、あるいは、タグなしとして u のサフィックスが付いた一番左の VLAN ID を選択します。 2． 装置は PVID としてポートにタグなしの VLAN を割り当て、タグづけられた VLAN はそのまま割り当てます。タグなし VLAN が割り当てられていない場合、ポートの PVID は変更しません。ポートは、タグづけ VLAN とタグなし VLAN からのトラフィックを通過するように許可します。 たとえば、認証サーバはユーザ用に、1u 2t 3の文字列をアクセス装置に送信します。装置はタグなしVLANとしてVLAN1を割り当てし、タグづけVLANとして他のVLANを割り当てます。VLAN1はPVIDになります。

🕮 **メモ：**

サフィックスを持つ VLAN ID は、ポートベースのアクセス制御を行うハイブリッドポートあるいはトランクポートのみ割り当てることができます。

表 3-2にアクセス装置が 802.1X が有効なポートで VLAN を処理する方法を記載します。（サフィックスを持つ VLAN を除きます。）

表 3-2 VLAN 操作

ポートアクセス制御方式	VLAN 操作
ポートベース	装置は最初の認証ユーザの許可VLANをポートに割り当てます。後続のすべての802.1Xユーザは認証なしでアクセスできます。 ポートにタグなしメンバとして許可VLANが割り当てられた場合、許可VLANはPVIDになります。ポートにタグ付きメンバとして許可VLANが割り当てられた場合、ポートのPVIDは変わりません。 🕮 **メモ**： タグ付き属性は、トランクポートとハイブリッドポートでのみサポートされています。

ポートアクセス制御方式	VLAN 操作
MACベース	• ポートがMACベースVLAN対応のハイブリッドポートの場合、装置は許可VLANに各ユーザのMACアドレスをマッピングします。ポートのPVIDは変更しません。ユーザがログオフすると、ユーザのMAC-VLANマッピングは削除されます。 • ポートがアクセス、トランク、あるいはMACベースVLANが無効のハイブリッドポートである場合 • ポートがタグなしメンバとして許可VLANに割り当てられた場合、装置は最初の認証ユーザの許可VLANをポートに割り当てます。許可VLANはPVIDになります。後続のユーザが認証に成功するために、同じVLANをすべてのポートの802.1Xユーザに許可します。異なるVLANが後続のユーザに許可されると、ユーザは認証をパスすることができません。 • ポートがタグ付きメンバとして許可VLANに割り当てられた場合、ポートのPVIDは変わりません。装置は許可VLANに各ユーザのMACアドレスをマッピングします。

🕮 **メモ：**

802.1X が有効なアクセスポートは、タグなしメンバとしてのみ許可 VLAN を割り当てられます。
ハイブリッドポートは、常にタグなしメンバとして VLAN に割り当ててください。割り当てられたのち、VLAN のタグ付きメンバとしてポートを再設定しないでください。

定期的にオンラインユーザの再認証を行うことで有効になるポートでは、MAC ベース VLAN 機能は、この機能が有効になる前にオンラインになったユーザに適用されません。

アクセス装置は、以下のユーザに MAC-VLAN マッピングを作成します。

- ユーザが再認証にパスします。
- ユーザの許可 VLAN が変更されました。

VLAN の設定と MAC ベース VLAN の詳細は、オペレーションマニュアルのセクション 2 *アクセス”VLAN”*を参照してください。

3.2.2 ゲスト VLAN

ポート上の 802.1X ゲスト VLAN は、802.1X 認証を実行していないユーザに対応します。

ゲスト VLAN のユーザは、アンチウィルスソフトウェアやシステムパッチをダウンロードするためにソフトウェアサーバなどの制限されたネットワークリソースにアクセスすることができます。ゲスト VLAN でユーザが一度 802.1X 認証にパスすると、ゲスト VLAN から削除され、許可されたネットワークリソースにアクセスすることができます。

アクセス装置は、802.1X アクセス制御方式にもとづいて、802.1X が有効なポートで VLAN を処理します。

- ポートベースアクセス制御を実行するポート

認証状態	VLAN 操作
ユーザが802.1X認証にパスしていない	装置はPVIDとして802.1XゲストVLANをポートに割り当てます。ポートのすべての802.1Xユーザはゲスト VLANのリソースのみアクセスできます。802.1XゲストVLANが設定されていない場合、アクセス装置は任意のVLANの操作を実行しません。
802.1XゲストVLANのユーザが802.1X認証に失敗した	802.1X制限VLAN（Auth-Fail VLAN、オペレーショマニュアルのセクション7 *セキュリティ”802.1X”の”制限VLAN*”を参照してください）が有効である場合、装置はPVIDとして制限VLANを割り当てます。 制限VLANが設定されていない場合、ポートのPVIDは802.1XゲストVLANのままとなります。ポートのすべてのユーザはゲストVLANの中にいます。
802.1XゲストVLANのユーザが802.1X認証に成功した	● 装置はPVIDとしてユーザの認証VLANを割り当てます。802.1XゲストVLANからポートを削除します。ユーザがログオフしたのち、ポートの最初のPVIDがもとに戻ります。 ● 認証サーバがVLANを許可しない場合、初期のPVIDを適用します。ユーザと後続のすべての802.1Xユーザは初期ポートに割り当てられます。ユーザがログオフしたのち、ポートVLANは変更されません。 🕮 **メモ：** 802.1Xが有効なポートの初期のPVIDは、ポートが任意の802.1X VLANに割り当てられる前にポートで使用されたPVIDです。

- MAC ベースアクセス制御を実行するポート

認証状態	VLAN 操作
ユーザが認証プロセス中に802.1X認証にパスしていない	装置はユーザのMACアドレスと802.1XゲストVLANのマッピングを作成します。ユーザはゲストVLANのリソースのみアクセスできます。
802.1XゲストVLANのユーザが802.1X認証に失敗した	802.1X制限VLANが有効である場合、装置はユーザのMACアドレスを制限VLANに再マッピングします。ユーザは制限VLANのリソースのみアクセスできます。
802.1XゲストVLANのユーザが802.1X認証に成功した	装置はユーザのMACアドレスを許可VLANに再マッピングします。 認証ユーザがVLANを許可しない場合、装置はユーザのMACアドレスをポートの初期のPVIDに再マッピングします。

802.1X ゲスト VLAN 機能のため、MAC ベースアクセス制御を実行するポートで以下の要件に対応してください。

- □ ポートがハイブリッドポートです。
- □ ポートで MAC ベースアクセス VLAN が有効です。

ネットワーク装置はハイブリッドポートをタグなしメンバとして 802.1X ゲスト VLAN に割り当てます。

VLAN の設定と MAC ベース VLAN の詳細は、オペレーションマニュアルのセクション 2 *アクセス”VLAN*”を参照してください。

3.2.3 制限 VLAN

組織のセキュリティ戦略に適合できずに失敗したことが原因で 802.1X 認証に失敗したユーザに対応するため、制限 VLAN を設定することができます。たとえば間違ったパスワードを入力したユーザに VLAN が適応します。制限 VLAN は、アンチウィルスソフトウェアやシステムパッチをダウンロードするためにソフトウェアサーバなどの制限されたネットワークリソースのみアクセスすることができます。

制限 VLAN は、認証のタイムアウトやネットワーク接続の問題のために認証に失敗した 802.1X のユーザには対応していません。

アクセス装置がポート上の VLAN を処理する方法は、802.1X アクセス制御モードによって異なります。

- ポートベースアクセス制御を実行するポート

認証状態	VLAN 操作
ユーザが802.1X認証に失敗した	装置はPVIDとしてポートに制限VLANを割り当てます。ポートのすべての802.1Xユーザは制限VLANのリソースのみアクセスすることができます。
サーバ到達不能の理由を除いた他の理由によって、802.1X制限VLANのユーザが802.1X認証に失敗した	制限VLANが設定されている場合、ポートのPVIDは制限VLAN IDに変更されます。ポートのすべての802.1Xユーザはこの VLANにいます。
ユーザが802.1X認証にパスした	• 装置はPVIDとしてポートにユーザの許可VLANを割り当て、制限VLANからポートを削除します。ユーザがログオフしたのち、ゲストVLANがPVIDとしてポートに割り当てられます。ゲストVLANが設定されていない場合、初期のPVIDに戻ります。 • 認証サーバがVLANを許可しない場合、ポートの初期のPVIDが適用されます。ユーザと後続のすべての802.1Xユーザは初期のPVIDに割り当てられますユーザがログオフしたのち、PVIDは変更されません。

- MAC ベースアクセス制御を実行するポート

認証状態	VLAN 操作
ユーザが802.1X認証に失敗した	装置はユーザのMACアドレスを802.1X制限VLANにマッピングします。ユーザは制限VLANのリソースのみアクセスすることができます。
サーバ到達不能の理由を除いた他の理由によって、802.1X制限VLANのユーザが802.1X認証に失敗した	ユーザは制限VLANのままです。
制限VLANのユーザが802.1X認証にパスした	装置はユーザのMACアドレスを認証VLANに再マッピングします。 認証サーバがVLANを許可しない場合、装置はユーザのMACアドレスをポートの初期のPVIDに再マッピングします。

802.1X 制限 VLAN 機能のため、MAC ベースアクセス制御を実行するポートがハイブリッドポートであることを確認し、ポート上で MAC ベース VLAN を有効にしてください。

アクセス装置はハイブリッドポートをタグなしメンバとして 802.1X 制限 VLAN に割り当てます。

VLAN の設定と MAC ベース VLAN の詳細は、オペレーションマニュアルのセクション 2 *アクセス ”VLAN”* を参照してください。MAC ベース VLAN 機能のサポートは装置の種類によって異なります。

3.3 他の機能を用いた802.1X認証

3.3.1 ACL の割り当て

ネットワークリソースへのアクセスを制御するため、802.1X ユーザに ACL を指定することができます。ユーザが 802.1X 認証にパスしたのち、認証サーバはユーザのトラフィックをフィルタするためアクセスポートに ACL を割り当てます。認証サーバはローカルアクセス装置あるいは RADIUS サーバで行えます。どちらの場合でも、アクセス装置で ACL を設定する必要があります。ユーザはオンライン中に ACL を変更することができます。ACL の詳細は、オペレーションマニュアルのセクション 6 *ACL and QoS ”ACL”* を参照してください。

装置は、static ACL の許可 ACL としての割り当てをサポートしています。

- **Static ACLs**—static ACL は、RADIUS サーバまたはアクセス装置によって割り当てることができます。サーバまたはアクセス装置が static ACL をユーザに割り当てる場合、ACL 番号のみが割り当てられます。ACL を手動で作成し、アクセス装置でそのルールを設定する必要があります。
  ユーザのアクセス許可を変更するには、次のいずれかの方法を使用できます。
  - □　アクセス装置の認証 ACL で ACL ルールを変更します。
  - □　別の RADIUS サーバまたはアクセス装置から別の ACL をユーザに割り当てます。

  static ACL とそのルールは、アクセス装置から手動で削除できます。

3.4 802.1X設定制限とガイドライン

802.1X を設定する場合には、以下の制限とガイドラインに従ってください。

- 802.1X の設定は、レイヤ 2 イーサネットインタフェースでのみサポートされます。
- レイヤ 2 イーサネットインタフェースで 802.1X を有効にする前に、インタフェースがレイヤ 2 アグリゲーショングループに加えられていないことを確認してください。

3.4.1 設定要件

802.1X を設定する前に、以下の作業を完了してください。

- 802.1X ユーザのために ISP ドメインと AAA スキーム（ローカルまたは RADIUS 認証）を設定してください。
- RADIUS 認証を使用する場合は、RADIUS サーバにユーザアカウントを作成してください。
- ローカル認証を使用する場合は、アクセス装置にローカルユーザアカウントを作成し、サービスタイプを lan-access に設定してください。

RADIUS クライアントの設定の詳細は、オペレーションマニュアルのセクション 7 *セキュリティ*”*AAA*”を参照してください。

3.5 802.1X設定作業リスト

作業リスト
（必須設定項目）802.1X認証の有効化
（必須設定項目）EAP relayまたはEAP terminationの有効化
（オプション設定項目）ポート許可状態の設定
（オプション設定項目）アクセス制御方式の指定
（オプション設定項目）ポートの802.1Xユーザの最大同時接続数の設定
（オプション設定項目）認証リクエストの最大送信数の設定
（オプション設定項目）802.1X認証タイムアウトタイマの設定
（オプション設定項目）オンラインユーザハンドシェイク機能の設定
（オプション設定項目）認証トリガ機能の設定
（オプション設定項目）ポートでの強制認証ドメインの設定
（オプション設定項目）quietタイマの設定
（オプション設定項目）802.1X再認証機能の有効化
（オプション設定項目）802.1XゲストVLANの設定
（オプション設定項目）802.1XゲストVLAN割り当て遅延の有効化
（オプション設定項目）802.1X制限VLANの設定
（オプション設定項目）MACアドレス移動機能の有効化

3.6 802.1X認証の有効化

802.1X 認証を有効にする場合、以下のガイドラインに従ってください。

- PVID が Voice VLAN である場合、802.1X 機能はポートに適用できません。Voice VLAN の詳細は、オペレーションマニュアルのセクション 2 *アクセス*“*Voice VLAN*”を参照してください。
- 802.1X 認証が有効なポートでリンクアグリゲーションまたはループバックグループサービスを設定することができません。

以下に 802.1X 認証の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． グローバルで 802.1X 認証を有効にする	**dot1x**	デフォルト：無効
3． interface view に移行する	**interface** *interface-type interface-number*	―
4． ポートで 802.1X 認証を有効にする	**dot1x**	デフォルト：無効

3.7 EAP relayまたはEAP terminationの有効化

EAP relay または EAP termination を設定する場合に、以下の点を考慮してください。

- EAP パケットに関する RADIUS サーバのサポート
- 802.1X クライアントと RADIUS サーバでサポートされている認証方式

以下の状況では EAP relay と EAP termination の両方を設定することができます。

- クライアントが MD5-Challenge EAP 認証のみを使用します。
- クライアントが"ユーザ名+パスワード"の EAP 認証のみを使用します。

EAP-TL、PEAP、またはその他の EAP 認証方式を使用するには、EAP relay を使用する必要があります。

EAP relay と EAP termination の詳細は、オペレーションマニュアルのセクション 7 *セキュリティ”802.1X の概要”*”を参照してください。

以下に EAP relay と EAP termination の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． EAP relay または EAP termination を設定する	**dot1x authentication-method** { **chap** | **eap** | **pap** }	デフォルトでは、ネットワークアクセス装置は、EAP terminationを実行し、RADIUS サーバとの通信にCHAPを使用します。 EAP terminationを有効にするためには、**eap**パラメータを指定してください。 CHAP対応またはPAP対応のEAP relayを有効にするためには、**chap**または**pap**パラメータを指定してください。

🕮 **メモ：**

EAP relay モードが使用されている場合、RADIUS scheme view で設定された **user-name-format** コマンドは適用されません。アクセス装置はクライアントからの認証データを何も変更せずにサーバに送信します。

3.8 ポート許可状態の設定

ポートの許可状態は、クライアントがネットワークへのアクセスを許可されているかどうかを決定します。**dot1x port-control** コマンドと以下のキーワードを使用して、ポートの認証状態を制御できます。

- **authorized-force**－ポートを authorized 状態にすると、認証なしでネットワークにアクセスするポート上のユーザを有効にします。
- **unauthorized-force**－ポートを unauthorized 状態にすると、ポート上のユーザからのアクセス要求を拒否します。
- **auto**－EAPOL パケットのみの通過を許可するために、最初にポートを unauthorized 状態にし、ユーザが認証を通過した後、ネットワークへのアクセスを許可するために、ポートを authorized 状態にします。ほとんどの場合で、このオプションを使用することができます。

以下にポート許可状態の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． interface view に移行する	**interface** *interface-type interface-number*	―
3． ポート認証状態を設定する	**dot1x port-control** { **authorized-force** | **auto** | **unauthorized-force** }	デフォルト：**auto**

3.9 アクセス制御方式の指定

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． interface view に移行する	**interface** *interface-type interface-number*	―
3． アクセス制御方式を指定する	**dot1x port-method** { **macbased** | **portbased** }	デフォルト：**macbased**

3.10 ポートの802.1Xユーザの最大同時接続数の設定

この設定を行うことにより、ユーザ過多によりシステムリソース不足になることを防ぎます。

以下にポートでの 802.1X ユーザの最大同時接続数の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． interface view に移行する	**interface** *interface-type interface-number*	―
3． ポートでの 802.1X ユーザの最大同時接続数を設定する	**dot1x max-user** *user-number*	デフォルト：4294967295

🕮 **メモ：**

Version 7.1.5 を含むそれ以降は、2048 まで認証動作が可能です。
QVesion 7.1.3 では、2000 まで認証動作が可能です。

3.11 認証リクエストの最大送信数の設定

アクセス装置は、指定した時間内にクライアントからの応答がない場合、認証リクエストの再送信を行います。この時間を設定する場合、**dot1x timer tx-period** *tx-period-value* コマンドまたは **dot1x timer supp-timeout** *supp-timeout-value* コマンドを使用します。

アクセス装置からリクエストの最大送信数まで再送信しても応答がない場合、リクエストの再送信を停止します。

以下に認証リクエストの最大送信数の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． クライアントへの認証リクエストの最大送信数を設定する	**dot1x retry** *max-retry-value*	デフォルト：2

3.12 802.1X認証タイムアウトタイマの設定

ネットワーク装置は、以下の 802.1X 認証タイムアウトタイマを使用しています。

- **クライアントタイムアウトタイマ**－アクセス装置がクライアントに EAP-Request/MD5 Challenge パケットを送信する場合に起動します。このタイマが時間切れになるまで応答がなかった場合、アクセス装置は、クライアントにリクエストを再送します。
- **サーバタイムアウトタイマ**－アクセス装置が認証サーバに RADIUS Access-Request パケットを送信する場合に起動します。このタイマが時間切れになるまでに応答がなかった場合、アクセス装置は、サーバにリクエストを再送します。

ほとんどの場合、デフォルトの設定で十分です。ネットワークの状況に応じてタイマを設定することができます。

- パフォーマンスの低いネットワークで、クライアントタイムアウトタイマを高い値に設定します。
- 異なる性能の認証サーバがあるネットワークでサーバタイムアウトタイマを調整します。

以下に 802.1X 認証タイムアウトタイマの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． クライアントタイムアウトタイマを設定する	**dot1x timer supp-timeout** *supp-timeout-value*	デフォルト：30秒
3． サーバタイムアウトタイマを設定する	**dot1x timer server-timeout** *server-timeout-value*	デフォルト：100秒

3.13 オンラインユーザハンドシェイク機能の設定

オンラインユーザハンドシェイク機能は、オンラインの 802.1X ユーザの接続状態をチェックします。ネットワークアクセス装置は、**dot1x timer handshake-period** コマンドで指定された間隔でオンラインユーザにハンドシェイクメッセージを送信します。ハンドシェイクの最大試行回数後もオンラインユーザから応答を受信しない場合、ネットワークアクセス装置は、ユーザを offline 状態に設定します。ハンドシェイクの最大試行回数を設定する場合、**dot1x retry** コマンドを使用します。

また、本装置はデフォルトでオンラインユーザからの EAP-response に対する EAP-success を返しません。EAP-response に対する EAP-success を返すには、**dot1x handshake reply enable** コマンドを使用します。

3.13.1 設定ガイドライン

オンラインユーザハンドシェイク機能を設定する場合、以下の制限とガイドラインに従ってください。

- ネットワークに、ネットワークアクセス装置とのハンドシェイクパケットを交換できない 802.1X クライアントがある場合、オンラインユーザハンドシェイク機能を無効にしてください。これは 802.1X 接続が不適切に切断されることを防ぎます。

3.13.2 設定手順

以下にオンラインユーザハンドシェイク機能の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． （オプション設定項目）ハンドシェイクタイマを設定する	**dot1x timer handshake-period** *handshake-period-value*	デフォルト：15秒
3． interface view に移行する	**interface** *interface-type interface-number*	―
4． オンラインユーザハンドシェイク機能を有効にする	**dot1x handshake**	デフォルト： RJ-45ポート：無効 SFPポート：有効
5． ハンドシェイクリプライ機能を有効にする	**dot1x handshake reply enable**	デフォルト：無効

3.14 認証トリガ機能の設定

認証トリガ機能は、802.1X クライアントが認証を開始できない場合 802.1X 認証を開始するためにネットワークアクセス装置を有効にします。

この機能はマルチキャストトリガとユニキャストトリガをサポートします。オペレーションマニュアルのセクション 7 *セキュリティ*“*802.1X の概要*”を参照してください。

3.14.1 設定ガイドライン

認証トリガ機能を設定する場合は、以下のガイドラインに従ってください。

- ポートに接続されたクライアントが、802.1X 認証を開始するために EAPOL-Start パケットを送信できない場合、ポート上でマルチキャストトリガを有効にします。
- 802.1X クライアントがほとんどいないポートに接続され、これらのクライアントが認証を開始できない場合は、ポート上でユニキャストトリガを有効にします。
- 重複した認証パケットを避けるために、ポート上で両方のトリガを有効にしないでください。

3.14.2 設定手順

以下にポートでの認証トリガ機能の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． （オプション設定項目）ユーザ名リクエストタイムアウトタイマを設定する	**dot1x timer tx-period** *tx-period-value*	デフォルト：30秒
3． interface view に移行する	**interface** *interface-type interface-number*	―
4． 認証トリガ機能を有効にする	**dot1x** { **multicast-trigger** | **unicast-trigger** }	デフォルト： ・マルチキャストトリガ RJ-45ポート：無効 SFPポート：有効 ・ユニキャストトリガ RJ-45ポート：有効 SFPポート：無効

3.15 ポートでの強制認証ドメインの設定

ポート上で認証、許可、アカウンティングのための強制認証ドメイン内にすべての 802.1X ユーザを配置することができます。ユーザは、他のドメイン内のアカウントを使用して、ポートを介してネットワークにアクセスすることはできません。強制認証ドメインの実装で、802.1X アクセス制御の導入時の柔軟性を高めます。

以下にポートでの強制認証ドメインの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． interface view に移行する	**interface** *interface-type interface-number*	―
3． ポートで 802.1X 強制認証ドメインを指定する	**dot1x mandatory-domain** *domain-name*	デフォルト：設定なし

3.16 quietタイマの設定

quiet タイマを有効にすると、アクセス装置は、802.1X 認証に失敗したクライアントからの認証リクエストを処理する前に一定時間待ちます。

ネットワークの状況に応じて quiet タイマを設定することができます。

- 脆弱なネットワークでは高い値を設定してください。
- 認証応答を速くするためには低い値を設定してください。

以下に quiet タイマの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． quiet タイマを有効にする	**dot1x quiet-period**	デフォルト：無効
3． quiet タイマを設定する	**dot1x timer quiet-period** *quiet-period-value*	デフォルト：60秒

3.17 802.1X再認証の設定

3.17.1 概要

802.1X 再認証は、オンラインユーザの接続状態をトラッキングし、サーバによって割り当てられた属性を更新します。属性は ACL、VLAN が含まれます。

802.1X 再認証では、再認証の間隔はユーザが設定できます。

デフォルトでは、802.1X 再認証のサーバが到達不能である場合、装置はユーザをログオフします。オンライン保持機能は、サーバが到達不能な場合、802.1X ユーザの再認証を継続します。

3.17.2 設定ガイドライン

802.1X 再認証を設定する場合は、以下のガイドラインに従ってください。

サーバで割り当てられたセッションタイムアウトタイマ（セッションタイムアウト属性）と終了行動（終了行動属性）は定期的な再認証に影響することがあります。サーバで割り当てられたセッションタイムアウトと終了行動の属性を表示するには、**display dot1x connection** コマンドを使用してください。

- 終了行動が **Default**（ログオフ）の場合、session timeout タイマよりも定期的な再認証タイマが短い際に効果があります。
- 終了行動が **Radius-request** の場合、定期的な再認証は効果がありません。session timeout タイマが終了後にオンライン 802.1X ユーザを再認証します。

session timeout と termination action 属性の割り当てサポートは、サーバモデルによります。

- **dot1x timer reauth-period** コマンドを使用して、定期的な再認証タイマをシステム view とインタフェース view のどちらでも設定できます。

  装置は、以下の順に定期的な再認証タイマを選択します。

a) サーバ割り当てされた再認証タイマ

b) ポート指定の再認証タイマ

c) グローバル再認証タイマ

d) デフォルト再認証タイマ

- 認証前後でオンラインユーザに割り当てられた VLAN は、同一でも異なっても可能です。

ユーザがオンライン同期を待機している間に定期的な再認証がトリガされると、システムはオンライン同期を実行し、ユーザの再認証は実行しません。

3.17.3 802.1X 定期的な再認証の設定

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

操作	コマンド	補足
2．（オプション設定項目）定期的な認証タイマを設定する	**dot1x timer reauth-period** *reauth-period-value*	デフォルト：3600秒
3．interface view に移行する	**interface** *interface-type interface-number*	―
4．定期的なオンラインユーザの再認証を設定する	**dot1x re-authenticate**	デフォルト：無効
5．（オプション設定項目）ポートに定期的な認証タイマを設定する	**dot1x timer reauth-period** *reauth-period-value*	デフォルト：無効 グローバルの定期的な802.1X再認証タイマを使用します。

3.18 802.1XゲストVLANの設定

3.18.1 設定ガイドライン

802.1X ゲスト VLAN を設定する場合、以下のガイドラインに従ってください。

- ポートに 1 つのみ 802.1X ゲスト VLAN を設定することができます。異なるポートで異なる 802.1X ゲスト VLAN を設定することができます。
- ポートでポート VLAN、802.1X ゲスト VLAN に異なる ID を割り当ててください。ポートで、VLAN にタグづけられた入力トラフィックの処理を正しく処理できるように割り当ててください。
- 802.1X ゲスト VLAN 機能が正しく機能するためには、この機能を EAD アシスタントと一緒に設定しないでください。
- ハイブリッドポートでは、ゲスト VLAN はタグなし VLAN のみにすることができます。
- voice VLAN と 802.1X ゲスト VLAN の両方がハイブリッドポートで設定されている場合、voice VLAN は 802.1X ゲスト VLAN よりも優先されます。パケットが voice VLAN 設定と一致する場合、パケットは voice VLAN から転送されます。voice VLAN 設定と一致しない場合、その送信元 MAC アドレスが 802.1X ゲスト VLAN に追加されている可能性があります。
- ポートで複数のセキュリティ機能を設定する場合、表 3-3に示すガイドラインに従ってください。

表 3-3 802.1X ゲスト VLAN と他のセキュリティ機能の関係

機能	関係	補足
MACベースのアクセス制御を行うポート上の802.1X制限VLAN	802.1X制限VLANは802.1XゲストVLANより優先順位が高くなります。	オペレーションマニュアルのセクション *7 セキュリティ” 802.1X*”を参照してください。
MACベースのアクセス制御を行うポート上のポート侵入防御	802.1XゲストVLAN機能は、MACアドレスのブロック動作よりも優先順位が高くなります。ポート侵入保護機能のポートシャットダウン動作よりも優先順位が低いです。	オペレーションマニュアルのセクション *7 セキュリティ”* ポートセキュリティ”を参照してください。

3.18.2 設定要件

802.1X ゲスト VLAN を設定する前に、以下の作業を完了してください。

- 802.1X ゲスト VLAN として指定される VLAN を作成してください。
- 802.1X 対応ポートが MAC ベースのアクセス制御を行う場合、以下の作業を完了してください。
  - □ ハイブリッドポートとして設定してください。
  - □ ポートで MAC ベース VLAN を有効にしてください。MAC ベース VLAN の詳細は、オペレーションマニュアルのセクション 2 *アクセス”VLAN”*を参照してください。
  - □ ポートタイプがハイブリッドの場合、802.1X ゲスト VLAN として指定する VLAN がポートのタグ付き VLAN リストにないことを確認してください。

3.18.3 設定手順

以下に 802.1X ゲスト VLAN の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. interface view に移行する	**interface** *interface-type interface-number*	―
3. ポートで 802.1X ゲスト VLAN を設定する	**dot1x guest-vlan** *guest-vlan-id*	デフォルト：設定なし

3.19 802.1XゲストVLAN割り当て遅延の有効化

3.19.1 設定ガイドライン

この機能は、ポートで 802.1X 認証が行われる場合に 802.1X ゲスト VLAN への 802.1X が有効なポートを割り当てるのを遅らせます。

この機能は、EAPOL 開始パケットまたはアンノウン MAC アドレスからのパケットにより 802.1X 認証が行われる場合にのみ適用されます。

この機能を使用するには、802.1X 有効ポートは MAC ベースのアクセス制御を行わなければなりません。MAC トリガの 802.1X ゲスト VLAN 割り当て遅延を使用するには、ポートに 802.1X ユニキャストトリガも設定しなければなりません。

802.1X 認証がポートで行われる場合、装置は以下の操作を行います。

- ユニキャスト EAP-Request/Identity パケットを認証のトリガとなった MAC アドレスに送信します。
- **dot1x timer tx-period** コマンドで設定されたユーザネーム要求タイムアウト期間内に応答がなかった場合、パケットを再送します。
- dot1x retry コマンドで設定された最大リクエスト試行回数に達した後、ポートに 802.1x ゲスト VLAN を割り当てます。

以下にポートへの 802.1X ゲスト VLAN 割り当て遅延の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． interface view に移行する	**interface** *interface-type interface-number*	―
3． ポートで 802.1X ゲスト VLAN 割り当て遅延を設定する	**dot1x guest-vlan-delay** { **eapol** | **new-mac** }	デフォルト：無効

3.20 802.1X制限VLANの設定

3.20.1 設定ガイドライン

802.1X 制限 VLAN を設定する前に、以下の制限とガイドラインに従ってください。

- ポートで Voice VLAN、ポート VLAN、802.1X 制限 VLAN に異なる ID を割り当ててください。ポートで、VLAN にタグづけられた入力トラフィックの処理を正しく処理できるように割り当ててください。
- ポートに 1 つのみ 802.1X 制限 VLAN を設定することができます。異なるポートで異なる 802.1X 制限 VLAN を設定することができます。
- ハイブリッドポートでは、802.1X 制限 VLAN はタグなし VLAN のみにすることができます。
- ポートで複数のセキュリティ機能を設定する場合、表 3-4に示すガイドラインに従ってください。

表 3-4 802.1X 制限 VLAN と他のセキュリティ機能の関係

機能	関係	補足
MACベースのアクセス制御を行うポート上のMACアドレス認証ゲストVLAN	802.1X制限VLANは優先順位が高くなります。	オペレーションマニュアルのセクション *7 セキュリティ”MAC アドレス認証”* を参照してください。
MACベースのアクセス制御を行うポート上のポート侵入防御	802.1X制限VLAN機能は、MAC動作のブロックよりも優先順位が高くなります。ポート侵入保護機能のポートシャットダウン動作よりも優先順位が低いです。	オペレーションマニュアルのセクション *7 セキュリティ”ポートセキュリティ”* を参照してください。

3.20.2 設定要件

802.1X 制限 VLAN を設定する前に、以下の作業を完了してください。

- 802.1X 制限 VLAN として指定される VLAN を作成してください。
- 802.1X 対応ポートが MAC ベースのアクセス制御を行う場合、以下の作業を完了してください。
  - □ ハイブリッドポートとして設定してください。

- □ ポートで MAC ベース VLAN を有効にしてください。MAC ベース VLAN の詳細は、オペレーションマニュアルのセクション 2 *アクセス”VLAN”*を参照してください。
- □ ポートタイプがハイブリッドの場合、802.1X 制限 VLAN として指定する VLAN がポートのタグ付き VLAN リストにないことを確認してください。

3.20.3 設定手順

以下に 802.1X 制限 VLAN の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． interface view に移行する	**interface** *interface-type interface-number*	―
3． ポートで 802.1X 制限 VLAN を設定する	**dot1x auth-fail vlan** *authfail-vlan-id*	デフォルト：設定なし

3.21 MACアドレス移動機能の有効化

MAC アドレス移動機能を有効にすることで、認証が許可されたユーザが装置のポートを移動できるようになります。たとえば、認証ユーザが別のポートに移動する場合、認証セッションが最初のポートから削除され、新しいポートで再認証されます。

MAC アドレス移動機能が無効で認証ユーザが別のポートに移動した場合、再認証されません。

（ローカルまたはリモートの）認証サーバのオンラインユーザ数が上限に達した場合、認証ユーザは装置上のポート間で移動はできません。

ポートのローミングを行うワイヤレスユーザがネットワークにアクセスできるように MAC アドレス移動機能を有効にすることを推奨します。

以下に MAC アドレス移動機能の有効化の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． MAC アドレス移動機能を有効にする	**port-security mac-move permit**	デフォルト：有効

3.22 802.1 Xユニキャストトリガーサイレント機能

🕮 **メモ：**

802.1 X ユニキャストトリガーサイレント機能は Version7.1.13 を含む以降のソフトウェアからサポートしています。

I. 概要

ユニキャストトリガーがイネーブルになっているポートで未知の送信元 MAC アドレスを持つパケットを受信すると、デバイスは EAP-Request/Identity 要求パケットをクライアントにユニキャストします。dot 1 x timer tx-period コマンドを使用して設定された期間内にクライアントから応答がない場合、デバイスはクライアントに要求を再送信します。デバイスは、最大回数の送信試行を行ってもクライアントから応答を受信できない場合、タイマアドレスのユニキャストトリガーサイレント MAC を開始します。要求パケットを送信する最大試行回数を設定するには、dot 1 x retry コマンドを使用します。

ユニキャストトリガー抑制タイマアドレスがある MAC アドレスから始まる場合、この MAC アドレスはユニキャストトリガー抑制アドレスと呼ばれます。タイマが期限切れになるまでは、デバイスはこの MAC アドレスを送信元 MAC アドレスとして持つパケットを受信しても、この MAC アドレスに対して EAP-Request/Identity 要求パケットをユニキャストしません。

II. 制約事項およびガイドライン

この機能は、802.1 X ユーザがオンラインになるレートに影響する場合があります。

また､次の機能と組み合わせて使用しないでください｡正常に 802.1X 認証が出来ません。

- ゲスト VLAN
- ゲスト VSI
- EAD アシスタント

III. 設定手順

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． ユニキャストトリガーサイレントタイマを設定する	**dot1x timer unicast-trigger quiet-period** *quiet-period-value*	デフォルト：ディセーブル ユニキャストトリガー待機時間は0秒です。

3.23 802.1Xの表示と維持

すべての view で **display** コマンドを実行でき、user view で **reset** コマンドを実行できます。

操作	コマンド
特定、またはすべてのポートの802.1X認証情報、統計情報、設定情報を表示する	**display dot1x** [**sessions** | **statistics**] [**interface** *interface-type interface-number*]

操作	コマンド
オンライン802.1Xユーザ情報を表示する	**display dot1x connection** [**interface** *interface-type interface-number* | **slot** *slot-number* | **user-mac** *mac-addr* | **user-name** *name-string*]
802.1X統計情報をクリアする	**reset dot1x statistics** [**interface** *interface-type interface-number*]
ポートで802.1Xゲスト VLAN からユーザを取り除く	**reset dot1x guest-vlan interface** *interface-type interface-number* [**mac-address** *mac-address*]

3.24 802.1X認証の設定例

3.24.1 基本的な 802.1X 認証の設定例

I. ネットワーク要件

図 3-1に示すように、アクセス装置は、GigabitEthernet 1/0/1 に接続するユーザ用に 802.1X 認証を実行します。ポート上で MAC ベースのアクセス制御を行ってください。1 ユーザのログオフは、他のオンラインの 802.1X ユーザには影響しません。

802.1X ユーザの認証、許可、アカウンティングを実行するために RADIUS サーバを使用してください。 RADIUS 認証が失敗した場合、アクセス装置上でローカル認証を実行します。

プライマリ認証およびアカウンティングサーバとして 10.1.1.1/24 のホスト、セカンダリ認証とアカウンティングサーバとして 10.1.1.2/24 のホストを設定します。すべてユーザを収容できる ISP ドメイン bbb にすべてのユーザを割り当てます。

アクセス装置と認証サーバ間のパケットに name という名称で共有鍵を、アクセス装置とアカウンティングサーバ間のパケットに money という名称で共有鍵を設定します。

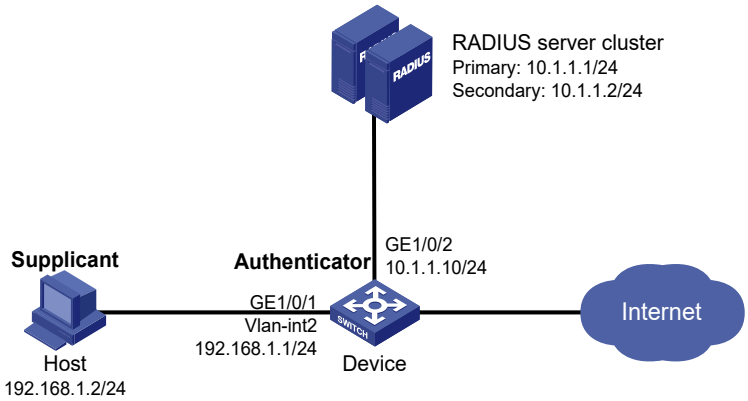


図 3-1 ネットワーク図

II. 設定手順

1)　802.1X クライアントを設定します。（詳細は省略）

2) RADIUS サーバを設定し、802.1X ユーザ用のユーザアカウントを追加します。（詳細は省略します。）

アクセス装置で使用される RADIUS コマンドについての詳細は、コマンドマニュアルのセクション 7 *セキュリティ*”*AAA*”を参照してください。

3) 各インタフェースに IP アドレスを割り当てます。（詳細は省略します。）
4) アクセス装置上で 802.1X ユーザ用のユーザアカウントを設定します。

ユーザ名とパスワードがそれぞれ localuser と localpass のローカルユーザをプレーンテキストで追加します。（ユーザ名とパスワードは RADIUS サーバに設定されたものと同じにしてください。）

```
<Device> system-view
[Device] local-user localuser class network
[Device-luser-network-localuser] password simple localpass
```

サービスタイプに lan-access を選択します。

```
[Device-luser-network-localuser] service-type lan-access
[Device-luser-network-localuser] quit
```

5) RADIUS スキームを設定します。

RADIUS スキーム radius1 を作成し、RADIUS scheme view に移行します。

```
[Device] radius scheme radius1
```

プライマリ認証/アカウンティング RADIUS サーバの IP アドレスを指定します。

```
[Device-radius-radius1] primary authentication 10.1.1.1
[Device-radius-radius1] primary accounting 10.1.1.1
```

セカンダリ認証/アカウンティング RADIUS サーバの IP アドレスを指定します。

```
[Device-radius-radius1] secondary authentication 10.1.1.2
[Device-radius-radius1] secondary accounting 10.1.1.2
```

アクセス装置と認証サーバ間の共有鍵を指定します。

```
[Device-radius-radius1] key authentication simple name
```

アクセス装置とアカウンティングサーバ間の共有鍵を指定します。

```
[Device-radius-radius1] key accounting simple money
```

RADIUS サーバに送信されるユーザ名から ISP のドメイン名を除外します。

```
[Device-radius-radius1] user-name-format without-domain
[Device-radius-radius1] quit
```

メモ：

アクセス装置は、RADIUS サーバと同じユーザ名のフォーマットを使用する必要があります。 RADIUS サーバがユーザ名に ISP のドメイン名を含む場合、アクセス装置です。

6)　ISP ドメインを設定します。

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

```
[Device] domain bbb
```

RADIUS スキーム radius1 を ISP ドメインに適用し、セカンダリ認証方式としてローカル認証を指定します。

```
[Device-isp-bbb] authentication lan-access radius-scheme radius1 local
[Device-isp-bbb] authorization lan-access radius-scheme radius1 local
[Device-isp-bbb] accounting lan-access radius-scheme radius1 local
[Device-isp-bbb] quit
```

7)　802.1X を設定します。

GigabitEthernet 1/0/1 で 802.1X を有効にします。

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] dot1x
```

ポート上で MAC ベースのアクセス制御を有効にします。デフォルトでポートは MAC ベースアクセス制御を使用します。

```
[Device-GigabitEthernet1/0/1] dot1x port-method macbased
```

bbb を強制認証ドメインとして設定します。

```
[Device-GigabitEthernet1/0/1] dot1x mandatory-domain bbb
[Device-GigabitEthernet1/0/1] quit
```

802.1X をグローバルで有効にします。

```
[Device] dot1x
```

III. 設定の確認

GigabitEthernet 1/0/1 の 802.1X 認証の設定を確認します。

```
[Device] display dot1x interface gigabitethernet 1/0/1
```

802.1X ユーザが RADIUS 認証を通過した後、ユーザ接続情報を表示します。

```
[Device] display dot1x connection
```

3.24.2 802.1X ゲスト VLAN と許可 VLAN の設定例

I. ネットワーク要件

図 3-2に示すように、GigabitEthernet 1/0/2 に接続される 802.1X ユーザの認証、許可、アカウンティングを実行するため、RADIUS サーバを使用します。ポートでポートベースのアクセス制御を実装します。

GigabitEthernet 1/0/2 で一定の期間内に 802.1X 認証を実行するユーザがいない場合、装置はゲスト VLAN である VLAN10 に GigabitEthernet 1/0/2 を追加します。ホストとアップデートサーバは両方とも VLAN10 にあります。ホストはアップデートサーバにアクセスでき、802.1X クライアントソフトウェアをダウンロードできます。

ホストが 802.1X 認証にパスしたのち、アクセス装置は GigabitEthernet 1/0/3 が所属する VLAN5 にホストを割り当てます。ホストはインタネットにアクセスできます。

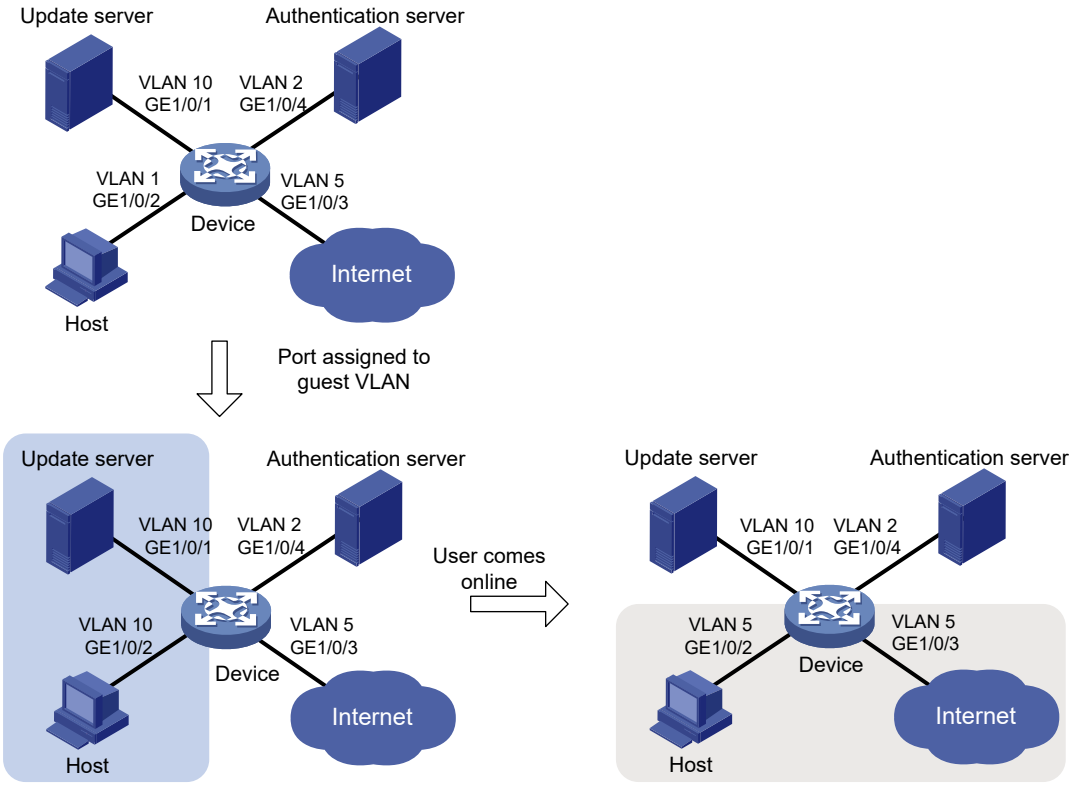


図 3-2 ネットワーク図

II. 設定手順

1) 802.1X クライアントの設定を行います。802.1X クライアントは、アクセスポートがゲスト VLAN あるいは許可 VLAN に割り当てられたのち、IP アドレスをアップデートできます。（詳細は省略します）

2) 認証、許可、アカウンティングサービスを許可する RADIUS サーバを設定します。ユーザのユーザアカウント、許可 VLAN（この例では VLAN 5）を設定します。（詳細は省略します。）

3) VLAN を作成し、アクセス装置の VLAN にポートを割り当てます。

```
<Device> system-view
[Device] vlan 1
[Device-vlan1] port gigabitethernet 1/0/2
[Device-vlan1] quit
[Device] vlan 10
[Device-vlan10] port gigabitethernet 1/0/1
[Device-vlan10] quit
[Device] vlan 2
[Device-vlan2] port gigabitethernet 1/0/4
[Device-vlan2] quit
[Device] vlan 5
[Device-vlan5] port gigabitethernet 1/0/3
[Device-vlan5] quit
```

4) アクセス装置で RADIUS スキームを設定します。

RADIUS スキーム 2000 を作成し、RADIUS scheme view に移行します。

```
[Device] radius scheme 2000
```

プライマリ認証サーバとして 10.11.1.1 を指定し、認証ポートとして 1812 を指定します。

```
[Device-radius-2000] primary authentication 10.11.1.1 1812
```

プライマリアカウンティングサーバとして 10.11.1.1 を指定し、アカウンティングポートとして 1813 を指定します。

```
[Device-radius-2000] primary accounting 10.11.1.1 1813
```

認証サーバとデバイス装置間でセキュアな通信を行うため、プレーンテキストで abc の共有鍵を設定します。

```
[Device-radius-2000] key authentication simple abc
```

アカウンティングサーバと装置間でセキュアな通信を行うため、プレーンテキストで abc の共有鍵を設定します。

```
[Device-radius-2000] key accounting simple abc
```

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

```
[Device-radius-2000] user-name-format without-domain
[Device-radius-2000] quit
```

5) ISP ドメインを設定します。

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

```
[Device] domain bbb
```

認証、許可、アカウンティング用の RADIUS スキーム 2000 を ISP ドメインに適用します。

```
[Device-isp-bbb] authentication lan-access radius-scheme 2000
[Device-isp-bbb] authorization lan-access radius-scheme 2000
[Device-isp-bbb] accounting lan-access radius-scheme 2000
[Device-isp-bbb] quit
```

6)　アクセス装置で 802.1X を設定します。

GigabitEthernet 1/0/2 で 802.1X を有効にします。

```
[Device] interface gigabitethernet 1/0/2
[Device-GigabitEthernet1/0/2] dot1x
```

ポートでポートベースのアクセス制御を行います。

```
[Device-GigabitEthernet1/0/2] dot1x port-method portbased
```

ポートの許可モードを auto に設定します。デフォルトでポートは auto モードを使用します。

```
[Device-GigabitEthernet1/0/2] dot1x port-control auto
```

GigabitEthernet 1/0/2 で 802.1X ゲスト VLAN として VLAN10 を設定します。

```
[Device-GigabitEthernet1/0/2] dot1x guest-vlan 10
[Device-GigabitEthernet1/0/2] quit
```

グローバルに 802.1X を有効にします。

```
[Device] dot1x
```

III. 設定の確認

GigabitEthernet 1/0/2 の 802.1X ゲスト VLAN の設定を確認します。

```
[Device] display dot1x interface gigabitethernet 1/0/2
```

ポートでユーザが認証にパスしない場合、GigabitEthernet 1/0/2 が VLAN10 に割り当てられていることを確認します。

```
[Device] display vlan 10
```

ユーザが認証にパスしたのち、GigabitEthernet 1/0/2 の情報を表示します。GigabitEthernet 1/0/2 が VLAN5 に割り当てられていることを確認します。

```
[Device] display interface gigabitethernet 1/0/2
```

3.24.3 ACL の割り当てによる 802.1X の設定例

I. ネットワーク要件

図 3-3に示すように、GigabitEthernet 1/0/1 に接続するホストはインタネットにアクセスするため、802.1X 認証にパスする必要があります。

GigabitEthernet 1/0/1 で 802.1X 認証を実行します。認証サーバと許可サーバとして 10.1.1.1 の RADIUS サーバを使用します。アカウンティングサーバとして 10.1.1.2 の RADIUS サーバを使用します。

平日の 8:00～18:00 までの営業時間中、FTP サーバに 802.1X ユーザのアクセスを拒否するため、GigabitEthernet 1/0/1 で ACL の割り当てを設定します。

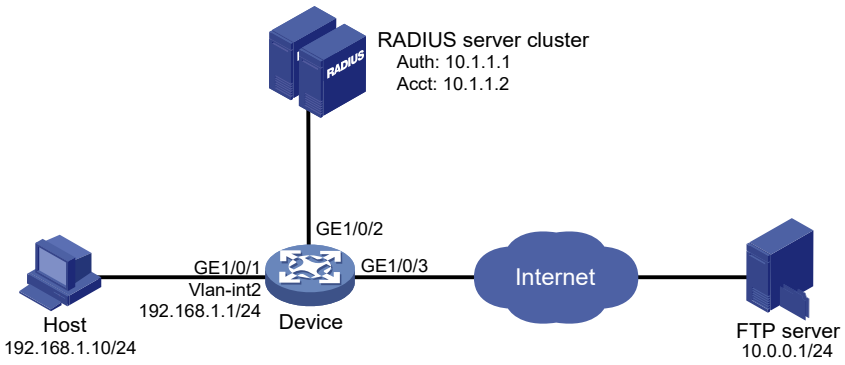


図 3-3 ネットワーク図

II. 設定手順

1) 802.1X クライアントを設定します。アクセスポートが 802.1X ゲスト VLAN あるいは許可 VLAN に割り当てられたのち、クライアントが IP アドレスをアップデートできることを確認してください。（詳細は省略します。）
2) 認証、許可、アカウンティングサービスを提供するため、RADIUS サーバを設定します。ユーザアカウントを追加し、ユーザに ACL（この例では ACL3000）を指定します。（詳細は省略します。）
3) 図 3-3に示すように、各インタフェースに IP アドレスを割り当てます。（詳細は省略します。）
4) RADIUS スキームを設定します。

RADIUS スキーム 2000 を作成し、RADIUS scheme view に移行します。

```
<Device> system-view
[Device] radius scheme 2000
```

プライマリ認証サーバとして 10.1.1.1 のサーバを指定し、認証ポートとして 1812 を指定します。

```
[Device-radius-2000] primary authentication 10.1.1.1 1812
```

プライマリアカウンティングサーバとして 10.1.1.2 のサーバを指定し、認証ポートとして 1813 を指定します。

```
[Device-radius-2000] primary accounting 10.1.1.2 1813
```

認証サーバと装置間でセキュアな通信を行うため、プレーンテキストで abc の共有鍵を設定します。

```
[Device-radius-2000] key authentication simple abc
```

アカウンティングサーバと装置間でセキュアな通信を行うため、プレーンテキストで abc の共有鍵を設定します。

```
[Device-radius-2000] key accounting simple abc
```

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

```
[Device-radius-2000] user-name-format without-domain
[Device-radius-2000] quit
```

5) ISP ドメインを設定します。

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

```
[Device] domain bbb
```

認証、許可、アカウンティング用の RADIUS スキーム 2000 を ISP ドメインに適用します。

```
[Device-isp-bbb] authentication lan-access radius-scheme 2000
[Device-isp-bbb] authorization lan-access radius-scheme 2000
[Device-isp-bbb] accounting lan-access radius-scheme 2000
[Device-isp-bbb] quit
```

6) 平日の 8:00～18:00 に時間範囲 ftp を設定します。

```
[Device] time-range ftp 8:00 to 18:00 working-day
```

7) 指定された時間範囲で、10.0.0.1 の FTP サーバ宛のパケットを拒否する ACL を設定します。

```
[Device] acl advanced 3000
[Device-acl-ipv4-adv-3000] rule 0 deny ip destination 10.0.0.1 0 time-range ftp
[Device-acl-ipv4-adv-3000] quit
```

8) 802.1X を設定します。

GigabitEthernet 1/0/1 で 802.1X を有効にします。

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] dot1x
[Device-GigabitEthernet1/0/1] quit
```

802.1X をグローバルで有効にします。

```
[Device] dot1x
```

III. 設定の確認

認証にパスするユーザアカウントを使用します。（詳細は省略します。）

平日の 8:00 から 18:00 の期間内に、ユーザが FTP サーバに ping できないことを確認します。

```
C:\>ping 10.0.0.1

Pinging 10.0.0.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.0.0.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

出力では、ACL 3000 がユーザに適用され、ユーザが FTP サーバにアクセスできないことを示します。

目次

このセクションのページは**7-x-x**です。

4章 MACアドレス認証 4-1
4.1 概要 4-1
4.1.1 ユーザアカウントポリシー 4-1
4.1.2 認証方式 4-2
4.1.3 VLANの割り当て 4-2
4.1.4 ACLの割り当て 4-4
4.2 設定要件 4-4
4.3 設定ガイドライン 4-5
4.4 設定作業リスト 4-5
4.5 MACアドレス認証の有効化 4-5
4.6 MACアドレス認証ドメインの指定 4-6
4.7 ユーザアカウントフォーマットの設定 4-6
4.8 MACアドレス認証タイマの設定 4-7
4.9 ポート上のMACアドレス認証ユーザの同時接続最大数の設定 4-8
4.10 MACアドレス認証の開始を遅らせる遅延時間の設定 4-8
4.11 MACアドレス認証と802.1X認証の並列処理の設定 4-9
4.11.1 設定ガイドライン 4-9
4.11.2 設定手順 4-9
4.12 MACアドレス認証ゲストVLANの設定 4-10
4.13 MACアドレス認証のオフライン状態検出の設定 4-11
4.14 MACアドレス移動機能の有効化 4-11
4.15 MACアドレス認証の表示と維持 4-11
4.16 MACアドレス認証の設定例 4-12
4.16.1 ローカルMACアドレス認証の設定例 4-12
4.16.2 RADIUSベースのMACアドレス認証の設定例 4-14
4.16.3 ACLの割り当ての設定例 4-17

4章 MAC アドレス認証

4.1 概要

MAC アドレス認証はポート上で送信元 MAC アドレスを認証することによって、ネットワークアクセスを制御します。クライアントソフトウェアを必要とせず、ネットワークアクセス用のユーザ名とパスワードの入力も必要ありません。

MAC アドレス認証が有効になっているポート上で未知の送信元 MAC アドレスが検出された場合、装置は MAC アドレス認証プロセスを開始します。

- 認証が成功した場合、ユーザは許可されたネットワークリソースにアクセスすることができます。
- 認証が失敗した場合、装置はユーザの MAC アドレスをサイレント MAC アドレスとして登録し、パケットをドロップし、Quiet タイマを開始します。Quiet タイマは、サイレント MAC に登録された MAC アドレスからのすべての後続パケットを破棄することで、短時間に何度も認証が行われることを回避します。

🕮 **メモ：**

- 認証に失敗した MAC アドレスがスタティック MAC アドレスまたは任意のセキュリティ認証をパスした MAC アドレスである場合、装置はその MAC アドレスをサイレントアドレスとして記憶しません。
- QX-S1100G シリーズの MAC アドレス認証は、CHAP での認証には対応していません。

4.1.1 ユーザアカウントポリシー

MAC アドレス認証は、以下のユーザアカウントポリシーをサポートしています。

- **グローバルユーザアカウントポリシー**—以下のオプションのいずれかになります。
  - **MAC ベースユーザアカウントポリシー**—各ユーザに 1 つの MAC ベースユーザアカウントです。アクセス装置はパケットの送信元 MAC アドレスを MAC 認証のユーザのユーザ名とパスワードとして使用します。このポリシーは、安全でない環境に適しています

🕮 **メモ：**

MAC ベースユーザアカウントポリシーは、すべての MAC ベースユーザアカウントで共有されるパスワードの設定もサポートしています。

  - **共有ユーザアカウントポリシー**—すべてのユーザに対して 1 つの共有ユーザアカウントです。アクセス装置上のすべての MAC 認証ユーザに対して、必ずしも MAC アドレスではない 1 つのユーザ名とパスワードを指定します。このポリシーは、安全な環境に適しています

- **MAC範囲固有のユーザアカウントポリシー**—特定のMACアドレス範囲ユーザ用の1つの共有ユーザアカウントです。アクセス装置の特定の MAC アドレス範囲ユーザに対して 1 つのユーザ名とパスワード（必ずしも MAC アドレスではない）を指定します。たとえば、特定の OUI を持つユーザのユーザ名とパスワードを指定できます。

重要：

- グローバルと MAC 範囲固有のユーザアカウントポリシーを一緒に使用できます。MAC アドレス範囲内のユーザの場合、MAC 範囲固有のユーザアカウント設定は、グローバルユーザアカウント設定よりも優先されます。
- RADIUS サーバを MAC 認証に使用する場合は、アクセス装置のユーザアカウントポリシーに基づいて、RADIUS サーバにユーザアカウントを作成する必要があります。

4.1.2 認証方式

アクセス装置上（ローカル認証）または、RADIUS （Remote Authentication Dial-In User Service） サーバを介して、MAC アドレス認証を行うことができます。

ローカル認証：

- **MAC ベースアカウント**－アクセス装置は、デフォルトで一致するローカルアカウントデータベースを検索するためのユーザ名とパスワードとして、パケットの送信元 MAC アドレスを使用します。MAC ベースのアカウントにパスワードが設定されている場合、装置は設定されたパスワードを使用して、ローカルアカウントデータベースで一致を検索します。
- **共有アカウント**－アクセス装置は、一致するローカルアカウントデータベースを検索するために、共有アカウントのユーザ名とパスワードを使用します。

RADIUS 認証：

- **MAC ベースアカウント**－アクセス装置は、デフォルトで認証用の RADIUS サーバにユーザ名とパスワードとして送信元 MAC アドレスを送信します。MAC ベースのアカウントにパスワードが設定されている場合、アクセス装置は設定されたパスワードをパスワードとして RADIUS サーバに送信します。
- **共有アカウント**－アクセス装置は、認証用の RADIUS サーバに共有アカウントのユーザ名とパスワードを送信します。

ローカル認証と RADIUS 認証の詳細は、オペレーションマニュアルのセクション 7 *セキュリティ*”*AAA*”を参照してください。

4.1.3 VLAN の割り当て

MAC アドレス認証は許可 VLAN、ゲスト VLAN をサポートします。

I. 許可 VLAN

MAC アドレス認証ユーザの許可されたネットワークリソースへのアクセスを制御するため、許可 VLAN を使用します。

- **Remote VLAN authorization**—MAC 認証ユーザの許可 VLAN 情報は、リモートサーバにより割り当てられます。装置は VLAN ID または VLAN 名でサーバ割り当て VLAN を解決できます。

  ユーザが装置にアクセスするポートは、タグ付きまたはタグなしメンバとして許可 VLAN に割り当てられます。

- **Local VLAN authorization**— MAC 認証ユーザの許可 VLAN は、装置の VLAN ID でユーザ view またはユーザグループ view で指定されます。

  ユーザが装置にアクセスするポートは、タグ付きメンバとして VLAN に割り当てられます。

  詳細はオペレーションマニュアルのセクション 7 *セキュリティ*”*AAA*”を参照してください。

表 4-1にネットワークアクセス装置が MAC アドレス認証ユーザの許可 VLAN を処理する方法を示します。

表 4-1 VLAN 操作

ポートタイプ	VLAN 操作
• アクセスポート • トランクポート • MACベースVLANが無効となったハイブリッドポート	• ポートがタグなしメンバとして許可VLANへ割り当てられた場合、装置は最初に認証されたユーザの許可VLANにポートを割り当てます。許可VLANはPVIDになります。ポートの全MAC認証ユーザは同じ許可VLANに割り当てられます。その後のユーザに異なる許可VLANが割り当てられる場合、ユーザはMAC認証に成功しません。 • ポートがタグ付きメンバとして許可VLANへ割り当てられた場合、ポートのPVIDは変わりません。装置はそれぞれのユーザのMACアドレスと許可VLANとをマッピングします。 🕮 **メモ：** タグ付きメンバは、トランクポートとハイブリッドポートでのみサポートされています。
MACベースVLANが有効となったハイブリッドポート	装置は許可VLANに各ユーザのMACアドレスをマッピングします。ポートのPVIDは変更しません。ユーザがログオフすると、ユーザのMAC-to-VLANのマッピングは削除されます。

🕮 **メモ：**

タグなしメンバとしてハイブリッドポートを VLAN に割り当ててください。割り当てた後は、タグ付きメンバとしてポートを再設定しないでください。

II. ゲスト VLAN

ポートで MAC アドレス認証に失敗したユーザを適応させるため、ポートで MAC アドレス認証ゲスト VLAN を設定することができます。MAC アドレス認証ゲスト VLAN のユーザは、ソフトウェアやシステムパッチなどをダウンロードするため、ソフトウェアサーバのような制限されたネットワークリソースにアクセスすることができます。MAC アドレス認証ゲスト VLAN が設定されていない場合、MAC アドレス認証に失敗したユーザはネットワークリソースにアクセスすることができません。

ハイブリッドポートは、常に、タグなしメンバとして MAC アドレス認証ゲスト VLAN に割り当てられます。割り当て後、VLAN のタグづけメンバとしてポートを再設定しないでください。

表 4-2にネットワークアクセス装置が MAC アドレス認証ユーザのゲスト VLAN を処理する方法を示します。

表 4-2 VLAN 操作

ポートタイプ	VLAN 操作
MACアドレス認証に失敗したMACアドレス認証ゲストVLANのユーザ	ユーザはMACアドレス認証ゲストVLANに属します。
MACアドレス認証にパスしたMACアドレス認証ゲストVLANのユーザ	装置はユーザのMACアドレスを認証ユーザによって割り当てられた許可VLANに再マッピングします。 ユーザ用の許可VLANが認証サーバで設定されていない場合、ユーザのMACアドレスをポートのPVIDに再マッピングします。

4.1.4 ACL の割り当て

ネットワークリソースへのアクセスを制御するため、MAC アドレス認証ユーザに ACL を指定することができます。ユーザが MAC アドレス認証にパスしたのち、認証サーバ（ローカルあるいはリモート）はユーザのアクセスポートに許可された ACL を割り当てます。ACL はユーザのトラフィックをフィルタします。ACL の割り当て機能のために、アクセス装置で許可 ACL の ACL を設定する必要があります。

装置は、static ACL の許可 ACL としての割り当てをサポートしています。

- **Static ACLs**—RADIUS サーバあるいはアクセス装置によって割り当てることができます。サーバあるいはアクセス装置が static ACL をユーザに割り当てる場合、ACL 番号のみが割り当てられます。ACL を手動で作成し、アクセス装置でそのルールを設定する必要があります。
  ユーザのアクセス許可を変更するために、以下の方法の 1 つを使用することができます。
  - □ アクセス装置の ACL ルールを修正します。
  - □ 認証サーバで別の許可 ACL を指定します。

  static ACL とそのルールは、アクセス装置から手動で削除できます。

ACL の詳細は、オペレーションマニュアルのセクション 6 *ACL and QoS* ”*ACL*”を参照してください。

4.2 設定要件

MAC アドレス認証を設定する前に、以下の作業を完了してください。

1) 認証ドメイン（ISP ドメイン）を設定し、AAA 方式を指定してください。詳細はオペレーションマニュアルのセクション 7 *セキュリティ* ”*AAA*”を参照してください。
   - □ ローカル認証の場合、ローカルユーザアカウント（ユーザ名とパスワードを含みます。）を作成し、**lan-access** サービスを指定してください。

- □ RADIUS 認証の場合、装置と RADIUS サーバ間のルートで通信ができることを確認し、RADIUS サーバにユーザアカウントを作成してください。MAC ベースアカウントを使用する場合、それぞれのアカウントのユーザ名とパスワードは MAC アドレス認証ユーザの MAC アドレスと同じにしてください。

2) ポートセキュリティが無効であることを確認してください。ポートセキュリティの詳細は、オペレーションマニュアルのセクション 7 *セキュリティ”ポートセキュリティ”*を参照してください。

4.3 設定ガイドライン

MAC 認証を設定する際には、以下の制限とガイドラインに従ってください。

- MAC 認証設定は、レイヤ 2 イーサネットインタフェースでのみサポートします。
- MAC 認証を有効にする前に、インタフェースがレイヤ 2 アグリゲーショングループに加わっていないことを確認してください。

4.4 設定作業リスト

作業リスト
（必須設定項目） MACアドレス認証の有効化
（オプション設定項目）MACアドレス認証ドメインの指定
（オプション設定項目）ユーザアカウントフォーマットの設定
（オプション設定項目）MACアドレス認証タイマの設定
（オプション設定項目）ポート上のMACアドレス認証ユーザの同時接続最大数の設定
（オプション設定項目）MACアドレス認証の開始を遅らせる遅延時間の設定
（オプション設定項目）MACアドレス認証と802.1X認証の並列処理の設定
（オプション設定項目）MACアドレス認証ゲストVLANの設定
（オプション設定項目）MACアドレス認証のオフライン状態検出の設定
（オプション設定項目）MACアドレス移動機能の有効化

4.5 MACアドレス認証の有効化

次のいずれかの操作を実行したときに装置が ACL リソースを使い果たした場合、MAC 認証はポートで有効になりません。

- MAC 認証がグローバルに有効になっているときに、ポートで MAC 認証を有効にします。
- ポートで MAC 認証が有効になっているときに、システムで MAC 認証をグローバルに有効にします。

以下に MAC アドレス認証の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． グローバルで MAC アドレス認証を有効にする	**mac-authentication**	デフォルト：無効

操作	コマンド	補足
3． Ethernet interface view に移行する	**interface** *interface-type interface-number*	―
4． ポートで MAC アドレス認証を有効にする	**mac-authentication**	デフォルト：無効

4.6 MACアドレス認証ドメインの指定

デフォルトでは、MAC アドレス認証ユーザはシステムデフォルト認証ドメイン内にあります。ユーザごとに異なるアクセスポリシーを適用するには、次の方法で MAC アドレス認証ユーザ用の認証ドメインを指定することができます。

- system view でグローバルの認証ドメインを指定します。このドメインの設定は、すべてのポートに適用されます。
- interface view で個別のポートの認証ドメインを指定します。

MAC アドレス認証は、インタフェース固有のドメイン、グローバルドメイン、デフォルトドメインの順序でポート上のユーザの認証ドメインを選択します。認証ドメインの詳細は、オペレーションマニュアルのセクション 7 *セキュリティ”AAA”*を参照してください。

以下に MAC アドレス認証ユーザの認証ドメインの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． MAC アドレス認証ユーザの認証ドメインを指定する	● system viewで設定する：**mac-authentication domain** *domain-name* ● Ethernet interface viewで設定する： 1． **interface** *interface-type interface-number* 2． **mac-authentication domain** *domain-name*	デフォルト：システムのデフォルト認証ドメインが使われます。

4.7 ユーザアカウントフォーマットの設定

MAC アドレス範囲内のユーザの場合、MAC アドレス範囲固有のユーザアカウントは、グローバルユーザアカウント設定よりも優先されます。

最大 16 の MAC アドレス範囲を設定でき、MAC アドレス範囲が重複しないようにする必要があります。

同じ MAC アドレス範囲に対してユーザアカウントを複数回設定すると、最新の設定に上書きされます。

MAC 範囲固有のアカウントは、ユニキャスト MAC アドレスにのみ適用されます。

- マルチキャスト MAC アドレスのみを含む MAC アドレス範囲を指定すると、このコマンドの実行は失敗します。
- ユニキャスト MAC アドレスとマルチキャスト MAC アドレスの両方を含む MAC アドレス範囲を指定した場合、コマンドはユニキャスト MAC アドレスでのみ有効になります。

すべてゼロの MAC アドレスは MAC 認証には無効です。すべてゼロの MAC アドレスを持つユーザは、MAC 認証にパスできません。

以下にユーザアカウントフォーマットの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． グローバル MAC アドレス認証ユーザアカウントポリシーを設定する	• 各ユーザにMACベースユーザアカウントを使用する： **mac-authentication user-name-format mac-address** [{ **with-hyphen** | **without-hyphen** } [**lowercase** | **uppercase**]] [**password** { **cipher** | **simple** } *string*] • すべてのユーザに共有ユーザアカウントを使用する： **mac-authentication user-name-format fixed** [**account** *name*] [**password** { **cipher** | **simple** } *string*]	デフォルト：MACアドレス認証のユーザ名とパスワードとしてユーザのMACアドレスを使用します。 MACアドレスは16進数でハイフンなし、小文字のみです。

4.8 MACアドレス認証タイマの設定

MAC アドレス認証では以下のタイマを使用します。

- **Offline detect timer**－ユーザがアイドル状態であることを検出するために、装置がユーザからのトラフィックを待つ期間を設定します。装置はタイマが終了するとユーザをログオフし、ユーザのアカウントの停止を要求します。このタイマは、MAC 認証オフライン検出機能が有効な場合にのみ効果があります。
- **Quiet timer**－MAC アドレス認証に失敗したユーザが MAC アドレス認証を実行できるようになるまで、装置が待つ時間をタイマに設定します。 Quiet タイムの間は、MAC アドレスからのパケットはすべて廃棄されます。この Quiet メカニズムは、認証が繰り返されシステムのパフォーマンスに影響を与えることを防ぎます。
- **Server timeout timer**－RADIUS サーバが使用不能であることを検出するために、アクセス装置が RADIUS サーバからの応答を待つ時間をタイマに設定します。MAC アドレス認証中にタイムアウトした場合、ユーザは MAC 認証に失敗します。

以下に MAC アドレス認証タイマの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． MAC アドレス認証タイマを設定する	**mac-authentication timer** { **offline-detect** *offline-detect-value* | **quiet** *quiet-value* | **server-timeout** *server-timeout-value* }	デフォルト： offline detect timer：300秒 quiet timer：60秒 server timeout timer：100秒

4.9 ポート上のMACアドレス認証ユーザの同時接続最大数の設定

同時に接続する認証ユーザを制限することで、システムリソース不足になることを防ぎます。

以下にポート上の MAC アドレス認証ユーザの同時接続最大数の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． Ethernet interface view に移行する	**interface** *interface-type interface-number*	―
3． ポート上の MAC アドレス認証ユーザの同時接続最大数を設定する	**mac-authentication max-user** *user-number*	デフォルト：4294967295

🕮 **メモ：**

Version 7.1.5 を含むそれ以降は、2048 まで認証動作が可能です。
Vesion 7.1.3 では、2000 まで認証動作が可能です。

4.10 MACアドレス認証の開始を遅らせる遅延時間の設定

ポートで 802.1X 認証と MAC アドレス認証の両方の設定が有効である場合、802.1X 認証を優先させるため、MAC アドレス認証を開始する時間を遅らせます。

遅延時間内に、802.1X 認証が動作しない、あるいは 802.1X 認証に失敗した場合、MAC アドレス認証を行います。

MAC アドレス認証の開始を遅らせる遅延時間を設定する場合、ポートセキュリティで **mac-else-userlogin-secure** あるいは **mac-else-userlogin-secure-ext** を設定しないでください。2 つのモードのどちらかでは遅延時間の設定は動作しません。ポートセキュリティの詳細は、オペレーションマニュアルのセクション *7 セキュリティ ”ポートセキュリティ”* を参照してください。

以下に MAC アドレス認証の開始を遅らせる遅延時間の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． Ethernet interface view に移行する	**interface** *interface-type interface-number*	―
3． MAC アドレス認証の開始を遅らせる遅延時間を有効にし、タイマを設定する	**mac-authentication timer auth-delay** *auth-delay time*	デフォルト：無効

4.11 MACアドレス認証と802.1X認証の並列処理の設定

本機能は、802.1X 認証が完了したあとに MAC 認証を処理するポートで、MAC アドレス認証と 802.1X 認証を並列に処理できるようにします。

ポートがアンノウン MAC アドレスからのパケットを受信すると、ユニキャスト EAP-Request/Identity パケットを MAC アドレス宛てに送信します。その後、ポートは 802.1X 認証の結果を待つことなく MAC アドレス認証をただちに処理します。

MAC アドレス認証が成功した後、ポートは MAC 認証許可 VLAN に割り当てられます。

- 802.1X 認証が失敗した場合、MAC アドレス認証の結果が効果を生じます。
- 802.1X 認証が成功した場合、装置は 802.1X 認証の結果をもとにポートと MAC アドレスを処理します。

4.11.1 設定ガイドライン

ポートで MAC アドレス認証と 802.1X 認証の並列処理を有効にする場合、以下の制限とガイドラインに従ってください。

- ポートが以下の要件に対応していることを確認してください。
  - □ ポートは 802.1X 認証と MAC アドレス認証の両方が設定されており、また 802.1X 認証のための MAC ベースアクセス制御を実行している。
  - □ ポートは 802.1X ユニキャストトリガ機能を有効にしている。
- 802.1X ゲスト VLAN に割り当てられる前の MAC 認証を実行するポートには、新しい MAC アドレスによる 802.1X ゲスト VLAN へのポートの割り当て遅延を有効にしてください。

  新しい MAC アドレスによる 802.1X ゲスト VLAN へのポートの割り当て遅延の設定の詳細は、オペレーションマニュアルのセクション *7 セキュリティ”802.1X*”を参照してください。
- 並列処理機能を正しく動作させるためには、ポートに MAC アドレス認証遅延を有効にしないでください。この操作は、802.1X 認証が引き起こされた後の MAC アドレス認証を遅延させます。
- 802.1X 認証と MAC アドレス認証の両方をポートに設定するには、以下のいずれかの方法を用います。
  - □ ポートに 802.1X 認証と MAC アドレス認証の機能を別々に有効にします。
  - □ ポートのセキュリティを有効にします。ポートセキュリティモードは **userlogin-secure-or-mac** または **userlogin-secure-or-mac-ext** にしなければなりません。

  ポートセキュリティモードの設定の詳細は、オペレーションマニュアルのセクション *7 セキュリティ”ポートセキュリティ”*を参照してください。

4.11.2 設定手順

以下に MAC アドレス認証と 802.1X 認証の並列処理を有効にする設定を示します。

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

操作	コマンド	補足
2． Ethernet interface view に移行する	**interface** *interface-type interface-number*	—
3． MAC アドレス認証と 802.1X 認証の並列処理の有効に設定する	**mac-authentication parallel-with-dot1x**	デフォルト： RJ-45ポート：有効 SFPポート：無効

4.12 MACアドレス認証ゲストVLANの設定

MAC アドレス認証ゲスト VLAN を使用する場合、ハイブリッドポートを設定する必要があります。ハイブリッドポートで MAC アドレス認証ゲスト VLAN を設定する前に、以下の作業を完了してください。

- グローバルおよびポートで MAC アドレス認証を有効にします。
- ポートで MAC ベース VLAN を有効にします。
- MAC アドレス認証ゲスト VLAN として指定される VLAN を作成します。
- ポートでタグなしメンバとして VLAN を設定します。

表 4-3にポートで MAC アドレス認証ゲスト VLAN を設定する場合のガイドラインを示します。

表 4-3 MAC アドレス認証ゲスト VLAN と他のセキュリティ機能との関係

機能	関係	補足
MACアドレス認証のQuiet機能	MACアドレス認証ゲスト VLAN機能は優先順位が高くなります。 ユーザがMACアドレス認証に失敗した場合、ゲストVLANにアクセスできます。 ユーザのMACアドレスはサイレントMACアドレスとして記憶されません。	オペレーションマニュアルのセクション*7 セキュリティ”MACアドレス認証*”を参照してください。
ポート侵入防止機能	ゲストVLAN機能は、ブロックMAC動作よりも優先順位が高く、ポート侵入防止機能のシャットダウン動作よりも優先順位が低くなります。	オペレーションマニュアルのセクション*7 セキュリティ”ポートセキュリティ*”を参照してください。

以下に MAC アドレス認証ゲスト VLAN の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． Ethernet interface view に移行する	**interface** *interface-type interface-number*	—
3． ポートで MAC アドレス認証ゲスト VLAN を指定する	**mac-authentication guest-vlan** *guest-vlan-id*	デフォルト：設定なし 1つのポートに1つのMACアドレス認証ゲストVLANのみ設定することができます。
4． MAC アドレス認証ゲスト VLAN のユーザを認証する間隔を設定する	**mac-authentication guest-vlan auth-period** *period-value*	デフォルト：30秒

4.13 MACアドレス認証のオフライン状態検出の設定

offline detect timer の期間内にユーザからパケットを受信しない場合、この機能はユーザを装置からログオフします。装置は同時にユーザにアカウンティングの停止を要求します。オフライン検出機能の設定の詳細は、オペレーションマニュアルのセクション 7 *セキュリティ*“*MAC アドレス認証*”の”*MAC アドレス認証タイマの設定*”を参照してください。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． Ethernet interface view に移行する	**interface** *interface-type interface-number*	―
3． MAC アドレス認証オフライン検出機能を有効に設定する	**mac-authentication offline-detect enable**	デフォルト：有効

4.14 MACアドレス移動機能の有効化

MAC アドレス移動機能を有効にすることで、認証が許可されたユーザが装置のポートを移動できるようになります。たとえば、認証ユーザが別のポートに移動する場合、認証セッションが最初のポートから削除され、新しいポートで再認証されます。

MAC アドレス移動機能が無効で認証ユーザが別のポートに移動した場合、再認証されません。

（ローカルまたはリモートの）認証サーバのオンラインユーザ数が上限に達した場合、認証ユーザは装置上のポート間で移動はできません。

ポートのローミングを行うワイヤレスユーザがネットワークにアクセスできるように MAC アドレス移動機能を有効にすることを推奨します。

以下に MAC アドレス移動機能の有効化の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． MAC アドレス移動機能を有効にする	**port-security mac-move permit**	デフォルト：有効

4.15 MACアドレス認証の表示と維持

display コマンドはすべての view で、**reset** コマンドは user view で使用できます。

操作	コマンド
MACアドレス認証情報を表示する	**display mac-authentication** [**interface** *interface-type interface-number*]
MACアドレス認証接続を表示する	**display mac-authentication connection** [**interface** *interface-type interface-number* | **slot** *slot-number* | **user-mac** *mac- address* | **user-name** *user-name*]
MACアドレス認証の統計情報を削除する	**reset mac-authentication statistics** [**interface** *interface-type interface-number*]

操作	コマンド
ポートのMACアドレス認証ゲストVLANからユーザを取り除く	**reset mac-authentication guest-vlan interface** *interface-type interface-number* [**mac-address** *mac-address*]

4.16 MACアドレス認証の設定例

4.16.1 ローカル MAC アドレス認証の設定例

I. ネットワーク要件

図 4-1に示すように、ユーザのインターネットアクセスを制御するためにポート GigabitEthernet 1/0/1 でローカル MAC アドレス認証を設定します。

以下の要件に従うように装置を設定します。

- ユーザが 180 秒ごとにオフラインになっているかどうかを検出します。
- ユーザが認証に失敗した場合、180 秒間、ユーザを拒否します。
- すべてのユーザは ISP ドメイン bbb に属します。
- ローカルユーザは、MAC アドレス認証のユーザ名とパスワードとして、ユーザ自身の MAC アドレスを使用します。MAC アドレスは 16 進数でハイフン付き、小文字を使用します。

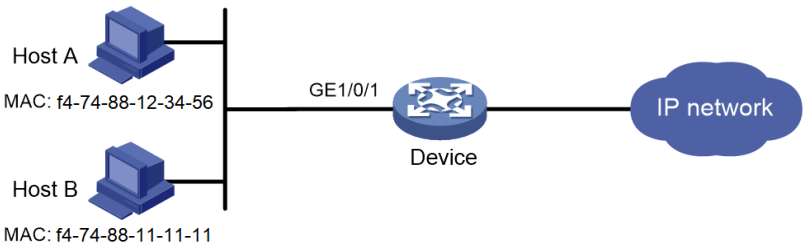


図 4-1 ネットワーク図

II. 設定手順

ローカルユーザを追加します。この例ではホストの MAC アドレス f4-74-88-12-34-56 をユーザ名とパスワードに設定し、LAN アクセスサービスを有効にします。

```
<Device> system-view
[Device] local-user f4-74-88-12-34-56 class network
[Device-luser-network-f4-74-88-12-34-56] password simple f4-74-88-12-34-56
```

ユーザの LAN アクセスサービスを指定します。

```
[Device-luser-network-f4-74-88-12-34-56] service-type lan-access
[Device-luser-network-f4-74-88-12-34-56] quit
```

LAN ユーザのローカル認証を実行するため、ISP ドメイン bbb を設定します。

```
[Device] domain bbb
[Device-isp-bbb] authentication lan-access local
[Device-isp-bbb] quit
```

GigabitEthernet 1/0/1 で MAC アドレス認証を有効にします。

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] mac-authentication
[Device-GigabitEthernet1/0/1] quit
```

ISP ドメイン bbb として MAC アドレス認証ドメインを指定します。

```
[Device] mac-authentication domain bbb
```

MAC アドレス認証タイマを設定します。

```
[Device] mac-authentication timer offline-detect 180
[Device] mac-authentication timer quiet 180
```

MAC ベースのアカウントを使うよう MAC アドレス認証を設定します。MAC アドレスのユーザ名とパスワードはハイフンありで、小文字です。

```
[Device] mac-authentication user-name-format mac-address with-hyphen lowercase
```

MAC アドレス認証をグローバルで有効にします。

```
[Device] mac-authentication
```

III. 設定の確認

MAC アドレス認証の設定と統計情報を表示します。

```
[Device] display mac-authentication
Global MAC authentication parameters:
   MAC authentication                  : Enabled
   Authentication method               : PAP
   User name format                : MAC address in lowercase(xx-xx-xx-xx-xx-xx)
           Username                    : mac
           Password                    : Not configured
   Offline detect period               : 180 s
   Quiet period                        : 180 s
   Server timeout                      : 100 s
   Reauth period                       : 3600 s
   User aging period for critical VLAN : 1000 s
   User aging period for guest VLAN    : 1000 s
   Authentication domain               : bbb
 Online MAC-auth wired users           : 1

 Silent MAC users:
          MAC address       VLAN ID  From port               Port index
          f474-8811-1111    8        GE1/0/1                1

 GigabitEthernet1/0/1 is link-up
   MAC authentication               : Enabled
   Carry User-IP                    : Disabled
   Authentication domain            : Not configured
   Auth-delay timer                 : Disabled
   Periodic reauth                  : Disabled
   Re-auth server-unreachable       : Logoff
   Guest VLAN                       : Not configured
   Guest VLAN reauthentication      : Enabled
     Guest VLAN auth-period         : 30 s
   Critical VLAN                    : Not configured
   Critical voice VLAN              : Disabled
   Host mode                        : Single VLAN
   Offline detection                : Enabled
   Authentication order             : Default
   User aging                       : Enabled
   Server-recovery online-user-sync : Enabled

   Auto-tag feature                 : Disabled
   VLAN tag configuration ignoring  : Disabled
   Max online users                 : 4294967295
   Authentication attempts          : successful 1, failed 0
   Current online users             : 1
          MAC address       Auth state
          f474-8812-3456    Authenticated
```

出力では、Host A が MAC アドレス認証にパスし、オンラインになっています。Host B は MAC アドレス認証に失敗し、サイレント MAC アドレスとして MAC アドレスが記録されます。

4.16.2 RADIUS ベースの MAC アドレス認証の設定例

I. ネットワーク要件

図 4-2に示すように、装置はユーザの認証、許可、アカウンティングを実行するため、RADIUS サーバを使用します。

MAC アドレス認証によってインタネットにアクセスするユーザを制御するため、以下の作業を実行します。

- グローバルと GigabitEthernet 1/0/1 で MAC アドレス認証を有効にします。
- ユーザが 180 秒ごとにオフラインになっているかどうかを検出します。
- ユーザが認証に失敗した場合、装置は 180 秒間ユーザを拒否します。
- すべてのユーザは ISP ドメイン bbb に属します。
- すべてのユーザは、ユーザ名 aaa、パスワード 123456 の共有ユーザアカウントを使用します。

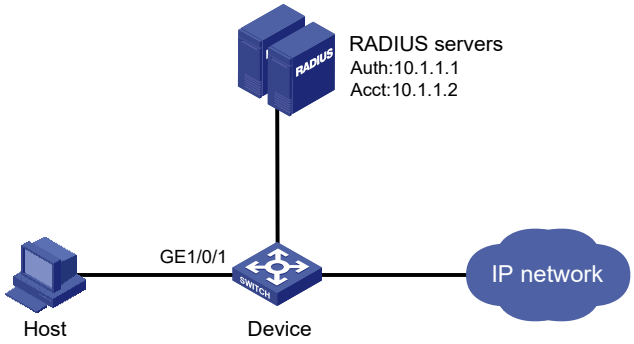


図 4-2 ネットワーク図

II. 設定手順

1)　RADIUS サーバとアクセス装置で互いに通信できることを確認してください。（詳細は省略します。）

2)　RADIUS サーバを設定します。

MAC アドレス認証ユーザの共有アカウントを作成します。（詳細は省略します。）

アカウントにユーザ名 aaa、パスワード 123456 を設定します。（詳細は省略します。）

3)　装置上で RADIUS ベースの MAC アドレス認証を設定します。

RADIUS スキームを設定します。

```
<Device> system-view
[Device] radius scheme 2000
[Device-radius-2000] primary authentication 10.1.1.1 1812
[Device-radius-2000] primary accounting 10.1.1.2 1813
[Device-radius-2000] key authentication simple abc
[Device-radius-2000] key accounting simple abc
[Device-radius-2000] user-name-format without-domain
[Device-radius-2000] quit
```

認証、許可、アカウンティング用の ISP ドメイン bbb の RADIUS スキームを適用します。

```
[Device] domain bbb
[Device-isp-bbb] authentication default radius-scheme 2000
[Device-isp-bbb] authorization default radius-scheme 2000
[Device-isp-bbb] accounting default radius-scheme 2000
```

```
[Device-isp-bbb] quit
```

GigabitEthernet 1/0/1 で MAC アドレス認証を有効にします。

```
[Device] interface gigabitethernet 1/0/1[Device-GigabitEthernet1/0/1] mac-authentication
[Device-GigabitEthernet1/0/1] quit
```

ISP ドメイン bbb として MAC アドレス認証ドメインを指定します。

```
[Device] mac-authentication domain bbb
```

MAC アドレス認証タイマを設定します。

```
[Device] mac-authentication timer offline-detect 180
[Device] mac-authentication timer quiet 180
```

MAC アドレス認証のユーザによって共有されるアカウントのユーザ名 aaa とパスワード 123456 を指定します。

```
[Device] mac-authentication user-name-format fixed account aaa password simple 123456
```

MAC アドレス認証をグローバルで有効にします。

```
[Device] mac-authentication
```

III. 設定の確認

MAC アドレス認証の設定を表示します。

```
[Device] display mac-authentication
Global MAC authentication parameters:
   MAC authentication     : Enabled
   Username format        : Fixed account
            Username      : aaa
            Password      : ******
   Offline detect period  : 180 s
   Quiet period           : 180 s
   Server timeout         : 100 s
   Reauth period          : 3600 s
   Authentication domain  : bbb
 Max MAC-auth users       : 2048 per slot
 Online MAC-auth wired users    : 1

 Silent MAC users:
          MAC address       VLAN ID  From port               Port index

 GigabitEthernet1/0/1  is link-up
   MAC authentication         : Enabled
   Carry User-IP              : Disabled
   Authentication domain      : Not configured
   Auth-delay timer           : Disabled
   Periodic reauth            : Disabled
   Re-auth server-unreachable : Logoff
   Guest VLAN                 : Not configured
   Guest VLAN auth-period     : 30 s
   Critical VLAN              : Not configured
   Critical voice VLAN        : Disabled
   Host mode                  : Single VLAN
   Offline detection          : Enabled
   Authentication order       : Default
```

```
  Guest VSI                    : Not configured
  Guest VSI auth-period        : 30 s
  Critical VSI                 : Not configured
  Max online users             : 4294967295
  Authentication attempts      : successful 1, failed 0
  Current online users         : 1
         MAC address       Auth state
         f474-8812-3456    Authenticated
```

4.16.3 ACL の割り当ての設定例

I. ネットワーク要件

図 4-3に示すように、以下の要件に従うように装置を設定します。

- ユーザの認証、許可、アカウンティングを実行する RADIUS サーバを使用します。
- インターネットアクセスを制御するため、GigabitEthernet 1/0/1 で MAC アドレス認証を実行します。
- 各ユーザの MAC アドレスを、MAC 認証のユーザ名とパスワードの両方として使用します。MAC アドレスは 16 進数でハイフンあり、小文字を使用します。
- FTP サーバ 10.0.0.1 にアクセスする認証ユーザを拒否するように ACL を設定します。

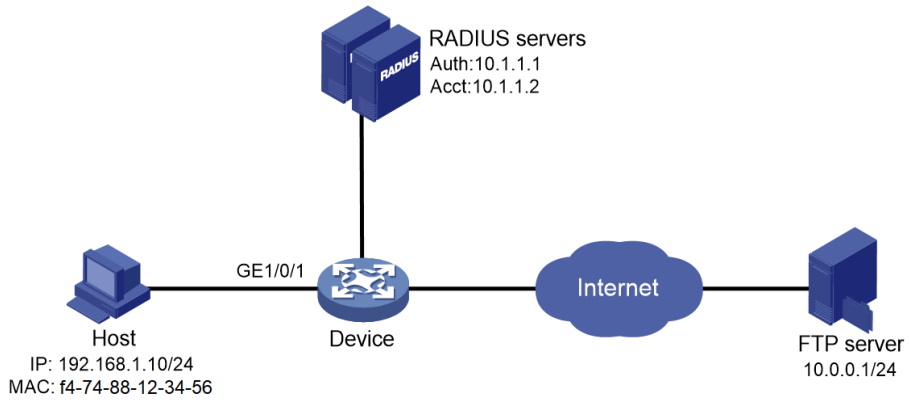


図 4-3 ネットワーク図

II. 設定手順

RADIUS サーバとアクセス装置が互いに通信できることを確認してください。

1)　10.0.0.1 へのパケットを拒否するように ACL 3000 を設定します。

```
<Switch> system-view
[Switch] acl advanced 3000
[Switch-acl-ipv4-adv-3000] rule 0 deny ip destination 10.0.0.1 0
[Switch-acl- ipv4-adv-3000] quit
```

2)　装置で RADIUS ベース MAC アドレス認証を設定します。

RADIUS スキームを設定します。

```
[Switch] radius scheme 2000
[Switch-radius-2000] primary authentication 10.1.1.1 1812
[Switch-radius-2000] primary accounting 10.1.1.2 1813
[Switch-radius-2000] key authentication simple abc
[Switch-radius-2000] key accounting simple abc
[Switch-radius-2000] user-name-format without-domain
[Switch-radius-2000] quit
```

認証、許可、アカウンティングの RADIUS スキームを ISP ドメインに適用します。

```
[Switch] domain bbb
[Switch-isp-bbb] authentication default radius-scheme 2000
[Switch-isp-bbb] authorization default radius-scheme 2000
[Switch-isp-bbb] accounting default radius-scheme 2000
[Switch-isp-bbb] quit
```

MAC アドレス認証の ISP ドメインを指定します。

```
[Switch] mac-authentication domain bbb
```

各ユーザの MAC アドレスを、MAC 認証のユーザ名とパスワードの両方として使用します。MAC アドレスは 16 進数でハイフンあり、小文字を使用します。

```
[Switch] mac-authentication user-name-format mac-address with-hyphen lowercase
```

GigabitEthernet 1/0/1 で MAC アドレス認証を有効にします。

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] mac-authentication
[Switch-GigabitEthernet1/0/1] quit
```

MAC アドレス認証をグローバルで有効にします。

```
[Switch] mac-authentication
```

3)　RADIUS サーバを設定します。

各 RADIUS サーバでユーザ名とパスワードが f4-74-88-12-34-56 のユーザアカウントを追加します。（詳細は省略します。）

ユーザアカウントに ACL 3000 を許可します。（詳細は省略します。）

III. 設定の確認

MAC アドレス認証の設定を確認します。

[Device] display mac-authentication

```
 Global MAC authentication parameters:
   MAC authentication                   : Enable
   Authentication method                : PAP
   Username format                 : MAC address in lowercase(xx-xx-xx-xx-xx-xx)
           Username                     : mac
           Password                     : Not configured
   Offline detect period                : 300 s
   Quiet period                         : 60 s
   Server timeout                       : 100 s
   Reauth period                        : 3600 s
   User aging period for critical VLAN : 1000 s
   User aging period for guest VLAN    : 1000 s
   Authentication domain                : bbb
 Online MAC-auth wired users            : 1

 Silent MAC users:
          MAC address       VLAN ID  From port               Port index

 GigabitEthernet1/0/1  is link-up
   MAC authentication               : Enabled
   Carry User-IP                    : Disabled
   Authentication domain            : Not configured
   Auth-delay timer                 : Disabled
   Periodic reauth                  : Disabled
   Re-auth server-unreachable       : Logoff
   Guest VLAN                       : Not configured
   Guest VLAN reauthentication      : Enabled
     Guest VLAN auth-period         : 30 s
   Critical VLAN                    : Not configured
   Critical voice VLAN              : Disabled
   Host mode                        : Single VLAN
   Offline detection                : Enabled
   Authentication order             : Default
   User aging                       : Enabled
   Server-recovery online-user-sync : Enabled

   Auto-tag feature                 : Disabled
   VLAN tag configuration ignoring  : Disabled
   Max online users                 : 4294967295
   Authentication attempts          : successful 1, failed 0
   Current online users             : 1
          MAC address       Auth state
          f474-8812-3456    Authenticated
```

Host から FTP サーバへの ping ができないことを確認します。

C:\>ping 10.0.0.1

```
Pinging 10.0.0.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.0.0.1:
   Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

出力は、FTP サーバにアクセスを拒否するため、ACL 3000 が GigabitEthernet 1/0/1 に割り当てられていることを示します。

目次

このセクションのページは**7-x-x**です。

5 章 ポートセキュリティ 5-1
5.1 概要.....5-1
5.1.1 ポートセキュリティの機能.....5-1
5.1.2 ポートセキュリティのモード.....5-2
5.2 設定ガイドライン.....5-5
5.3 設定作業リスト.....5-5
5.3.1 ポートセキュリティの有効化.....5-6
5.4 ポートでのセキュア MAC アドレスの最大数の設定.....5-6
5.5 ポートセキュリティモードの設定.....5-7
5.6 ポートセキュリティ機能の設定.....5-8
5.6.1 NTK の設定.....5-8
5.6.2 侵入防止の設定.....5-9
5.7 セキュア MAC アドレスの設定.....5-9
5.7.1 設定要件.....5-10
5.7.2 設定手順.....5-10
5.8 サーバからの許可情報の無視.....5-11
5.9 MAC アドレス移動機能の有効化.....5-11
5.10 ポートセキュリティの拡張ハードウェア モードの有効化.....5-12
5.11 ポートセキュリティに関する SNMP notification.....5-12
5.12 ポートでの認証方式のトリガー順序の設定.....5-13
5.13 ポートセキュリティの表示と維持.....5-14
5.14 ポートセキュリティの設定例.....5-14
5.14.1 autoLearn モードの設定例.....5-14
5.14.2 userLoginWithOUI モードの設定例.....5-17
5.14.3 macAddressElseUserLoginSecure モードの設定例.....5-20
5.15 ポートセキュリティのトラブルシューティング.....5-24
5.15.1 ポートセキュリティのモードが設定できない.....5-24
5.15.2 セキュア MAC アドレスが設定できない.....5-24

5章 ポートセキュリティ

5.1 概要

ポートセキュリティは、MAC アドレスベースのネットワークアクセス制御を提供するため、802.1X 認証と MAC アドレス認証の拡張機能を組み合わせた機能です。ポート上でユーザごとに異なる認証方式を必要とするネットワークに適用されます。

ポートセキュリティは、以下の機能を提供します。

- 受信トラフィックの送信元 MAC アドレスをチェックすることによるネットワークへの非認証端末のアクセスを防止します。
- 送信トラフィックの宛先 MAC アドレスをチェックすることによる非許可の装置あるいは端末へのアクセスを防止します。
- ポートが信頼できる MAC アドレスのみを学習するようにするために、ポート上で MAC アドレス学習と認証を制御することができます。

フレームの送信元 MAC アドレスがポートセキュリティモードで学習できない場合、または、802.1X または MAC アドレス認証に失敗したクライアントからのフレームの場合、それは不正なフレームです。不正なフレームを検知した場合、ポートセキュリティ機能は、自動的にあらかじめ定義した処理を実行します。これにより、メンテナンスの作業負担を減らし、システムセキュリティを大幅に強化することができます。

🕮 **メモ：**

アクセス制御に 802.1X 認証または、MAC アドレス認証のどちらか一方のみが必要な場合、ポートセキュリティではなく 802.1X 認証、または MAC アドレス認証のみ設定することを推奨します。802.1X と MAC アドレス認証についての詳細は、オペレーションマニュアルのセクション *7 セキュリティ”802.1X”、”MAC アドレス認証”* を参照してください。

5.1.1 ポートセキュリティの機能

I. NTK

NTK （Need To Know） 機能は、出力フレームの宛先 MAC アドレスをチェックすることでトラフィックの傍受を防ぎます。この機能は以下のホストにのみフレームを送信することを保証します。

- 認証をパスしたホスト
- MAC アドレスが学習されている、あるいはアクセス装置で設定されたホスト

II. 侵入防止

侵入防止機能は、受信フレームの送信元 MAC アドレスをチェックし、不正フレームを検知すると、あらかじめ定義されたアクションを実行します。処理には、一時的/永久的に

ポートを切断する、または、3 分間（変更不可）その MAC アドレスからのフレームをブロックするといった処理があります。

5.1.2 ポートセキュリティのモード

ポートセキュリティモードには以下のタイプがあります。

- **MAC アドレス学習制御** － autoLearn と secure の 2 つのモードがあります。autoLearn は MAC アドレス学習が許可され、secure モードは無効にされます。
- **認証制御** － このタイプのセキュリティモードは、MAC アドレス認証、802.1X 認証、あるいはそれらを組み合わせて認証を実行します。

フレームを受信すると、セキュリティモードのポートは MAC アドレステーブルから送信元 MAC アドレスを検索します。一致する MAC アドレスがある場合、ポートはフレームを転送します。一致しない場合、セキュリティモードに従い、MAC アドレスの学習あるいは認証動作を行います。不正なフレームを受信すると、ポートはあらかじめ設定しておいた NTK や侵入防止機能の実行を行います。NTK 機能が動作しない限り、出力フレームは、ポートセキュリティの NTK アクションによって制限されません。

ポートがサポートするユーザの最大数は、以下の値よりも少ない値になります。

- ポートセキュリティが許可するセキュア MAC アドレスの最大数
- セキュリティモードがサポートする認証ユーザの同時接続最大数

たとえば 802.1X が許可する同時接続ユーザは、userLoginSecureExt モードのポートで MAC アドレス数のポートセキュリティの制限よりも大きいです。そのポートではポートセキュリティの制限が適用されます。

表 5-1にポートセキュリティモードとセキュリティ機能について記載します。

表 5-1 ポートセキュリティモード

目的	セキュリティモード		起動される機能
ポートセキュリティ機能の削除	noRestrictions （デフォルトモード） ポートセキュリティは無効です。また、ポートへのアクセス制限はありません。		－
MACアドレス学習の制御	autoLearn		NTK/侵入防止機能
	secure		
802.1X認証の実行	userLogin		－
	userLoginSecure		NTK/侵入防止機能
	userLoginSecureExt		
	userLoginWithOUI		
MACアドレス認証の実行	macAddressWithRadius		NTK/侵入防止機能
MACアドレス認証と802.1X認証の組み合わせの実行	Or	macAddressOrUserLoginSecure	NTK/侵入防止機能
		macAddressOrUserLoginSecureExt	
	Else	macAddressElseUserLoginSecure	
		macAddressElseUserLoginSecureExt	

🕮 **ポイント**:

- **userLogin** は 802.1X 認証とポートベースのアクセス制御を指定します。**Secure** の **userLogin** は 802.1X 認証と MAC ベースアクセス制御を指定します。**Ext** は複数の 802.1X 認証ユーザが認証し、同時にオンライン状態になることを許可します。**Ext** がないセキュリティモードの場合、1 つの 802.1X 認証ユーザのみオンライン状態になることを許可します。
- **macAddress** は MAC アドレス認証を指定します。
- **Else** は、**Else** の文字列の前にある認証方法が最初に実行されることを指します。たとえば、macAddressElseUserLoginSecure の **Else** の文字列の前にある認証方法は macAddress で、**Else** の文字列の後ろにある認証方法は UserLoginSecure です。最初の認証に失敗した場合、認証リクエストのプロトコルタイプに依存して、**Else** の後ろにある文字列の認証方法に変更するかどうかを判断します。
- **Or** は、**Or** の文字列の後ろにある認証方法が最初に実行されることを指します。認証が失敗した場合、**Or** の前の認証方式が適用されます。

I. MAC アドレス学習の制御

- autoLearn

  この autoLearn モードのポートは MAC アドレスを学習できます。自動的に学習された MAC アドレスはダイナミックアドレスとして MAC アドレステーブルに追加されませんが、セキュアな MAC アドレスとしてセキュア MAC アドレステーブルに追加されます。**port-security mac-address security** コマンドによってセキュア MAC アドレスを設定することもできます。

  autoLearn モードのポートは、以下の MAC アドレスからの送信元のフレームを許可します。

  - □ セキュア MAC アドレス
  - □ **mac-address dynamic** コマンドと **mac-address static** コマンドで設定された MAC アドレス

  セキュア MAC アドレスの数が上限に達すると、ポートは secure モードに移行します。

- secure

  secure モードでは、ポート上の MAC アドレス学習は無効です。**mac-address static** コマンドと **mac-address dynamic** コマンドを使用して MAC アドレスを設定することができます。MAC アドレステーブルエントリの設定についての詳細は、オペレーションマニュアルのセクション 2 *アクセス”MAC アドレステーブル*”を参照してください。

  secure モードのポートは以下の MAC アドレスからの送信元のフレームのみ許可します。

  - □ セキュア MAC アドレス
  - □ **mac-address dynamic** コマンドと **mac-address static** コマンドで設定された MAC アドレス

II. 802.1X 認証の実行

- userLogin

  この userLogin モードのポートは、802.1X 認証を実行し、ポートベースのアクセス制御を実装しています。ポートは複数の 802.1X ユーザを処理できます。一度 802.1X

ユーザが認証を通過すると、後続の 802.1X ユーザは認証なしでネットワークにアクセスできます。

- userLoginSecure

  この userLoginSecure モードのポートは、802.1X 認証を実行し、MAC ベースのアクセス制御を実装しています。ポートは、802.1X 認証をパスする 1 ユーザのみを処理します。

- userLoginSecureExt

  この userLoginSecureExt モードは、複数のオンライン 802.1X ユーザをサポートしていることを除いて、userLoginSecure モードと同じです。

- userLoginWithOUI

  この userLoginWithOUI モードは、userLoginSecure モードに似ています。違いは、このモードのポートが、特定の OUI（organizationally unique identifier）を含む MAC アドレスの 1 ユーザからのフレームを許可することです。

  このモードでは、ポートは OUI のチェックを最初に実行します。OUI のチェックに失敗した場合、ポートは 802.1X 認証を実行します。ポートは OUI のチェックあるいは 802.1X 認証にパスしたフレームを許可します。

🕮 **メモ：**

IEEE で定義によって定義される OUI は、装置ベンダ、メーカー、組織を識別する MAC アドレスの最初の 24 ビットです。MAC アドレスの最初の 3 オクテットは OUI です。

III. アドレス認証の実行

この macAddressWithRadius モードのポートは、複数のユーザに MAC アドレス認証を実行します。

IV. MAC アドレス認証と 802.1X 認証の組み合わせの実行

- macAddressOrUserLoginSecure

  このモードは、macAddressWithRadius と userLoginSecure モードの組み合わせです。1 つの 802.1X 認証ユーザと複数の MAC アドレス認証ユーザがログインすることを許可します。

  このモードでは、ポートは 802.1X 認証を最初に実行します。802.1X 認証に失敗した場合、MAC アドレス認証が実行されます。

  しかし以下の条件が存在する場合、このモードのポートは異なる認証動作になります。

  - ポートが MAC アドレス認証と 802.1X 認証の並列処理が有効になっている。
  - ポートが 802.1X ユニキャストトリガが有効になっている。
  - ポートがアンノウン MAC アドレスのパケットを受信する。

  このような場合、ポートは 802.1X 認証を開始するために MAC アドレスあてにユニキャスト EAP-Request/Identity パケットを送信します。その後、ポートは 802.1X 認証の結果を待つことなく、ただちに MAC アドレス認証を実行します。

- macAddressOrUserLoginSecureExt

この macAddressOrUserLoginSecureExt モードは、ポートが複数の 802.1X と MAC アドレス認証のユーザをサポートしているのを除いて、macAddressOrUserLoginSecure モードと同じです。

- macAddressElseUserLoginSecure

  このモードは、**Else** キーワードが示すように、MAC アドレス認証が高いプライオリティを持つ macAddressWithRadius と userLoginSecure モードの組み合わせです。1 つの 802.1X 認証ユーザと複数の MAC アドレス認証ユーザがログインすることを許可します。

  このポートは非 802.1X フレームを受信した際、MAC アドレス認証を実行します。802.1X フレームを受信した際、ポートは MAC アドレス認証を実行します。MAC アドレス認証に失敗すると 802.1X 認証を実行します。

- macAddressElseUserLoginSecureExt

  このモードは、**Ext** キーワードが示すように、ポートが複数の 802.1X と MAC アドレス認証のユーザをサポートしているのを除いて、macAddressElseUserLoginSecure モードと同じです。

5.2 設定ガイドライン

ポートセキュリティを設定する際、以下のガイドラインに従ってください。

- 802.1X 認証または MAC アドレス認証のみを必要とするシナリオでは、ポートセキュリティではなく 802.1X認証またはMACアドレス認証を使用してください。802.1X 認証と MAC アドレス認証の設定の詳細については、オペレーションマニュアルのセクション *7 セキュリティ”802.1X”と”MAC アドレス認証”*を参照してください。
- ポートセキュリティを有効にする前に、ポートがアグリゲーショングループに加えられていないことを確認してください。

5.3 設定作業リスト

作業リスト	補足
（必須設定項目） ポートセキュリティの有効化	ー
（オプション設定項目） ポートでのセキュアMACアドレスの最大数の設定	ー
（必須設定項目） ポートセキュリティモードの設定	ー
（必須設定項目） ポートセキュリティ機能の設定 • NTKの設定 • 侵入防止の設定	ネットワーク要件に従い、1つ以上のポートセキュリティ機能を設定してください。
（オプション設定項目） セキュアMACアドレスの設定	ー
（オプション設定項目） サーバからの許可情報の無視	ー
（オプション設定項目） MACアドレス移動機能の有効化	ー

5.3.1 ポートセキュリティの有効化

ポートセキュリティを有効にする前に、グローバルで 802.1X 認証と MAC アドレス認証を無効にしてください。

ポートセキュリティが有効の場合、手動で 802.1X 認証または MAC アドレス認証を有効にしたり、アクセス制御モードやポート許可状態を変更したりすることはできません。ポートセキュリティは自動的に別のセキュリティモードでこれらの設定を変更します。

以下にポートセキュリティの有効化の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． ポートセキュリティを有効にする	**port-security enable**	デフォルト：無効

undo port-security コマンドでポートセキュリティを無効にすることができます。ポートセキュリティを無効にするために、オンラインユーザがいないことを確認してください。

ポートセキュリティの有効あるいは無効にすることで、以下のセキュリティの設定をデフォルトにします。

- 802.1X アクセス制御モードのデフォルトは MAC アドレスベースです。
- 802.1X ポート許可状態のデフォルトは auto です。

802.1X 認証と MAC アドレス認証の設定の詳細については、オペレーションマニュアルのセクション *7 セキュリティ”802.1X”、”MAC アドレス認証”* を参照してください。

5.4 ポートでのセキュアMACアドレスの最大数の設定

ポートで許可するセキュア MAC アドレスの最大数を設定することで、以下のことが可能になります。

- ポートで同時に接続するユーザ数を制御します。

  security モード（autoLearn と secure を除きます。）で動作するポートで、以下の値のいずれか小さい方が上限と等しくなります。

  - ポートセキュリティが許可するセキュア MAC アドレスの制限
  - authentication モードで許可される同時接続数
- autoLearn モードのポートでセキュア MAC アドレス数を制御します。

  ポートセキュリティにおけるポートでのセキュア MAC アドレス最大数は、MAC アドレステーブルに学習できる制限と独立しています。MAC アドレステーブルの設定の詳細については、オペレーションマニュアルのセクション *2 アクセス”MAC アドレステーブル”* を参照してください。

以下にポートでのセキュア MAC アドレスの最大数の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． interface view に移行する	**interface** *interface-type interface-number*	―

操作	コマンド	補足
3． ポートでのセキュア MAC アドレスの最大数を設定する	**port-security max-mac-count** *max-count*	デフォルト：制限なし

5.5 ポートセキュリティモードの設定

ポートでポートセキュリティモードを設定する前に、以下の作業を完了してください。

- 802.1X 認証と MAC アドレス認証を無効にしてください。
- ポートがアグリゲーショングループあるいはサービスループバックグループに属していないことを確認してください。
- autoLearn モードを設定する場合、セキュア MAC アドレスの最大許可数を設定してください。autoLearn モードに入ると設定を変更することができません。

ポートセキュリティモードを設定する場合、以下のガイドラインに従ってください。

- ポートセキュリティが無効の場合、ポートセキュリティモードを指定することができますが、設定は適用されません。
- ポートのセキュリティモードを変更すると、オンラインユーザを切断します。
- ポートセキュリティが設定されている場合、ポートで 802.1X 認証あるいは MAC アドレス認証を有効にできません。
- 以下のポートセキュリティモードで RADIUS サーバにより割り当てられる URL 属性をサポートします。
  - □ mac-and-userlogin-secure-ext
  - □ mac-authentication
  - □ mac-else-userlogin-secure
  - □ mac-else-userlogin-secure-ext
  - □ userlogin-secure
  - □ userlogin-secure-ext
  - □ userlogin-secure-or-mac
  - □ userlogin-secure-or-mac-ext
  - □ userlogin-withoui

  認証の間、ユーザはサーバ割り当ての URL 属性によって指定された Web インタフェースにリダイレクトされます。Web 認証に成功した後、RADIUS サーバは Web ユーザの MAC アドレスを記録し Web ユーザをログオフするために DM（Disconnect Message）を使用します。ユーザが 802.1X または MAC アドレス認証を再び開始する際に、認証が成功し、オンラインになります。

以下にポートセキュリティモードの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． （オプション設定項目）ユーザ認証の OUI 値を設定する	**port-security oui index** *index-value* **mac-address** *oui-value*	デフォルト：設定なし この設定は**userlogin-withoui** モードで必要です。 複数のOUIを設定することができますが、**userlogin-withoui** モードの場合、ポートは指定されたOUIの1つにマッチした1つの802.1Xユーザのみ許可されます。
3． interface view に移行する	**interface** *interface-type interface-number*	―

操作	コマンド	補足
4． ポートセキュリティモードを設定する	**port-security port-mode** { **autolearn** | **mac-and-userlogin-secure-ext** | **mac-authentication** | **mac-else-userlogin-secure** | **mac-else-userlogin-secure-ext** | **secure** | **userlogin** | **userlogin-secure** | **userlogin-secure-ext** | **userlogin-secure-or-mac** | **userlogin-secure-or-mac-ext** | **userlogin-withoui** }	デフォルト：**noRestrictions** ポートセキュリティを有効にした後、モードを **noRestrictions**（デフォルト）にした場合のみ、ポートセキュリティのモードを変更することができます。ポートセキュリティのモードを変更する場合は、最初に**undo port-security port-mode**コマンドで、ポートセキュリティのモードをデフォルトに戻す必要があります。

🕮 **メモ：**

mac-and-userlogin-secure-ext オプションは Version7.1.13 を含む以降のソフトウェアからサポートしています。

5.6 ポートセキュリティ機能の設定

5.6.1 NTK の設定

NTK（Need To Know）機能は、認証をパスした装置に対してのみフレームを転送させるため、出力フレームの宛先 MAC アドレスをチェックします。

NTK 機能は以下のモードをサポートしています。

- **ntkonly** – 認証をパスした宛先 MAC アドレス宛のユニキャストフレームのみ転送します。
- **ntk-withbroadcasts** – 認証をパスした宛先 MAC アドレス宛の、ブロードキャストフレーム、ユニキャストフレームのみを転送します。
- **ntk-withmulticasts** – 認証をパスした宛先 MAC アドレス宛のブロードキャストフレーム、マルチキャストフレーム、ブロードキャストフレームのみを転送します。
- **ntkauto** – ポートにオンラインユーザがいる場合にのみ、認証された宛先 MAC アドレスを持つブロードキャスト、マルチキャスト、およびユニキャストフレームのみを転送します。

NTK 機能を使用すると、未知の宛先 MAC アドレスのユニキャストフレームは廃棄されます。すべてのポートセキュリティモードが NTK 機能を動作するわけではありません。詳細は表 5-1を参照してください。

以下に NTK 機能の設定を示します。

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

操作	コマンド	補足
3． NTK 機能を設定する	**port-security ntk-mode** { **ntk-withbroadcasts** | **ntk-withmulticasts** | **ntkauto** | **ntkonly** }	デフォルト：無効 すべてのフレームが転送されます。

5.6.2 侵入防止の設定

侵入防止機能は不正なフレームに対して以下のアクションの 1 つを実行します。

- **blockmac** － 不正なフレームの送信元 MAC アドレスをブロック MAC アドレスリストに追加し、フレームを破棄します。ブロック MAC アドレスは、3 分間ブロックされた後に、標準状態に戻ります。このブロックする時間は変更できません。
- **disableport** － 手動でポートをアップするまで、ポートを無効にします。
- **disableport-temporarily** － 指定した期間、ポートを無効にします。この期間は **port-security timer disableport** コマンドで設定できます。

以下に侵入防止の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． interface view に移行する	**interface** *interface-type interface-number*	―
3． 侵入防止機能を設定する	**port-security intrusion-mode** { **blockmac** | **disableport** | **disableport-temporarily** }	デフォルト：無効
4． system view に戻る	**quit**	―
5． （オプション設定項目）ポートを無効にする時間を設定する	**port-security timer disableport** *time-value*	デフォルト：20秒

🕮 **メモ：**

macAddressElseUserLoginSecure モードあるいは macAddressElseUserLoginSecureExt はモードで動作するポートにおいて、侵入防止機能は、同一フレームで MAC アドレス認証と 802.1X 認証の両方が失敗した後に動作します。

5.7 セキュアMACアドレスの設定

セキュア MAC アドレスは autoLearn モードで設定、あるいは学習されます。アドレスが保存されると、装置の再起動を行っても保持されます。セキュア MAC アドレスを VLAN の 1 つのポートにのみ割り当てることができます。

セキュア MAC アドレスエントリが最大数に到達した場合、ポートはセキュアモードに変更押します。セキュアモードでは、ポートはセキュア MAC アドレスを追加あるいは学習することができません。ポートはセキュア MAC アドレスからの送信元フレームあるいは **mac-address dynamic** コマンド、**mac-address static** コマンドで設定された MAC アドレスのみがパスすることができます。

表 5-2 スタティックセキュア MAC アドレス、Sticky セキュア MAC アドレスの比較

タイプ	アドレスソース	エージングメカニズム	再起動で保存されるか？
Static	手動で追加されます。（sticky パラメータを使用しない **port-security mac-address security**コマンドを使用します）	利用できません。 スタティックアドレスは以下の作業の1つを実行しない限り、エージアウトしません。 ● 手動でMACアドレスを削除します。 ● ポートセキュリティモードを変更します。 ● ポートセキュリティモードを無効にします。	Yes
Sticky	手動で追加されます。（**port-security mac-address security sticky**コマンドを使用します）	Sticky MACアドレスはデフォルト設定ではエージアウトしませんが、エージング時間を設定することができます。 ● エージングタイマが設定されている場合、sticky MACアドレスからのトラフィックデータに関わらずエージングを行います。	Yes 再起動でセキュアMACエージングタイマが再起動します。

5.7.1 設定要件

セキュア MAC アドレスを設定する前に、以下の作業を完了してください。

- ポートセキュリティを有効にしてください。
- autoLearn モードを有効にする前に、ポートのセキュア MAC アドレスの最大許可数を設定してください。
- ポートセキュリティのモードを autoLearn に設定してください。
- ポートで指定した VLAN のパケットが通過できるように許可する、あるいは VLAN にポートを追加するように設定を行ってください。VLAN が既に存在することを確認してください。

5.7.2 設定手順

以下にセキュア MAC アドレスの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. （オプション設定項目）セキュア MAC アドレスエージングタイマを設定する	**port-security timer autolearn aging** *time-value*	デフォルト：セキュアMACアドレスはエージアウトしません。

操作	コマンド	補足
3. セキュア MAC アドレスを設定する	● system viewで設定する： **port-security mac-address security** [**sticky**] *mac-address* **interface** *interface-type interface-number* **vlan** *vlan-id* ● interface viewで設定する： 1. **interface** *interface-type interface-number* 2. **port-security mac-address security** [**sticky**] *mac-address* **vlan** *vlan-id*	デフォルト：設定なし 同一VLANでは、スタティックセキュアMACアドレスにMACアドレスを指定することはできません。

5.8 サーバからの許可情報の無視

802.1X ユーザ、または MAC アドレス認証ユーザが認証をパスした後、サーバ（ローカルあるいはリモート）から受信した許可情報を無視するようにポートに設定することができます。

以下にサーバからの許可情報を無視する設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. interface view に移行する	**interface** *interface-type interface-number*	―
3. 認証サーバから受信した許可情報を無視するように設定する	**port-security authorization ignore**	デフォルト：ポートは認証サーバからの許可情報を使用します。

5.9 MACアドレス移動機能の有効化

MAC アドレス移動機能を有効にすることで、802.1X 認証あるいは MAC アドレス認証が許可されたユーザが装置のポートを移動できるようになります。たとえば、802.1X 認証ユーザが、802.1X が有効な装置の別のポートに移動する場合、認証セッションが最初のポートから削除され、新しいポートで再認証されます。

MAC アドレス移動機能が無効で 802.1X 認証ユーザが別のポートに移動した場合、再認証されません。

（ローカルまたはリモートの）認証サーバのオンラインユーザ数が上限に達した場合、802.1X または MAC アドレス認証ユーザは装置上のポート間で移動はできません。

ポートのローミングを行うワイヤレスユーザがネットワークにアクセスできるように MAC アドレス移動機能を有効にすることを推奨します。

以下に MAC アドレス移動機能の有効化の設定を示します。

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

操作	コマンド	補足
2． MAC アドレス移動機能を有効にする	**port-security mac-move permit**	デフォルト：有効

5.10 ポートセキュリティの拡張ハードウェア モードの有効化

デフォルトでは、ハードウェア リソースを節約するために、ポート セキュリティは、一部のプロセスで認証をトリガーするユーザ パケットの VLAN 情報をチェックしません。その結果、ユーザは同じスイッチの VLAN 間を移動できない可能性があります。この問題を解決するには、ポート セキュリティ MAC の移動を有効にします。

この機能により、ポート セキュリティは、アクセス ポートと MAC アドレス情報のチェックに加えて、認証をトリガーするユーザ パケットの VLAN 情報をチェックできます。ポート セキュリティは、アクセス ポート、MAC アドレス、および VLAN によってユーザを正確に識別します。これにより、ポート セキュリティ MAC 移動が有効になっている場合に、ユーザが同じスイッチの VLAN 間を移動できるようになります。

以下に MAC アドレス移動機能の有効化の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． MAC アドレス移動機能を有効にする	port-security enhanced-hardware-mode	デフォルト：無効

5.11 ポートセキュリティに関するSNMP notification

重大なポートセキュリティイベントを NMS に通知するために使用します。ポートセキュリティイベントを正しく送信するには、装置に SNMP も設定しておかなければなりません。SNMP 設定の詳細については、オペレーションマニュアルのセクション 9 *システム管理*“*SNMP*”を参照してください。

以下にポートセキュリティに関する SNMP notification の有効化の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． ポートセキュリティの SNMP notification 機能を有効にする	**snmp-agent trap enable port-security** [**address-learned** | **dot1x-failure** | **dot1x-logoff** | **dot1x-logon** | **intrusion** | **mac-auth-failure** | **mac-auth-logoff** | **mac-auth-logon**] *	デフォルト：無効

5.12 ポートでの認証方式のトリガー順序の設定

🕮 **メモ：**

ポートでの認証方式のトリガー順序の設定は Version7.1.13 を含む以降のソフトウェアからサポートしています。

I. 概要

この機能は、トリプル認証がイネーブルになっているポートでのみ有効です。トリプル認証を使用すると、ユーザアクセス用のレイヤ 2 ポートで Web 認証、MAC アドレス認証、802.1 X 認証を同時にイネーブルにできます。エンドポイントパケットのタイプが異なると、最初に異なるタイプの認証がトリガーされます。

エンドポイントパケットが最初に MAC アドレス認証をトリガーできるようにするには、この機能を使用します。

ポートは、複数の認証方式に対して同時に認証プロセスを実行できます。1 つの認証が失敗しても、他の認証方式のプロセスには影響しません。ただし、エンドポイントがポート上で 1 つの認証を渡すと、デバイスはポート上の他の認証方式のプロセスを次のように処理します。

- エンドポイントが MAC アドレス認証を通過する場合、デバイスはポート上に MAC アドレス認証 ユーザ エントリを生成し、ポート上のエンドポイントに対して 802.1 X 認証を実行し続けます。ただし、デバイスはポート上のエンドポイントの Web 認証を続行できません。
  - MAC アドレス認証の後にエンドポイントが 802.1 X 認証に合格すると、デバイスはポート上のエンドポイントに対して 802.1 X ユーザ エントリを生成します。802.1 X ユーザ エントリは、MAC アドレス認証 ユーザ エントリを上書きします。
  - MAC アドレス認証後にエンドポイントが 802.1 X 認証に合格しない場合、MAC アドレス認証 ユーザ エントリはポートに保持されます。エンドポイントは 802.1 X 認証を再度トリガーできますが、Web 認証はトリガーできません。
- エンドポイントが MAC アドレス認証に失敗し、802.1 X または Web 認証を通過した場合、デバイスは、エンドポイントが通過した認証方式を除き、ポート上のすべての認証方式をただちに停止します。さらに、デバイスは、ポート上のエンドポイントに対して停止した認証方法の認証プロセスをトリガーできなくなります。

II. 制約事項およびガイドライン

この機能により、認証されるユーザは認証に失敗します。ユーザは、オンラインになるために認証を再トリガーする必要があります。ユーザがオンラインにならないようにするためのベストプラクティスとして、この機能は注意して使用してください。

III. 設定手順

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

操作	コマンド	補足
3． ポートの認証方式 (MAC アドレス認証、802.1 X 認証、Web 認証) のトリガー順序を設定する	**port-security triple-auth-order mac-dot1x-web**	デフォルト : エンドポイントから送信されるパケットのタイプによって異なる

5.13 ポートセキュリティの表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
ポートセキュリティの設定、動作情報、統計情報を表示する	**display port-security** [**interface** *interface-type interface-number*]
セキュアMACアドレス情報を表示する	**display port-security mac-address security** [**interface** *interface-type interface-number*] [**vlan** *vlan-id*] [**count**]
ブロックしたMACアドレスを表示する	**display port-security mac-address block** [**interface** *interface-type interface-number*] [**vlan** *vlan-id*] [**count**]

5.14 ポートセキュリティの設定例

5.14.1 autoLearn モードの設定例

I. ネットワーク要件

図 5-1に示すように、装置の GigabitEthernet 1/0/1 で以下の要件を設定します。

- 認証なしでアクセスできるユーザを最大 64 にします。
- ポートを学習、追加できるように設定し、セキュア MAC アドレスエージングタイマを 30 分に設定します。
- セキュア MAC アドレスの数が 64 に到達すると、ポートは MAC アドレスの学習を止めます。未知の MAC アドレスを持つフレームを受信した場合は、侵入防止機能が実行します。ポートはシャットダウンされ、30 秒間無効化されます。

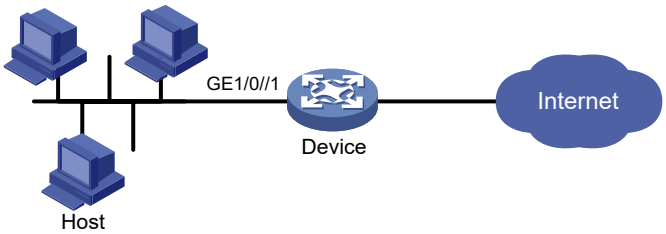


図 5-1 ネットワーク図

II. 設定手順

ポートセキュリティを有効にします。

```
<Device> system-view
[Device] port-security enable
```

セキュア MAC アドレスタイマを 30 分に設定します。

```
[Device] port-security timer autolearn aging 30
```

GigabitEthernet 1/0/1 のセキュア MAC アドレスの最大許可数を 64 に設定します。

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] port-security max-mac-count 64
```

ポートセキュリティのモードを autoLearn に設定します。

```
[Device-GigabitEthernet1/0/1] port-security port-mode autolearn
```

侵入防止機能が起動した後、30 秒後に復旧するように設定します。

```
[Device-GigabitEthernet1/0/1] port-security intrusion-mode disableport-temporarily
[Device-GigabitEthernet1/0/1] quit
[Device] port-security timer disableport 30
```

III. 設定の確認

ポートセキュリティの設定を表示します。

[Device] display port-security interface gigabitethernet 1/0/1

```
Grobal Port security parameters:
   Port security          : Enabled
   AutoLearn aging time   : 30 min
   Disableport timeout    : 30 s
   Blockmac timeout       : 180 s
   MAC move               : Denied
   Authorization fail     : Online
   NAS-ID profile         : Not configured
   Dot1x-failure trap     : Disabled
   Dot1x-logon trap       : Disabled
   Dot1x-logoff trap      : Disabled
   Intrusion trap         : Disabled
   Address-learned trap   : Disabled
   Mac-auth-failure trap  : Disabled
   Mac-auth-logon trap    : Disabled
   Mac-auth-logoff trap   : Disabled
   Open authentication    : Disabled
   OUI value list         :
    Index :  1           Value : 123401

 GigabitEthernet1/0/1 is link-up
   Port mode                     : autoLearn
   NeedToKnow mode               : Disabled
   Intrusion protection mode     : DisablePortTemporarily
   Security MAC address attribute
       Learning mode             : Sticky
       Aging type                : Periodical
   Max secure MAC addresses      : 64
   Current secure MAC addresses  : 0
   Authorization                 : Permitted
   NAS-ID profile                : Not configured
   Free VLANs                    : Not configured
   Open authentication           : Disabled
   MAC-move VLAN check bypass    : Disabled
```

設定が適用された後、ポートで MAC アドレスの学習が行われます。Current number of secure MAC addresses フィールドに学習した MAC アドレスを表示することができます。

学習した MAC アドレスの追加情報を表示します。

[Device] interface gigabitethernet 1/0/1

[Device-GigabitEthernet1/0/1] display this

```
#
interface GigabitEthernet1/0/1
 port-security max-mac-count 64
 port-security port-mode autolearn
 port-security mac-address security sticky 0002-0000-0015 vlan 1
 port-security mac-address security sticky 0002-0000-0014 vlan 1
 port-security mac-address security sticky 0002-0000-0013 vlan 1
 port-security mac-address security sticky 0002-0000-0012 vlan 1
 port-security mac-address security sticky 0002-0000-0011 vlan 1
#
```

[Device-GigabitEthernet1/0/1] quit

ポートで学習した MAC アドレスの数が 64 に到達した後、ポートセキュリティのモードが **secure** モードに変更したことを確認します。

[Device] display port-security interface gigabitethernet 1/0/1

未知の MAC アドレスのフレームを受信したのち、30 秒後にポートが無効になることを確認します。（詳細は省略します。）

ポートが再度有効になった後、いくつかのセキュア MAC アドレスを削除します。

```
[Device] undo port-security mac-address security sticky 0002-0000-0015 vlan 1
[Device] undo port-security mac-address security sticky 0002-0000-0014 vlan 1
```

ポートセキュリティのモードは **autoLearn** に戻り、再度 MAC アドレスを学習できるようになることを確認します。（詳細は省略します。）

5.14.2 userLoginWithOUI モードの設定例

I. ネットワーク要件

図 5-2に示すようにクライアントは Device のポート GigabitEthernet 1/0/1 に接続されます。Device は RADIUS サーバによってクライアントを認証します。認証に成功した場合、クライアントはインターネットへのアクセスが許可されます。

- プライマリ認証サーバとセカンダリアカウンティングサーバとして RADIUS サーバ 192.168.1.2 を、セカンダリ認証サーバとプライマリアカウンティングサーバとして RADIUS サーバ 192.168.1.3 を指定します。認証用の共有鍵を name、アカウンティング用の共有鍵を money に設定します。
- すべてのユーザは、ISP ドメイン sun のデフォルトの認証、許可、アカウンティング方式を使用します。
- RADIUS サーバのレスポンスタイムアウト時間を 5 秒、RADIUS サーバへの許容再送信数を 5 回に設定します。Device は 15 分ごとにリアルタイムアカウンティングパケットを送信し、RADIUS サーバ宛にドメイン名なしでユーザ名を送信します。

Device の GigabitEthernet 1/0/1 は 802.1X ユーザ、および認証するために指定された OUI の値の 1 つを使用するユーザのみを許可します。

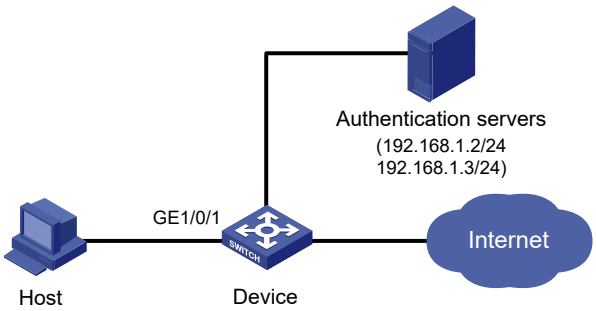


図 5-2 ネットワーク図

II. 設定手順

以下の設定手順は AAA/RADIUS の設定コマンドが含まれます。詳細はコマンドマニュアルのセクション 7 *セキュリティ”AAA”* を参照してください。

Host と RADIUS サーバが互いに通信可能であることを確認してください。

1)　AAA を設定します。

RADIUS スキーム radsun を設定します。

```
<Device> system-view
[Device] radius scheme radsun
[Device-radius-radsun] primary authentication 192.168.1.2
[Device-radius-radsun] primary accounting 192.168.1.3
[Device-radius-radsun] secondary authentication 192.168.1.3
[Device-radius-radsun] secondary accounting 192.168.1.2
[Device-radius-radsun] key authentication simple name
[Device-radius-radsun] key accounting simple money
[Device-radius-radsun] timer response-timeout 5
[Device-radius-radsun] retry 5
[Device-radius-radsun] timer realtime-accounting 15
[Device-radius-radsun] user-name-format without-domain
[Device-radius-radsun] quit
```

ISP ドメイン sun を設定します。

```
[Device] domain sun
[Device-isp-sun] authentication lan-access radius-scheme radsun
[Device-isp-sun] authorization lan-access radius-scheme radsun
[Device-isp-sun] accounting lan-access radius-scheme radsun
[Device-isp-sun] quit
```

2) 802.1X 認証方式を CHAP に設定します。802.1X のデフォルトの認証方式の設定は CHAP です。

```
[Device] dot1x authentication-method chap
```

ISP ドメインを sun に指定します。

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] dot1x mandatory-domain sun
[Device-GigabitEthernet1/0/1] quit
```

3) ポートセキュリティを設定します。

ポートセキュリティを有効にします。

```
[Device] port-security enable
```

5 つの OUI の値を追加します。（16 の OUI の値を追加することができます。ポートは 1 ユーザが認証をパスするため、1 つの OUI のみにマッチするように許可します。）

```
[Device] port-security oui index 1 mac-address 1234-0100-1111
[Device] port-security oui index 2 mac-address 1234-0200-1111
[Device] port-security oui index 3 mac-address 1234-0300-1111
```

```
[Device] port-security oui index 4 mac-address 1234-0400-1111
[Device] port-security oui index 5 mac-address 1234-0500-1111
```

ポートセキュリティのモードを userLoginWithOUI に設定します。

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] port-security port-mode userlogin-withoui
[Device-GigabitEthernet1/0/1] quit
```

III. 設定の確認

GigabitEthernet 1/0/1 が 1 つの 802.1X ユーザのみに認証されていることを確認します。

```
[Device] display port-security interface gigabitethernet 1/0/1
Global port security parameters:
   Port security          : Enabled
   AutoLearn aging time   : 30 min
   Disableport timeout    : 30 s
   Blockmac timeout       : 180 s
   MAC move               : Denied
   Authorization fail     : Online
   NAS-ID profile         : Not configured
   Dot1x-failure trap     : Disabled
   Dot1x-logon trap       : Disabled
   Dot1x-logoff trap      : Disabled
   Intrusion trap         : Disabled
   Address-learned trap   : Disabled
   Mac-auth-failure trap  : Disabled
   Mac-auth-logon trap    : Disabled
   Mac-auth-logoff trap   : Disabled
   Open authentication    : Disabled
   OUI value list         :
       Index :  1       Value : 123401
       Index :  2       Value : 123402
       Index :  3       Value : 123403
       Index :  4       Value : 123404
       Index :  5       Value : 123405

 GigabitEthernet1/0/1 is link-up
   Port mode                       : userLoginWithOUI
   NeedToKnow mode                 : Disabled
   Intrusion protection mode       : NoAction
   Security MAC address attribute
       Learning mode               : Sticky
       Aging type                  : Periodical
   Max secure MAC addresses        : Not configured
   Current secure MAC addresses    : 1
   Authorization                   :Permitted
   NAS-ID profile                  : Not configured
   Free VLANs                      : Not configured
   Open authentication             : Disabled
   MAC-move VLAN check bypass      : Disabled
```

802.1X の設定を確認するため、802.1X オンラインユーザの情報を表示します。

```
[Device] display dot1x
```

認証にパスするために指定された OUI を持つ MAC アドレスのユーザがポートで許可されているかどうか確認します。

```
[Device] display mac-address interface gigabitethernet 1/0/1
MAC Address     VLAN ID   State          Port/NickName         Aging
1234-0300-0011  1         Learned        GE1/0/1               Y
```

5.14.3 macAddressElseUserLoginSecure モードの設定例

I. ネットワーク要件

図 5-3に示すように、GigabitEthernet 1/0/1 を通してクライアントが Device に接続されます。Device は RADIUS サーバを使用してクライアントを認証します。認証が成功すると、クライアントはインターネットにアクセスするように許可されます。

Device のポート GigabitEthernet 1/0/1 を以下のように制限します。

- 1 つ以上の MAC アドレス認証ユーザがログオンすることを許可します。
- 802.1X ユーザのために、最初に MAC アドレス認証が実行されます。MAC アドレス認証に失敗した場合、802.1X 認証が実行されます。そして 1 つの 802.1X ユーザのみがログオンすることを許可します。
- MAC アドレス認証のために固定ユーザ名とパスワードを設定します。MAC アドレスはハイフン付きの 16 進数で大文字です。
- MAC アドレス認証ユーザと 802.1X 認証ユーザの総計を 64 に設定します。
- 未知の MAC アドレス宛にフレーム送信されることを防ぐために NTK（ntkonly モード）を有効にします。

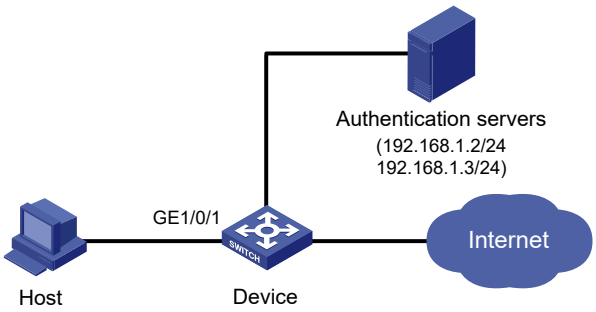


図 5-3 ネットワーク図

II. 設定手順

Host と RADIUS サーバが互いに通信可能であることを確認してください。

1) RADIUS 認証／許可、ISP ドメインの設定を行います。（オペレーションマニュアルのセクション 7 *セキュリティ”ポートセキュリティ”の”userLoginWithOUI モードの設定例*”を参照してください。）
2) ポートセキュリティを設定します。

ポートセキュリティを有効にします。

```
<Device> system-view
[Device] port-security enable
```

#MAC アドレスに、MAC 認証のユーザ名とパスワードを使用します。各 MAC アドレスは 16 進数でハイフンあり、大文字を使用します。

```
[Device] mac-authentication user-name-format mac-address with-hyphen uppercase
```

MAC アドレス認証ドメインを指定します。

```
[Device] mac-authentication domain sun
```

802.1X 認証方式を CHAP に設定します。802.1X のデフォルトの認証方式の設定は CHAP です。

```
[Device] dot1x authentication-method chap
```

MAC アドレスの最大許可数を 64 に設定します。

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] port-security max-mac-count 64
```

ポートセキュリティのモードを macAddressElseUserLoginSecure に設定します。

```
[Device-GigabitEthernet1/0/1] port-security port-mode mac-else-userlogin-secure
```

ISP ドメインを sun に指定します。

```
[Device-GigabitEthernet1/0/1] dot1x mandatory-domain sun
```

ポートの NTK モードを ntkonly に設定します。

```
[Device-GigabitEthernet1/0/1] port-security ntk-mode ntkonly
[Device-GigabitEthernet1/0/1] quit
```

III. 設定の確認

ポートセキュリティの設定を表示します。

```
[Device] display port-security interface gigabitethernet 1/0/1
Global Port security parameters:
   Port security          : Enabled
   AutoLearn aging time   : 30 min
   Disableport timeout    : 30 s
   Blockmac timeout       : 180 s
   MAC move               : Denied
   Authorization fail     : Online
   NAS-ID profile         : Not configured
   Dot1x-failure trap     : Disabled
   Dot1x-logon trap       : Disabled
   Dot1x-logoff trap      : Disabled
   Intrusion trap         : Disabled
   Address-learned trap   : Disabled
   Mac-auth-failure trap  : Disabled
   Mac-auth-logon trap    : Disabled
   Mac-auth-logoff trap   : Disabled
   Open authentication    : Disabled
   OUI value list

 GigabitEthernet1/0/1 is link-up
   Port mode                      : macAddressElseUserLoginSecure
   NeedToKnow mode                : NeedToKnowOnly
   Intrusion protection mode      : NoAction
```

```
   Security MAC address attribute
       Learning mode              : Sticky
       Aging type                 : Periodical
   Max secure MAC addresses       : 64
   Current secure MAC addresses   : 0
   Authorization                  : Permitted
   NAS-ID profile                 : Not configured
   Free VLANs                     : Not configured
   Open authentication            : Disabled
   MAC-move VLAN check bypass     : Disabled
```

ユーザが認証にパスした後、MAC アドレス認証の情報を表示します。GigabitEthernet 1/0/1 で複数の MAC アドレス認証のユーザが許可されていることを確認してください。

[Device] display mac-authentication interface gigabitethernet 1/0/1

```
Global MAC authentication parameters:
   MAC authentication                  : Enabled
   Authentication method               : PAP
   User name format                 : MAC address in uppercase(XX-XX-XX-XX-XX-XX)
           Username                    : mac
           Password                    : Not configured
   Offline detect period               : 300 s
   Quiet period                        : 180 s
   Server timeout                      : 100 s
   Reauth period                       : 3600 s
   User aging period for critical VLAN : 1000 s
   User aging period for guest VLAN    : 1000 s
   Authentication domain               : sun
 Online MAC-auth wired users           : 3

 Silent MAC users:
          MAC address       VLAN ID  From port               Port index

GigabitEthernet1/0/1 is link-up
   MAC authentication               : Enabled
   Carry User-IP                    : Disabled
   Authentication domain            : Not configured
   Auth-delay timer                 : Disabled
   Periodic reauth                  : Disabled
   Re-auth server-unreachable       : Logoff
   Guest VLAN                       : Not configured
   Guest VLAN auth-period           : 30 s
   Critical VLAN                    : Not configured
   Critical voice VLAN              : Disabled
   Host mode                        : Single VLAN
   Offline detection                : Enabled
   Authentication order             : Default
   User aging                       : Enabled
   Server-recovery online-user-sync : Enabled

   Auto-tag feature                 : Disabled
   VLAN tag configuration ignoring  : Disabled
   Max online users                 : 4294967295
   Authentication attempts          : successful 3, failed 7
   Current online users             : 3
          MAC address       Auth state
          1234-0300-0011    Authenticated
          1234-0300-0012    Authenticated
          1234-0300-0013    Authenticated
```

802.1X 認証情報を表示します。GigabitEthernet 1/0/1 で 1 つの 802.1X ユーザのみ許可していることを確認してください。

[Device] display dot1x interface gigabitethernet 1/0/1

```
Global 802.1X parameters:
   802.1X authentication                : Enabled
   CHAP authentication                  : Enabled
   Max-tx period                        : 30 s
   Handshake period                     : 15 s
   Quiet timer                          : Disabled
       Quiet period                     : 60 s
   Supp timeout                         : 30 s
   Server timeout                       : 100 s
   Reauth period                        : 3600 s
   Max auth requests                    : 2
   User aging period for Auth-Fail VLAN : 1000 s
   User aging period for critical VLAN  : 1000 s
   User aging period for guest VLAN     : 1000 s
   EAD assistant function               : Disabled
       EAD timeout                      : 30 min
   Domain delimiter                     : @
 Online 802.1X wired users              : 1

GigabitEthernet1/0/1  is link-up
   802.1X authentication            : Enabled
   Handshake                        : Enabled
   Handshake reply                  : Disabled
   Handshake security               : Disabled
   Unicast trigger                  : Disabled
   Periodic reauth                  : Disabled
   Port role                        : Authenticator
   Authorization mode               : Auto
   Port access control              : MAC-based
   Multicast trigger                : Enabled
   Mandatory auth domain            : sun
   Guest VLAN                       : Not configured
   Auth-Fail VLAN                   : Not configured
   Critical VLAN                    : Not configured
   Critical voice VLAN              : Disabled
   Add Guest VLAN delay             : Disabled
   Re-auth server-unreachable       : Logoff
   Max online users                 : 4294967295
   User IP freezing                 : Disabled
   Reauth period                    : 60 s
   Send Packets Without Tag         : Disabled
   Max Attempts Fail Number         : 0
   User aging                       : Enabled
   Server-recovery online-user-sync : Enabled

   EAPOL packets: Tx 16331, Rx 102
   Sent EAP Request/Identity packets : 16316
        EAP Request/Challenge packets: 6
        EAP Success packets: 4
        EAP Failure packets: 5
   Received EAPOL Start packets : 6
            EAPOL LogOff packets: 2
            EAP Response/Identity packets : 80
            EAP Response/Challenge packets: 6
            Error packets: 0
   Online 802.1X users: 1
          MAC address         Auth state
          0002-0000-0011      Authenticated
```

未知の宛先 MAC アドレス、マルチキャストアドレス、ブロードキャストアドレスのフレームは破棄されることを確認してください。（詳細は省略します。）

5.15 ポートセキュリティのトラブルシューティング

5.15.1 ポートセキュリティのモードが設定できない

I. 症状

ポートセキュリティのモードが設定できません。

II. 分析

ポートで noRestrictions 以外のポートセキュリティのモードが動作している場合、**port-security port-mode** コマンドによって、モードを変更することができません。

III. 解決策

問題を解決するため、以下を行います。

1) ポートセキュリティモードを noRestrictions に設定します。

```
[Device-GigabitEthernet1/0/1] undo port-security port-mode
```

2) 新しいポートセキュリティのモードを設定します。たとえば、autoLearn です。

```
[Device-GigabitEthernet1/0/1] port-security port-mode autolearn
```

3) 問題が解決しない場合、NEC に問い合わせてください。

5.15.2 セキュア MAC アドレスが設定できない

I. 症状

セキュア MAC アドレスが設定できません。

II. 分析

ポートセキュリティのモードが autoLearn 以外で動作するポートでは、セキュア MAC アドレスを設定することはできません。

III. 解決策

問題を解決するため、以下を行います。

1) ポートセキュリティのモードを autoLearn に設定します。

```
[Device-GigabitEthernet1/0/1] undo port-security port-mode
[Device-GigabitEthernet1/0/1] port-security max-mac-count 64
[Device-GigabitEthernet1/0/1] port-security port-mode autolearn
[Device-GigabitEthernet1/0/1] port-security mac-address security 1-1-2 vlan 1
```

2) 問題が解決しない場合、NEC に問い合わせてください。

目次

このセクションのページは **7-x-x** です。

6 章 公開鍵 6-1
6.1 概要 6-1
6.2 ローカル鍵ペアの作成 6-2
6.2.1 設定ガイドライン 6-2
6.2.2 設定手順 6-2
6.3 ローカルホスト公開鍵の分配 6-3
6.3.1 指定したフォーマットのホスト公開鍵のファイルへのエクスポート 6-3
6.3.2 ホスト公開鍵の表示 6-3
6.4 ローカル鍵ペアの削除 6-4
6.5 ピア公開鍵の設定 6-4
6.5.1 公開鍵ファイルからピアへのホスト公開鍵のインポート 6-4
6.5.2 ピアの公開鍵の入力 6-5
6.6 公開鍵の表示と維持 6-5
6.7 公開鍵の設定例 6-5
6.7.1 ピアのホスト公開鍵の入力例 6-5
6.7.2 公開鍵ファイルからの公開鍵のインポート例 6-7

6章 公開鍵

6.1 概要

この章では、以下の非対称鍵アルゴリズムの公開鍵の管理について記載します。

- RSA（Revest-Shamir-Adleman）アルゴリズム
- DSA（Digital Signature Algorithm）アルゴリズム

SSH を含む多くのセキュリティアプリケーションは、図 6-1に示すように 2 つの群の間でセキュリティの通信を行うため、非対称鍵アルゴリズムを使用します。暗号化と複号化を行うため、非対象鍵アルゴリズムは、2 つの分離した鍵（公開鍵と秘密鍵）を使用します。対称鍵は 1 つの鍵のみを使用します。

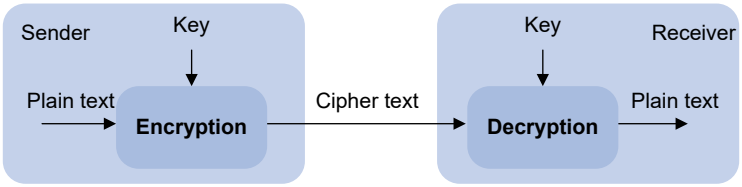


図 6-1 暗号化と複号化

鍵の所有者はプレーンテキスト（平文）で公開鍵を配布することができますが、秘密鍵を保持する必要があります。たとえ攻撃者がアルゴリズムと公開鍵を知っていたとしても秘密鍵を計算することは、数学上、実現不可能です。

SSH などのセキュリティアプリケーションは以下の目的で非対象鍵アルゴリズムを使用します。

- **暗号化と複号化** – 公開鍵の受信者が情報を暗号化するために公開鍵を使用し、秘密鍵の所有者のみが情報を複号化できます。
- **デジタル署名** – 鍵の所有者は送信する”署名”情報に秘密鍵を使用します。受信者は情報が信頼できるか確認するため、送信者の公開鍵で情報を複号化します。

RSA、DSA はすべてのデジタル署名を実行できますが、RSA のみが暗号化と複号化を行うことができます。

非対称鍵アルゴリズムは、安全でないネットワークでセキュアな鍵の配布を行うことができますが、非対称鍵アルゴリズムのセキュリティの強度は、対称鍵アルゴリズムの鍵の長さに依存します。

6.2 ローカル鍵ペアの作成

6.2.1 設定ガイドライン

ローカル鍵ペアを作成する場合、以下のガイドラインに従います。

- 鍵アルゴリズムはセキュリティアルゴリズムで要求されたアルゴリズムと同一にする必要があります。
- RSA または DSA 鍵ペアを作成する際に、鍵の長さは適切に設定してください。鍵の長さが長いと高いセキュリティとなりますが、鍵を作成する時間も長くなります。
- 鍵ペアの名前を割り当てない場合、システムは鍵ペアにデフォルトの名前を割り当て、鍵ペアを default としてマーキングします。デフォルトの名前を別の鍵ペアに割り当てることができますが、鍵ペアを default としてマーキングしません。鍵ペアの名前は、同じ鍵アルゴリズムを使用する鍵ペア間で一意にする必要があります。名前が重複している場合、存在する鍵ペアに上書きしていいか確認メッセージが表示されます。
- 鍵ペアは自動で保存され、装置の再起動が行われても削除されません。

表 6-1 非対称鍵ペアの異なるタイプの比較

タイプ	鍵ペアの数	鍵の長さ	推奨値
RSA	• 鍵ペアの名前を指定する場合、ホスト鍵ペアを作成します。 • 鍵ペアの名前を指定しない場合、1つのサーバ鍵ペアと1つのホスト鍵ペアを作成します。鍵ペアの名前はデフォルト名です。	範囲 : 512～4096ビット デフォルト : 1024ビット	少なくとも768ビットにしてください。
DSA	1つのホスト鍵ペアを作成します。	範囲 : 512～2048ビット デフォルト : 1024ビット	少なくとも768ビットにしてください。

🕮 **メモ :**

SSH 1.5 のみが RSA サーバ鍵ペアを使用します。

6.2.2 設定手順

以下にローカル鍵ペアを作成する設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. ローカル DSA あるいは RSA 鍵ペアを作成する	**public-key local create** { **dsa** | **rsa** } [**name** *key-name*]	デフォルト : 作成なし

6.3 ローカルホスト公開鍵の分配

ピアの装置が以下のことを行えるようにピアの装置にローカルホスト公開鍵を分配する必要があります。

- 公開鍵を使用して、ローカル装置に送信された情報を暗号化します。
- ローカル装置によって署名されたデジタル署名を認証します。

ローカルホスト公開鍵を分配するためには以下の方法を行います。

1) 鍵を記録あるいはファイルにエクスポートします。
2) 鍵を転送します。たとえば FTP や TFTP を使用します。

ローカルホスト公開鍵を分配するには最初に鍵をエクスポートあるいは表示します。

- ホスト公開鍵をエクスポートします。
  - □ ホスト公開鍵をファイルにエクスポートします。
  - □ ホスト公開鍵をモニタ画面に表示し、表示したデータをファイルに保存します。

  ホスト公開鍵をファイルにエクスポートした後、ピアの装置にファイルを転送します。ピアの装置ではファイルからホスト公開鍵をインポートします。
- ホスト公開鍵を表示します。

ホスト公開鍵を表示した後、鍵を記録します。たとえば、フォーマットされていないファイルにコピーします。ピアの装置で鍵を正確に入力する必要があります。

6.3.1 指定したフォーマットのホスト公開鍵のファイルへのエクスポート

操作	コマンド
1. system view に移行する	**system-view**
2. 指定したフォーマットのローカルホスト公開鍵をファイルへエクスポートする	• RSAホスト公開鍵をエクスポートする： **public-key local export rsa** [**name** *key-name*] { **openssh** | **ssh1** | **ssh2** } [*filename*] • DSAホスト公開鍵をエクスポートする： **public-key local export dsa** [**name** *key-name*] { **openssh** | **ssh2** } [*filename*]

6.3.2 ホスト公開鍵の表示

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

操作	コマンド
ローカルRSA公開鍵を表示する	**display public-key local rsa public** [**name** *key-name*]
ローカルDSA公開鍵を表示する	**display public-key local dsa public** [**name** *key-name*]

🕮 **メモ：**
ピアの装置に RSA サーバの公開鍵の serverkey（デフォルト）を配布しないでください。

6.4 ローカル鍵ペアの削除

以下の状況が発生した後、ローカル非対称鍵ペアを削除し、新しいペアを生成する必要があります。

- 不正侵入が発生した場合
- 装置の記憶媒体を交換した場合
- ローカル証明書の有効期限が切れた場合

以下にローカル鍵ペアを削除する設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. ローカル鍵ペアを削除する	**public-key local destroy** { **dsa** | **rsa** } [**name** *key-name*]	ー

6.5 ピア公開鍵の設定

以下の方法を用いてピアのホスト公開鍵を設定することができます。

- 公開鍵ファイルから公開鍵をインポートします。（推奨）
- 公開鍵を手動で設定します。（鍵データを入力またはコピー）

6.5.1 公開鍵ファイルからピアへのホスト公開鍵のインポート

ホスト公開鍵をインポートする前に、ピアの装置にホスト公開鍵がエクスポートされており、ピアの装置からファイルを取得していることを確認してください。ホスト公開鍵のエクスポートについては、オペレーションマニュアルのセクション 7 *セキュリティ”公開鍵”の”ローカルホスト公開鍵の分配”*を参照してください。

鍵をインポートしたのち、システムは自動的に公開鍵を PKCS（Public Key Cryptography Standards）フォーマットの文字列へ変換します。

以下に公開鍵ファイルからピアへのホスト公開鍵のインポート手順を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. 公開鍵ファイルからピアのホスト公開鍵をインポートする	**public-key peer** *keyname* **import sshkey** *filename*	デフォルト：ピアのホスト公開鍵は存在しません。

6.5.2 ピアの公開鍵の入力

ホスト公開鍵をインポートする前に、ピアの装置にホスト公開鍵が表示されており、ホスト公開鍵が記録されていることを確認してください。

display public-key local public コマンドを使用して、公開鍵を表示してください。他の方法で表示された公開鍵のフォーマットは、正確ではない場合があります。

ホスト公開鍵が正しいフォーマットでない場合、システムはホスト公開鍵を廃棄し、エラーメッセージを表示します。ホスト公開鍵が正しいフォーマットである場合、システムはホスト公開鍵を保存します。

記録されたピアのホスト公開鍵のフォーマットをサポートしているか不明な場合、ピアのホスト公開鍵を入力する方法ではなく、ホスト公開鍵ファイルからインポートする方法を行ってください。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． ピアの公開鍵の名前を指定し、public key view に移行する	**public-key peer** *keyname*	デフォルト : ピアのホスト公開鍵は存在しません。
3． 鍵を入力あるいはコピーする	ー	空白と改行は使用できますが保存しません。
4． system view に戻る	**peer-public-key end**	public key viewから戻ると、自動的に公開鍵を保存します。

6.6 公開鍵の表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
ローカル公開鍵を表示する	**display public-key local** { **dsa** | **rsa** } **public**
ピアのホスト公開鍵を表示する	**display public-key peer** [**brief** | **name** *publickey-name*]

6.7 公開鍵の設定例

6.7.1 ピアのホスト公開鍵の入力例

I. ネットワーク要件

図 6-2に示すように、不正なアクセスを防止するため、Device B は Device A をデジタル署名によって認証します。Device B 上で認証パラメータを設定する前に、以下の手順を利用して Device B 上で Device A の公開鍵を設定します。

- Device A の認証に RSA の鍵ペアを作成し、RSA の鍵ペアの公開鍵を表示します。
- Device B 上で、Device A の RSA のホスト公開鍵を手動で指定します。

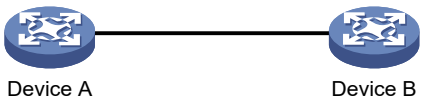


図 6-2 ネットワーク図

II. 設定手順

1)　Device A を設定します。

Device A にデフォルト名のローカル RSA 鍵ペアを作成し、鍵の長さをデフォルトの 1024 ビットに設定します。

```
<DeviceA> system-view
[DeviceA] public-key local create rsa
The range of public key modulus is (512 ~ 4096).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
...
Create the key pair successfully.
```

すべての RSA 鍵ペアの公開鍵を表示します。

```
[DeviceA] display public-key local rsa public
=============================================
Key name: hostkey (default)
Key type: RSA
Time when key pair created: 16:48:31 2011/05/12
Key code:
   30819F300D06092A864886F70D010101050003818D003081890281810 0DA3B90F59237347B
   8D41B58F8143512880139EC9111BFD31EB84B6B7C7A1470027AC8F04A827B30C2CAF79242E
   45FDFF51A9C7E917DB818D54CB7AEF538AB261557524A7441D288EC54A5D31EFAE4F681257
   6D7796490AF87A8C78F4A7E31F0793D8BA06FB95D54EBB9F94EB1F2D561BF66EA27DFD4788
   CB47440AF6BB25ACA50203010001
=============================================
Key name: serverkey (default)
Key type: RSA
Time when key pair created: 16:48:31 2011/05/12
Key code:
   307C300D06092A864886F70D0101010500036B003068026100C9451A80F7F0A9BA1A90C7BC
   1C02522D194A2B19F19A75D9EF02219068BD7FD90FCC2AF3634EEB9FA060478DD0A1A49ACE
   E1362A4371549ECD85BA04DEE4D6BB8BE53B6AED7F1401EE88733CA3C4CED391BAE633028A
   AC41C80A15953FB22AA30203010001
```

2)　Device B を設定します。

public key view で Device A のホスト公開鍵を入力します。鍵は Device A での表示と同一になるように、正確に入力してください。

```
<DeviceB> system-view
[DeviceB] public-key peer devicea
Enter public key view. Return to system view with "peer-public-key end" command.
[DeviceB-pkey-public-key-devicea]30819F300D06092A864886F70D010101050003818D
0030818902818100DA3B90F59237347B
[DeviceB-pkey-public-key-devicea]8D41B58F8143512880139EC9111BFD31EB84B6B7C
7A1470027AC8F04A827B30C2CAF79242E
```

```
[DeviceB-pkey-public-key-devicea]45FDFF51A9C7E917DB818D54CB7AEF538AB26155
7524A7441D288EC54A5D31EFAE4F681257
[DeviceB-pkey-public-key-devicea]6D7796490AF87A8C78F4A7E31F0793D8BA06FB95
D54EBB9F94EB1F2D561BF66EA27DFD4788
[DeviceB-pkey-public-key-devicea]CB47440AF6BB25ACA50203010001
```

system view に戻り、公開鍵を保存します。

```
[DeviceB-pkey-public-key-devicea] peer-public-key end
```

III. 設定の確認

Device A と同一の鍵であることを確認してください。

```
[DeviceB] display public-key peer name devicea

=============================================
Key name: devicea
Key type: RSA
Key modulus: 1024
Key code:
   30819F300D06092A864886F70D010101050003818D0030818902818100DA3B90F59237347B
   8D41B58F8143512880139EC9111BFD31EB84B6B7C7A1470027AC8F04A827B30C2CAF79242E
   45FDFF51A9C7E917DB818D54CB7AEF538AB261557524A7441D288EC54A5D31EFAE4F681257
   6D7796490AF87A8C78F4A7E31F0793D8BA06FB95D54EBB9F94EB1F2D561BF66EA27DFD4788
   CB47440AF6BB25ACA50203010001
```

6.7.2 公開鍵ファイルからの公開鍵のインポート例

I. ネットワーク要件

図 6-3に示すように、Device B は Device A をデジタル署名によって認証します。Device B 上で認証パラメータを設定する前に、以下の手順を使用して Device B 上で Device A の公開鍵を設定します。

- Device A の認証に RSA の鍵ペアを作成し、RSA ホスト公開鍵をファイルにエクスポートします。
- 公開鍵ファイルから Device B へ、Device A のホスト公開鍵をインポートします。

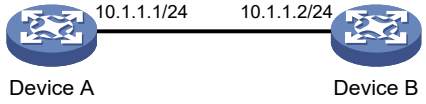


図 6-3 ネットワーク図

II. 設定手順

1)　Device A を設定します。

Device A にデフォルト名のローカル RSA 鍵ペアを作成し、鍵の長さをデフォルトの 1024 ビットに設定します。

```
<DeviceA> system-view
[DeviceA] public-key local create rsa
The range of public key modulus is (512 ~ 4096).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
...
Create the key pair successfully.
```

すべてのローカル RSA 鍵ペアの公開鍵を表示します。

```
[DeviceA] display public-key local rsa public
=============================================
Key name: hostkey (default)
Key type: RSA
Time when key pair created: 16:48:31 2011/05/12
Key code:
   30819F300D06092A864886F70D010101050003818D0030818902818100DA3B90F59237347B
   8D41B58F8143512880139EC9111BFD31EB84B6B7C7A1470027AC8F04A827B30C2CAF79242E
   45FDFF51A9C7E917DB818D54CB7AEF538AB261557524A7441D288EC54A5D31EFAE4F681257
   6D7796490AF87A8C78F4A7E31F0793D8BA06FB95D54EBB9F94EB1F2D561BF66EA27DFD4788
   CB47440AF6BB25ACA50203010001
=============================================
Key name: serverkey (default)
Key type: RSA
Time when key pair created: 16:48:31 2011/05/12
Key code:
   307C300D06092A864886F70D0101010500036B003068026100C9451A80F7F0A9BA1A90C7BC
   1C02522D194A2B19F19A75D9EF02219068BD7FD90FCC2AF3634EEB9FA060478DD0A1A49ACE
   E1362A4371549ECD85BA04DEE4D6BB8BE53B6AED7F1401EE88733CA3C4CED391BAE633028A
   AC41C80A15953FB22AA30203010001
```

RSA ホスト公開鍵をファイル **devicea.pub** にエクスポートします。

```
[DeviceA] public-key local export rsa ssh2 devicea.pub
[DeviceA] quit
```

FTP サーバ機能を有効にし、FTP ユーザをユーザ名 **ftp**、パスワード **123**、FTP のユーザロールを **network-admin** で作成します。

```
[DeviceA] ftp server enable
[DeviceA] local-user ftp
[DeviceA-luser-manage-ftp] password simple 123
[DeviceA-luser-manage-ftp] service-type ftp
[DeviceA-luser-manage-ftp] authorization-attribute user-role network-admin
[DeviceA-luser-manage-ftp] quit
```

2)　Device B を設定します。

Device A から、公開鍵ファイル **devicea.pub** を FTP のバイナリモードで取得します。

```
<DeviceB> ftp 10.1.1.1
Connected to 10.1.1.1 (10.1.1.1).
220 FTP service ready.
User(10.1.1.1:(none)):ftp
331 Password required for ftp.
Password:
230 User logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> binary
200 TYPE is now 8-bit binary
ftp> get devicea.pub
227 Entering Passive Mode (10,1,1,1,118,252)
150 Accepted data connection
226 File successfully transferred
301 bytes received in 0.003 seconds (98.0 kbyte/s)
ftp> quit
221-Goodbye. You uploaded 0 and downloaded 1 kbytes.
221 Logout.
```

鍵ファイル **devicea.pub** からホスト公開鍵をインポートします。

```
<DeviceB> system-view
[DeviceB] public-key peer devicea import sshkey devicea.pub
```

III. 設定の確認

ホスト公開鍵が Device A の公開鍵と同一であることを確認します。

```
[DeviceB] display public-key peer name devicea
=============================================
Key name: devicea
Key type: RSA
Key modulus: 1024
Key code:
   30819F300D06092A864886F70D010101050003818D0030818902818100DA3B90F59237347B
   8D41B58F8143512880139EC9111BFD31EB84B6B7C7A1470027AC8F04A827B30C2CAF79242E
   45FDFF51A9C7E917DB818D54CB7AEF538AB261557524A7441D288EC54A5D31EFAE4F681257
   6D7796490AF87A8C78F4A7E31F0793D8BA06FB95D54EBB9F94EB1F2D561BF66EA27DFD4788
   CB47440AF6BB25ACA50203010001
```

目次

このセクションのページは **7-x-x** です。

7 章 SSH 7-1
7.1 概要 7-1
7.1.1 SSH の動作 7-1
7.1.2 SSH 認証方式 7-2
7.2 SSH サーバの設定 7-4
7.2.1 ローカル鍵ペアの作成 7-4
7.2.2 Stelnet サーバ機能の有効化 7-5
7.2.3 SFTP サーバ機能の有効化 7-5
7.2.4 SSH ログインのユーザラインの設定 7-5
7.2.5 クライアントのホスト公開鍵の設定 7-6
7.2.6 SSH ユーザの設定 7-7
7.2.7 SSH 管理パラメータの設定 7-8
7.3 Stelnet クライアントの設定 7-10
7.3.1 Stelnet クライアントの作業設定リスト 7-10
7.3.2 ローカル鍵ペアの作成 7-10
7.3.3 SSH パケットの送信元 IP アドレスの指定 7-10
7.3.4 Stelnet サーバとの接続の確立 7-11
7.4 SFTP クライアントの設定 7-12
7.4.1 SFTP クライアントの設定作業リスト 7-12
7.4.2 ローカル鍵ペアの作成 7-12
7.4.3 SFTP パケットの送信元 IP アドレスの指定 7-13
7.4.4 SFTP サーバとの接続の確立 7-13
7.4.5 SFTP ディレクトリの操作 7-14
7.4.6 SFTP ファイルの操作 7-15
7.4.7 ヘルプ情報の表示 7-15
7.4.8 SFTP サーバの接続の切断 7-15
7.5 SSH の表示と維持 7-15
7.6 Stelnet 設定例 7-16
7.6.1 パスワード認証を有効にした Stelnet サーバ設定例 7-16
7.6.2 公開鍵認証を有効にした Stelnet サーバの設定例 7-18
7.6.3 パスワード認証を有効にした Stelnet クライアント設定例 7-25
7.6.4 公開鍵認証を有効にした Stelnet クライアント設定例 7-29
7.7 SFTP 設定例 7-31
7.7.1 パスワード認証を有効にした SFTP サーバの設定例 7-31
7.7.2 公開鍵認証を有効にした SFTP クライアント設定例 7-34

7章 SSH

7.1 概要

SSH（Secure Shell）はネットワークセキュリティプロトコルです。暗号化と認証を使用して、安全にリモートアクセスや、ファイルを転送することができます。

一般的なクライアント／サーバモデルを適用して、SSH は TCP をもとにしてデータの転送を保護するチャネルを確立させます。

SSH は SSH1.x と SSH2.0 の 2 つのバージョンをサポートしています。（以降、SSH1 と SSH2 と記載します。）SSH1 と SSH2 では互換性がありません。SSH2 は SSH1 よりも性能とセキュリティを向上しています。

装置は SSH サーバあるいは SSH クライアントとして動作することができます。

- SSH サーバとして動作する場合、装置は SSH クライアントのサービスを提供し、以下のバージョンを SSH サポートします。
  - Stelnet（Secure Telnet）、SFTP（Secure File Transfer Protocol）で装置は SSH2、SSH1 の SSH バージョンをサポートします。
- SSH クライアントとして動作する場合、装置は SSH2 のみサポートします。ユーザが SSH サーバと SSH 接続を確立するために使用します。

装置は以下の SSH アプリケーションをサポートします。

- **Stelnet（Secure Telnet）** – Stelnet は安全で信頼性のあるネットワーク端末アクセスサービスを提供します。Stelnet を使用して、ユーザはリモートサーバに安全にログインすることができます。Stelnet は、IP スプーフィングやプレーンテキストのパスワードの傍受のような装置への攻撃を保護することができます。装置は Stelnet サーバあるいは Stelnet クライアントとして動作することができます。
- **SFTP（Secure File Transfer Protocol）** – SSH2 をもとにして SSH を使用した SFTP は安全なファイル転送を提供します。装置は SFTP サーバとして動作し、リモートユーザが安全なファイル管理と転送を行うため、SFTP サーバにログインできます。また装置は SFTP クライアントとして動作します。ユーザが装置からリモート装置にログインし、安全なファイル転送を行うことができます。

7.1.1 SSH の動作

この章では、SSH セッションの確立に関連するステージの例を、SSH2 を使用して示します。ステージの詳細は SSH の技術書を参照してください。

表 7-1 SSH セッションを確立するステージ

ステージ	説明
接続の確立	SSHサーバはポート番号22で接続リクエストを受け入れます。クライントが接続要求を初期化した後、サーバとクライントはTCP接続を確立します。
バージョンのネゴシエーション	2つの群（サーバとクライアント）間で使用するバージョンを決めます。

ステージ	説明
アルゴリズムのネゴシエーション	SSHは複数のアルゴリズムをサポートします。ローカルアルゴリズムにもとづいて、2つの群（サーバとクライアント）は、以下のアルゴリズムを決定します。 ● セッション鍵を作成するアルゴリズムの鍵交換アルゴリズム ● 暗号データ用の暗号アルゴリズム ● デジタル署名と認証のための公開鍵アルゴリズム ● データの完全性を保護するためのHMACアルゴリズム
鍵交換	2つの群（サーバとクライアント）は、セッション鍵とセッションIDを動的に作成するため、DH交換アルゴリズムを使用します。 ● セッション鍵はデータの転送を保護するために使用します。 ● セッションIDはSSH接続を認識するために使用します。 このステージでは、クライアントはサーバと同様に認証します。
認証	SSHサーバはクライアントからの認証要求に応答し、認証を実行します。
セッション要求	認証にパスした後、クライアントがセッション要求（あるいはStelnet、SFTPサービスのリクエスト）をサーバに送信します。
データ交換	サーバが要求に承諾した後、クライアントとサーバはセッションで互いに通信を行います。 このステージでは、テキストフォーマットでコマンドを貼り付け、CLIで実行することができます。一度に貼り付けることができるテキストは、2000バイトよりも少ない値としてください。コマンドを正常に実行するため同じviewで使用することを推奨します。 2000バイト以上のコマンドを実行する場合、設定ファイルにコマンドを保存し、SFTPを通してサーバにアップロードし、サーバを再起動してください。

7.1.2 SSH 認証方式

この章では装置を SSH サーバとして動作させる場合、サポートする認証方式について記載します。

I. パスワード認証

SSH サーバは、AAA を使用してクライアントを認証します。パスワード認証は以下のように処理します。

1) SSH クライアントは暗号化されたユーザ名とパスワードが含まれる認証要求をサーバに送信します。
2) SSH サーバは以下の処理を行います。

a) プレーンテキストのユーザ名とパスワードを取得するため要求を復号化します。

b) ローカル、あるいはリモートAAA認証によってユーザ名とパスワードが正しいか確認します。

c) 認証結果をクライアントに通知します。

セカンダリ認証のため AAA サーバがユーザのパスワードを必要とする場合、ユーザはプロンプトが運ばれる認証応答を SSH サーバに送ります。プロンプトは透過的にクライアントに送信され、ユーザに指定のパスワードを入力するように通知します。ユーザが正しいパスワードを入力した場合、AAA サーバ上でパスワードの妥当性をチェックします。

パスワードが有効である場合、SSH サーバはクライアントに認証成功メッセージを返します。

AAA についての詳細は、オペレーションマニュアルのセクション 7 *セキュリティ”AAA”* を参照してください。

🕮 **メモ：**

SSH1 は AAA サーバによって開始されるセカンダリパスワード認証をサポートしていません。

II. 公開鍵認証

サーバは、クライアントのデジタル署名を使用してクライアントを認証します。公開鍵認証は以下のように処理します。

1) クライアントはユーザ名、公開鍵、公開鍵アルゴリズム名が含まれる認証要求をサーバに送信します。

   クライアントのデジタル署名が認証で要求される場合、クライアントは認証要求のデジタル署名をカプセル化します。デジタル署名にはクライアントの公開鍵情報が含まれます。

2) サーバは公開鍵が有効かどうかを確認します。

- 公開鍵が無効である場合、認証が失敗します。サーバは認証が失敗したことをクライアントに通知します。
- 公開鍵が有効である場合、サーバはクライアントのデジタル署名を要求します。デジタル署名を受信したのち、サーバはデジタル署名を確認するために公開鍵を使用します。最後に認証結果をクライアントに送信します。

SSH サーバとして動作する場合、装置はデジタル署名を確認するため、公開鍵アルゴリズム RSA と DSA を使用します。

SSH クライアントとして動作する場合、装置はデジタル署名を作成するため、公開鍵アルゴリズム RSA と DSA を使用します。

公開鍵の設定についての詳細は、オペレーションマニュアルのセクション 7 *セキュリティ”公開鍵”* を参照してください。

III. パスワード-公開鍵認証

サーバは SSH2 クライアントに、パスワード認証と公開鍵認証の両方にパスするように要求します。SSH1 クライアントは、サーバの要求に関係なく、いずれか 1 つの認証のみ必要です。

IV. すべての認証

サーバは、クライアントに keyboard-interactiv 認証、パスワード認証、または公開鍵認証を渡すことを要求します。 サーバに接続するには、いずれかの認証方法で成功すれば十分です。

7.2 SSHサーバの設定

作業リスト	補足
（オプション設定項目） ローカル鍵ペアの作成	ー
（必須設定項目） Stelnetサーバ機能の有効化	Stelnetでのみ必須設定項目です。
（必須設定項目） SFTPサーバ機能の有効化	SFTPサーバでのみ必須設定項目です。
（必須設定項目）SSHログインのユーザラインの設定	Stelnetでのみ必須設定項目です。
（必須設定項目） クライアントのホスト公開鍵の設定	認証方法が公開鍵、パスワード-公開鍵認証あるいはいずれかの方法を使用する場合、必須設定項目です。
（必須設定項目/オプション設定項目） SSHユーザの設定	認証方法が公開鍵、パスワード-公開鍵認証あるいはいずれかの方法を使用する場合、必須設定項目です。 パスワード認証のみ使用するユーザでは、オプション設定項目です。
（オプション設定項目）SSH管理パラメータの設定	ー

7.2.1 ローカル鍵ペアの作成

DSA または RSA 鍵ペアは、鍵交換ステージのセッション鍵とセッション ID を作成するために必要です。DSA または RSA 鍵ペアは、クライアントがサーバを認証するために、クライアントによって使用されます。クライアントがサーバを認証する場合、サーバから受信した公開鍵を、ローカルに保存したサーバ公開鍵と比較します。鍵が一致している場合、クライアントはサーバから受信したデジタル署名を復号化するため、クライアントがローカルに保存したサーバの公開鍵を使用します。デジタル署名の復号化に成功した場合、認証は成功します。

SSH アプリケーションを実行させるため、装置で SSH コマンドを実行する場合、SSH サーバは自動で 2 つの RSA 鍵ペアを作成します。装置の DSA 鍵ペアあるいは RSA 鍵ペアを作成するため **public-key local create** コマンドを使用します。

I. 設定ガイドライン

ローカル鍵ペアを作成する場合、以下の制限とガイドラインに従ってください。

- SSH は、デフォルト名でローカルに作成された DSA と RSA の鍵ペアのみをサポートします。
- 鍵ペアの異なるタイプを使用する SSH クライアントをサポートするため、SSH サーバで DSA と RSA 鍵ペアの両方を作成します。
- **public-key local create rsa** コマンドは RSA のサーバ鍵ペアとホスト鍵ペアのみを作成します。SSH1 ではサーバ鍵ペアの公開鍵はセッション鍵の安全な転送を行うため暗号化するのに使用されます。
- SSH2 は、SSH サーバとクライアントの各セッション鍵を作成する DH アルゴリズムを使用するため、セッション鍵の転送は必要ありません。サーバ鍵ペアは SSH2 で使われません。
- **public-key local create dsa** コマンドは DSA ホスト鍵ペアのみを作成します。SSH1 は DSA アルゴリズムをサポートしません。
- SSH サーバで **public-key local create dsa** コマンドを使用する場合、鍵の長さは 2048 ビットよりも短くしてください。

II. 設定手順

以下に SSH サーバでローカル DSA あるいは RSA 鍵ペアを生成する設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． ローカル DSA または RSA 鍵ペアを作成する	**public-key local create** { **dsa** | **rsa** }	デフォルト : 鍵ペアは存在しません。

7.2.2 Stelnet サーバ機能の有効化

装置で Stelnet サーバ機能を有効にしたのち、クライアントは Stelnet を通して装置にログインすることができます。

以下に Stelnet サーバ機能の有効化の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． Stelnet サーバ機能を有効にする	**ssh server enable**	デフォルト：無効

7.2.3 SFTP サーバ機能の有効化

装置で SFTP サーバ機能を有効にしたのち、クライアントは SFTP を通して装置にログインすることができます。

SFTP サーバとして動作する装置は SSH1 クライアントから開始された SFTP 接続をサポートしません。

以下に SFTP サーバ機能の有効化の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． SFTP サーバ機能を有効にする	**sftp server enable**	デフォルト：無効

7.2.4 SSH ログインのユーザラインの設定

SSH アプリケーションに応じて、SSH クライアントは Stelnet クライアント、あるいは SFTP クライアントとなります。

Stelnet 接続を確立するため、Stelnet クライアントは VTY ユーザラインを通して装置にアクセスする必要があります。SSH クライアントが SSH ログインできるようにユーザラインを設定する必要があります。この設定は次回ログインした場合にのみ適用します。

SFTP クライアントは VTY ユーザラインを使用しないで装置にアクセスします。

以下に Stelnet クライアントのユーザラインの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． VTY line view に移行する	**line vty** *first-number2* [*last-number2*]	―
3． ログイン認証モードをスキームに設定する	**authentication-mode scheme**	デフォルト：**password** コマンドの詳細は、コマンドマニュアルのセクション1 *はじめに”ログイン”* を参照してください。

7.2.5 クライアントのホスト公開鍵の設定

サーバがクライアントを認証するために公開鍵を使用する場合、サーバは SSH ユーザ名とクライアントから受信したホスト公開鍵をローカルに保存されている内容と比較します。内容が一致した場合、クライアントが送信したデジタル署名を確認します。クライアントはホスト公開鍵に関連する秘密鍵にもとづいてデジタル署名を作成します。

公開鍵認証、パスワード-公開鍵認証、あるいはあらゆる認証を使用する SSH サーバのために、以下の処理を行う必要があります。

1) サーバ上でクライアントの DSA あるいは RSA ホスト公開鍵を設定します。

   SSH サーバの SSH クライアントホスト公開鍵は 20 以下に設定することを推奨します。

2) デジタル署名を作成するため関連するクライアントのホスト秘密鍵を指定します。装置が SSH クライアントとして動作する場合、クライアントの公開鍵アルゴリズムを指定します。アルゴリズムは、デジタル署名を作成するため、関連する秘密鍵を決定します。

クライアントのホスト公開鍵の内容を入力する、あるいは公開鍵ファイルからクライアントのホスト公開鍵をインポートすることができます。クライアントのホスト公開鍵をインポートすることを推奨します。

I. クライアントのホスト公開鍵の入力

クライアントのホスト公開鍵を入力する前に、クライアントのホスト公開鍵を取得するため、クライアントで **display public-key local public** コマンドを使用してください。他の方法で取得したホスト公開鍵は正式な形式でない可能性があるため、サーバに保存することができません。

以下にクライアントのホスト公開鍵を入力する方法を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． public key view に移行する	**public-key peer** *keyname*	―

操作	コマンド	補足
3． クライアントのホスト公開鍵を設定する	ホスト公開鍵の内容を入力する	ホスト公開鍵は変換されないDER復号形式である必要があります。 ホスト公開鍵の内容を入力する場合、空白と改行を使用することができます。 ホスト公開鍵を保存する場合、空白と改行は自動で削除されます。 詳細はオペレーションマニュアルのセクション*7 セキュリティ" 公開鍵*"を参照してください。
4． system view に戻る	**peer-public-key end**	―

II. 公開鍵ファイルからのクライアントのホスト公開鍵のインポート

ホスト公開鍵をインポートする前に、クライアントの公開鍵ファイル（バイナリ形式）を FTP あるいは TFTP を使用してサーバにアップロードします。インポートを行う間、サーバは自動的に公開鍵ファイルのホスト公開鍵を、PKCS 形式に変換します。

以下に公開鍵ファイルからクライアントのホスト公開鍵をインポートする設定を示します。

操作	コマンド
1． system view に移行する	**system-view**
2． 公開鍵ファイルからクライアントの公開鍵をインポートする	**public-key peer** *keyname* **import sshkey** *filename*

7.2.6 SSH ユーザの設定

認証方式に応じて SSH ユーザとローカルユーザを設定します。

- 認証方式が公開鍵である場合、サーバに SSH ユーザとローカルユーザを作成する必要があります。SSH ユーザに正しい作業ディレクトリとユーザロールを割り当てることができるように、2 つのユーザは同一のユーザ名にする必要があります。
- 認証方式がパスワード認証である場合、以下の処理を実行する必要があります。
  - □ ローカル認証用に **local-user** コマンドを使用してローカルユーザアカウントを設定します。
  - □ リモート認証用に RADIUS サーバのようなリモート認証サーバで SSH ユーザを設定します。

  ssh user コマンドを使用して SSH ユーザあるいはローカルユーザを作成する必要はありません。しかし集中管理を行うため、パスワード認証のみの SSH ユーザを含むすべての SSH ユーザを表示する場合、**ssh user** コマンドを使用することができます。そのような SSH ユーザが作成される場合、サービスタイプと認証方式が正しく指定されていることを確認してください。
- 認証方式がパスワード公開鍵あるいはそれ以外の認証方式である場合、SSH ユーザを作成し、以下の処理を実行する必要があります。

- □ ローカル認証用に **local-user** コマンドを使用してローカルユーザアカウントを設定します。
- □ リモート認証用に RADIUS サーバのようなリモート認証サーバで SSH ユーザを設定します。

どちらの場合においても、ローカルユーザあるいはリモート認証サーバで設定される SSH ユーザは SSH ユーザと同じユーザ名にする必要があります。

I. 設定ガイドライン

SSH ユーザを設定する場合、以下の制限とガイドラインに従ってください。

- SSH サーバは 1024 の SSH ユーザをサポートします。
- SFTP ユーザの作業ディレクトリは認証方式に応じます。
  - □ 認証方式が公開鍵あるいはパスワード-公開鍵認証である場合、作業ディレクトリは関連した local user view で **authorization-attribute** コマンドを使用して指定されます。
  - □ 認証方式がパスワードの場合、作業ディレクトリは AAA によって承認されます。
- SSH ユーザでは、ユーザロールは認証方式に応じます。
  - □ 認証方式が公開鍵あるいはパスワード-公開鍵認証である場合、ユーザロールは関連した local user view で **authorization-attribute** コマンドを使用して指定されます。
  - □ 認証方式がパスワードの場合、ユーザロールは AAA によって承認されます。
- すでにログインしている SSH ユーザの認証方式あるいは公開鍵を変更する場合、変更内容は次回ユーザがログインした場合に適用されます。
- パスワード認証を除いて、他の認証方式は、指定されたクライアントのホスト公開鍵が必要です。
  - □ クライアントが直接サーバにユーザの公開鍵の情報を送信する場合、サーバのクライアントの公開鍵を指定する必要があります。指定される公開鍵はすでに存在している必要があります。公開鍵の詳細は、オペレーションマニュアルのセクション 7 *セキュリティ”SSH”の”クライアントのホスト公開鍵の設定”*を参照してください。

ローカルユーザとリモート認証を設定する方法の詳細は、オペレーションマニュアルのセクション 7 *セキュリティ”AAA”*を参照してください。

II. 設定手順

以下に SSH ユーザを設定し、サービスタイプと認証方式を指定する手順を示します。

操作	コマンド
1. system view に移行する	**system-view**
2. SSH ユーザを作成し、サービスタイプと認証方式を指定する	**ssh user** *username* **service-type** { **all** | **sftp** | **stelnet** } **authentication-type** { **password** | { **any** | **password-publickey** | **publickey** } [**assign publickey** *keyname*&<1-6>] }

7.2.7 SSH 管理パラメータの設定

以下に SSH 管理パラメータの設定を示します。

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

操作	コマンド	補足
2． SSH1 クライアントのサポートを有効にする	**ssh server compatible-ssh1x enable**	デフォルト：無効
3． RSA サーバ鍵ペアの最小アップデート間隔を設定する	**ssh server rekey-interval** *interval*	デフォルト：RSAサーバ鍵ペアのアップデートを行いません。 このコマンドはSSH1ユーザのみ適用します。
4． SSH ユーザ認証タイムアウトタイマを設定する	**ssh server authentication-timeout** *time-out-value*	デフォルト：60秒 タイムアウトタイマが終了した場合、接続用の認証が終了していない場合、接続を確立することができません。
5． SSH 認証の最大試行回数を設定する	**ssh server authentication-retries** *retries*	デフォルト：3
6． SSH ユーザの接続を管理する ACL を設定する	● SSHユーザのIPv4 ACLを設定する： **ssh server acl** { *advanced-acl-number* | *basic-acl-number* | **mac** *mac-acl-number* } ● SSHユーザのIPv6 ACLを設定する： **ssh server ipv6 acl** { **ipv6** { *advanced-acl-number* | *basic-acl-number* } | **mac** *mac-acl-number* }	デフォルト：設定なし
7． SSH サーバが SSH クライアントに送信するパケットの DSCP を設定する	● IPv4パケットのDSCPを設定する： **ssh server dscp** *dscp-value* ● IPv6パケットのDSCPを設定する： **ssh server ipv6 dscp** *dscp-value*	デフォルト：48 DSCPはパケットのプライオリティを決定し、パケットを転送する優先度を決定します。DSCPの値が大きいほど優先度は高くなります。
8． SFTP 接続アイドルタイムアウトタイマを設定する	**sftp server idle-timeout** *time-out-value*	デフォルト：10分 アイドルタイマが指定したしきい値を超えた場合、システムは自動的に接続を切断します。
9． オンライン SSH ユーザの最大同時接続数を指定する	**aaa session-limit ssh** *max-sessions*	デフォルト：32 オンラインSSHユーザが上限に到達した場合、システムは新しいSSH接続要求を拒否します。オンラインSSHユーザには影響しません。

7.3 Stelnetクライアントの設定

7.3.1 Stelnet クライアントの作業設定リスト

設定リスト	補足
（必須設定項目） ローカル鍵ペアの作成	Stelnetサーバが**publickey**、**password-publickey**の認証方式を使用する際は必須です。
（オプション設定項目） SSHパケットの送信元IPアドレスの指定	―
（必須設定項目） Stelnetサーバとの接続の確立	―
（オプション設定項目）スーツBに基づくStelnetサーバとの接続の確立	―

7.3.2 ローカル鍵ペアの作成

Stelnet サーバが **publickey**、**password-publickey**、あるいは **any** の認証方式を使用する際は、Stelnet クライアントでローカル鍵ペアを作成してください。

I. 設定ガイドライン

Stelnet クライアントでローカル鍵ペアを設定する際には、以下のガイドラインに従ってください。

- SSH のローカル DSA、ECDSA 及び RSA 鍵ペアはデフォルト名を使用します。鍵ペアに名前を割り当てることはできません。
- DSA 鍵ペアを作成する場合、鍵の長さは 2048 ビットよりも短くしてください。

II. 設定手順

以下に Stelnet クライアントでローカル鍵ペアを生成する設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． ローカル鍵ペアを作成する	**public-key local create** { **dsa** | **rsa** }	デフォルト : 鍵ペアは存在しません。

7.3.3 SSH パケットの送信元 IP アドレスの指定

以下のため、SSH パケットの送信元インタフェースとしてループバックインタフェースの IP アドレスを指定することを推奨します。

- Stelnet クライアントと Stelnet サーバが互いに通信できることを保証します。
- 認証サービスの Stelnet クライアントの管理を向上します。

以下に SSH パケットの送信元 IP アドレスの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. SSH パケットの送信元 IP アドレスを設定する	• SSHパケットの送信元IPv4アドレスを指定する: **ssh client source** { **interface** *interface-type interface-number* | **ip** *ip-address* } • SSHパケットの送信元IPv6アドレスを指定する: **ssh client ipv6 source** { **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }	デフォルト：設定なし IPv4 SSHパケットは送信元アドレスとして一致するルートで指定された送信インタフェースのプライマリIPアドレスを使用します。 IPv6 SSHパケットはRFC3484互換で定義された送信元アドレスとして、自動で選択されたIPv6アドレスを選択します。

7.3.4 Stelnet サーバとの接続の確立

Stelnet サーバにアクセスする場合、装置はサーバを認証するためサーバのホスト公開鍵を使用します。装置でサーバのホスト公開鍵が設定されていない場合、装置はアクセスを継続するかどうかを確認するメッセージを表示します。

- アクセスを継続する場合、装置はサーバにアクセスし、サーバのホスト公開鍵をダウンロードします。
- アクセスを継続しない場合、接続は確立することができません。

安全でないネットワークでは装置でサーバのホスト公開鍵を設定することを推奨します。

以下に Stelnet サーバの接続を確立する設定を示します。

操作	コマンド	補足
Stelnetサーバの接続を確立する	• IPv4 Stelnetサーバの接続を確立する： **ssh2** *server* [*port-number*] [**identity-key** { **dsa** | **rsa** } | **prefer-compress zlib** | **prefer-ctos-cipher** { **3des-cbc** | **aes128-cbc** | **des-cbc** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** } | **prefer-kex** { **dh-group-exchange-sha1** | **dh-group1-sha1** | **dh-group14-sha1** } | **prefer-stoc-cipher** { **3des-cbc** | **aes128-cbc** | **des-cbc** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** }] * [**dscp** *dscp-value* | **escape** *character* | **public-key** *keyname* | **source** { **interface** *interface-type interface-number* | **ip** *ip-address* }] * • IPv6 Stelnetサーバの接続を確立する： **ssh2 ipv6** *server* [*port-number*] [**-i** *interface-type interface-number*] [**identity-key** { **dsa** | **rsa** } | **prefer-compress zlib** | **prefer-ctos-cipher** { **3des-cbc** | **aes128-cbc** | **des-cbc** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** } | **prefer-kex** { **dh-group-exchange-sha1** | **dh-group1-sha1** | **dh-group14-sha1** } | **prefer-stoc-cipher** { **3des-cbc** | **aes128-cbc** | **des-cbc** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** }] * [**dscp** *dscp-value* | **escape** *character* | **public-key** *keyname* | **source** { **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }] *	いずれか一方の設定を使用します。 user viewで実行できます。

7.4 SFTPクライアントの設定

7.4.1 SFTP クライアントの設定作業リスト

作業リスト	補足
（必須設定項目） ローカル鍵ペアの作成	Stelnetサーバが**publickey**、**password-publickey**の認証方式を使用する際は必須です。
（オプション設定項目）SFTPパケットの送信元IPアドレスの指定	―
（必須設定項目） SFTPサーバとの接続の確立	―
（オプション設定項目） SFTPディレクトリの操作	―
（オプション設定項目） SFTPファイルの操作	―
（オプション設定項目） ヘルプ情報の表示	―
（オプション設定項目） SFTPサーバの接続の切断	―

7.4.2 ローカル鍵ペアの作成

SFTP サーバが **publickey**、**password-publickey**、あるいは **any** の認証方式を使用する際は、SFTP クライアントでローカル鍵ペアを作成してください。

I. 設定ガイドライン

SFTP クライアントでローカル鍵ペアを設定する際には、以下のガイドラインに従ってください。

- SSH のローカル DSA、ECDSA 及び RSA 鍵ペアはデフォルト名を使用します。鍵ペアに名前を割り当てることはできません。
- DSA 鍵ペアを作成する場合、鍵の長さは 2048 ビットよりも短くしてください。

II. 設定手順

以下に SFTP クライアントでローカル鍵ペアを生成する設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． ローカル鍵ペアを作成する	**public-key local create** { **dsa** | **rsa** }	デフォルト : 鍵ペアは存在しません。

7.4.3 SFTP パケットの送信元 IP アドレスの指定

以下のため、SFTP パケットの送信元インタフェースとしてループバックインタフェースの IP アドレスを指定することを推奨します。

- SFTP クライアントと SFTP サーバが互いに通信できることを保証します。
- 認証サービスの SFTP クライアントの管理を向上します。

以下に SFTP パケットの送信元 IP アドレスの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． SFTP パケットの送信元 IP アドレスを指定する	• SFTPパケットの送信元IPv4アドレスを指定する: **sftp client source** { **ip** *ip-address* | **interface** *interface-type interface-number* } • SFTPパケットの送信元IPv6アドレスを指定する: **sftp client ipv6 source** { **ipv6** *ipv6-address* | **interface** *interface-type interface-number* }	デフォルト : 設定なし IPv4 SFTPパケットは送信元アドレスとして一致するルートで指定された送信インタフェースのプライマリIPv4アドレスを使用します。 IPv6 SFTPパケットはRFC3484互換で定義された送信元アドレスとして、自動で選択されたIPv6アドレスを選択します。

7.4.4 SFTP サーバとの接続の確立

SFTP サーバにアクセスする場合、装置はサーバを認証するためサーバのホスト公開鍵を使用します。装置でサーバのホスト公開鍵が設定されていない場合、装置はアクセスを継続するかどうかを確認するメッセージを表示します。

- アクセスを継続する場合、装置はサーバにアクセスし、サーバのホスト公開鍵をダウンロードします。

- アクセスを継続しない場合、接続は確立することができません。

安全でないネットワークでは装置でサーバのホスト公開鍵を設定することを推奨します。

接続が完了したのち、ディレクトリあるいはファイルのような操作を行うため、サーバの SFTP client view に直接移行することができます。

操作	コマンド	補足
SFTPサーバの接続を確立する	• IPv4 SFTPサーバの接続を確立する： **sftp** *server* [*port-number*] [**identity-key** { **dsa** | **rsa** } | **prefer-compress zlib** | **prefer-ctos-cipher** { **3des-cbc** | **aes128-cbc** | **des-cbc** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** } | **prefer-kex** { **dh-group-exchange-sha1** | **dh-group1-sha1** | **dh-group14-sha1** } | **prefer-stoc-cipher** { **3des-cbc** | **aes128-cbc** | **des-cbc** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** }] * [**dscp** *dscp-value* | **public-key** *keyname* | **source** { **interface** *interface-type interface-number* | **ip** *ip-address* }] * • IPv6 SFTPサーバの接続を確立する： **sftp ipv6** *server* [*port-number*] [**-i** *interface-type interface-number*] [**identity-key** { **dsa** | **rsa** } | **prefer-compress zlib** | **prefer-ctos-cipher** { **3des-cbc** | **aes128-cbc** | **des-cbc** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** } | **prefer-kex** { **dh-group-exchange-sha1** | **dh-group1-sha1** | **dh-group14-sha1** } | **prefer-stoc-cipher** { **3des-cbc** | **aes128-cbc** | **des-cbc** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** }] * [**dscp** *dscp-value* | **public-key** *keyname* | **source** { **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }] *	いずれか一方の設定を使用します。 user viewで実行できます。

7.4.5 SFTP ディレクトリの操作

操作	コマンド	補足
SFTPサーバの作業ディレクトリを変更する	**cd** [*remote-path*]	SFTP client viewで有効です。
上位のディレクトリに戻る	**cdup**	SFTP client viewで有効です。
SFTPサーバの現在の作業ディレクトリを表示する	**pwd**	SFTP client viewで有効です。
指定したディレクトリにあるファイルを表示する	• **dir** [**-a** | **-l**] [*remote-path*] • **ls** [**-a** | **-l**] [*remote-path*]	SFTP client viewで有効です。 **dir**コマンドは**ls**コマンドと同一です。
SFTPサーバの指定したディレクトリ名を変更する	**rename** *oldname newname*	SFTP client viewで有効です。
SFTPサーバで新しいディレクトリを作成する	**mkdir** *remote-path*	SFTP client viewで有効です。
SFTPサーバから1つ以上のディレクトリを削除する	**rmdir** *remote-path*	SFTP client viewで有効です。

7.4.6 SFTP ファイルの操作

操作	コマンド	補足
SFTPサーバの指定したディレクトリ名を変更する	**rename** *old-name new-name*	SFTP client viewで有効です。
SFTPサーバからファイルをダウンロードし、ローカルに保存する	**get** *remote-file* [*local-file*]	SFTP client viewで有効です。
SFTPサーバにローカルファイルをアップロードする	**put** *local-file* [*remote-file*]	SFTP client viewで有効です。
指定したディレクトリにあるファイルを表示する	• **dir** [**-a** | **-l**] [*remote-path*] • **ls** [**-a** | **-l**] [*remote-path*]	SFTP client viewで有効です。 **dir**コマンドは**ls**コマンドと同一です。
SFTPサーバから1つ以上のディレクトリを削除する	• **delete** *remote-file* • **remove** *remote-file*	SFTP client viewで有効です。 **delete**コマンドは**remove**コマンドと同一です。

7.4.7 ヘルプ情報の表示

コマンドのフォーマットやパラメータのような SFTP クライアントコマンドのヘルプ情報を表示することができます。

以下にヘルプ情報の表示を示します。

操作	コマンド	補足
SFTPクライアントコマンドのヘルプ情報を表示する	• **help** • **?**	いずれか一方のコマンドを使用します。 SFTP client viewで有効です。 2つのコマンドは同一機能です。

7.4.8 SFTP サーバの接続の切断

操作	コマンド	補足
SFTPサーバの接続を切断し、user viewに戻る	• **bye** • **exit** • **quit**	いずれか1つのコマンドを使用します。 SFTP client viewで有効です。 3つのコマンドは同一機能です。

7.5 SSHの表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
SFTPクライアントの送信元IPアドレスを表示する	**display sftp client source**

操作	コマンド
Stelnetクライアントの送信元IPアドレスを表示する	**display ssh client source**
SSHサーバのステータス情報あるいはセッション情報を表示する	**display ssh server** { **session** | **status** }
SSHサーバのSSHユーザ情報を表示する	**display ssh user-information** [*username*]
ローカル鍵ペアの公開鍵を表示する	**display public-key local** { **dsa** | **rsa** } **public** [**name** *publickey-name*]
SSHピアの公開鍵を表示する	**display public-key peer** [**brief** | **name** *publickey-name*]

7.6 Stelnet設定例

7.6.1 パスワード認証を有効にした Stelnet サーバ設定例

I. ネットワーク要件

図 7-1に示すように設定します。

- Switch は Stelnet サーバとして動作し、Stelnet クライアントを認証するためにパスワード認証を使用します。クライアントのユーザ名とパスワードは Switch に保存されます。
- ホストは Stelnet クライアントとして動作し、Stelnet クライアントソフトウェア（SSH2）を使用します。ホストのユーザが Stelnet を通じてスイッチにログインした後、ユーザは network-administrator としてスイッチを管理できます。

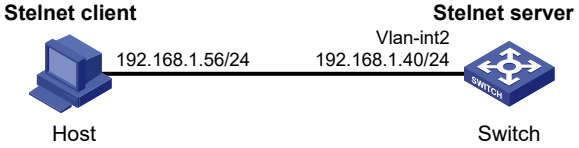


図 7-1 ネットワーク図

II. 設定手順

1)　Stelnet サーバを設定します。

RSA 鍵ペアを作成します。

```
<Switch> system-view
[Switch] public-key local create rsa
The range of public key modulus is (512 ~ 4096).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.....................++++++
.................++++++
..++++++++
............++++++++
Create the key pair successfully.
```

DSA 鍵ペアを作成します。

```
[Switch] public-key local create dsa
The range of public key modules is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.++++++++++++++++++++++++++++++++++++++++++++++++*
........+......+.....+.....................................+
...+.................+..........+...+.
Create the key pair successfully.
```

SSH サーバ機能を有効にします。

```
[Switch] ssh server enable
```

VLAN インタフェース 2 に IP アドレスを割り当てます。SSH 接続の宛先アドレスとして Stelnet クライアントは VLAN インタフェース 2 の IP アドレスを使用します。

```
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ip address 192.168.1.40 255.255.255.0
[Switch-Vlan-interface2] quit
```

ユーザラインの認証モードを AAA に設定します。

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

ローカル装置管理ユーザ **client001** を作成します。

```
[Switch] local-user client001 class manage
```

ユーザのプレーンテキストのパスワードを **aabbcc**、サービスタイプを **ssh** に設定します。

```
[Switch-luser-manage-client001] password simple aabbcc
[Switch-luser-manage-client001] service-type ssh
```

ユーザにユーザロールを **network-admin** に割り当てます。

```
[Switch-luser-manage-client001] authorization-attribute user-role network-admin
[Switch-luser-manage-client001] quit
```

SSH ユーザ **client001** を作成します。ユーザのサービスタイプを **stelnet**、認証方式を **password** に設定します。SSH ユーザが作成されていない場合、デフォルトでパスワード認証が使用されます。

```
[Switch] ssh user client001 service-type stelnet authentication-type password
```

2)　Stelnet サーバとの接続を確立します。

Stelnet クライアントのソフトウェアは、PuTTY、OpenSSH など異なるタイプがあります。この例では PuTTY バージョン 0.58 を Stelnet クライアントとして使用します。

Stelnet サーバとの接続を確立します。

a)　図 7-2に示すようにPuTTY.exeを起動させ、インタフェースを入力します。

b)　**Host Name**フィールド（あるいは**IP address**）で、StelnetサーバのIPアドレス192.168.1.40を入力します。

c)　**Open**をクリックします。

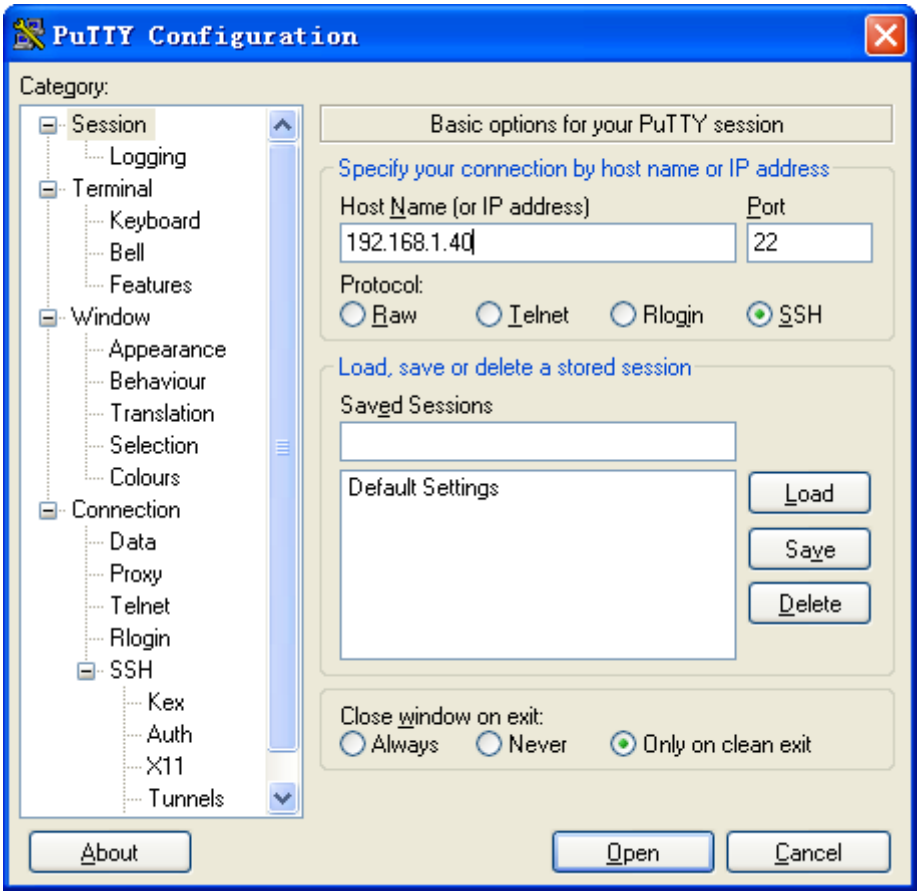


図 7-2 ホスト名（あるいは IP アドレス）の指定

d)　ユーザ名（この例では**client001**）とパスワード（この例では**aabbcc**）を入力してサーバにログインします。

7.6.2 公開鍵認証を有効にした Stelnet サーバの設定例

I. ネットワーク要件

図 7-3に示すように設定します。

- スイッチは Stelnet サーバとして動作し、パスワード認証と RSA 公開鍵アルゴリズムを使用します。

- ホストは Stelnet クライアントとして動作し、Stelnet クライアントソフトウェア（SSH2）を使用します。ホストのユーザが Stelnet を通じてスイッチにログインした後、ユーザは network-administrator としてスイッチを管理できます。

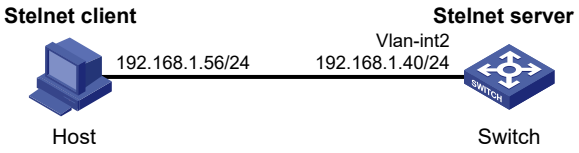


図 7-3 ネットワーク図

II. 設定手順

サーバの設定では、クライアントのホスト公開鍵が必要となります。Stelnet サーバを設定する前に、クライアントで RSA 鍵ペアを作成するため、クライアントソフトウェアを使用します。

Stelnet クライアントのソフトウェアは、PuTTY、OpenSSH など異なるタイプがあります。この例では PuTTY バージョン 0.58 を Stelnet クライアントとして使用します。

設定手順を以下に示します。

1) Stelnet クライアントで RSA 鍵ペアを作成します。

a) クライアントでPuTTY.exeを起動させ、SSH-2 RSAを選択し、Generateをクリックします。

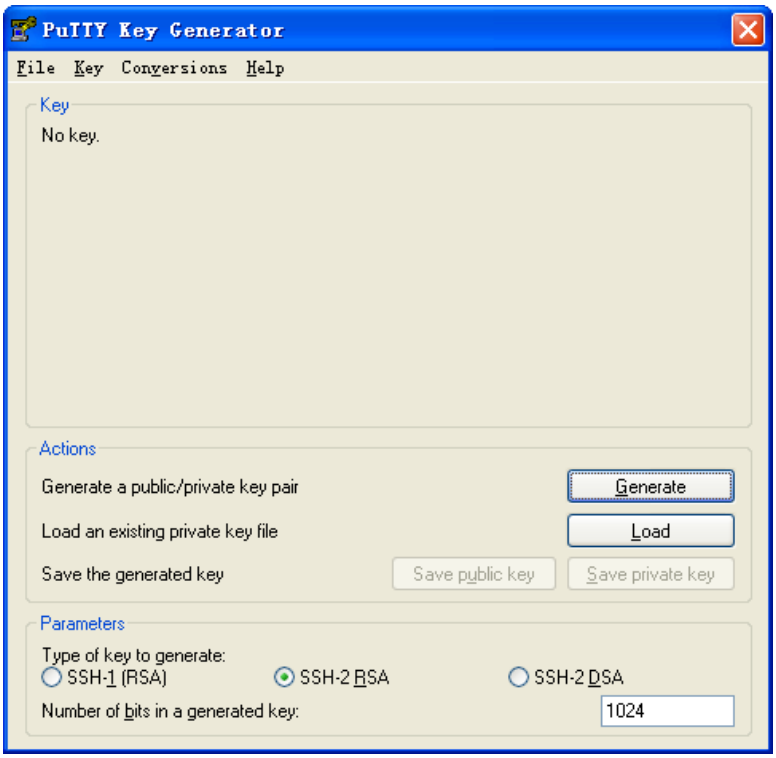


図 7-4 クライアントの鍵ペアの作成

b)　鍵ペアを作成している場合、マウスを継続して動かしてください。図 7-5に示すように、緑の進捗バーの上にマウスを置かないでください。そうでない場合、進捗バーが動作をストップしてしまい、鍵ペアの作成をとめてしまいます。

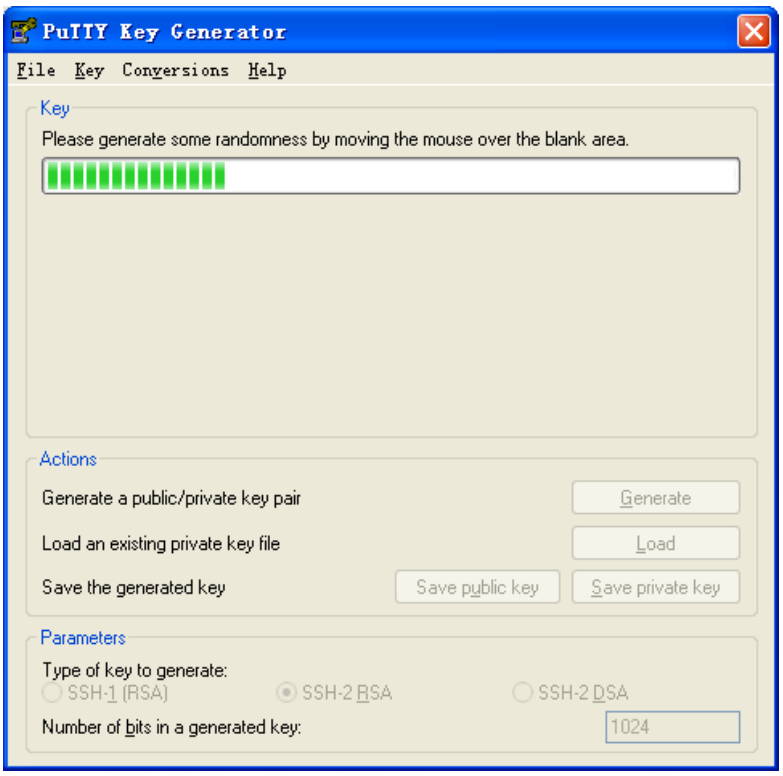


図 7-5 プロセスの作成

c)　鍵ペアが作成された後、**Save public key**をクリックし、ファイル名**key.pub**を入力し、**Save**をクリックします。ファイルの保存ウィンドウ画面が表示されます。

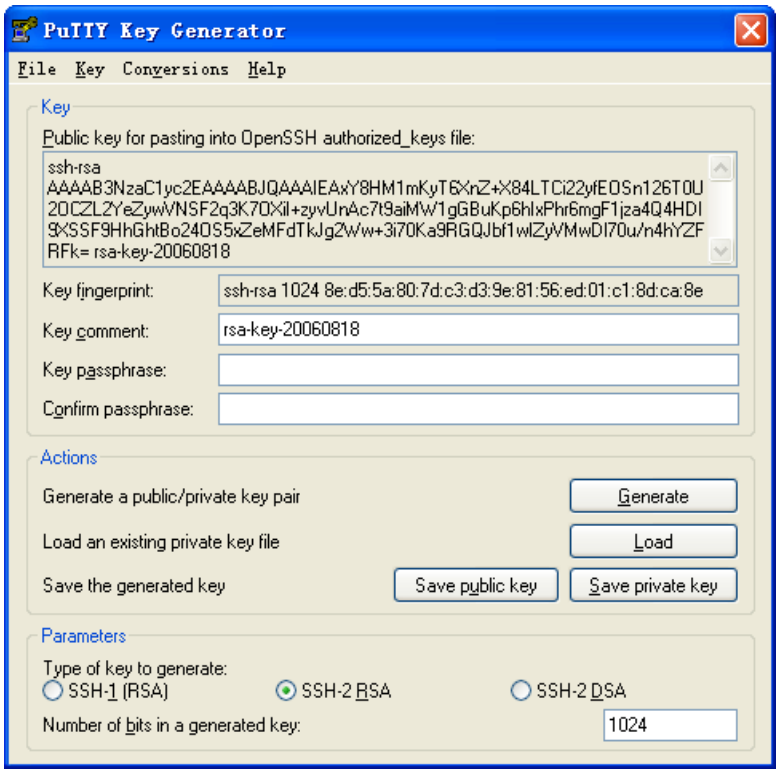


図 7-6 クライアントの鍵ペアの保存

d) ファイル名（この例では**key.pub**）を入力し、**Save**をクリックします。

e) 図 7-6に示すページで、秘密鍵を保存するため、**Save private key**をクリックします。確認ダイアログボックスが表示されます。

f) **Yes**をクリックします。ファイルの保存ウィンドウが表示されます。

g) ファイル名（この例では**private.ppk**）を入力し、**Save**をクリックします。

h) FTPあるいはTFTPを使用してサーバに公開鍵ファイルを転送します。（詳細は省略します）

2) Stelnet サーバを設定します。

RSA 鍵ペアを作成します。

<Switch> system-view

[Switch] public-key local create rsa

```
The range of public key modulus is (512 ~ 4096).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.....................++++++
.................++++++
..++++++++
............++++++++
Create the key pair successfully.
```

DSA 鍵ペアを作成します。

```
[Switch] public-key local create dsa
The range of public key modules is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.++++++++++++++++++++++++++++++++++++++++++++++++*
........+......+.....+.....................................+
...+................+.........+...+
Create the key pair successfully.
```

SSH サーバ機能を有効にします。

```
[Switch] ssh server enable
```

VLAN インタフェース 2 に IP アドレスを割り当てます。SSH 接続の宛先アドレスとして Stelnet クライアントは VLAN インタフェース 2 の IP アドレスを使用します。

```
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ip address 192.168.1.40 255.255.255.0
[Switch-Vlan-interface2] quit
```

ユーザラインの認証モードを AAA に設定します。

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

ファイル **key.pub** からクライアントの公開鍵をインポートし、名前を **switchkey** とします。

```
[Switch] public-key peer switchkey import sshkey key.pub
```

SSH ユーザ **client002** を作成します。ユーザの認証方式を公開鍵に指定します。公開鍵 **switchkey** をユーザに割り当てます。

```
[Switch] ssh user client002 service-type stelnet authentication-type publickey assign publickey switchkey
```

ローカル装置管理ユーザ **client002** を作成します。ユーザのサービスタイプを **ssh**、ユーザロールを **network-admin** に設定します。

```
[Switch] local-user client002 class manage
[Switch-luser-manage-client002] service-type ssh
[Switch-luser-manage-client002] authorization-attribute user-role network-admin
[Switch-luser-manage-client002] quit
```

3) 秘密鍵ファイルを指定し、Stelnet サーバとの接続を確立します。

a) 図 7-7に示すようにStelnetクライアントでPuTTY.exeを起動させ、インタフェースに移行します。

b) **Host Name**フィールド（あるいは**IP address**）で、StelnetサーバのIPアドレス

192.168.1.40を入力します。

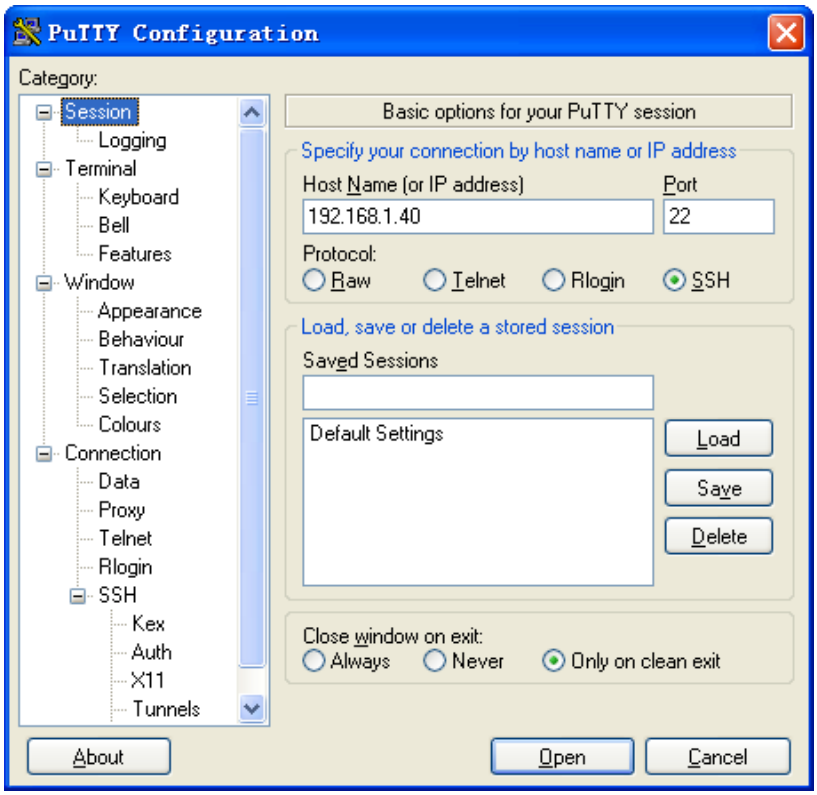


図 7-7 ホスト名（あるいは IP アドレス）の指定

c) ナビゲーションツリーから**Connection**を選択し、**SSH**を選択します。図 7-8に示すようにウィンドウ画面が表示されます。

d) **Protocol options**の**Preferred SSH protocol version**で**2**を選択します。

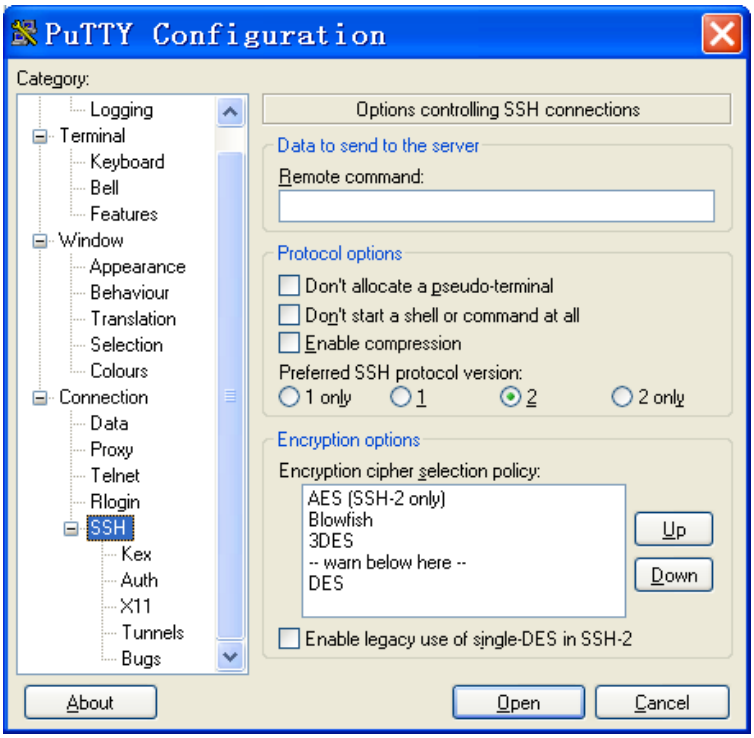


図 7-8 SSH バージョンの指定

e) ナビゲーションツリーから**Connection**を選択し、**SSH**を選択し、**Auth**を選択します。図 7-9に示すようにウィンドウ画面が表示されます。

f) ファイル選択画面から**Browse**をクリックし、秘密鍵ファイル（この例では**private.ppk**）を選択し、**OK**をクリックします。

g) **Open**をクリックします。

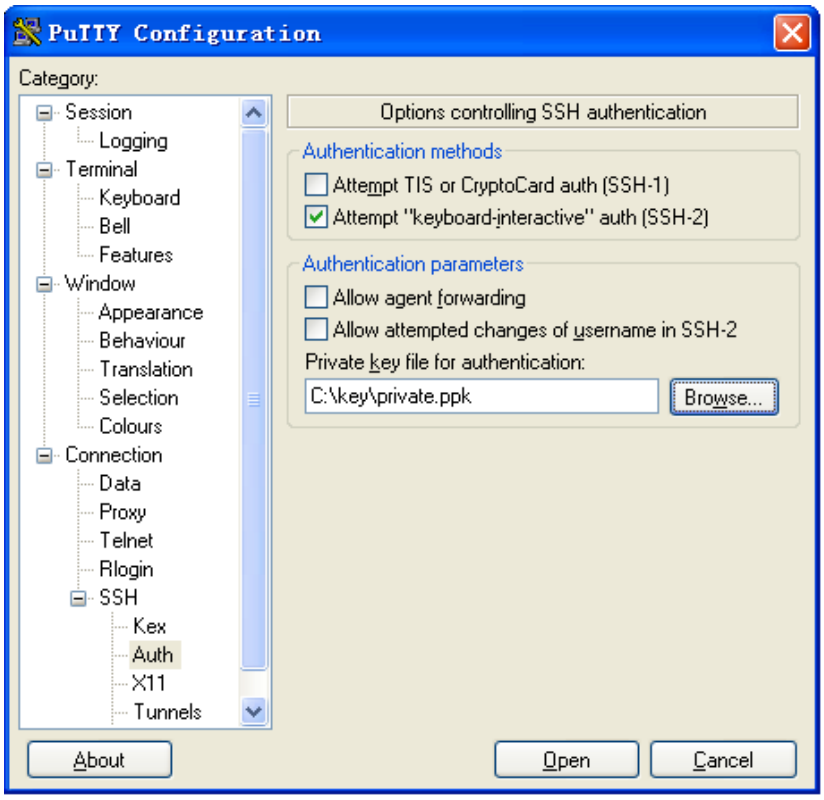


図 7-9 秘密鍵ファイルの指定

h)　ユーザ名を**client002**と入力し、Stelnetサーバにログインします。

7.6.3 パスワード認証を有効にした Stelnet クライアント設定例

I. ネットワーク要件

図 7-10に示すように設定します。

- スイッチ B は Stelnet サーバとして動作し、Stelnet クライアントを認証するためにパスワード認証を使用します。クライアントのユーザ名とパスワードはスイッチ B に保存されます。
- スイッチ A は Stelnet クライアントとして動作します。スイッチ A のユーザが Stelnet を通じてスイッチ B にログインした後、ユーザは network-administrator としてスイッチ B を管理することができます。

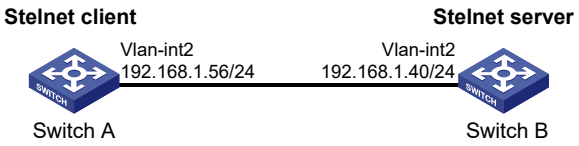


図 7-10 ネットワーク図

II. 設定手順

1)　Stelnet サーバを設定します。

RSA 鍵ペアを作成します。

```
<SwitchB> system-view
[SwitchB] public-key local create rsa
The range of public key modulus is (512 ~ 4096).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.....................++++++
.....................++++++
..++++++++
............++++++++
Create the key pair successfully.
```

DSA 鍵ペアを作成します。

```
[SwitchB] public-key local create dsa
The range of public key modules is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.++++++++++++++++++++++++++++++++++++++++++++++++*
........+......+.....+.....................................+
...+.................+.........+...+
Create the key pair successfully.
```

SSH サーバ機能を有効にします。

```
[SwitchB] ssh server enable
```

VLAN インタフェース 2 に IP アドレスを割り当てます。SSH 接続の宛先アドレスとして Stelnet クライアントは VLAN インタフェース 2 の IP アドレスを使用します。

```
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] ip address 192.168.1.40 255.255.255.0
[SwitchB-Vlan-interface2] quit
```

ユーザラインの認証モードを AAA に設定します。

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

ローカル装置管理ユーザ **client001** を作成します。

```
[SwitchB] local-user client001 class manage
```

ユーザのプレーンテキストのパスワードを **aabbcc**、サービスタイプを **ssh** に指定します。

```
[SwitchB-luser-manage-client001] password simple aabbcc
[SwitchB-luser-manage-client001] service-type ssh
```

ユーザのユーザロールを **network-admin** と設定します。

```
[SwitchB-luser-manage-client001] authorization-attribute user-role network-admin
[SwitchB-luser-manage-client001] quit
```

SSH ユーザ **client001** を作成します。ユーザのサービスタイプを **stelnet**、認証方式を **password** に設定します。SSH ユーザが作成されていない場合、デフォルトでパスワード認証が使用されます。

```
[SwitchB] ssh user client001 service-type stelnet authentication-type password
```

2)　Stelnet サーバ 192.168.1.40 との接続を確立します。

VLAN インタフェース 2 に IP アドレスを割り当てます。

```
<SwitchA> system-view
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ip address 192.168.1.56 255.255.255.0
[SwitchA-Vlan-interface2] quit
[SwitchA] quit
```

サーバとの接続を確立する前に、クライアントでサーバのホスト公開鍵を設定するかどうかを決定することができます。

- クライアントでサーバのホスト公開鍵を設定する場合、以下の作業を行います。

サーバのホスト公開鍵を表示するため、サーバで **display public-key local dsa public** コマンドを使用します。（詳細は省略します。）

クライアントの public key view に移行し、サーバのホスト公開鍵をクライアントにコピーします。

```
[SwitchA] public-key peer key1
```

public key view に移行します。**peer-public-key end** コマンドで system view に戻ります。

```
[SwitchA-pkey-public-key-key1]308201B73082012C06072A8648CE3804013082011F028
18100D757262C4584C44C211F18BD96E5F0
[SwitchA-pkey-public-key-key1]61C4F0A423F7FE6B6B85B34CEF72CE14A0D3A5222F
```

```
E08CECE65BE6C265854889DC1EDBD13EC8B274
[SwitchA-pkey-public-key-key1]DA9F75BA26CCB987723602787E922BA84421F22C3C8
9CB9B06FD60FE01941DDD77FE6B12893DA76E
[SwitchA-pkey-public-key-key1]EBC1D128D97F0678D7722B5341C8506F358214B16A2
FAC4B368950387811C7DA33021500C773218C
[SwitchA-pkey-public-key-key1]94184CCDFCEAE96EC4D5EF93133E84B47093C52B20
CD35D02492B3959EC6499625BC4FA5082E22C5
[SwitchA-pkey-public-key-key1]B374E16DD00132CE71B020217091AC717B612391C76
C1FB2E88317C1BD8171D41ECB83E210C03CC9
[SwitchA-pkey-public-key-key1]B32E810561C21621C73D6DAAC028F4B1585DA7F4251
9718CC9B09EEF0381840002818000AF995917
[SwitchA-pkey-public-key-key1]E1E570A3F6B1C2411948B3B4FFA256699B3BF871221
CC9C5DF257523777D033BEE77FC378145F2AD
[SwitchA-pkey-public-key-key1]D716D7DB9FCABB4ADBF6FB4FDB0CA25C761B308EF
53009F7101F7C62621216D5A572C379A32AC290
[SwitchA-pkey-public-key-key1]E55B394A217DA38B65B77F0185C8DB8095522D1EF04
4B465E8716261214A5A3B493E866991113B2D
[SwitchA-pkey-public-key-key1]485348
[SwitchA-pkey-public-key-key1] peer-public-key end
[SwitchA] quit
```

サーバへの SSH 接続を確立し、サーバのホスト公開鍵を指定します。

```
<SwitchA> ssh2 192.168.1.40 public-key key1
Username: client001
Press CTRL+C to abort.
Connecting to 192.168.1.40 port 22.
client001@192.168.1.40's password:
Enter a character ~ and a dot to abort.
<SwitchB>
```

正しいパスワードを入力した後、Switch B にログインすることができます。

- クライアントにサーバのホスト公開鍵がない場合、システムはサーバにアクセスする場合、アクセスを継続するかどうか確認する画面を表示します。サーバにアクセスするため、**Yes** を選択し、サーバのホスト公開鍵をダウンロードします。

```
<SwitchA> ssh2 192.168.1.40
Username: client001
Press CTRL+C to abort.
Connecting to 192.168.1.40 port 22.
The server is not authenticated. Continue? [Y/N]:y
Do you want to save the server public key? [Y/N]:y
client001@192.168.1.40's password:
Enter a character ~ and a dot to abort.
<SwitchB>
```

正しいパスワードを入力した後、Switch B にログインすることができます。サーバのホスト公開鍵はクライアントに保存されます。次回接続を行う場合、システムはサーバに認証するかどうか確認する画面を表示しません。

7.6.4 公開鍵認証を有効にした Stelnet クライアント設定例

I. ネットワーク要件

図 7-11に示すように設定します。

- スイッチ B は Stelnet サーバとして動作し、公開鍵認証と DSA 公開鍵アルゴリズムを使用します。
- スイッチ A は Stelnet クライアントとして動作します。スイッチ A のユーザが Stelnet を通じてスイッチ B にログインした後、ユーザは network-administrator としてスイッチ B を管理することができます。

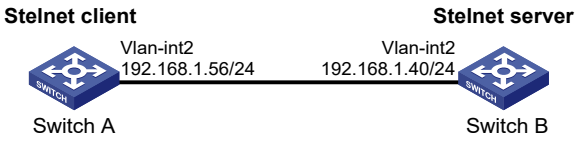


図 7-11 ネットワーク図

II. 設定手順

サーバの設定ではクライアント公開鍵が必要となります。Stelnetサーバを設定する前に、クライアントで DSA 鍵ペアを作成するためにクライアントソフトウェアを使用します。

1)　Stelnet クライアントを設定します。

VLAN インタフェース 2 に IP アドレスを割り当てます。

```
<SwitchA> system-view
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ip address 192.168.1.56 255.255.255.0
[SwitchA-Vlan-interface2] quit
```

DSA 鍵ペアを作成します。

```
[SwitchA] public-key local create dsa
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.++++++++++++++++++++++++++++++++++++++++++++++++++*
........+......+.....+.....................................+
...+.................+..........+...+
Create the key pair successfully.
```

DSA ホスト公開鍵をファイル **key.pub** にエクスポートします。

```
[SwitchA] public-key local export dsa ssh2 key.pub
[SwitchA] quit
```

FTP あるいは TFTP を使用して、サーバに公開鍵ファイル **key.pub** を転送します。（詳細は省略します）

2)　Stelnet サーバを設定します。

RSA 鍵ペアを作成します。

```
<SwitchB> system-view
[SwitchB] public-key local create rsa
The range of public key modulus is (512 ~ 4096)
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.....................++++++
.................++++++
..++++++++
............++++++++
Create the key pair successfully.
```

DSA 鍵ペアを作成します。

```
[SwitchB] public-key local create dsa
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.++++++++++++++++++++++++++++++++++++++++++++++++*
........+......+.....+.................................+
...+.................+..........+...+
Create the key pair successfully.
```

SSH サーバ機能を有効にします。

```
[SwitchB] ssh server enable
```

VLAN インタフェース 2 に IP アドレスを割り当てます。SSH 接続の宛先アドレスとして Stelnet クライアントは VLAN インタフェース 2 の IP アドレスを使用します。

```
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] ip address 192.168.1.40 255.255.255.0
[SwitchB-Vlan-interface2] quit
```

ユーザラインの認証モードを AAA に設定します。

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

ファイル **key.pub** からピアの公開鍵をインポートし、名前を **switchkey** とします。

```
[SwitchB] public-key peer switchkey import sshkey key.pub
```

ローカル装置管理ユーザ **client002** を作成します。ユーザの認証方式を公開鍵に指定します。ユーザに公開鍵 **switchkey** を割り当てます。

```
[SwitchB] ssh user client002 service-type stelnet authentication-type publickey assign publickey switchkey
```

ローカル装置管理ユーザ **client002** を作成します。ユーザのサービスタイプを SSH に指定します。ユーザにユーザロール **network-admin** を割り当てます。

```
[SwitchB] local-user client002 class manage
[SwitchB-luser-manage-client002] service-type ssh
[SwitchB-luser-manage-client002] authorization-attribute user-role network-admin
[SwitchB-luser-manage-client002] quit
```

3)　Stelnet サーバ 192.168.1.40 に SSH 接続を確立します。

```
<SwitchA> ssh2 192.168.1.40 identity-key dsa
Username: client002
Press CTRL+C to abort.
Connecting to 192.168.1.40 port 22.
The server is not authenticated. Continue? [Y/N]:y
Do you want to save the server public key? [Y/N]:n
Enter a character ~ and a dot to abort.
<SwitchB>
```

サーバにアクセスするため **Yes** を選択し、サーバのホスト公開鍵をダウンロードします。次回接続を行う場合、クライアントはクライアントで保存されたサーバのホスト公開鍵を使用してサーバを認証します。

7.7 SFTP設定例

7.7.1 パスワード認証を有効にした SFTP サーバの設定例

I. ネットワーク要件

図 7-12に示すように設定します。

- SFTP サーバとしてスイッチが動作し、SFTP クライアントを認証するためにパスワード認証を使用します。クライアントのユーザ名とパスワードはスイッチに保存されます。
- ホストは SFTP クライアントとして動作します。クライアントのユーザが SFTP を通じてスイッチにログインした後、ユーザは network-administrator としてスイッチの設定や管理をすることができます。

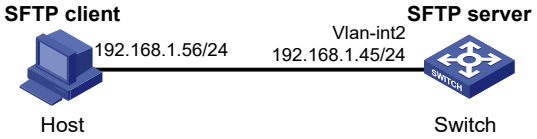


図 7-12 ネットワーク図

II. 設定手順

1)　SFTP サーバを設定します。

RSA 鍵ペアを作成します。

```
<Switch> system-view
[Switch] public-key local create rsa
The range of public key modulus is (512 ~ 4096).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.....................++++++
.................++++++
..++++++++
............++++++++
Create the key pair successfully.
```

DSA 鍵ペアを作成します。

```
[Switch] public-key local create dsa
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.++++++++++++++++++++++++++++++++++++++++++++++++*
........+......+.....+.................................+
...+................+.........+...+
Create the key pair successfully.
```

SFTP サーバ機能を有効にします。

```
[Switch] sftp server enable
```

VLAN インタフェース 2 に IP アドレスを割り当てます。SFTP クライアントは SSH 接続用の宛先アドレスとして VLAN インタフェース 2 の IP アドレスを使用します。

```
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ip address 192.168.1.45 255.255.255.0
[Switch-Vlan-interface2] quit
```

ローカル装置管理ユーザ **client002** を作成します。プレーンテキストのパスワードを **aabbcc** とし、サービスタイプを **ssh** とします。ユーザにユーザロール **network-admin** を割り当て、作業ディレクトリを **flash:/**に設定します。

```
[Switch] local-user client002 class manage
[Switch-luser-manage-client002] password simple aabbcc
[Switch-luser-manage-client002] service-type ssh
[Switch-luser-manage-client002] authorization-attribute user-role network-admin work-directory flash:/
[Switch-luser-manage-client002] quit
```

ローカル装置管理ユーザ **client002** を作成します。ユーザの認証モードを **password**、サービスタイプを **sftp** に設定します。SSH ユーザが作成されていない場合、デフォルトでパスワード認証が使用されます。

```
[Switch] ssh user client002 service-type sftp authentication-type password
```

2)　SFTP クライアントとサーバ間の接続を確立します。

装置は SFTP クライアントソフトウェアの異なるタイプをサポートします。この例では PuTTY バージョン 0.58 の PSFTP を動作させる SFTP クライアントを使用します。

SFTP サーバへの接続を確立するために、以下を行います。

a)　図 7-13に示すようにクライアントインタフェースを起動させるため、**psftp.exe**を動作させ、以下のコマンドを入力します。

open 192.168.1.45

b)　SFTPサーバにログインするため、ユーザ名**client002**、パスワード**aabbcc**を入力します。

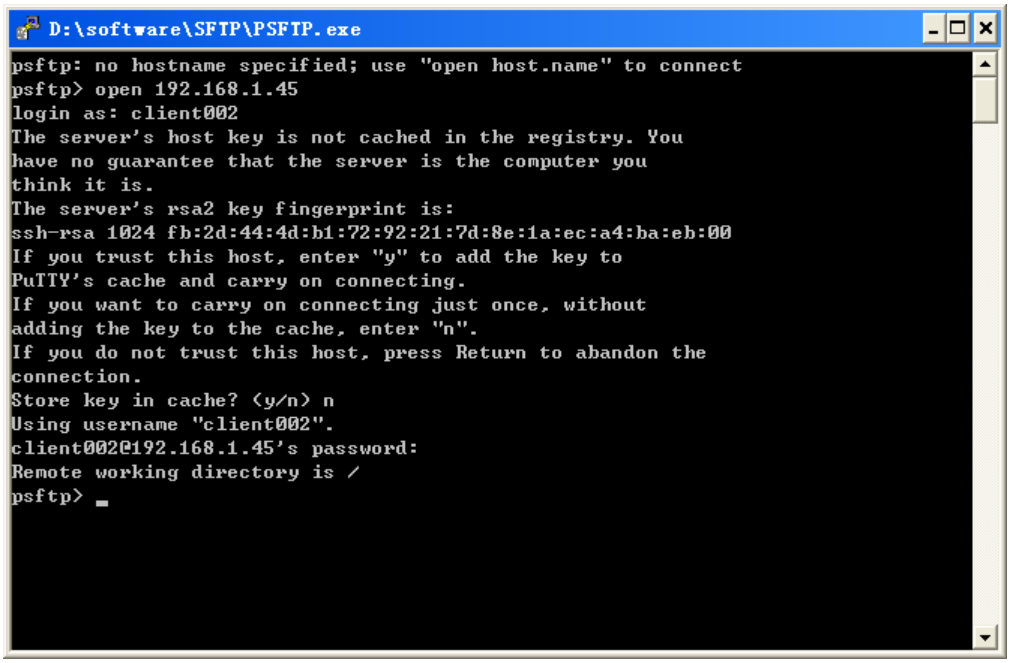


図 7-13 SFTP クライアントインタフェース

7.7.2 公開鍵認証を有効にした SFTP クライアント設定例

I. ネットワーク要件

図 7-14に示すように設定します。

- SFTP サーバとしてスイッチ B が動作し、公開鍵認証、RSA 公開鍵アルゴリズムを使用します。
- スイッチ A は SFTP クライアントとして動作します。スイッチ A のユーザが SFTP を通じてスイッチにログインした後、ユーザは network-administrator としてスイッチ B でファイルの管理ができます。

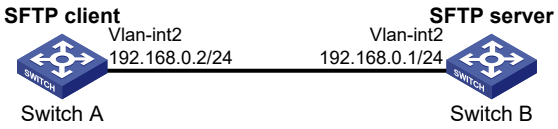


図 7-14 ネットワーク図

II. 設定手順

サーバの設定では、クライアントのホスト公開鍵が必要です。SFTP サーバを設定する前に、クライアントの RSA 鍵ペアを作成するため、クライアントソフトウェアを使用します。

1)　SFTP クライアントを設定します。

VLAN インタフェース 2 に IP アドレスを設定します。

```
<SwitchA> system-view
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ip address 192.168.0.2 255.255.255.0
[SwitchA-Vlan-interface2] quit
```

RSA 鍵ペアを作成します。

```
[SwitchA] public-key local create rsa
The range of public key size is (512 ~ 4096).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.....................++++++
.................++++++
..++++++++
............++++++++
Create the key pair successfully.
```

ホスト公開鍵をファイル **pubkey** にエクスポートします。

```
[SwitchA] public-key local export rsa ssh2 pubkey
[SwitchA] quit
```

公開鍵ファイル **pubkey** を FTP あるいは TFTP を使用してサーバに転送します。（詳細は省略します）

2)　SFTP サーバを設定します。

RSA 鍵ペアを作成します。

```
<SwitchB> system-view
[SwitchB] public-key local create rsa
The range of public key size is (512 ~ 4096).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.....................++++++
...................++++++
..++++++++
............++++++++
Create the key pair successfully.
```

DSA 鍵ペアを作成します。

```
[SwitchB] public-key local create dsa
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.++++++++++++++++++++++++++++++++++++++++++++++++*
........+......+.....+.................................+
...+.................+.........+...+
Create the key pair successfully.
```

SFTP サーバ機能を有効にします。

```
[SwitchB] sftp server enable
```

VLAN インタフェース 2 に IP アドレスを割り当てます。SFTP クライアントは SSH 接続用の宛先アドレスとして VLAN インタフェース 2 の IP アドレスを使用します。

```
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] ip address 192.168.0.1 255.255.255.0
[SwitchB-Vlan-interface2] quit
```

ファイルからピアの公開鍵 **pubkey** をインポートし、名前を **switchkey** とします。

```
[SwitchB] public-key peer switchkey import sshkey pubkey
```

SSH ユーザ **client001** を作成し、サービスタイプを **sftp** とし、認証方式を **publickey** とし、公開鍵を **switchkey** と設定します。

```
[SwitchB] ssh user client001 service-type sftp authentication-type publickey assign publickey switchkey
```

ローカル装置管理ユーザ **client001** を作成します。

```
[SwitchB] local-user client001 class manage
```

ユーザのサービスタイプを **ssh** に指定します。

```
[SwitchB-luser-manage-client001] service-type ssh
```

ユーザにユーザロール **network-admin** を割り当て、作業ディレクトリを **flash:/**に設定します。

```
[SwitchB-luser-manage-client001] authorization-attribute user-role network-admin work-directory flash:/

[SwitchB-luser-manage-client001] quit
```

3)　SFTP クライアントとの接続を確立します。

SFTP サーバと接続を確立し、SFTP client view に移行します。

```
<SwitchA> sftp 192.168.0.1 identity-key rsa
Username: client001
Press CTRL+C to abort.
Connecting to 192.168.0.1 port 22.
The server is not authenticated. Continue? [Y/N]:y
Do you want to save the server public key? [Y/N]:n
sftp>
```

サーバで現在の作業ディレクトリのファイルを表示し、ファイル名 **z** を削除し、正常に削除されているか確認します。

```
sftp> dir -l
-rwxrwxrwx   1 noone    nogroup      1759 Aug 23 06:52 config.cfg
-rwxrwxrwx   1 noone    nogroup       225 Aug 24 08:01 pubkey2
-rwxrwxrwx   1 noone    nogroup       283 Aug 24 07:39 pubkey
drwxrwxrwx   1 noone    nogroup         0 Sep 01 06:22 new
-rwxrwxrwx   1 noone    nogroup       225 Sep 01 06:55 pub
-rwxrwxrwx   1 noone    nogroup         0 Sep 01 08:00 z
sftp> delete z
Removing /z
sftp> dir -l
-rwxrwxrwx   1 noone    nogroup      1759 Aug 23 06:52 config.cfg
-rwxrwxrwx   1 noone    nogroup       225 Aug 24 08:01 pubkey2
-rwxrwxrwx   1 noone    nogroup       283 Aug 24 07:39 pubkey
drwxrwxrwx   1 noone    nogroup         0 Sep 01 06:22 new
-rwxrwxrwx   1 noone    nogroup       225 Sep 01 06:55 pub
```

ディレクトリ名 **new1** を追加し、正常に作成されているか確認します。

```
sftp> mkdir new1
sftp> dir -l
-rwxrwxrwx   1 noone    nogroup      1759 Aug 23 06:52 config.cfg
-rwxrwxrwx   1 noone    nogroup       225 Aug 24 08:01 pubkey2
-rwxrwxrwx   1 noone    nogroup       283 Aug 24 07:39 pubkey
drwxrwxrwx   1 noone    nogroup         0 Sep 01 06:22 new
-rwxrwxrwx   1 noone    nogroup       225 Sep 01 06:55 pub
drwxrwxrwx   1 noone    nogroup         0 Sep 02 06:30 new1
```

ディレクトリ **new1** を **new2** に名前を変換し、正常に変更されていることを確認します。

```
sftp> rename new1 new2

sftp> dir -l
-rwxrwxrwx   1 noone    nogroup      1759 Aug 23 06:52 config.cfg
-rwxrwxrwx   1 noone    nogroup       225 Aug 24 08:01 pubkey2
-rwxrwxrwx   1 noone    nogroup       283 Aug 24 07:39 pubkey
drwxrwxrwx   1 noone    nogroup         0 Sep 01 06:22 new
-rwxrwxrwx   1 noone    nogroup       225 Sep 01 06:55 pub
drwxrwxrwx   1 noone    nogroup         0 Sep 02 06:33 new2
```

サーバからファイル **pubkey2** をダウンロードし、ローカルファイル **public** として保存します。

```
sftp> get pubkey2 public
Fetching / pubkey2 to public
/pubkey2                                      100% 225     1.4KB/s   00:00
```

ローカルファイル **pu** をサーバにアップロードし、**puk** として保存し、正常にアップロードされていることを確認します。

```
sftp> put pu puk
Uploading pu to / puk

sftp> dir -l
-rwxrwxrwx   1 noone    nogroup      1759 Aug 23 06:52 config.cfg
-rwxrwxrwx   1 noone    nogroup       225 Aug 24 08:01 pubkey2
-rwxrwxrwx   1 noone    nogroup       283 Aug 24 07:39 pubkey
drwxrwxrwx   1 noone    nogroup         0 Sep 01 06:22 new
drwxrwxrwx   1 noone    nogroup         0 Sep 02 06:33 new2
-rwxrwxrwx   1 noone    nogroup       283 Sep 02 06:35 pub
-rwxrwxrwx   1 noone    nogroup       283 Sep 02 06:36 puk
sftp>
```

SFTP client view から戻ります。

```
sftp> quit
<SwitchA>
```

目次

このセクションのページは **7-x-x** です。

8 章 IP ソースガード 8-1
8.1 概要 8-1
8.1.1 スタティック IP ソースガードバインディングエントリ 8-2
8.1.2 ダイナミック IP ソースバインディングエントリ 8-2
8.2 IP ソースガード設定作業リスト 8-3
8.3 IPv4 ソースガード機能の設定 8-3
8.3.1 IPv4 ソースガード機能の有効化 8-3
8.3.2 スタティック IPv4 ソースガードバインディングエントリの設定 8-4
8.4 IPv6 ソースガード機能の設定 8-5
8.4.1 IPv6 ソースガード機能の有効化 8-5
8.4.2 スタティック IPv6 ソースガードバインディングエントリの設定 8-5
8.5 IP ソースガードの表示と維持 8-6
8.6 IP ソースガードの設定例 8-6
8.6.1 スタティック IPv4 ソースガードの設定例 8-6
8.6.2 DHCP snooping を使用したダイナミック IPv4 ソースガードの設定例 8-8
8.6.3 スタティック IPv6 ソースガード設定例 8-10

8章 IP ソースガード

8.1 概要

IP ソースガード（IPSG）は、正式なパケットに一致させている IP ソースガードバインディングテーブルを使用して、なりすまし攻撃を防止します。IP ソースガードはテーブルに一致しないすべてのパケットを廃棄します。IP ソースガードはインタフェースごとのパケットフィルタです。ひとつのインタフェースに機能設定しても別のインタフェースのパケット転送には影響しません。

IP ソースガードバインディングテーブルは、グローバルとインタフェース指定バインディングを含むことができます。IP ソースガードは、最初にパケットの適合のためにインタフェース指定バインディングを使用します。適合しなかった場合、IP ソースガードはグローバルバインディングを使用します。IP ソースガードバインディングは以下のタイプに分かれます。

- IP-interface バインディングエントリ
- MAC-interface バインディングエントリ
- IP-MAC-interface バインディングエントリ
- IP-VLAN-interface バインディングエントリ
- MAC-VLAN-interface バインディングエントリ
- IP-MAC-VLAN-interface バインディングエントリ

IP ソースガードのバインディングエントリは手動で設定されたスタティックバインディングエントリと他のモジュールからの情報をもとに作成されたダイナミックバインディングエントリがあります。

図 8-1に示すように、インタフェースの IP ソースガードは IP ソースガードバインディングエントリの 1 つに一致するパケットのみ転送します。

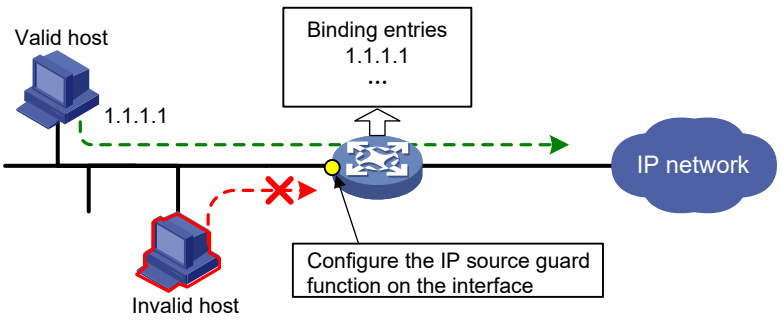


図 8-1 IP ソースガード機能のネットワーク図

🕮 **メモ：**

IP ソースガードはインタフェース毎にパケットをフィルタします。インタフェースで設定された IP ソースガード機能は他のインタフェースのパケットの転送には影響しません。

8.1.1 スタティック IP ソースガードバインディングエントリ

スタティックバインディングエントリは手動で設定されます。LAN 上に少数のホストしかなく、IP アドレスを手動で設定する場合に適しています。たとえば、サーバに接続するインタフェースでスタティック IP ソースガードバインディングエントリを設定することができます。このバインディングはサーバからのパケットのみ受信するインタフェースを許可します。

インタフェースの IP ソースガードバインディングは以下の機能をサポートします。

- インタフェースで受信する IPv4 パケットあるいは IPv6 をフィルタします。
- ユーザの妥当性を確認するため IPv4 パケットの ARP 検出機能と連携します。

ARP 検出についての詳細は、オペレーションマニュアルのセクション 7 *セキュリティ” ARP アタックプロテクション*”を参照してください。

スタティック IP ソースガードバインディングはインタフェースで有効です。IP ソースガードは最初にインタフェースで指定したバインディングを使用します。

- **指定インタフェースのスタティックバインディング**－interface view で IP アドレス、MAC アドレス、VLAN、あるいは IP アドレスと MAC アドレスと VLAN の組み合わせを割り当てます。バインディングはインタフェースにアクセスを試みるユーザの正当性を確認するため、インタフェースでのみ適用します。

🕮 **メモ：**

QX-S1100G シリーズはグローバルのスタティックバインディングをサポートしていません。

8.1.2 ダイナミック IP ソースバインディングエントリ

IP ソースガードはダイナミック IP ソースガードバインディングエントリを作成するため、他のモジュールからのユーザ情報を自動的に取得します。送信元モジュールは 802.1X、DHCP relay、DHCP snooping、DHCP server が含まれます。

DHCP ベースのダイナミック IP ソースガードバインディングは、LAN 上のホストが DHCP を通して IP アドレスを取得する場合に適しています。IP ソースガードは DHCP サーバ、DHCP snooping 装置で設定されます。DHCP サーバ、DHCP snooping エントリをもとにしてダイナミック IP ソースガードバインディングエントリを作成します。IP ソースガードは通過できるように DHCP クライアントからのパケットのみ許可します。

I. ダイナミック IPv4 ソースガード

異なる送信元モジュールをもとにして作成されたダイナミックバインディングエントリは使用方法が異なります。

インタフェースタイプ	送信元モジュール	バインディングエントリの使用方法
レイヤ2 Ethernetポート	DHCP snooping 802.1X ARP snooping	パケットフィルタリング
VLANインタフェース	DHCPサーバ	モジュール（たとえばARP検出機能モジュール）と連携するため、セキュリティサービスを提供します。

802.1X についての詳細は、オペレーションマニュアルのセクション *7 セキュリティ ” 802.1X*” を参照してください。DHCP snooping、DHCP server についての詳細は、オペレーションマニュアルのセクション 3 *IP サービス ” DHCP スヌーピング*”、”*DHCP サーバ*” を参照してください。

8.2 IPソースガード設定作業リスト

以下に IPv4 ソースガードを設定する作業リストを示します。

作業リスト
（必須設定項目）インタフェースのIPv4ソースガード機能の有効化
（オプション設定項目） スタティックIPv4ソースガードエントリの設定

以下に IPv6 ソースガードを設定する作業リストを示します。

作業リスト
（必須設定項目）インタフェースのIPv6ソースガード機能の有効化
（オプション設定項目） スタティックIPv6ソースガードエントリの設定

8.3 IPv4ソースガード機能の設定

8.3.1 IPv4 ソースガード機能の有効化

インタフェースで IP ソースガードを有効にする場合、スタティック IP ソースガード、ダイナミック IP ソースガードの両方が有効となります。

- スタティック IPv4 ソースガードは **ip source binding** コマンドを使用して設定されたスタティックバインディングを使用します。
- ダイナミック IPv4 ソースガードは関連する送信元モジュールからダイナミックバインディングを作成します。IPv4 ソースガードは **ip verify source** コマンドで指定された条件をもとにして受信 IPv4 パケットをフィルタするためバインディングを使用します。

ダイナミック IPv4 ソースガードを設定するために、802.1X、DHCP snooping あるいは DHCP relay 機能がネットワークで正常に動作することを確認してください。

以下にインタフェースで IPv4 ソースガード機能を有効にする設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． interface view に移行する	**interface** *interface-type interface-number*	サポートするインタフェースは以下です。 ● レイヤ2 Ethernetインタフェース ● VLANインタフェース
3． IPv4 ソースガード機能を有効にする	**ip verify source** { **ip-address** | **ip-address mac-address** | **mac-address** }	デフォルト：無効 このコマンドを複数行うと最後の設定が適用されます。

🕮 **メモ：**

ip verify source コマンドは運用前に設定しておくことを推奨します。DHCP snooping エントリが存在している場合に **ip verify source** コマンドを設定すると、一時的に通信が途切れる可能性があります。

8.3.2 スタティック IPv4 ソースガードバインディングエントリの設定

スタティック IPv4 ソースガードバインディングエントリはインタフェースでスタティック IPv4 ソースガードバインディングエントリを設定します。

I. インタフェースのスタティック IPv4 ソースガードバインディングエントリの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． interface view に移行する	**interface** *interface-type interface-number*	サポートするインタフェースは以下です。 ● レイヤ2 Ethernetインタフェース ● VLANインタフェース
3． スタティック IPv4 ソースガードバインディングエントリを設定する	**ip source binding** { **ip-address** *ip-address* | **ip-address** *ip-address* **mac-address** *mac-address* | **mac-address** *mac-address* } [**vlan** *vlan-id*]	デフォルト：設定なし **vlan** *vlan-id*オプションはLayer 2 Ethernet interface viewでのみサポートされます。 ARP検出機能のスタティックバインディングエントリを設定する場合、以下の設定を確認してください。 ● **ip-address** *ip-address*、**mac-address** *mac-address*、**vlan** *vlan-id*が設定されていること。 ● 指定のVLANでARP検出機能が有効になっていること。 複数のインタフェースに同じバインディングエントリを設定することができます。

8.4 IPv6ソースガード機能の設定

8.4.1 IPv6 ソースガード機能の有効化

インタフェースで IPv6 ソースガードを有効にする場合、スタティック IPv6 ソースガード、ダイナミック IPv6 ソースガードの両方が有効となります。

スタティック IPv6 ソースガードは **ipv6 source binding** コマンドを使用して設定されたスタティックバインディングを使用します。

以下にインタフェースで IPv6 ソースガード機能を有効にする設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． interface view に移行する	**interface** *interface-type interface-number*	サポートするインタフェースは以下です。 ● レイヤ2 Ethernetインタフェース ● VLANインタフェース
3． IPv6 ソースガード機能を有効にする	**ipv6 verify source** { **ip-address** | **ip-address mac-address** | **mac-address** }	デフォルト：無効 このコマンドを複数行うと最後の設定が適用されます。

8.4.2 スタティック IPv6 ソースガードバインディングエントリの設定

スタティック IPv6 ソースガードバインディングエントリはインタフェースでスタティック IPv6 ソースガードバインディングエントリを設定します。

I. インタフェースのスタティック IPv6 ソースガードバインディングエントリの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． interface view に移行する	**interface** *interface-type interface-number*	サポートするインタフェースは以下です。 ● レイヤ2 Ethernetインタフェース ● VLANインタフェース
3． スタティック IPv6 ソースガードバインディングエントリを設定する	**ipv6 source binding** { **ip-address** *ipv6-address* | **ip-address** *ipv6-address* **mac-address** *mac-address* | **mac-address** *mac-address* } [**vlan** *vlan-id*]	デフォルト：設定なし **vlan** *vlan-id*オプションはLayer 2 Ethernet interface viewでのみサポートします。 複数のインタフェースに同じバインディングエントリを設定することができます。

8.5 IPソースガードの表示と維持

すべての view で **display** コマンドを実行でき、user view で **reset** コマンドを実行できます。

以下に IPv4 ソースガードのコマンドを示します。

操作	コマンド
IPv4ソースガードバインディングエントリを表示する	**display ip source binding** [**static** | [**dhcp-relay** | **dhcp-server** | **dhcp-snooping**]] [**ip-address** *ip-address*] [**mac-address** *mac-address*] [**vlan** *vlan-id*] [**interface** *interface-type interface-number*] [**slot** *slot-number*]

以下に IPv6 ソースガードのコマンドを示します。

操作	コマンド
IPv6ソースガードバインディングエントリを表示する	**display ipv6 source binding** [**static**] [**ip-address** *ipv6-address*] [**mac-address** *mac-address*] [**vlan** *vlan-id*] [**interface** *interface-type interface-number*] [**slot** *slot-number*]

8.6 IPソースガードの設定例

8.6.1 スタティック IPv4 ソースガードの設定例

I. ネットワーク要件

図 8-2に示すように、すべてのホストはスタティック IP アドレスを使用しています。

以下の要件に適合するように Switch A と Switch B でスタティック IPv4 ソースガードバインディングエントリを設定します。

- Switch A の GigabitEthernet 1/0/2 は Host C からの IP パケットのみ許可します。
- Switch A の GigabitEthernet 1/0/1 は Host A からの IP パケットのみ許可します。
- Switch B のすべてのインタフェースは Host A からの IP パケットのみ許可します。
- Switch B の GigabitEthernet 1/0/1 は Host B からの IP パケットのみ許可します。

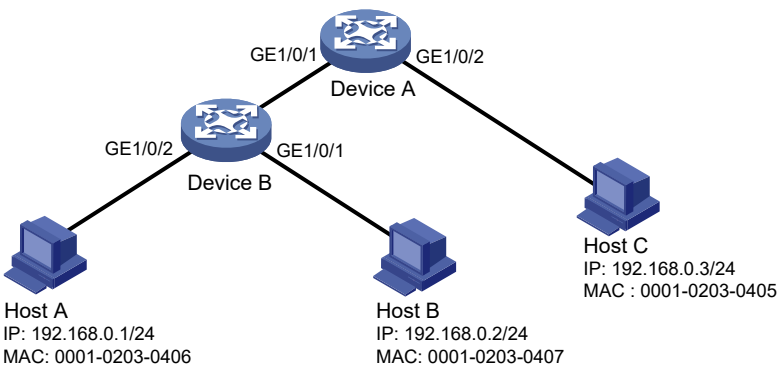


図 8-2 ネットワーク図

II. 設定手順

1)　Switch A を設定します。

インタフェースに IP アドレスを設定します。（詳細は省略します。）

GigabitEthernet 1/0/2 で IPv4 ソースガードを有効にします。

```
<SwitchA> system-view
[SwitchA] interface gigabitethernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] ip verify source ip-address mac-address
```

GigabitEthernet 1/0/2 で Host C のスタティック IPv4 ソースガードバインディングエントリを設定します。

```
[SwitchA-GigabitEthernet1/0/2] ip source binding ip-address 192.168.0.3 mac-address 0001-0203-0405
[SwitchA-GigabitEthernet1/0/2] quit
```

GigabitEthernet 1/0/1 で IPv4 ソースガードを有効にします。

```
[SwitchA] interface gigabitethernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] ip verify source ip-address mac-address
```

GigabitEthernet 1/0/1 で Host A のスタティック IPv4 ソースガードバインディングエントリを設定します。

```
[SwitchA-GigabitEthernet1/0/1] ip source binding ip-address 192.168.0.1 mac-address 0001-0203-0406
[SwitchA-GigabitEthernet1/0/1] quit
```

2)　Switch B を設定します。

インタフェースに IP アドレスを設定します。（詳細は省略します。）

GigabitEthernet 1/0/2 で IPv4 ソースガードを有効にします

```
<SwitchB> system-view
[SwitchB] interface gigabitethernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] ip verify source ip-address mac-address
[SwitchB-GigabitEthernet1/0/2] quit
```

Host A のスタティック IPv4 ソースガードバインディングエントリを設定します。

```
[SwitchB] ip source binding ip-address 192.168.0.1 mac-address 0001-0203-0406
```

GigabitEthernet 1/0/1 で IPv4 ソースガードを有効にします。

```
[SwitchB] interface gigabitethernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] ip verify source ip-address mac-address
```

GigabitEthernet 1/0/1 で Host B のスタティック IPv4 ソースガードバインディングエントリを設定します。

```
[SwitchB-GigabitEthernet1/0/1] ip source binding mac-address 0001-0203-0407
[SwitchB-GigabitEthernet1/0/1] quit
```

III. 設定の確認

Switch A でスタティック IPv4 ソースガードバインディングエントリが正しく設定されていることを確認します。

```
<SwitchA> display ip source binding static
Total entries found: 2
IP Address      MAC Address    Interface                VLAN Type
192.168.0.1     0001-0203-0405 GE1/0/2                  N/A  Static
192.168.0.3     0001-0203-0406 GE1/0/1                  N/A  Static
```

Switch B でスタティック IPv4 ソースガードバインディングエントリが正しく設定されていることを確認します。

```
<SwitchB> display ip source binding static
Total entries found: 2
IP Address      MAC Address    Interface              VLAN Type
192.168.0.1     0001-0203-0406 N/A                    N/A  Static
N/A             0001-0203-0407 GE1/0/1                N/A  Static
```

8.6.2 DHCP snooping を使用したダイナミック IPv4 ソースガードの設定例

I. ネットワーク要件

図 8-3に示すように、Host（DHCP クライアント）は DHCP サーバから IP アドレスを取得します。

DHCP snooping エントリにホストの IPv4 アドレスと MAC アドレスを記録するため、装置で DHCP snooping を有効にします。

DHCP snooping エントリをもとにして受信したパケットをフィルタするため、GigabitEthernet 1/0/1 でダイナミック IPv4 ソースガードを有効にします。DHCP サーバから IP アドレスを取得したクライアントからのパケットのみを許可するように、フィルタします。

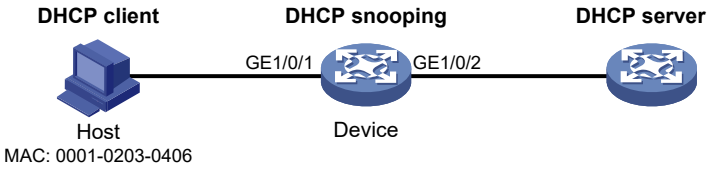


図 8-3 ネットワーク図

II. 設定手順

1)　DHCP サーバを設定します。

DHCP サーバの設定については、オペレーションマニュアルのセクション 3 *IP サービス" DHCP サーバ"* を参照してください。

2)　Switch を設定します。

インタフェースの IP アドレスを設定します。（詳細は省略します。）

DHCP snooping を有効にします。

```
<Switch> system-view
[Switch] dhcp snooping enable
```

トラステッドインタフェースとして GigabitEthernet 1/0/2 を設定します。

```
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] dhcp snooping trust
[Switch-GigabitEthernet1/0/2] quit
```

GigabitEthernet 1/0/1 で IPv4 ソースガードを有効にし、ダイナミック IP ソースガードの送信元 IP アドレスと送信元 MAC アドレスを確認します。

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] ip verify source ip-address mac-address
```

GigabitEthernet 1/0/1 で DHCP snooping エントリのクライアント情報を記録するように設定します。

```
[Switch-GigabitEthernet1/0/1] dhcp snooping binding record
[Switch-GigabitEthernet1/0/1] quit
```

III. 設定の確認

DHCP snooping から取得したダイナミック IPv4 ソースガードバインディングエントリを確認します。

```
[Switch] display ip source binding dhcp-snooping
Total entries found: 1
IP Address      MAC Address    Interface               VLAN Type
192.168.0.1     0001-0203-0406 GE1/0/1                 1    DHCP snooping
```

出力は、IP ソースガードに DHCP snooping エントリをもとにしたダイナミック IPv4 ソースガードバインディングエントリが作成されていることを示します。

8.6.3 スタティック IPv6 ソースガード設定例

I. ネットワーク要件

図 8-4に示すように、Hostからの IPv6パケットのみ許可するように装置の GigabitEthernet 1/0/1 のスタティック IPv6 ソースガードバインディングエントリを設定します。

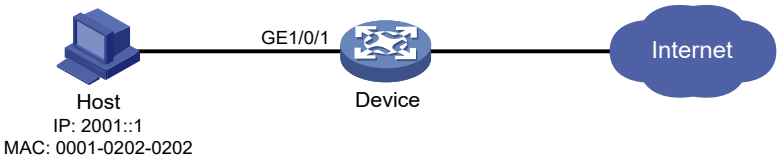


図 8-4 ネットワーク図

II. 設定手順

GigabitEthernet 1/0/1 で IPv6 ソースガードを有効にします。

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] ipv6 verify source ip-address mac-address
```

GigabitEthernet 1/0/1 で Host のスタティック IPv6 ソースガードバインディングエントリを設定します。

```
[Switch-GigabitEthernet1/0/1] ipv6 source binding ip-address 2001::1 mac-address 0001-0202-0202
[Switch-GigabitEthernet1/0/1] quit
```

装置でスタティック IPv6 ソースガードバインディングエントリを確認します。

```
[Switch] display ipv6 source binding static
Total entries found: 1
IPv6 Address         MAC Address    Interface              VLAN Type
2001::1              0001-0202-0202 GE1/0/1               N/A  Static
```

出力はスタティック IPv6 ソースガードバインディングエントリが正常に設定されていることを示します。

目次

このセクションのページは**7-x-x**です。

9章 ARPアタックプロテクション 9-1
9.1 ARPアタックプロテクション設定作業リスト 9-1
9.2 宛先不明のIPアタックプロテクションの設定 9-1
9.2.1 ARP送信元抑制機能の設定 9-2
9.2.2 ARPブラックホールルーティング機能の設定 9-2
9.2.3 宛先不明のIPアタックプロテクションの表示と維持 9-3
9.2.4 設定例 9-3
9.3 ARPパケットレートリミットの設定 9-4
9.4 送信元MACアドレスにもとづくARPアタックdetectionの設定 9-4
9.4.1 設定手順 9-5
9.4.2 送信元MACアドレスにもとづくARPアタックdetectionの表示と維持 9-5
9.4.3 設定例 9-6
9.5 ARPパケット送信元MACアドレス正当性チェックの設定 9-8
9.6 ARP確認応答の設定 9-8
9.7 ARP アタックdetectionの設定 9-8
9.7.1 ユーザの正当性の確認の設定 9-9
9.7.2 設定ガイドライン 9-9
9.7.3 設定手順 9-10
9.7.4 ARPパケット正当性の確認の設定 9-10
9.7.5 ARP制限転送の設定 9-11
9.7.6 ARPアタックdetectionの表示と維持 9-11
9.7.7 ユーザの正当性の確認の設定例 9-12
9.7.8 ユーザの正当性の確認とARPパケットの正当性の確認の設定例 9-13
9.7.9 ARP制限転送の設定例 9-15
9.8 ARPゲートウェイプロテクションの設定 9-18
9.8.1 設定ガイドライン 9-18
9.8.2 設定手順 9-18
9.8.3 設定例 9-18
9.9 ARPフィルタリングの設定 9-19
9.9.1 設定ガイドライン 9-20
9.9.2 設定手順 9-20
9.9.3 設定例 9-20

9章 ARP アタックプロテクション

ARP アタックとウイルスは LAN のセキュリティを脅かしています。この章では、そのような ARP アタックを発見、防御するための機能について記載します。

ARP は実装が容易ですが、セキュリティメカニズムを持っていないため、ネットワーク攻撃に対して脆弱です。攻撃者は ARP の脆弱性を悪用し、以下の方法でネットワーク装置を攻撃する可能性があります。

- 信頼されたユーザあるいは、ゲートウェイによるものとして見せかけた ARP パケットを送信し、装置は不正な ARP をエントリに追加します。
- 大量の宛先 MAC アドレス到達不能の IP パケットによって、受信装置の CPU が過負荷になるまで IP アドレスの解決処理を行います。ARP は到達不能の IP パケットに対応する MAC アドレスを検出することができません。
- 大量の ARP パケットによって、受信装置の CPU が過負荷になります。

ARP 攻撃の機能とタイプの詳細は ARP アタックプロテクションの技術資料を参照してください。

9.1 ARPアタックプロテクション設定作業リスト

作業リスト
フラッド防御： • 宛先不明のIPアタックプロテクションの設定（ゲートウェイで設定します。） 　• ARP送信元抑制機能の設定 　• ブラックホールルーティング機能の設定 • パケットレートリミットの設定（アクセス装置で設定します。） • 送信元MACアドレスにもとづくARPアタックdetectionの設定（ゲートウェイで設定します。）
ユーザとゲートウェイのなりすましの防御： • ARPパケット送信元MACアドレス正当性チェックの設定（ゲートウェイで設定します。） • ARP 確認応答の設定（ゲートウェイで設定します。） • ARP detectionの設定（アクセス装置で設定します。）

9.2 宛先不明のIPアタックプロテクションの設定

装置がホストから大量の宛先不明の IP パケットを受信した場合、以下の状況が発生します。

- 装置は宛先サブネットに対して大量の ARP リクエストを送信して、宛先サブネットの負荷が増大します。
- 装置は宛先 IP アドレスの解決処理を続けて、CPU の負荷が増大します。

宛先不明の IP パケット攻撃から装置を守るため、以下の機能を設定することができます。

- **ARP 送信元抑制機能**– 攻撃パケットが同じ送信元アドレスである場合、ARP 送信元抑制機能を有効にすることができます。5 秒以内にホストから受信した宛先不明の IP パケットが指定したしきい値を超えた場合、装置は次の 5 秒間にホストから受信したパケットによる ARP リクエスト送信を停止します。この機能は ARP 攻撃のパケットが同一送信元アドレスである場合、適用可能です。
- **ARP ブラックホールルーティング機能**– 宛先不明の IP アドレス宛のブラックホールのルートを作成します。装置はブラックホールのルートが削除されるまで宛先不明の IP アドレス宛にマッチするパケットを廃棄します。ブラックホールのルートはエージングタイマが終了する、あるいはルートが到達可能になった場合、削除されます。

  宛先不明の IP アドレスのブラックホールのルートが作成された後、装置はすぐに ARP リクエストを行う、最初の ARP ブラックホールの調査を開始します。IP アドレスの解決に失敗した場合、装置は設定に従って調査を継続します。装置がすべての調査を完了する前に ARP ブラックホールのエージングタイマが終了した場合、装置はブラックホールのルートを削除します。残りの調査は行いません。

  この機能は、攻撃パケットが同じ送信元アドレスかどうかにかかわらず、適用可能です。

9.2.1 ARP 送信元抑制機能の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. ARP 送信元抑制機能を有効にする	**arp source-suppression enable**	デフォルト：無効
3. 装置が 5 秒以内にホストから受信できる宛先不明のパケットの最大数を設定する	**arp source-suppression limit** *limit-value*	デフォルト：10

9.2.2 ARP ブラックホールルーティング機能の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. ARP ブラックホールルーティング機能を有効にする	**arp resolving-route enable**	デフォルト：有効
3. （オプション設定項目）宛先不明の IP アドレスの ARP ブラックホールのルートを調査する回数を設定する	**arp resolving-route probe-count** *count*	デフォルト：3回
4. （オプション設定項目）ARP ブラックホールのルートを調査する間隔を設定する	**arp resolving-route probe-interval** *interval*	デフォルト：1秒

9.2.3 宛先不明の IP アタックプロテクションの表示と維持

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

操作	コマンド
ARP送信元抑制機能の設定情報を表示する	**display arp source-suppression**

9.2.4 設定例

I. ネットワーク要件

図 9-1に示すように、LAN には VLAN10 の R&D エリアと VLAN20 の Office エリアが含まれます。これら 2 つのエリアはアクセススイッチを通してゲートウェイ（Device）に接続します。

大量の ARP リクエストが Office エリアで検出された場合、宛先不明の IP パケットによる攻撃が考えられます。このような攻撃を避けるために、ARP 送信元抑制や ARP ブラックホールルーティングの設定を行います。

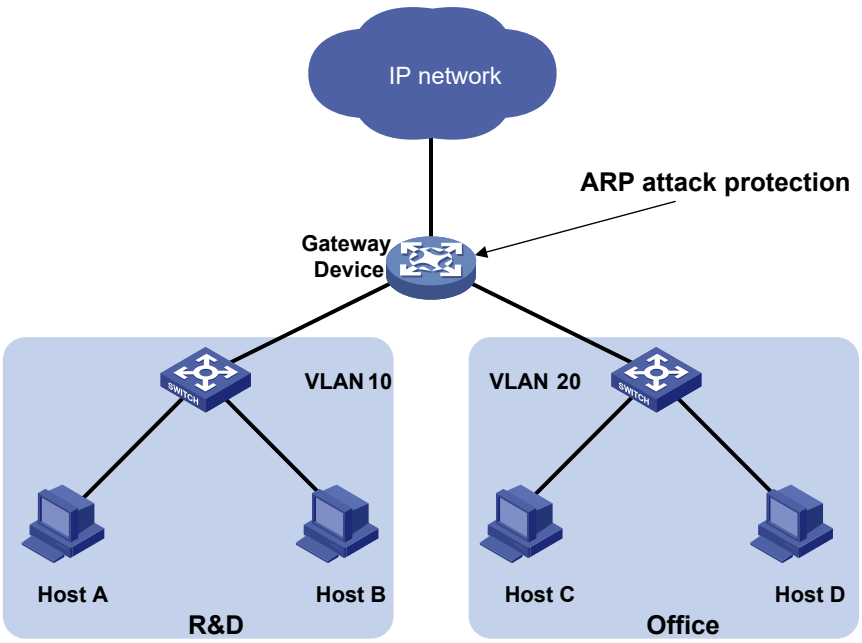


図 9-1 ネットワーク図

II. 設定手順

- 攻撃パケットが同一送信元アドレスである場合、ARP 送信元抑制機能を以下のように設定します。

ARP 送信元抑制機能を有効にします。

```
<Device> system-view
[Device] arp source-suppression enable
```

5 秒間の同一送信元からの ARP パケットのしきい値を 100 に設定します。

```
[Device] arp source-suppression limit 100
```

- 攻撃パケットが異なる送信元アドレスである場合、ゲートウェイで ARP ブラックホールルーティング機能を有効にします。

ARP ブラックホールルーティング機能を有効にします。

```
[Device] arp resolving-route enable
```

9.3 ARPパケットレートリミットの設定

I. ARP パケットレートリミットの設定

ARP パケットレートリミット機能は CPU に送信される ARP パケットのレートを制限します。ARP 検出が有効な装置は確認するため CPU に受信したすべての ARP パケットを送信します。大量の ARP パケットの処理を行う結果、他の機能への悪影響、あるいは装置がクラッシュする可能性があります。これを防ぐために、ARP パケットレートリミットを設定します。

II. 制限とガイドライン

ARP アタック検知を有効にしたとき、あるいは ARP フラッド攻撃を検出したとき、ARP パケットレートリミットの設定を行うことを推奨します。

III. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Layer 2 Ethernet interface あるいは Layer 2 aggregate interface view に移行する	**interface** *interface-type interface-number*	―
3. ARP パケットレートリミットを有効にし、レートリミットを設定する	**arp rate-limit** [*pps*]	デフォルト：有効 レートリミット：100pps

9.4 送信元MACアドレスにもとづくARPアタックdetectionの設定

この機能は CPU に送られる ARP パケットの数を確認します。5 秒間に同じ送信元からの ARP パケットの受信した数がしきい値を超えた場合、装置は、この MAC アドレスを ARP アタックエントリテーブルに追加します。エントリのエージングタイマが終了する前に、装置は以下の方法で攻撃に対応します。

- **モニタモード** ― ログメッセージを作成します。
- **フィルタモード** ― ログメッセージを作成し、攻撃する MAC アドレスからの後続の ARP パケットをフィルタします。

送信元 MAC アドレスにもとづく ARP アタック detection 機能を有効にする前に、ARP ロギング機能を有効にしたことを確認してください。ARP ロギング機能の詳細は、オペレーションマニュアルのセクション 3 *IP サービス ”ARP”* を参照してください。

この機能ではゲートウェイやサーバの MAC アドレスを除外するように設定することができます。ゲートウェイやサーバの MAC アドレスを除外した場合、たとえ攻撃者からの ARP パケットだとしても、除外された ARP パケットの確認を行いません。

9.4.1 設定手順

以下に送信元 MAC アドレスにもとづく ARP アタック detection の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. 送信元 MAC アドレスにもとづく ARP アタック detection を有効にし、モードを指定する	**arp source-mac** { **filter** | **monitor** }	デフォルト：無効
3. しきい値を設定する	**arp source-mac threshold** *threshold-value*	デフォルト：30
4. ARP アタックエントリのエージングタイマを設定する	**arp source-mac aging-time** *time*	デフォルト：300秒
5. （オプション設定項目）ARP アタック detection 機能から除外する MAC アドレスを設定する	**arp source-mac exclude-mac** *mac-address*&<1-10>	デフォルト：設定なし

メモ：

ARP アタックエントリのエージングタイマが終了した場合、エントリの MAC アドレスからの ARP パケットは正常に処理することができます。

9.4.2 送信元 MAC アドレスにもとづく ARP アタック detection の表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
送信元MACアドレスにもとづくARPアタックdetectionで検出されたARPアタックエントリを表示する	**display arp source-mac** { **interface** *interface-type interface-number* [**slot** *slot-number*] | **slot** *slot-number* }

9.4.3 設定例

I. ネットワーク要件

図 9-2に示すように、Host はゲートウェイ（Device）を介してインターネットにアクセスします。悪意のあるユーザがゲートウェイに大量の ARP 要求を送信した場合、ゲートウェイがクラッシュする可能性があり、クライアントからの要求を処理できません。この問題を解決するために、ゲートウェイ上で送信元 MAC アドレスにもとづく ARP アタック detection を設定します。

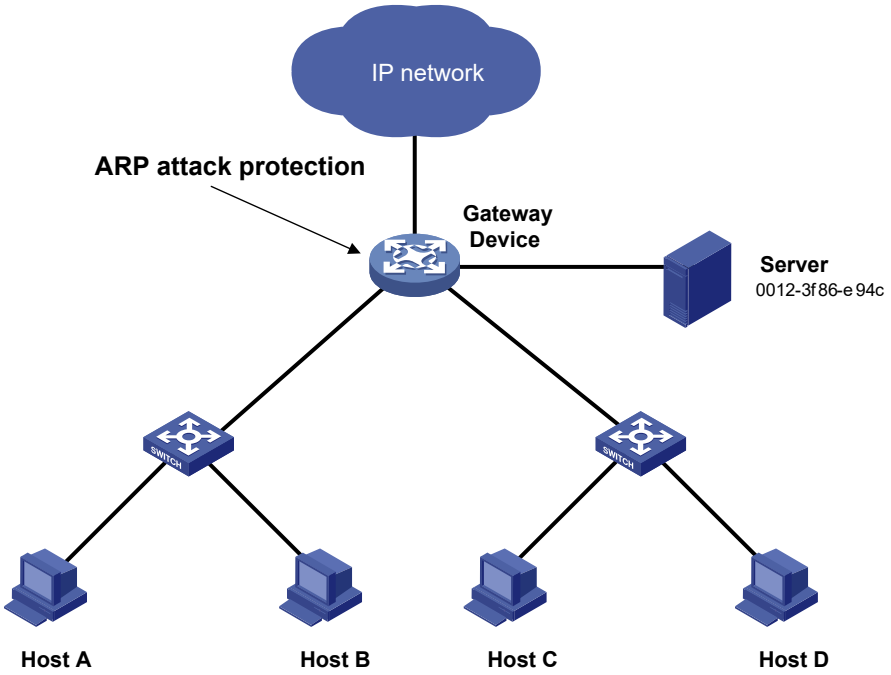


図 9-2 ネットワーク図

II. 設定要件

攻撃者は、有効な Host の MAC アドレスを送信元 MAC アドレスとして使用し、ARP パケットを大量に偽造することがあります。このような攻撃を防ぐために、次の手順でゲートウェイを設定します。

1) 送信元 MAC アドレスにもとづく ARP アタック detection を有効にし、フィルタモードを指定します。
2) しきい値を設定します。
3) ARP アタックエントリのエージングタイマを設定します。
4) この機能からサーバの MAC アドレスを除外します。

III. 設定手順

送信元 MAC アドレスにもとづく ARP アタック detection を有効にし、フィルタモードを指定します。

```
<Device> system-view
[Device] arp source-mac filter
```

しきい値を 30 に設定します。

```
[Device] arp source-mac threshold 30
```

ARP アタックエントリのエージングタイマを 60 秒に設定します。

```
[Device] arp source-mac aging-time 60
```

MAC アドレス 0012-3f86-e94c を除外します。

```
[Device] arp source-mac exclude-mac 0012-3f86-e94c
```

9.5 ARPパケット送信元MACアドレス正当性チェックの設定

この機能を有効にすることで、ゲートウェイはイーサネットヘッダの送信元 MAC アドレスが ARP メッセージのメッセージ部分にある送信元 MAC アドレスと異なる場合、ARP パケットをフィルタします。これによりゲートウェイは正しい ARP エントリを学習します。

以下に ARP パケット送信元 MAC アドレス正当性チェックの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. ARP パケット送信元 MAC アドレス正当性チェックを設定する	**arp valid-check enable**	デフォルト：無効

9.6 ARP確認応答の設定

ユーザのなりすましを防御するため、ARP 確認応答機能をゲートウェイで設定します。

ARP 確認応答機能は、ゲートウェイが不正な ARP エントリを作成することを防御します。

以下に ARP 確認応答機能の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. ARP 確認応答機能を有効にする	**arp active-ack enable**	デフォルト：無効

9.7 ARP アタックdetectionの設定

ARP アタック detection 機能は、ユーザやゲートウェイのなりすまし攻撃を防ぐため、許可されていないクライアントの ARP パケットをブロックするようにアクセス装置で有効にします。ARP detection 機能は ARP トラステッドポートから受信した ARP パケットを確認しません。

ARP アタック detection 機能は、以下の機能を提供します

- ユーザの正当性確認
- ARP パケットの正当性の確認
- ARP 制限転送
- ARP アタック detection ロギング
- ユーザの正当性の確認と ARP パケットの正当性の確認

ARP パケットの正当性とユーザの正当性の両方が有効である場合、最初に ARP パケットの正当性の確認を行い、次にユーザの正当性の確認を行います。

ARP snooping と一緒に ARP アタック detection を設定しないでください。同時に設定した場合、ARP snooping エントリは作成することができません。

9.7.1 ユーザの正当性の確認の設定

以下の順に受信 ARP パケットの送信元 IP アドレスと送信元 MAC アドレスを比較します。

- ユーザの正当性確認のルール
  - □ 一致した場合、装置はルールに従って ARP パケットを処理します。
  - □ 一致するアドレスがない場合や、ユーザの正当性確認が設定されていない場合、以下の処理をします。
- スタティック IP ソースガードバインディング、DHCP snooping エントリ、802.1X セキュリティエントリ
  - □ 一致した場合、装置は ARP パケットを転送します。
  - □ 一致するアドレスがなかった場合、装置は ARP パケットを廃棄します。

スタティック IP ソースガードバインディングエントリは、**ip source binding** コマンドを使用して作成されます。詳細はオペレーションマニュアルのセクション *7 セキュリティ” IP ソースガード”*を参照してください。

DHCP snooping エントリは、DHCP snooping によって自動的に作成されます。詳細はオペレーションマニュアルのセクション *3 IP サービス ” DHCP スヌーピング”*を参照してください。

802.1X セキュリティエントリは、802.1X クライアントに IP と MAC のマッピングを記録します。クライアントが 802.1X 認証に成功し ARP アタック detection が有効となった装置に IP アドレスをアップロードした後、装置は自動的に 802.1X セキュリティエントリを作成します。装置に IP アドレスをアップロードするため、802.1X クライアントを有効にする必要があります。詳細はオペレーションマニュアルのセクション *7 セキュリティ ” 802.1X”*を参照してください。

9.7.2 設定ガイドライン

ユーザの正当性確認を設定する際は、以下のガイドラインに従ってください。

- 以下の 1 つ以上のアイテムが設定されていることを確認してください。
  - □ ユーザの正当性確認ルール
  - □ スタティック IP ソースガードバインディング
  - □ DHCP snooping
  - □ 802.1X

  上記の機能が設定されていない場合、トラステッド ARP インタフェース上のすべての受信 ARP パケットは転送されます。
- IP ソースガードバインディングのために ARP アタック detection が有効となっている IP アドレス、MAC アドレス、VLAN を指定してください。それ以外の場合、ARP パケットは IP ソースガードバインディングと一致できません。

9.7.3 設定手順

以下にユーザの正当性の確認の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. VLAN view に移行する	**vlan** *vlan-id*	ー
3. ARP detection を有効にする	**arp detection enable**	デフォルト：無効 装置はユーザの正当性の確認を実行しません。
4. system view に戻る	**quit**	ー
5. Ethernet interface view あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	ー
6. （オプション設定項目）ARP 検出を除外するトラステッドインタフェースとして設定する	**arp detection trust**	デフォルト : 非トラステッドインタフェース

9.7.4 ARP パケット正当性の確認の設定

非トラステッドポートで受信された ARP パケットが正当かどうか確認を行い、以下のオブジェクトについて指定します。

- **src-mac**– ARP パケットのメッセージ部分にある送信元 MAC アドレスが、イーサネットヘッダの送信元 MAC アドレスと一致するかどうか確認します。一致する場合には通過、そうでなければパケットは廃棄されます。
- **dst-mac**– ARP 応答の宛先 MAC アドレスを確認します。宛先 MAC アドレスがすべて 0、すべて 1、あるいはイーサネットヘッダの宛先 MAC アドレスと矛盾する場合、パケットは無効と判断され廃棄されます。
- **ip**– ARP 応答の送信元 IP アドレスと宛先 IP アドレスを確認します。すべて 1、あるいはマルチキャスト IP アドレスである場合、パケットは無効と判断して廃棄されます。

以下に ARP パケット正当性の確認を有効にします。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. ARP パケット正当性の確認を有効にし、オブジェクトを指定する	**arp detection validate** { **dst-mac** | **ip** | **src-mac** } *	デフォルト：無効

VLAN での ARP 攻撃 detection を有効にします。

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

操作	コマンド	補足
3. ARP detection を有効にする	**arp detection enable**	デフォルト：無効 装置はARPパケット正当性の確認を実行しません。
4. system view に戻る	**quit**	ー
5. Ethernet interface view あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	ー
6. （オプション設定項目）ARP 検出を除外するトラステッドインタフェースとして設定する	**arp detection trust**	デフォルト : 非トラステッドインタフェース

9.7.5 ARP 制限転送の設定

🕮 **メモ：**

ARP 制限転送は宛先 MAC アドレスのようなマルチポート MAC アドレスの ARP パケットには適用されません。

ARP 制限転送は、非トラステッドインタフェースで受信され、ユーザの正当性の確認をパスした ARP パケットの転送を以下のように制御します。

- パケットが ARP 要求である場合、トラステッドインタフェースを通して転送されます。
- パケットが ARP 応答である場合、宛先 MAC アドレスに従って転送されます。MAC アドレステーブル内に一致するアドレスがない場合、トラステッドインタフェースを通して転送されます。

ARP 制限転送の設定をする前に、ユーザの正当性の確認の設定を行ってください。

以下に ARP 制限転送の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. VLAN view に移行する	**vlan** *vlan-id*	ー
3. ARP 制限転送を有効にする	**arp restricted-forwarding enable**	デフォルト：無効

9.7.6 ARP アタック detection の表示と維持

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

操作	コマンド
ARP detectionが有効なVLANを表示する	**display arp detection**
ARP detectionの統計情報を表示する	**display arp detection statistics** [**interface** *interface-type interface-number*]

操作	コマンド
ARP detectionの統計情報を削除する	**reset arp detection statistics** [**interface** *interface-type interface-number*]

9.7.7 ユーザの正当性の確認の設定例

I. ネットワーク要件

図 9-3に示すように、Device B で 802.1X セキュリティエントリをもとにユーザの正当性の確認の設定を行います。

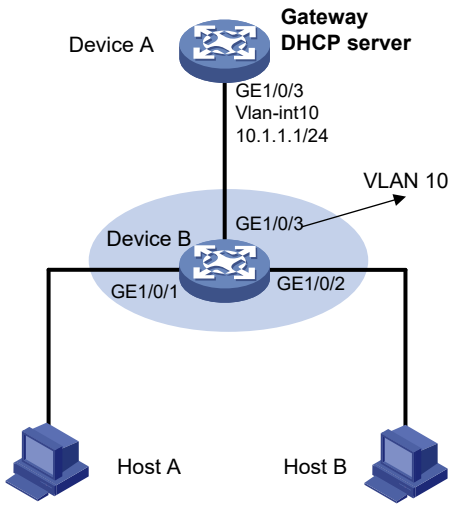


図 9-3 ネットワーク図

II. 設定手順

1) Device B のすべてのインタフェースに VLAN10 を追加し、Device A の VLAN インタフェース 10 の IP アドレスを設定します。（詳細は省略します。）
2) Device A の DHCP サーバを設定し、DHCP アドレスプール 0 を設定します。

```
<DeviceA> system-view
[DeviceA] dhcp enable
[DeviceA] dhcp server ip-pool 0
[DeviceA-dhcp-pool-0] network 10.1.1.0 mask 255.255.255.0
```

3) Host A と Host B を 802.1X クライアントに設定し、ARP アタック detection の IP アドレスをアップロードするよう設定します。（詳細は省略します。）
4) Device B を設定します。

802.1X を有効にします。

```
<DeviceB> system-view
[DeviceB] dot1x
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] dot1x
[DeviceB-GigabitEthernet1/0/1] quit
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] dot1x
[DeviceB-GigabitEthernet1/0/2] quit
```

ローカルユーザ test を追加します

```
[DeviceB] local-user test
[DeviceB-luser-test] service-type lan-access
[DeviceB-luser-test] password simple test
[DeviceB-luser-test] quit
```

802.1X エントリをもとにユーザの正当性を確認するため VLAN10 で ARP アタック detection を有効にします。

```
[DeviceB] vlan 10
[DeviceB-vlan10] arp detection enable
```

ARP トラステッドインタフェースとしてアップストリームを設定します。デフォルトでは、インタフェースはアントラステッドインタフェースです。

```
[DeviceB-vlan10] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] arp detection trust
[DeviceB-GigabitEthernet1/0/3] quit
```

設定が完了すると、GigabitEthernet 1/0/1 と GigabitEthernet 1/0/2 のインタフェースで受信される ARP パケットは 802.1X エントリに対して確認が行われます。

9.7.8 ユーザの正当性の確認と ARP パケットの正当性の確認の設定例

I. ネットワーク要件

図 9-4に示すように、Device B でスタティック IP ソースガードバインディングと DHCP snooping エントリをもとに ARP パケットの正当性確認とユーザの正当性を実行するように設定します。

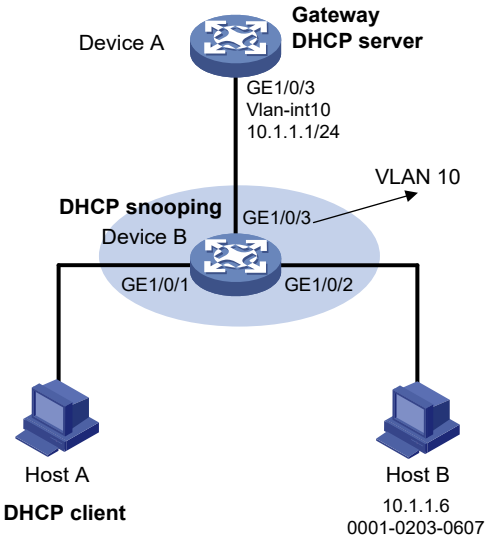


図 9-4 ネットワーク図

II. 設定手順

1) Device B のすべてのインタフェースに VLAN10 を追加し、Device A の VLAN インタフェース 10 の IP アドレスを設定します。（詳細は省略します。）
2) Device A の DHCP サーバを設定し、DHCP アドレスプール 0 を設定します。

```
<DeviceA> system-view
[DeviceA] dhcp enable
[DeviceA] dhcp server ip-pool 0
[DeviceA-dhcp-pool-0] network 10.1.1.0 mask 255.255.255.0
```

3) Host A と Host B を設定します。（詳細は省略します。）
4) Device B を設定します。

DHCP snooping を有効にします。

```
<DeviceB> system-view
[DeviceB] dhcp snooping enable
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] dhcp snooping trust
[DeviceB-GigabitEthernet1/0/3] quit
```

GigabitEthernet 1/0/1 で DHCP snooping エントリのクライアント情報を記録するように設定します。

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] dhcp snooping binding record
[DeviceB-GigabitEthernet1/0/1] quit
```

VLAN10 で ARP detection を有効にします。

```
[DeviceB] vlan 10
[DeviceB-vlan10] arp detection enable
```

トラステッドインタフェースとして上流インタフェースを設定します。（デフォルトでは非トラステッドインタフェースとなっています。）

```
[DeviceB-vlan10] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] arp detection trust
[DeviceB-GigabitEthernet1/0/3] quit
```

ユーザの正当性の確認を行うため、GigabitEthernet 1/0/2 でスタティック IP ソースガードバインディングエントリを設定します。

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] ip source binding ip-address 10.1.1.6 mac-address 0001-0203-0607 vlan 10
[DeviceB-GigabitEthernet1/0/2] quit
```

ARP パケットの MAC アドレスと IP アドレスを確認することによって、ARP パケットの正当性の確認を有効にします。

```
[DeviceB] arp detection validate dst-mac ip src-mac
```

設定を行った後、GigabitEthernet 1/0/1 と GigabitEthernet 1/0/2 で受信された ARP パケットは、最初に MAC アドレスと IP アドレスの正当性の確認を行います。ARP パケットが有効である場合、スタティック IP ソースガードバインディングエントリに対して確認を行います。最後に DHCP snooping エントリに対して確認を行います。

9.7.9 ARP 制限転送の設定例

I. ネットワーク要件

図 9-5に示すように、ARP detection が設定されている Device B で ARP 制限転送を設定します。Device B に設定された Port Isolation はブロードキャストの ARP 要求のために適用することができます。

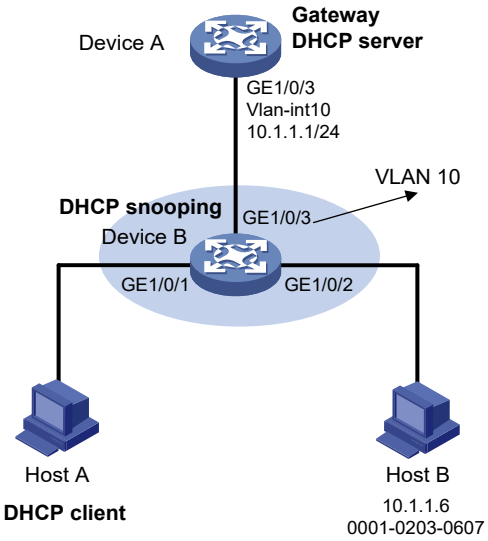


図 9-5 ネットワーク図

II. 設定手順

1) VLAN 10 を設定します。インタフェースに VLAN 10 を追加し、VLAN インタフェースの IP アドレスを設定します。（詳細は省略します。）
2) Device A で DHCP サーバを設定し、DHCP アドレスプール 0 を設定します。

```
<DeviceA> system-view
[DeviceA] dhcp enable
[DeviceA] dhcp server ip-pool 0
[DeviceA-dhcp-pool-0] network 10.1.1.0 mask 255.255.255.0
```

3) Host A と Host B を設定します。（詳細は省略します。）
4) Device B を設定します。

DHCP snooping を有効にします。DHCP トラステッドポートとして GigabitEthernet 1/0/3 を設定します。

```
<DeviceB> system-view
[DeviceB] dhcp snooping enable
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] dhcp snooping trust
[DeviceB-GigabitEthernet1/0/3] quit
```

ユーザの正当性の確認を行うため ARP detection を有効にします。

```
[DeviceB] vlan 10
[DeviceB-vlan10] arp detection enable
```

DHCP トラステッドポートとして GigabitEthernet 1/0/3 を設定します。

```
[DeviceB-vlan10] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] arp detection trust
[DeviceB-GigabitEthernet1/0/3] quit
```

GigabitEthernet 1/0/2 でスタティック IP ソースガードバインディングエントリを設定します。

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] ip source binding ip-address 10.1.1.6 mac-address 0001-0203-0607 vlan 10
[DeviceB-GigabitEthernet1/0/2] quit
```

ARP パケットの MAC アドレスと IP アドレスを確認することによって、ARP パケットの正当性の確認を有効にします。

```
[DeviceB] arp detection validate dst-mac ip src-mac
```

Port Isolation を設定します。

```
[DeviceB] port-isolate group 1
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port-isolate enable group 1
[DeviceB-GigabitEthernet1/0/1] quit
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] port-isolate enable group 1
[DeviceB-GigabitEthernet1/0/2] quit
```

設定を行った後、Device B は最初に GigabitEthernet 1/0/1 と GigabitEthernet 1/0/2 で受信された ARP パケットの MAC アドレスと IP アドレスの正当性の確認を行います。ARP パケットが有効である場合、スタティック IP ソースガードバインディングエントリと DHCP snooping エントリを使用してユーザの正当性の確認を行います。しかし Host A から送信された ARP ブロードキャスト要求は Device B の確認にパスし、Host B に到達します。

ARP 制限転送を有効にします。

```
[DeviceB] vlan 10
[DeviceB-vlan10] arp restricted-forwarding enable
[DeviceB-vlan10] quit
```

設定を行った後、Device B はトラステッドインタフェース GigabitEthernet 1/0/3 を通して Host A から Device A に ARP ブロードキャスト要求を転送します。Host B はパケットを受信することができません。Port isolation は正常に動作します。

9.8 ARPゲートウェイプロテクションの設定

ゲートウェイスプーフィング攻撃を防止するためにゲートウェイに接続していないインタフェースで設定してください。そのインタフェースで ARP パケットを受信した際は、パケット内の送信元 IP アドレスが保護されたゲートウェイと一致しているかを確認します。一致していれば、パケットを廃棄します。一致しない場合、パケットが正しいと認識して処理します。

9.8.1 設定ガイドライン

ARP ゲートウェイプロテクションを設定する際は、以下のガイドラインに従ってください。

- 一つのインタフェースで最大 8 個のゲートウェイに ARP ゲートウェイプロテクションを有効にできます。
- インタフェースでは **arp filter source** コマンドと **arp filter binding** コマンドの両方を設定することはしないでください。
- ARP ゲートウェイプロテクションを ARP アタック detection と ARP snooping と一緒に使用する場合、最初に ARP ゲートウェイプロテクションが適用されます。

9.8.2 設定手順

以下に ARP ゲートウェイプロテクションの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Ethernet interface view あるいはレイヤ 2aggregate interface view に移行する	**interface** *interface-type interface-number*	―
3. 指定のゲートウェイに ARP ゲートウェイプロテクションを設定する	**arp filter source** *ip-address*	デフォルト：無効

9.8.3 設定例

I. ネットワーク要件

図 9-6に示すように、ホスト B は装置 B にゲートウェイスプーフィング攻撃を始めます。結果として、装置 B は装置 A に送信しようとしている通信はホスト B に送信されます。

装置 B に攻撃をブロックするように設定します。

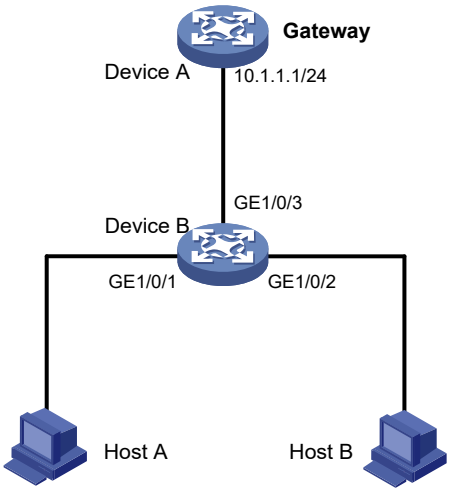


図 9-6 ネットワーク図

II. 設定手順

装置 B に ARP ゲートウェイプロテクションを設定します。

```
<DeviceB> system-view
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] arp filter source 10.1.1.1
[DeviceB-GigabitEthernet1/0/1] quit
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] arp filter source 10.1.1.1
```

III. 設定確認

送信元 IP アドレスがゲートウェイの IP アドレスになっている受信 ARP パケットを GigabitEthernet 1/0/1 と GigabitEthernet 1/0/2 ポートが廃棄していることを確認してください。

9.9 ARPフィルタリングの設定

ARP フィルタリング機能は、ゲートウェイスプーフィング攻撃とユーザスプーフィング攻撃を防ぐことができます。

ARP フィルタリングが有効なインタフェースは、パーミットされたエントリに対して受信 ARP パケットの IP アドレスと MAC アドレスを確認します。一致した場合、パケットは正しく処理されます。一致しなかった場合、パケットは廃棄されます。

9.9.1 設定ガイドライン

ARP フィルタリングを設定する際は、以下のガイドラインに従ってください。

- 一つのインタフェースで最大 8 個のパーミットエントリを設定できます。
- インタフェースでは **arp filter source** コマンドと **arp filter binding** コマンドの両方を設定することはしないでください。
- ARP フィルタリングを ARP アタック detection と ARP snooping と一緒に使用する場合、最初に ARP フィルタリングが適用されます。

9.9.2 設定手順

以下に ARP ゲートウェイプロテクションの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Ethernet interface view あるいはレイヤ 2aggregate interface view に移行する	**interface** *interface-type interface-number*	―
3. 指定のゲートウェイに ARP ゲートウェイプロテクションを設定する	**arp filter binding** *ip-address mac-address*	デフォルト：無効

9.9.3 設定例

I. ネットワーク要件

図 9-7に示すように、ホスト A の IP アドレスと MAC アドレスはそれぞれ 10.1.1.2 と 000f-e349-1233 です。ホスト B の IP アドレスと MAC アドレスはそれぞれ 10.1.1.3 と 000f-e349-1234 です。

ホスト A とホスト B からのみ ARP パケットをパーミットするために、装置 B の GigabitEthernet1/0/1 と GigabitEthernet1/0/2 に ARP フィルタリングを設定します。

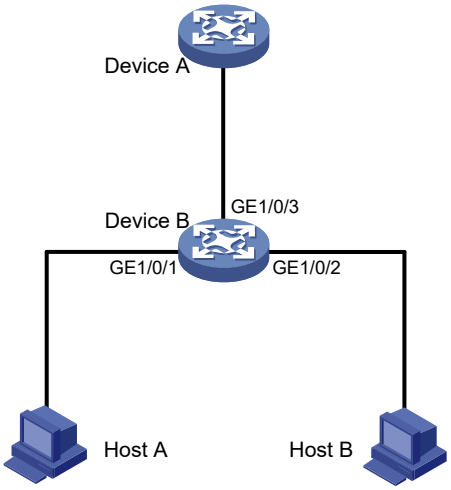


図 9-7 ネットワーク図

II. 設定手順

装置 B に ARP フィルタリングを設定します。

```
<DeviceB> system-view
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] arp filter binding 10.1.1.2 000f-e349-1233
[DeviceB-GigabitEthernet1/0/1] quit
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] arp filter binding 10.1.1.3 000f-e349-1234
```

III. 設定確認

GigabitEthernet 1/0/1 がホスト A からの ARP パケットを許可し、他の ARP パケットを廃棄していることを確認してください。

GigabitEthernet 1/0/2 がホスト B からの ARP パケットを許可し、他の ARP パケットを廃棄していることを確認してください。

目次

このセクションのページは **7-x-x** です。

10 章 TCP フラグメントアタックプロテクション..... 10-1
10.1 概要 10-1
10.2 TCP フラグメントアタックプロテクション機能の設定 10-1

10章 TCP フラグメントアタックプロテクション

10.1 概要

装置は、アタック検出機能、アタックプロテクション機能により攻撃者からの調査パケットを検出し、パケット廃棄によってプライベートネットワークの保護を行います。

装置は TCP フラグメントアタックプロテクションのみサポートします。

10.2 TCPフラグメントアタックプロテクション機能の設定

TCP フラグメントアタックプロテクション機能は、従来のパケットフィルタで検出できない TCP フラグメント攻撃を防ぐため、装置で TCP フラグメント攻撃のパケットを廃棄します。RFC 1858 で定義されているように、以下のフラグメントを調査します。

- TCP ヘッダが 20 バイトよりも小さい、最初のフラグメント
- 8 バイトのフラグメントオフセットの 2 番目以降のフラグメント

装置の従来のパケットフィルタは、送信元 IP アドレス、宛先 IP アドレス、送信元ポート、宛先ポート、TCP パケットの最初のフラグメントのトランスポートレイヤプロトコルを検出します。最初のフラグメントが検出にパスした場合、残り全てのフラグメントパケットが透過することも許可してしまいます。

攻撃者は以下のような方法で TCP フラグメント攻撃を仕掛けることができてしまいます。

- TCP ヘッダの内、いくつかのフィールドを 2 番目のフラグメントに移動させ、2 番目のフラグメントの TCP フラグを不正にすることで、最初のフラグメントを十分に小さくします。
- フラグメントオフセットが 8 バイトになっている 2 番目以降のフラグメントを構成し、TCP フラグを最初のフラグメントとは異なる不正なものにします。フラグメントを受け取った装置はフラグメントから再構成するとき、2 番目以降の不正な TCP フラグで最初のフラグメントにある正常な TCP フラグを上書きしてしまいます。

従来のパケットフィルタでは、この最初のフラグメントでのフィルタができないために、2 番目以降のフラグメントも透過してしまいます。TCP フラグメントアタックは装置がフラグメントを再構成した後に起こります。

TCP フラグメント攻撃を防ぐため TCP フラグメントアタックプロテクションの設定を有効にします。

以下に TCP フラグメントアタックプロテクションの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. TCP フラグメントアタックプロテクションを有効にする	**attack-defense tcp fragment enable**	有効

目次

このセクションのページは **7-x-x** です。

11 章 パスワード管理.....11-1
11.1 概要.....11-1
11.1.1 パスワードの設定.....11-1
11.1.2 パスワードのアップデートと有効期限の終了.....11-3
11.1.3 ユーザログイン管理.....11-4
11.1.4 すべての形式でのパスワードの非表示.....11-5
11.1.5 ロギング.....11-5
11.2 制限とガイドライン.....11-6
11.3 パスワード管理設定作業リスト.....11-6
11.4 パスワード管理の有効化.....11-6
11.5 グローバルパスワード管理パラメータの設定.....11-7
11.6 ユーザグループパスワード管理パラメータの設定.....11-8
11.7 ローカルユーザパスワード管理パラメータの設定.....11-9
11.8 super パスワード管理パラメータの設定.....11-10
11.9 パスワード管理の表示と維持.....11-10
11.10 パスワード管理の設定例.....11-11
11.10.1 パスワード管理の設定例.....11-11

11章 パスワード管理

🕮 **メモ:**
本機能は Version 7.1.5 を含む以降のソフトウェアからサポートしています。

11.1 概要

パスワード管理は、以下の機能ができます。

- 装置管理ユーザのログインと super パスワードのセットアップ、終了、アップデートを管理します。
- あらかじめ定義されたポリシーにもとづいたユーザログインステータスを制御します。

装置管理ユーザは、ローカルユーザの一種です。ローカルユーザについての詳細は、オペレーションマニュアルのセクション 9 *セキュリティ*”*AAA*”を参照してください。super パスワードについては、オペレーションマニュアルのセクション 1 *はじめに*”*RBAC*”を参照してください。

🕮 **メモ：**
パスワード管理機能はデフォルトで無効（**undo password-control enable**）に設定されていますが、以下に示すコマンドはパスワード管理機能が無効の場合でも動作します（以下はデフォルトの設定状態を示します）。以下に示すコマンド以外は、パスワード管理機能を有効にすると動作します。

- password-control length enable：文字列の最小値制限有効
- password-control length 10：10 文字以上の文字列（ローカルユーザ）
- password-control composition enable：文字タイプ数の最小値制限有効
- password-control composition type-number 2：最低 2 種類の文字タイプ数（ローカルユーザ）
- password-control complexity user-name check：パスワードにユーザ名と同じ文字列使用不可
- password-control super length 10：10 文字以上の文字列（super ユーザ）
- password-control super composition type-number 2：最低 2 種類の文字タイプ数（super ユーザ）

11.1.1 パスワードの設定

I. 最小パスワード長

ユーザパスワードの最小の長さを設定することができます。ユーザが最小パスワード長よりも短いパスワードを入力した場合、システムはパスワードを拒否します。

II. パスワード設定のポリシー

パスワードは以下のタイプの組み合わせで設定されます。

- A～Z の大文字の英字
- a～z の小文字の英字
- 0～9 の数字
- 特殊文字

表 11-1 特殊文字

文字名	記号	文字名	記号
アンパサンド	&	アポストロフィー	'
アスタリスク	*	アットマーク	@
逆クォート	`	バックスラッシュ	\
半角スペース	ー	キャロット	^
コロン	:	コンマ	,
ダラーマーク	$	ドット	.
イコール	=	感嘆符	!
左アングルブラケット	<	左波括弧	{
左角括弧	[	左丸括弧	(
ハイフン	-	パーセント	%
プラス	+	シャープ	#
右アングルブラケット	>	右波括弧	}
右角括弧	]	右丸括弧	)
セミコロン	;	スラッシュ	/
チルダ	~	アンダーライン	_
垂直バー	|		

システムのセキュリティ要件に応じて、パスワードに含めなくてはいけない文字タイプの最小数と、各種類の文字の最小数を設定することができます。表 9-2にパスワード設定のポリシーを示します。

表 11-2 パスワード設定のポリシー

パスワード組み合わせレベル	文字タイプの最小数	各タイプの最小文字数
Level 1	1	1
Level 2	2	1

パスワード組み合わせレベル	文字タイプの最小数	各タイプの最小文字数
Level 3	3	1
Level 4	4	1

すべての組み合わせレベルをパスワードとして使用できます。

ユーザがパスワードを設定あるいは変更するとき、システムはパスワードが要件の組み合わせを満たしているか確認します。満たしていない場合、パスワードの設定あるいは変更操作は失敗します。

III. パスワードの複雑性のポリシー

ユーザ名や連続した文字などのような文字が含まれる複雑でないパスワードは、不正に解読されやすくなります。より高いセキュリティを持たせるため、すべてのユーザのパスワードが相対的に複雑となっているかを確認するようにポリシーを設定することができます。ポリシーが設定され、ユーザがパスワードを設定したとき、パスワードの複雑性を確認します。パスワードがポリシーに適合しない場合、ユーザのパスワード設定は失敗します。

パスワードの複雑性の要件を以下に示します。

- パスワードはユーザ名あるいはユーザ名の逆の順番を含むことができません。たとえば、ユーザ名が **abc** であるとき、**abc982** や **2cba** のようなパスワードはポリシーに適合しません。
- 文字あるいは数字が 3 回以上連続して続くことはできません。たとえば、**a111** のパスワードはポリシーに適合しません。

11.1.2 パスワードのアップデートと有効期限の終了

I. パスワードのアップデート

この機能は、ユーザがパスワードを変更する最小間隔を設定します。ユーザがパスワードを変更するためにログインした際、最後にパスワードを変更してからの間隔が短い場合、システムはパスワードの変更を拒否します。たとえばパスワードを変更する最小間隔を 48 時間に設定した場合、ユーザが 48 時間以内に 2 回パスワードを変更することはできません。

この最小間隔は、以下の場合影響がありません。

- ユーザが最初にログインした後にパスワードを変更します。
- パスワードの有効期限が終了した後にパスワードを変更します。

II. パスワードの終了

パスワードの有効期限の終了は、ユーザのパスワードのライフサイクルを変更させるようにします。パスワードの有効期限が終了した後、ユーザはパスワードの変更が必要となります。

ユーザが期限の切れたパスワードでログインした場合、システムはエラーメッセージを表示します。新しいパスワードを入力するように表示し、新しいパスワードを確認するため、再度新しいパスワードを入力するように表示します。新しいパスワードは正式なもので、ユーザが再入力したとき、最初に入力したパスワードと同一のパスワードを正確に入力する必要があります。

Web ユーザ、Telnet ユーザ、SSH ユーザ、コンソールユーザは、自身のパスワードを変更することができます。管理者はFTPユーザ用にパスワードを変更する必要があります。

III. パスワード有効期限の終了までの早期通知

ユーザがログインするとき、システムは、パスワードの有効期限が少しで終了となるかどうかを確認します。有効期限が終了する場合、パスワードの変更を行うように通知します。

- ユーザがポリシーに適した新しいパスワードを適用した場合、新しいパスワードと時間を記録します。
- ユーザがパスワードを変更しない、あるいは変更に失敗した場合、システムは現在のパスワードを使用したユーザのログインを許可します。

Web ユーザ、Telnet ユーザ、SSH ユーザ、コンソールユーザは、自身のパスワードを変更することができます。管理者はFTPユーザ用にパスワードを変更する必要があります。

IV. 有効期限が終了したパスワードを使用したログイン

パスワードの有効期限が終了した後、ユーザが、指定した期間内に設定した回数のログインができるように設定することができます。たとえば、パスワードの有効期限が終了した後、最大 3 回、15 日間内にログインできるように設定した場合、ユーザは、パスワードの有効期限が終了した後、15 日以内に 3 回までログインすることができます。

V. パスワード履歴

この機能を有効にすると、システムはユーザが使用したパスワードを記録します。ユーザがパスワードを変更するとき、システムは現在のパスワードと、パスワード履歴にある記録されたパスワードを確認します。新しいパスワードは現在のパスワードとパスワード履歴に記録されたパスワードと、少なくとも 4 文字以上変更する必要があり、4 文字は互いに異なる必要があります。そうでなければ、エラーメッセージを表示し、パスワードは変更されません。

各ユーザ用でパスワード履歴に保持するパスワードの最大数を設定することができます。パスワード履歴の最大数を超えるとき、新しいパスワードが最初のパスワードに上書きされます。

装置管理ユーザの現在のログインパスワードはパスワード履歴に記録されません。これは装置管理ユーザのパスワードは暗号化テキストで保存され、プレーン（平文）テキストに回復することができないためです。

11.1.3 ユーザログイン管理

I. 初回ログイン

グローバルでパスワード管理機能が有効であるとき、ユーザはシステムにアクセスする前に初回ログイン時にパスワードを変更する必要があります。この状況では、パスワードの変更は最小変更間隔の設定に関係なく設定します。

II. ログイン試行制限

連続してログインの試行の失敗を制限することで、パスワードを類推することを効果的に防ぐことができます。

ログイン試行制限は FTP、Web および VTY ユーザに適用します。以下のタイプのユーザには適用しません。

- 存在しないユーザ（装置で設定されていないユーザ）
- コンソールポートを通して装置にログインするユーザ

ユーザがログインに失敗した場合、ユーザのアカウントとユーザの IP アドレスをパスワード管理のブラックリストに追加します。ユーザが最大連続試行回数を超えてログインに失敗した場合、ログイン試行回数の制限によりユーザとユーザアカウントを以下の方法で制限します。

- パスワード管理ブラックリストから手動でユーザを削除するまでユーザアカウントを無効にします。
- ユーザがユーザアカウントの継続使用を許可します。ユーザがこのアカウントを使用して装置に正常にログインしたとき、ユーザの IP アドレスとユーザアカウントはパスワード管理のブラックリストから削除されます。
- 一定の時間、ユーザアカウントを無効にします。

ユーザは以下の状況のどちらかの状態の時、ログインを行うアカウントを使用することができます。

- □ ログインの試行を無効にする時間が終了したとき、アカウントを使用することができます。
- □ ログインの試行を無効にする時間が終了する前に、パスワード管理のブラックリストから手動でアカウントが削除されたとき、アカウントを使用することができます。

🕮 **メモ：**

アカウントはブラックリストに追加されたユーザのみロックされます。他のユーザはアカウントを使用することができます。ブラックリストに追加されたユーザは他のユーザアカウントを使用することができます。

III. 最大アカウントアイドルタイム

ユーザアカウントの最大アカウントアイドルタイムを設定することができます。期間内にログインしないアカウントは、無効なアカウントで無効となります。

11.1.4 すべての形式でのパスワードの非表示

セキュリティ目的のため、ユーザがパスワードを入力したとき、表示されません。

11.1.5 ロギング

システムは、すべての正常なパスワードの変更イベントと、ユーザがパスワード管理ブラックリストへ追加するイベントをロギングします。

11.2 制限とガイドライン

重要 ：
グローバルでパスワード管理機能を正常に有効にするため、装置に装置管理ユーザがログインすることを許可し、装置に十分な記憶容量があることを確認してください。

パスワード管理機能は、いくつかの異なる view で設定することができます。異なる view は異なる機能をサポートします。異なる view の設定、異なる目的のために、以下に示すような設定範囲を持ちます。

- super パスワードの設定は、super パスワードのみ適用されます。
- local user view での設定は、ローカルユーザのパスワードのみに適用します。
- local user view でユーザのパスワード管理ポリシーが設定されていない場合、user group view での設定はユーザグループのローカルユーザのパスワードに適用します。
- local user view と user group view の両方でユーザのパスワード管理ポリシーが設定されていない場合、system view でのグローバルの設定はすべてのユーザグループのローカルユーザのパスワードに適用します。

ローカルユーザパスワードでは、より小さい設定範囲の設定が高い優先度を持ちます。

グローバルパスワード管理が有効の場合、ローカルユーザ用に設定されたパスワードは表示されず、パスワードは現在の設定に保存されません。グローバルパスワード管理が無効の場合、ローカルユーザ用に設定されたパスワードは現在の設定で回復されます。現在の設定を表示するには、**display current-configuration** コマンドを使用します。

11.3 パスワード管理設定作業リスト

以下にパスワード管理を設定するための作業リストを示します。

作業リスト
(必須設定項目) パスワード管理の有効化
(オプション設定項目) グローバルパスワード管理パラメータの設定
(オプション設定項目) ユーザグループパスワード管理パラメータの設定
(オプション設定項目) ローカルユーザパスワード管理パラメータの設定
(オプション設定項目) superパスワード管理パラメータの設定

11.4 パスワード管理の有効化

I. 概要

グローバルでパスワード管理機能を有効にすると、すべてのパスワード管理の設定が適用されます。指定したパスワード管理機能を有効にするには、独自のパスワード制御機能を有効にします。

II. 制限とガイドライン

グローバルパスワード管理をイ有効にした後は、次の制約事項および注意事項に従ってください。

- 対応する **display** コマンドを使用して装置管理者用のパスワードと super パスワードを表示することはできません。ただし、ネットワークアクセス用設定のユーザパスワードは表示できます。
- 装置管理ユーザ用に設定する最初のパスワードには、4 文字以上の異なる文字を含める必要があります。

III. 設定手順

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． グローバルパスワード制御機能を有効にする	**password-control enable**	デフォルト：無効
3． (オプション設定項目) 指定したパスワード機能を有効にする	**password-control** { **aging** | **composition** | **history** | **length** } **enable**	デフォルト：4つのすべてのパスワード管理機能は有効です。

11.5 グローバルパスワード管理パラメータの設定

I. 制限とガイドライン

グローバルパスワード管理パラメータを system view で設定すると、すべての装置管理ローカルユーザに適用されます。

パスワードエージング時間、最小パスワード長、およびパスワード設定ポリシーは、system view、user group view、および local user view で設定できます。アプリケーションスコープが小さい範囲でのパスワードの設定が高い優先度を持ちます。ローカルユーザの場合は、local user view で設定されたパスワード設定が最も優先され、system view のグローバル設定が最も優先度が低くなります。

password-control login-attempt コマンドは、即座に適用され、パスワード管理ブラックリストにあるユーザに適用させることができます。他のパスワード管理設定は、既にログインしているユーザ、あるいは設定したパスワードに適用されません。

II. 設定手順

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． パスワードの有効期限を設定する	**password-control aging** *aging-time*	デフォルト：90日
3． パスワードアップデートの最小間隔を設定する	**password-control update-interval** *interval*	デフォルト：24時間
4． 最小パスワード長を設定する	**password-control length** *length*	デフォルト：10文字

操作	コマンド	補足
5. パスワード設定ポリシーを設定する	**password-control composition type-number** *type-number* [**type-length** *type-length*]	デフォルト : パスワードは少なくとも2種類の文字と各タイプに1文字以上を含む必要があります。
6. パスワードの複雑性のポリシーを設定する	**password-control complexity** { **same-character** | **user-name** } **check**	デフォルト： **same-character** は無効、**user-name**は有効
7. 各ユーザのパスワード履歴の最大数を設定する	**password-control history** *max-record-number*	デフォルト : 4
8. ユーザが試行回数後にログインに失敗したときのアクションとログイン最大試行回数を設定する	**password-control login-attempt** *login-times* [**exceed** { **lock** | **lock-time** *time* | **unlock** }]	デフォルト : 最大試行回数 : 3 アクション : ユーザが試行回数後にログインに失敗したとき、1分間ログインの試行をブロックします。
9. ユーザに通知されるパスワードの有効期限までの日数を設定する	**password-control alert-before-expire** *alert-time*	デフォルト : 7日
10. パスワードの有効期限が終了した後､ユーザがログインできる最大日時と最大回数を設定する	**password-control expired-user-login delay** *delay* **times** *times*	デフォルト : 最大日時 : 30日 最大回数 : 3回
11. 最大アカウントアイドルタイムを設定する	**password-control login idle-time** *idle-time*	デフォルト : 90日 ユーザアカウントがこの期間アイドル状態になると、アカウントは無効になり、装置へのログインに使用できなくなります。アカウントのアイドルタイムの制限を無効にするには、アイドルタイムの値を0に設定します。
12. 初回ログイン時のパスワード変更機能を無効にする	**undo password-control change-password first-login enable**	デフォルト : 有効

11.6 ユーザグループパスワード管理パラメータの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. ユーザグループを作成し、user group view に移行する	**user-group** *group-name*	デフォルト : ユーザグループは存在しません。ユーザグループを設定する方法については、オペレーションマニュアルのセクション 9 *セキュリティ”AAA”*を参照してください。
3. パスワードの有効期限を設定する	**password-control aging** *aging-time*	デフォルト : グローバルパスワードの有効期限と同一です。

操作	コマンド	補足
4． 最小パスワード長を設定する	**password-control length** *length*	デフォルト : グローバル最小パスワード長と同一です。
5． パスワード設定ポリシーを設定する	**password-control composition type-number** *type-number* [**type-length** *type-length*]	デフォルト : グローバルパスワード設定ポリシーと同一です。
6． パスワードの複雑性のポリシーを設定する	**password-control complexity** { **same-character** | **user-name** } **check**	デフォルト : グローバルパスワードの複雑性のポリシーと同一です。
7． ユーザが試行回数後にログインに失敗したときのアクションとログイン最大試行回数を設定する	**password-control login-attempt** *login-times* [**exceed** { **lock** | **lock-time** *time* | **unlock** }]	デフォルト : グローバルパスワードのログイン試行ポリシーと同一です。

11.7 ローカルユーザパスワード管理パラメータの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． 装置管理ユーザを作成し、local user view に移行する	**local-user** *user-name* **class manage**	ローカルユーザパスワード管理は、ネットワークアクセスユーザではなく、装置管理ユーザに適用されます。ローカルユーザを設定する方法については、オペレーションマニュアルのセクション9 *セキュリティ”AAA”* を参照してください。
3． パスワードの有効期限を設定する	**password-control aging** *aging-time*	デフォルト : ローカルユーザが属しているユーザグループの有効期限と同一です。ユーザグループの有効期限が設定されていない場合、グローバルの設定が適用されます。
4． 最小パスワード長を設定する	**password-control length** *length*	デフォルト : ローカルユーザが属しているユーザグループの最小パスワード長と同一です。ユーザグループの最小パスワード長が設定されていない場合、グローバルの設定が適用されます。
5． パスワード設定ポリシーを設定する	**password-control composition type-number** *type-number* [**type-length** *type-length*]	デフォルト : ローカルユーザが属しているユーザグループのパスワード設定ポリシーと同一です。ユーザグループのパスワード設定ポリシーが設定されていない場合、グローバルの設定が適用されます。

操作	コマンド	補足
6. パスワードの複雑性のポリシーを設定する	**password-control complexity** { **same-character** | **user-name** } **check**	デフォルト : ローカルユーザが属しているユーザグループのパスワードの複雑性のポリシーと同一です。ユーザグループのパスワードの複雑性のポリシーが設定されていない場合、グローバルの設定が適用されます。
7. ユーザが試行回数後にログインに失敗したときのアクションとログイン最大試行回数を設定する	**password-control login-attempt** *login-times* [**exceed** { **lock** | **lock-time** *time* | **unlock** }]	ローカルユーザが所属するユーザグループの設定と同一です。ユーザグループでログイン試行ポリシーが設定されていない場合、グローバルの設定が適用されます。

11.8 superパスワード管理パラメータの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. パスワードの有効期限を設定する	**password-control super aging** *aging-time*	デフォルト：90日
3. 最小パスワード長を設定する	**password-control super length** *length*	デフォルト：10文字
4. パスワード設定ポリシーを設定する	**password-control super composition type-number** *type-number* [**type-length** *type-length*]	デフォルト : superパスワードは少なくとも2種類の文字と各タイプに1文字以上を含む必要があります。

11.9 パスワード管理の表示と維持

すべての view で **display** コマンドを実行でき、user view で **reset** コマンドを実行できます。

操作	コマンド
パスワード管理の設定を表示する	**display password-control** [**super**]
パスワード管理ブラックリストのユーザ情報を表示する	**display password-control blacklist** [**user-name** *name* | **ip** *ipv4-address* | **ipv6** *ipv6-address*]
パスワード管理ブラックリストからユーザを削除する	**reset password-control blacklist** [**user-name** *name*]
パスワード履歴を削除する	**reset password-control history-record** [**user-name** *user-name* | **super** [**role** *role-name*]]

🕮 **メモ:**

reset password-control history-record コマンドは、パスワード履歴機能が無効になったとき、1 つあるいはすべてのユーザのパスワード履歴を削除することができます。

11.10 パスワード管理の設定例

11.10.1 パスワード管理の設定例

I. ネットワーク要件

グローバルパスワード管理ポリシーを以下のように設定します。

- パスワードは少なくとも 16 文字が必要です。
- パスワードは少なくとも 4 種類以上の文字タイプが必要で各文字タイプに 4 文字以上が必要です。
- FTP あるいは VTY ユーザが 2 回連続してパスワードの試行に失敗すると、ログインの試行を恒久的に禁止します。
- ユーザはパスワードの有効期限後に、60 日内で 5 回ログインすることができます。
- パスワードの有効期限を 30 日に設定します。
- 最小パスワードアップデート間隔を 36 時間に設定します。
- 最大アカウントアイドルタイムを 30 日に設定します。
- パスワードはユーザ名、ユーザ名の逆の順番を含むことができません。
- パスワードに 3 回以上連続した文字を禁止します。

ユーザロール **network-operator** の super パスワード管理ポリシーを以下のように設定します。

- super パスワードは少なくとも 24 文字が必要です。
- super パスワードは少なくとも 4 種類以上の文字タイプが必要で各文字タイプに 5 文字以上が必要です。

ローカル Telnet ユーザ **test** のパスワード管理ポリシーを以下のように設定します。

- パスワードは少なくとも 24 文字が必要です。
- パスワードは少なくとも 4 種類以上の文字タイプが必要で各文字タイプに 5 文字以上が必要です。
- パスワードの有効期限を 20 日に設定します。

II. 設定手順

グローバルにパスワード管理機能を有効にします。

```
<Switch> system-view
[Switch] password-control enable
```

ユーザが 2 回連続してパスワードの試行に失敗すると、ログインの試行を恒久的に禁止します。

```
[Switch] password-control login-attempt 2 exceed lock
```

パスワードの有効期限を 30 日に設定します。

```
[Switch] password-control aging 30
```

グローバルの最小パスワード長を 16 に設定します。

```
[Switch] password-control length 16
```

最小パスワードアップデート間隔を 36 時間に設定します。

```
[Switch] password-control update-interval 36
```

パスワードの有効期限が終了した後、ユーザが 60 日内で 5 回ログインできるように設定します。

```
[Switch] password-control expired-user-login delay 60 times 5
```

最大アカウントアイドルタイムを 30 日に設定します。

```
[Switch] password-control login idle-time 30
```

ユーザ名、ユーザ名の逆の順番を含むパスワードを拒否するように設定します。

```
[Switch] password-control complexity user-name check
```

パスワードに 3 回以上連続した文字を禁止するように指定します。

```
[Switch] password-control complexity same-character check
```

グローバルのパスワードを、少なくとも 4 種類以上の文字タイプで、各文字タイプに 4 文字以上が含まれるように指定します。

```
[Switch] password-control composition type-number 4 type-length 4
```

super パスワードの最小パスワード長を 24 に設定します。

```
[Switch] password-control super length 24
```

super パスワードを、少なくとも 4 種類以上の文字タイプで、各文字タイプに 5 文字以上が含まれるように指定します。

```
[Switch] password-control super composition type-number 4 type-length 5
```

ユーザロール **network-operator** に切り替える super パスワードをプレーンテキストで **123456789ABGFTweuix@#$%!**に設定します。

```
[Switch] super password role network-operator simple 123456789ABGFTweuix@#$%!
```

装置管理ユーザ **test** を作成します。

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

ユーザのサービスタイプを **Telnet** に設定します。

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

ローカルユーザの最小パスワード長を 24 に設定します。

```
[Switch-luser-manage-test] password-control length 24
```

ローカルユーザのパスワードを、少なくとも 4 種類以上の文字タイプで各文字タイプに 5 文字以上が含まれるように指定します。

```
[Switch-luser-manage-test] password-control composition type-number 4 type-length 5
```

ローカルユーザのパスワードの有効期限を 20 日に設定します。

```
[Switch-luser-manage-test] password-control aging 20
```

ローカルユーザのパスワードをインタラクティブモードで設定します。

```
[Switch-luser-manage-test] password
Password:
Confirm :
Updating user information. Please wait ... ...
[Switch-luser-manage-test] quit
```

III. 設定の確認

グローバルパスワード管理の設定を表示します。

```
<Switch> display password-control
Global password control configurations:
 Password control:                       Enabled
 Password aging:                         Enabled (30 days)
 Password length:                        Enabled (16 characters)
 Password composition:                  Enabled (4 types, 4 characters per type)
 Password history:                       Enabled (max history record:4)
 Early notice on password expiration:  7 days
 Maximum login attempts:                 2
 Action for exceeding login attempts:  Lock
 Minimum interval between two updates: 36 hours
 User account idle time:                 30 days
 Logins with aged password:              5 times in 60 days
 Password complexity:                    Enabled (username checking)
                                         Enabled (repeated characters checking)
```

super パスワードのパスワード管理の設定を表示します。

```
<Switch> display password-control super
 Super password control configurations:
 Password aging:                         Enabled (90 days)
 Password length:                        Enabled (24 characters)
 Password composition:                  Enabled (4 types, 5 characters per type)
```

ローカルユーザ **test** のパスワード管理設定を表示します。

```
<Switch> display local-user user-name test class manage
Total 1 local users matched.

Device management user test:
  State:                    Active
  Service type:             Telnet
  User group:               system
  Bind attributes:
  Authorization attributes:
    Work directory:         flash:
    User role list:         network-operator
  Password control configurations:
    Password aging:         Enable (20 days)
    Password length:        Enable (24 characters)
    Password composition:   Enable (4 types, 5 characters per type)
```

QX-S1100G シリーズ Ethernet スイッチ

オペレーションマニュアル

8. 高可用性

本マニュアルは以下に示す章で構成されています。

01-DLDP

02-Smart Link

03-Monitor Link

04-Track

目次

このセクションのページは**8-x-x** です。

1章 DLDP 1-1
1.1 概要 1-1
1.1.1 基本概念 1-2
1.1.2 DLDPの動作 1-3
1.2 設定の制限とガイドライン 1-6
1.3 DLDP設定作業リスト 1-6
1.4 DLDPの有効化 1-7
1.5 Advertisementパケットの送信間隔の設定 1-7
1.6 DelayDownタイマの設定 1-7
1.7 ポートシャットダウンモードの設定 1-8
1.8 DLDP認証の設定 1-8
1.9 DLDPの表示と維持 1-9
1.10 DLDP設定例 1-9
1.10.1 片方向リンクの自動シャットダウンの設定例 1-9
1.10.2 片方向リンクの手動シャットダウンの設定例 1-12

1章 DLDP

1.1 概要

片方向リンクが発生すると、片方のリンクは反対側からパケットを受信できますが、もう一方のリンクはパケットを受信できません。

片方向リンクは、以下のタイプがあります。

- ファイバがクロス接続されている場合に発生します。
- ファイバがもう一方に接続されていない場合、あるいはファイバのペアケーブルの一本が断線した場合に発生します。

図 1-1に正常な接続と 2 つの片方向リンクの例を示します。

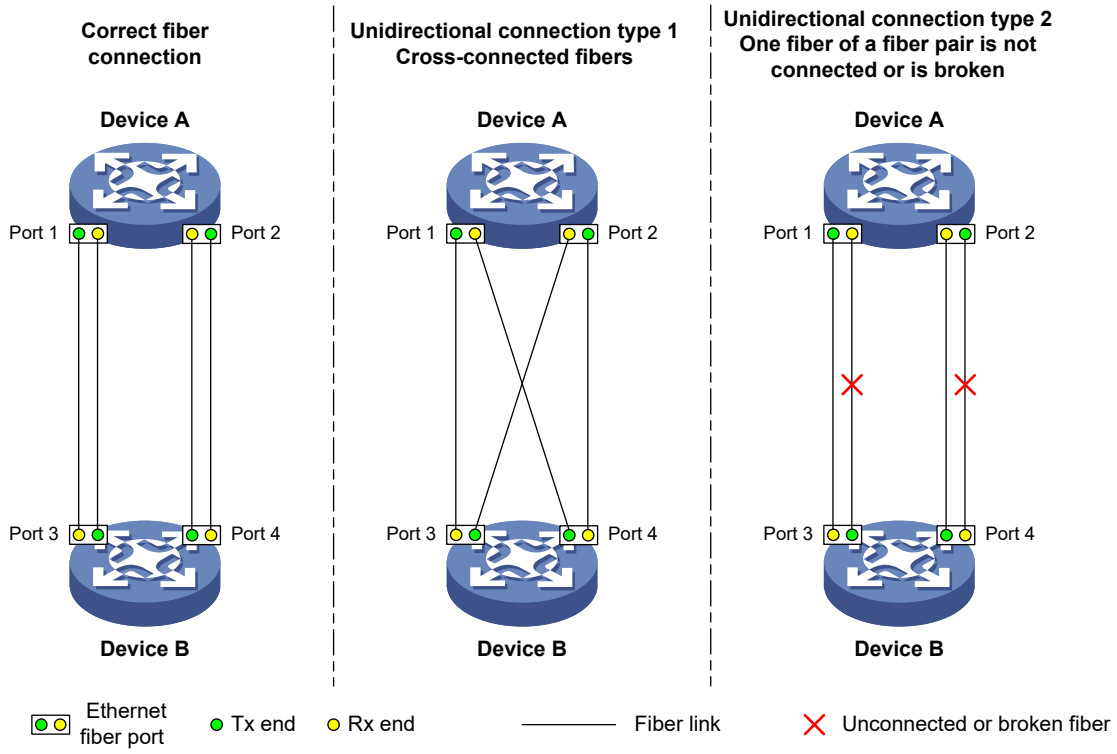


図 1-1 ファイバの正常な接続と異常な接続

オートネゴシエーションなどの物理レイヤの検出メカニズムが物理的な信号や故障を検出しても、物理レイヤで接続されているが片方向リンクによって接続故障を検出することはできません。

データリンクレイヤプロトコルの DLDP（Device Link Detection Protocol）は、リンクレイヤで正しく接続されているか、2 つのエンド間でパケットが正しく交換できるかどうかを検出します。DLDP が片方向リンクを検出した場合、ネットワークの問題を避けるため、故障ポートを自動的にシャットダウンする、あるいはユーザが故障ポートを手動でシャッ

トダウンすることができます。DLDP は物理レイヤプロトコルと連携して、リンク状態をモニタし、物理と論理の片方向リンクになることを回避します。

1.1.1 基本概念

I. DLDP ネイバ状態

ポート A とポート B が同一リンクにあり、ポート A がポート B からリンクレイヤパケットを受信できる場合、ポート B はポート A の DLDP ネイバとなります。パケットの交換を行うことができる 2 つのポートはネイバです。

表 1-1 DLDP ネイバ状態

DLDP タイマ	説明
Confirmed	DLDPネイバのリンクが双方向です。
Unconfirmed	新しく発見されたネイバのリンク状態が、確定されていません。

II. DLDP ポート状態

DLDP が有効なポートは、DLDP ポートと呼ばれます。DLDP ポートは複数のネイバを持つことができます。DLDP のポート状態は、DLDP ネイバの状態によって異なります。

表 1-2 DLDP ポート状態

状態	説明
Initial	DLDPがポートで有効ですが、グローバルで無効となっています。
Inactive	DLDPがポートとグローバルで有効ですが、リンクが物理的にダウンしています。
Bidirectional	DLDPがポートとグローバルで有効で、1つ以上のConfirmed 状態のネイバが存在します。
Unidirectional	DLDPがポートとグローバルで有効ですが、Confirmed 状態のネイバがありません。この状態では、ポートはこれ以上DLDPパケット以外のパケットを送受信しません。

III. DLDP タイマ

表 1-3 DLDP タイマ

DLDP タイマ	説明
Advertisementタイマ	Advertisementパケットの送信間隔です。（デフォルトは5秒で、設定可能です）
Probeタイマ	Probeパケットの送信間隔です。このタイマは1秒に設定されます。
Echoタイマ	新しいネイバ用にProbe状態になった場合にEchoタイマが起動します。タイマは10秒に設定されます。

DLDP タイマ	説明
Entryタイマ	新しいネイバが追加された場合、ネイバがConfirmedの場合、ネイバエントリが作成され、対応するEntryタイマが起動します。 Advertisementパケットを受信した場合、装置は対応するネイバエントリとEntryタイマをアップデートします。 Entryタイマの設定はAdvertisementタイマの3倍です。
Enhancedタイマ	Entryタイマが終了した場合、Echoタイマと一緒にEnhancedタイマが起動します。Enhancedタイマは1秒に設定されます。
DelayDownタイマ	ポートが物理的にダウンした場合、装置はDelayDownタイマを開始します。それは対応するネイバエントリを削除するまでの時間です。デフォルトは1秒で、設定可能です。 DelayDownタイマが終了した場合、ポートがダウンである場合、装置は対応するDLDPネイバ情報を削除します。ポートがアップである場合は、装置は対応するDLDPネイバ情報を削除しません。
RecoverProbeタイマ	タイマは2秒に設定されます。Unidirectional状態のポートは、片方向リンクが双方向リンクに回復したかどうかを検出するために、RecoverProbeパケットを規則的に送信します。

IV. DLDP 認証モード

ネットワークの攻撃と不正な検出を防ぐために、DLDP 認証を使用することができます。

表 1-4 DLDP 認証モード

認証モード	DLDP パケット送信側の処理	DLDP パケット受信側の処理
Non-authentication	DLDPパケットの認証フィールドを0に設定します。	受信したDLDPパケットの認証情報を確認し、認証情報がローカル設定と矛盾しているパケットを廃棄します。
Plaintext authentication	認証フィールドを平文で設定されたパスワードに設定します。	
MD5 authentication	MD5アルゴリズムを使用してユーザが設定したパスワードを暗号化し、認証フィールドをダイジェストで割り当てます。	

1.1.2 DLDP の動作

I. 1 つのネイバの検出

2 つの装置がファイバあるいはネットワークケーブルで接続されている場合、ネイバの片方向リンクを検出するため、DLDP を有効にします。片方向リンクの検出処理を以下の 2 つのケースで示します。

- DLDP を有効にする前に片方向リンクが発生

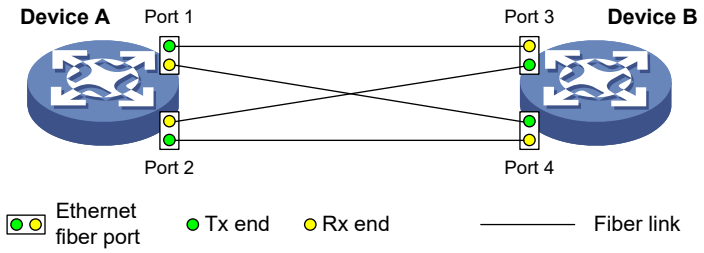


図 1-2 クロス接続ファイバ

図 1-2に示すように、DLDP を有効にする前に、Device A と Device B 間のファイバがクロス接続されています。DLDP を有効にした後、4 つのポートがすべてアップし、Unidirectional 状態になります。RecoverProbe パケットを送信します。例として、ポート 1 の片方向リンク検出処理を示します。

a) ポート1がポート4からRecoverProbeパケットを受信し、RecoverEchoパケットを返します。

b) ポート4はポート1からRecoverEchoパケットを受信することができないため、ポート4はポート1のネイバになることができません。

c) ポート3はポート1からRecoverEchoパケットを受信できますが、ポート3は宛先でないため、ポート3はポート1のネイバになることができません。

他の 3 つのポートで同一の処理が行われます。4 つのポートは Unidirectional 状態となります。

- DLDP を有効にした後に片方向リンクが発生します。

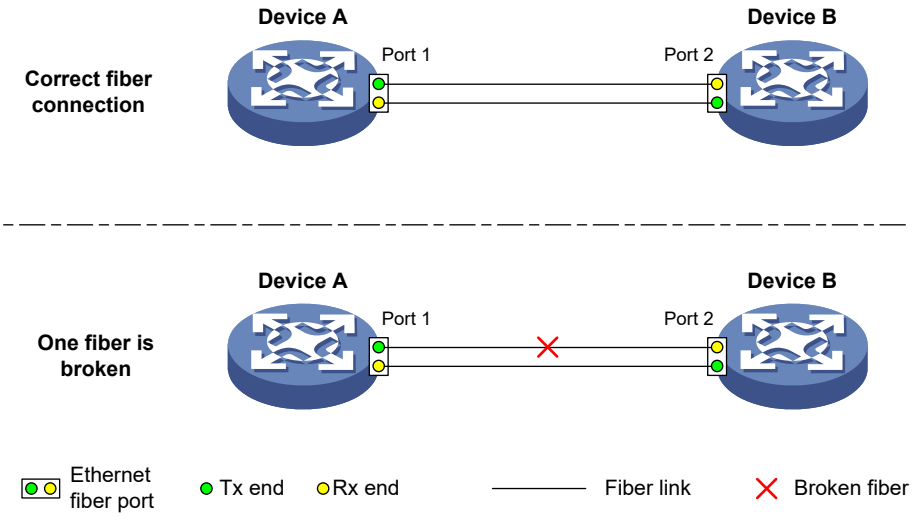


図 1-3 ファイバの故障

図 1-3に示すように、Device A と Device B はファイバで接続されています。DLDP を有効にした後、ポート 1 とポート 2 は以下のように双方向の隣接関係を構築します。

a) 物理的にアップ状態のポート1はUnidirectional状態になり、RecoverProbeパケットを送信します。

b) RecoverProbeパケットを受信した後、ポート2はRecoverEchoパケットを返します。

c) ポート1がRecoverEchoパケットを受信した後、パケットの隣接情報がローカルの情報にマッチするか確認します。ポート1はポート2と隣接関係を確立し、Bidirectional状態に移行します。ポート1はEntryタイマを開始し、Advertisementパケットを定期的に送信します。

d) ポート2がAdvertisementパケットを受信した後、ポート1と未確認の隣接状態を確立します。ポート2はEchoタイマ、Probeタイマを開始し、定期的にProbeパケットを送信します。

e) Probeパケットを受信した後、ポート1はEchoパケットを返します。

f) ポート2がEchoパケットを受信した後、パケットの隣接情報がローカル情報にマッチするか確認します。ポート1のneighbor状態がConfirmed状態になります。ポート2はBidirectional状態になります。ポート2はEntryタイマを開始し、定期的にAdvertisementパケットを送信します。

このようにして、ポート 1 とポート 2 の双方向隣接関係が確立されます。

隣接関係の構築が行われた後、ポート 2 の Rx のエンド側が信号を受信するのに失敗すると、ポート 2 は物理的にダウンし、Inactive 状態になります。ポート 2 の Tx のエンド側はポート 1 に信号を送信することができるため、ポート 1 はアップ状態となり続けます。ポート 2 の Entry タイマが終了した後、ポート 1 は Enhanced タイマと Echo タイマを開始し、ポート 2 に Probe パケットを送信します。ポート 1 の Tx ラインが故障しているため、Echo タイマが終了した後、ポート 1 はポート 2 から Echo パケットを受信することができません。ポート 1 は Unidirectional 状態になり、ポート 2 に Disable パケットを送信します。同時に、ポート 1 はポート 2 の隣接関係を削除し、RecoverProbe タイマを開始します。この処理の間、ポート 2 は Inactive 状態を維持します。

II. 複数ネイバの検出

複数の装置がハブを介して接続されている場合、ハブに接続されたすべてのインタフェースの DLDP をネイバ間の片方向リンクを検出するために有効にします。確認されたネイバが存在しない場合、インタフェースは Unidirectional 状態になります。

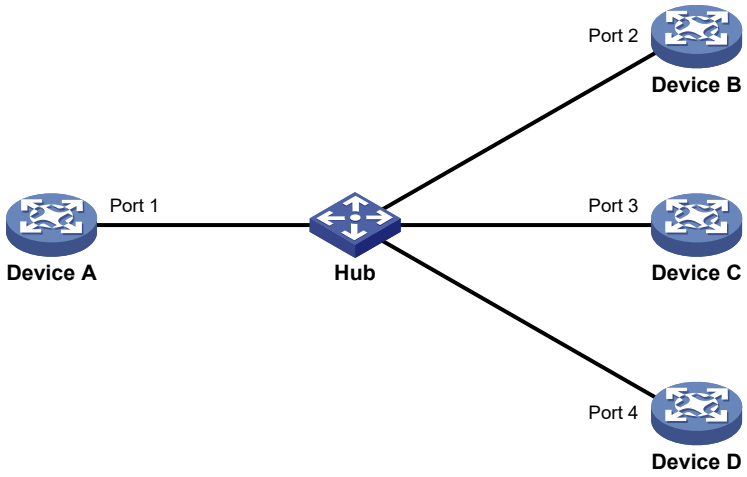


図 1-4 ネットワーク図

図 1-4に示すように、Device A から Device D はハブを介して接続され、DLDP が有効になっています。ポート 1、ポート 2、ポート 3 がポート 4 のリンクが故障したと検出した場合、ポート 4 との隣接関係を削除しますが、Bidirectional 状態を維持します。

1.2 設定の制限とガイドライン

DLDP を設定する場合、以下の設定の制限とガイドラインに従ってください。

- DLDP を正しく動作させるため、両端で DLDP を有効にし、Advertisement パケットを送信する間隔、DLDP 認証モード、パスワードの設定が同一であることを確認してください。
- DLDP を正しく動作させるため、2 つのリンクの終端ポートが全 2 重モードで、同一速度が設定されていることを確認してください。
- 両端のポートでオートネゴシエーションが動作する場合はリンクダウンが直ちに発生します。

1.3 DLDP設定作業リスト

作業リスト
（必須設定項目） DLDPの有効化
（オプション設定項目） Advertisementパケットの送信間隔の設定
（オプション設定項目） DelayDownタイマの設定
（オプション設定項目） ポートシャットダウンモードの設定
（オプション設定項目） DLDP認証の設定

1.4 DLDPの有効化

装置で DLDP を正しく設定するため、グローバルとポートで DLDP を有効にする必要があります。

以下に DLDP を有効にする設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． グローバルに DLDP を有効にする	**dldp global enable**	デフォルト：無効
3． Ethernet interface view に移行する	**interface** *interface-type interface-number*	―
4． DLDP を有効にする	**dldp enable**	デフォルト：無効

🕮 **メモ：**

両端のポートでオートネゴシエーションが動作する場合、リンクダウンが直ちに発生します。

1.5 Advertisementパケットの送信間隔の設定

ネットワーク性能が低下する前に、片方向リンクを検出することができるようするため、ネットワーク環境に適した Advertisement パケットの送信間隔を設定します。（デフォルトの間隔を使用することを推奨します。）

以下に Advertisement パケットの送信間隔の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． Advertisement パケットの送信間隔を設定する	**dldp interval** *time*	デフォルト：5秒

1.6 DelayDownタイマの設定

ポートで Tx ラインの故障が発生すると、一部のポートはアップダウンを繰り返し、Rx ラインの光信号ジッタを引き起こします。この問題を避けるため、Tx の故障によってポートがダウンする場合、装置は、対応するネイバエントリが削除されるのを防ぐため、DelayDown タイマを開始します。タイマが終了しポートがダウンしたままである場合、装置は DLDP ネイバ情報を削除します。ポートがアップである場合、何もアクションを行いません。

以下に DelayDown の設定を示します。

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

操作	コマンド	補足
2． DelayDown タイマを設定する	**dldp delaydown-timer** *time*	デフォルト：1秒 すべてのDLDPが設定されているポートに適用されます。

1.7 ポートシャットダウンモードの設定

片方向リンクを検出した場合、ポートを以下の 2 つのモードのどちらかでシャットダウンすることができます。

- **自動モード**－片方向リンクが検出された場合、DLDP は DLDP ポートの状態を片方向に変更します。片方向のポートは定期的に RecoverProbe パケットを送信します。正しい RecoverEcho パケットを受信した場合、ローカルポートとネイバ間のリンクは双方向リンクに回復し、ポートは Unidirectional 状態から Bidirectional 状態に遷移します。このプロセスはリンクオートリカバリメカニズムと呼ばれます。
- **手動モード**－片方向リンクが検出された場合、DLDP はポートをシャットダウンしません。手動でシャットダウンする必要があります。リンクの状態が双方向に回復した場合、手動でポートをアップにする必要があります。ネットワークの性能が低い、装置がビジー状態、CPU 使用率が高い場合、通常のリンクが片方向リンクとみなすことがあります。このような、誤った片方向リンクの報告による影響を軽減するため、手動モードにすることができます。

以下にポートシャットダウンモードの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	－
2． ポートシャットダウンモードを設定する	**dldp unidirectional-shutdown** { **auto** | **manual** }	デフォルト：**auto**

1.8 DLDP認証の設定

平文テキスト認証あるいは MD5 認証の DLDP 認証モードを適切に設定することにより、攻撃および悪意のあるアクセスからネットワークを保護できます。ネットワークが安全である場合、認証を行わないように選択することができます。

以下に DLDP 認証の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	－
2． DLDP 認証モードを設定する	**dldp authentication-mode** { **md5** | **none** | **simple** }	デフォルト：**none**
3． DLDP 認証のパスワードを設定する	**dldp authentication-password** { **cipher** | **simple** } *string*	デフォルト：設定なし 認証モードを設定した後、パスワードを設定しない場合、設定した認証モードにかかわらず、認証モードは**none**になります。

1.9 DLDPの表示と維持

すべての view で **display** コマンドを実行でき、user view で **reset** コマンドを実行できます。

操作	コマンド
グローバルとポートのDLDPの設定を表示する	**display dldp** [**interface** *interface-type interface-number*]
ポートを通過したDLDPパケットの統計情報を表示する	**display dldp statistics** [**interface** *interface-type interface-number*]
ポートを通過したDLDPパケットの統計情報をクリアする	**reset dldp statistics** [**interface** *interface-type interface-number*]

1.10 DLDP設定例

1.10.1 片方向リンクの自動シャットダウンの設定例

I. ネットワーク要件

図 1-5に示すように、Device A と Device B が 2 対のファイバで接続されています。

片方向リンクの検出時に障害のあるポートを自動的にシャットダウンし、障害をクリアした後に自動的にポートをアップするように DLDP を設定します。

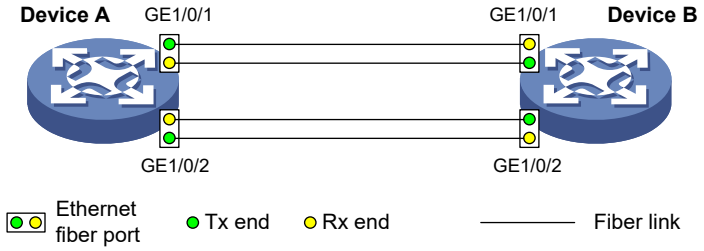


図 1-5 ネットワーク図

II. 設定手順

1)　Device A を設定します。

グローバルに DLDP を有効にします。

```
<DeviceA> system-view
[DeviceA] dldp global enable
```

GigabitEthernet 1/0/1 を全 2 重モード、1000 Mbps に設定し、ポートで DLDP を有効にします。

```
[DeviceA] interface gigabitethernet 1/0/1
```

```
[DeviceA-GigabitEthernet1/0/1] duplex full
[DeviceA-GigabitEthernet1/0/1] speed 1000
[DeviceA-GigabitEthernet1/0/1] dldp enable
[DeviceA-GigabitEthernet1/0/1] quit
```

GigabitEthernet 1/0/2 を全 2 重モード、1000 Mbps に設定し、ポートで DLDP を有効にします。

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] duplex full
[DeviceA-GigabitEthernet1/0/2] speed 1000
[DeviceA-GigabitEthernet1/0/2] dldp enable
[DeviceA-GigabitEthernet1/0/2] quit
```

ポートシャットダウンモードを auto に設定します。

```
[DeviceA] dldp unidirectional-shutdown auto
```

2) Device B を設定します。

グローバルに DLDP を有効にします。

```
<DeviceB> system-view
[DeviceB] dldp global enable
```

GigabitEthernet 1/0/1 を全 2 重モード、1000 Mbps に設定し、ポートで DLDP を有効にします。

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] duplex full
[DeviceB-GigabitEthernet1/0/1] speed 1000
[DeviceB-GigabitEthernet1/0/1] dldp enable
[DeviceB-GigabitEthernet1/0/1] quit
```

GigabitEthernet 1/0/2 を全 2 重モード、1000 Mbps に設定し、ポートで DLDP を有効にします。

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] duplex full
[DeviceB-GigabitEthernet1/0/2] speed 1000
[DeviceB-GigabitEthernet1/0/2] dldp enable
[DeviceB-GigabitEthernet1/0/2] quit
```

ポートシャットダウンモードを auto に設定します。

```
[DeviceB] dldp unidirectional-shutdown auto
```

3) 設定の確認

設定が完了した後、グローバルとポートで DLDP の設定を表示するため、**display dldp** コマンドを使用します。

Device A のグローバルと DLDP が有効になっているすべてのポートの DLDP の設定を表示します。

```
[DeviceA] display dldp
 DLDP global status: Enabled
 DLDP advertisement interval: 5s
 DLDP authentication-mode: None
 DLDP unidirectional-shutdown mode: Auto
 DLDP delaydown-timer value: 1s
 Number of enabled ports: 2

Interface GigabitEthernet1/0/1
 DLDP port state: Bidirectional
 DLDP initial-unidirectional-delay: 0s
 Number of the port's neighbors: 1
  Neighbor MAC address: 0023-8956-3600
  Neighbor port index: 1
  Neighbor state: Confirmed
  Neighbor aged time: 11s
  Neighbor echo time: -

Interface GigabitEthernet1/0/2
 DLDP port state: Bidirectional
 DLDP initial-unidirectional-delay: 0s
 Number of the port's neighbors: 1
  Neighbor MAC address: 0023-8956-3600
  Neighbor port index: 2
  Neighbor state: Confirmed
  Neighbor aged time: 12s
  Neighbor echo time: -
```

出力は、GigabitEthernet 1/0/1 と GigabitEthernet 1/0/2 の両方が、双方向リンクであることを示す Bidirectional 状態であることを示します。

Device A の現在の端末でログのモニタリングを有効にし、現在の端末に出力するログレベルをもっとも低いレベルの 6 に設定します。

```
[DeviceA] quit
<DeviceA> terminal monitor
<DeviceA> terminal logging level 6
```

以下のログ情報が Device A で表示されます。

```
<DeviceA>%Jul 11 17:40:31:089 2012 DeviceA IFNET/3/PHY_UPDOWN: Physical state on
the interface Physical state on the interface GigabitEthernet1/0/1 changed to
down.
%Jul 11 17:40:31:091 2012 DeviceA IFNET/5/LINK_UPDOWN: Line protocol state on the
interface GigabitEthernet1/0/1 changed to down.
%Jul 11 17:40:31:677 2012 DeviceA IFNET/3/PHY_UPDOWN: Physical state on the
interface Physical state on the interface GigabitEthernet1/0/2 changed to down.
%Jul 11 17:40:31:678 2012 DeviceA IFNET/5/LINK_UPDOWN: Line protocol state on the
interface GigabitEthernet1/0/2 changed to down.
%Jul 11 17:40:38:544 2012 DeviceA IFNET/3/PHY_UPDOWN: Physical state on the
interface Physical state on the interface GigabitEthernet1/0/1 l changed to up.
%Jul 11 17:40:38:836 2012 DeviceA IFNET/3/PHY_UPDOWN: Physical state on the
interface Physical state on the interface GigabitEthernet1/0/2 changed to up.
```

出力は、GigabitEthernet 1/0/1 と GigabitEthernet 1/0/2 の両方のポートの状態が、ダウンとなり、その後アップとなりますが、リンク状態がダウンのままとなっていることを示します。

グローバルと DLDP が有効になっているすべてのポートの DLDP の設定を表示します。

```
<DeviceA> display dldp
 DLDP global status: Enabled
 DLDP advertisement interval: 5s
 DLDP authentication-mode: None
 DLDP unidirectional-shutdown mode: Auto
 DLDP delaydown-timer value: 1s
 Number of enabled ports: 2

Interface GigabitEthernet1/0/1
 DLDP port state: Unidirectional
 DLDP initial-unidirectional-delay: 0s
 Number of the port’s neighbors: 0 (Maximum number ever detected: 1)
 DLDP initial-unidirectional-delay: 0s
Interface GigabitEthernet1/0/2
 DLDP port state: Unidirectional

 Number of the port’s neighbors: 0 (Maximum number ever detected: 1)
```

出力は、GigabitEthernet 1/0/1 と GigabitEthernet 1/0/2 の DLDP ポート状態が Unidirectional 状態であることを示します。それは DLDP が片方向リンクを検出し、2 つのポートを自動的にシャットダウンしたことを示します。

片方向リンクは、クロス接続ファイバによって引き起こされています。ファイバの接続を正しく接続します。その結果、DLDP によってポートのシャットダウンは自動的に回復します。Device A は以下のログ情報を表示します。

```
<DeviceA>%Jul 11 17:42:57:709 2012 DeviceA IFNET/3/PHY_UPDOWN: Physical state on
the interface GigabitEthernet1/0/1 changed to down.
%Jul 11 17:42:58:603 2012 DeviceA IFNET/3/PHY_UPDOWN: Physical state on the
interface GigabitEthernet1/0/2 changed to down.
%Jul 11 17:43:02:342 2012 DeviceA IFNET/3/PHY_UPDOWN: Physical state on the
interface GigabitEthernet1/0/1 changed to up.
%Jul 11 17:43:02:343 2012 DeviceA DLDP/6/DLDP_NEIGHBOR_CONFIRMED: A neighbor was
confirmed on interface GigabitEthernet1/0/1. The neighbor's system MAC is
0023-8956-3600, and the port index is 1.
%Jul 11 17:43:02:344 2012 DeviceA DLDP/6/DLDP_LINK_BIDIRECTIONAL: DLDP detected
a bidirectional link on interface GigabitEthernet1/0/1.
%Jul 11 17:43:02:353 2012 DeviceA IFNET/5/LINK_UPDOWN: Line protocol state on the
interface GigabitEthernet1/0/1 changed to up.
%Jul 11 17:43:02:357 2012 DeviceA IFNET/3/PHY_UPDOWN: Physical state on the
interface GigabitEthernet1/0/2 changed to up.
%Jul 11 17:43:02:362 2012 DeviceA DLDP/6/DLDP_NEIGHBOR_CONFIRMED: A neighbor was
confirmed on interface GigabitEthernet1/0/2. The neighbor's system MAC is
0023-8956-3600, and the port index is 2.
%Jul 11 17:43:02:362 2012 DeviceA DLDP/6/DLDP_LINK_BIDIRECTIONAL: DLDP detected
a bidirectional link on interface GigabitEthernet1/0/2.
%Jul 11 17:43:02:368 2012 DeviceA IFNET/5/LINK_UPDOWN: Line protocol state on the
interface GigabitEthernet1/0/2 changed to up.
```

出力は、GigabitEthernet 1/0/1 と GigabitEthernet 1/0/2 の両方のポート状態とリンク状態がアップになり、DLDP ネイバが確認されたことを示します。

1.10.2 片方向リンクの手動シャットダウンの設定例

I. ネットワーク要件

図 1-6に示すように、Device A と Device B が 2 対のファイバで接続されています。

片方向リンクを検出するように DLDP の設定を行います。片方向リンクの検出時、障害のあるポートを手動でシャットダウンする必要があります。

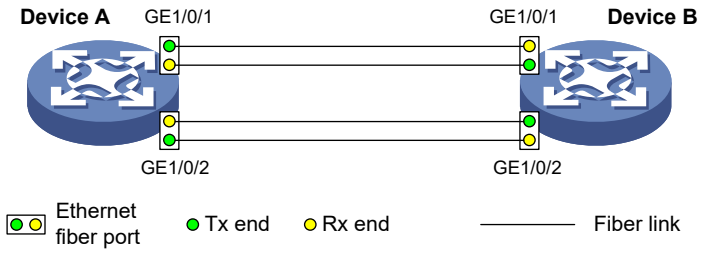


図 1-6 ネットワーク図

II. 設定手順

1)　Device A を設定します。

グローバルに DLDP を有効にします。

```
<DeviceA> system-view
[DeviceA] dldp enable
```

GigabitEthernet 1/0/1 を全 2 重モード、1000 Mbps に設定し、ポートで DLDP を有効にします。

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] duplex full
[DeviceA-GigabitEthernet1/0/1] speed 1000
[DeviceA-GigabitEthernet1/0/1] dldp enable
[DeviceA-GigabitEthernet1/0/1] quit
```

GigabitEthernet 1/0/2 を全 2 重モード、1000 Mbps に設定し、ポートで DLDP を有効にします。

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] duplex full
[DeviceA-GigabitEthernet1/0/2] speed 1000
[DeviceA-GigabitEthernet1/0/2] dldp enable
[DeviceA-GigabitEthernet1/0/2] quit
```

ポートシャットダウンモードを manual に設定します。

```
[DeviceA] dldp unidirectional-shutdown manual
```

2)　Device B を設定します。

グローバルに DLDP を有効にします。

```
<DeviceB> system-view
[DeviceB] dldp global enable
```

GigabitEthernet 1/0/1 を全 2 重モード、1000 Mbps に設定し、ポートで DLDP を有効にします。

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] duplex full
[DeviceB-GigabitEthernet1/0/1] speed 1000
[DeviceB-GigabitEthernet1/0/1] dldp enable
[DeviceB-GigabitEthernet1/0/1] quit
```

GigabitEthernet 1/0/2 を全 2 重モード、1000 Mbps に設定し、ポートで DLDP を有効にします。

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] duplex full
[DeviceB-GigabitEthernet1/0/2] speed 1000
[DeviceB-GigabitEthernet1/0/2] dldp enable
[DeviceB-GigabitEthernet1/0/2] quit
```

ポートシャットダウンモードを manual に設定します。

```
[DeviceB] dldp unidirectional-shutdown manual
```

3)　設定の確認

設定が完了した後、グローバルとポートで DLDP の設定を表示するため、**display dldp** コマンドを使用します。

Device A のグローバルと DLDP が有効になっているすべてのポートの DLDP の設定を表示します。

```
[DeviceA] display dldp
 DLDP global status: Enabled
 DLDP advertisement interval: 5s
 DLDP authentication-mode: None
 DLDP unidirectional-shutdown mode: Manual
 DLDP delaydown-timer value: 1s
 Number of enabled ports: 2

Interface GigabitEthernet1/0/1
 DLDP port state: Bidirectional
 DLDP initial-unidirectional-delay: 0s
 Number of the port's neighbors: 1
  Neighbor MAC address: 0023-8956-3600
  Neighbor port index: 1
  Neighbor state: Confirmed
  Neighbor aged time: 11s
  Neighbor echo time: -

Interface GigabitEthernet1/0/2
 DLDP port state: Bidirectional
 DLDP initial-unidirectional-delay: 0s
 Number of the port's neighbors: 1
  Neighbor MAC address: 0023-8956-3600
  Neighbor port index: 2
  Neighbor state: Confirmed
  Neighbor aged time: 12s
  Neighbor echo time: -
```

出力は、GigabitEthernet 1/0/1 と GigabitEthernet 1/0/2 の両方が、双方向リンクであることを示す Bidirectional 状態であることを示します。

Device A の現在の端末でログのモニタリングを有効にし、現在の端末に出力するログレベルをもっとも低いレベルの 6 に設定します。

```
[DeviceA] quit
<DeviceA> terminal monitor
<DeviceA> terminal logging level 6
```

以下のログ情報が Device A で表示されます。

```
<DeviceA>%Jul 12 08:29:17:786 2012 DeviceA IFNET/3/PHY_UPDOWN: Physical state on
the interface GigabitEthernet1/0/1 changed to down.
%Jul 12 08:29:17:787 2012 DeviceA IFNET/5/LINK_UPDOWN: Line protocol state on the
interface GigabitEthernet1/0/1 changed to down.
%Jul 12 08:29:17:800 2012 DeviceA IFNET/3/PHY_UPDOWN: Physical state on the
interface GigabitEthernet1/0/2 changed to down.
%Jul 12 08:29:17:800 2012 DeviceA IFNET/5/LINK_UPDOWN: Line protocol state on the
interface GigabitEthernet1/0/2 changed to down.
%Jul 12 08:29:25:004 2012 DeviceA IFNET/3/PHY_UPDOWN: Physical state on the
interface GigabitEthernet1/0/1 changed to up.
%Jul 12 08:29:25:005 2012 DeviceA IFNET/5/LINK_UPDOWN: Line protocol state on the
interface GigabitEthernet1/0/1 changed to up.
%Jul 12 08:29:25:893 2012 DeviceA IFNET/3/PHY_UPDOWN: Physical state on the
interface GigabitEthernet1/0/2 changed to up.
%Jul 12 08:29:25:894 2012 DeviceA IFNET/5/LINK_UPDOWN: Line protocol state on the
interface GigabitEthernet1/0/2 changed to up.
```

出力は、GigabitEthernet 1/0/1 と GigabitEthernet 1/0/2 の両方のポートの状態とリンクの状態がダウンとなり、その後アップとなります。

グローバルと DLDP が有効になっているすべてのポートの DLDP の設定を表示します。

```
<DeviceA> display dldp
 DLDP global status: Enabled
 DLDP advertisement interval: 5s
 DLDP authentication-mode: None
 DLDP unidirectional-shutdown mode: Manual
 DLDP delaydown-timer value: 1s
 Number of enabled ports: 2

Interface GigabitEthernet1/0/1
 DLDP port state: Unidirectional
 DLDP initial-unidirectional-delay: 0s
 Number of the port's neighbors: 0 (Maximum number ever detected: 1)

Interface GigabitEthernet1/0/2
 DLDP port state: Unidirectional
 DLDP initial-unidirectional-delay: 0s
 Number of the port's neighbors: 0 (Maximum number ever detected: 1)
```

出力は、GigabitEthernet 1/0/1 と GigabitEthernet 1/0/2 の DLDP ポート状態が unidirectional 状態であることを示します。それは DLDP が片方向リンクを検出しますが、2 つのポートをシャットダウンしていないことを示します。

片方向リンクは、クロス接続ファイバによって引き起こされています。2 つのポートを手動でシャットダウンします。

GigabitEthernet 1/0/1 をシャットダウンします。

```
<DeviceA> system-view
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] shutdown
```

以下のログ情報が Device A で表示されます。

```
[DeviceA-GigabitEthernet1/0/1]%Jul 12 08:34:23:717 2012 DeviceA
IFNET/3/PHY_UPDOWN: Physical state on the interface GigabitEthernet1/0/1 changed
to down.
%Jul 12 08:34:23:718 2012 DeviceA IFNET/5/LINK_UPDOWN: Line protocol state on the
interface GigabitEthernet1/0/1 changed to down.
%Jul 12 08:34:23:778 2012 DeviceA IFNET/3/PHY_UPDOWN: Physical state on the
interface GigabitEthernet1/0/2 changed to down.
%Jul 12 08:34:23:779 2012 DeviceA IFNET/5/LINK_UPDOWN: Line protocol state on the
interface GigabitEthernet1/0/2 changed to down.
```

出力は、GigabitEthernet 1/0/1 と GigabitEthernet 1/0/2 の両方のポートの状態とリンクの状態が、ダウンとなります。

GigabitEthernet 1/0/2 をシャットダウンします。

```
[DeviceA-GigabitEthernet1/0/1] quit
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] shutdown
```

ファイバの接続を正しく接続し、2 つのポートをアップにします。

GigabitEthernet 1/0/2 をアップにします。

```
[DeviceA-GigabitEthernet1/0/2] undo shutdown
```

以下のログ情報が Device A で表示されます。

```
[DeviceA-GigabitEthernet1/0/2]%Jul 12 08:46:17:677 2012 DeviceA
IFNET/3/PHY_UPDOWN: Physical state on the interface GigabitEthernet1/0/2 changed
to up.
%Jul 12 08:46:17:678 2012 DeviceA IFNET/5/LINK_UPDOWN: Line protocol state on the
interface GigabitEthernet1/0/2 changed to up.
%Jul 12 08:46:17:959 2012 DeviceA DLDP/6/DLDP_NEIGHBOR_CONFIRMED: A neighbor was
confirmed on interface GigabitEthernet1/0/2. The neighbor's system MAC is
0023-8956-3600, and the port index is 2.
%Jul 12 08:46:17:959 2012 DeviceA DLDP/6/DLDP_LINK_BIDIRECTIONAL: DLDP detected
a bidirectional link on interface GigabitEthernet1/0/2.
```

出力は、GigabitEthernet 1/0/2 のポートの状態とリンクの状態がアップとなり、DLDP ネイバが確認されたことを示します。

GigabitEthernet 1/0/1 をアップにします。

```
[DeviceA-GigabitEthernet1/0/2] quit
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] undo shutdown
```

以下のログ情報が Device A で表示されます。

```
[DeviceA-GigabitEthernet1/0/1]%Jul 12 08:48:25:952 2012 DeviceA
IFNET/3/PHY_UPDOWN: Physical state on the interface GigabitEthernet1/0/1 changed
to up.
%Jul 12 08:48:25:952 2012 DeviceA DLDP/6/DLDP_NEIGHBOR_CONFIRMED: A neighbor was
confirmed on interface GigabitEthernet1/0/1. The neighbor's system MAC is
0023-8956-3600, and the port index is 1.
%Jul 12 08:48:25:953 2012 DeviceA IFNET/5/LINK_UPDOWN: Line protocol state on the
interface GigabitEthernet1/0/1 changed to up.
%Jul 12 08:48:25:953 2012 DeviceA DLDP/6/DLDP_LINK_BIDIRECTIONAL: DLDP detected
a bidirectional link on interface GigabitEthernet1/0/1.
```

出力は、GigabitEthernet 1/0/1 のポートの状態とリンクの状態がアップとなり、DLDP ネイバが確認されたことを示します。

目次

このセクションのページは**8-x-x** です。

2章 Smart Link 2-1
2.1 概要 2-1
2.1.1 基本概念 2-2
2.1.2 Smart Linkの動作メカニズム 2-3
2.1.3 Smart LinkとMonitor Linkのコラボレーション 2-4
2.2 Smart Link 設定作業リスト 2-4
2.3 Smart Link装置の設定 2-4
2.3.1 設定要件 2-4
2.3.2 Smart Linkグループのプロテクトvlanの設定 2-5
2.3.3 Smart Linkグループのメンバポートの設定 2-7
2.3.4 Smart Linkグループのrole preemptionの設定 2-8
2.3.5 flushメッセージの送信の有効化 2-8
2.4 関連装置の設定 2-9
2.4.1 設定要件 2-9
2.4.2 flushメッセージの受信の有効化 2-9
2.5 Smart Linkの表示と維持 2-9
2.6 Smart Linkの設定例 2-10
2.6.1 単一Smart Link groupグループの設定例 2-10
2.6.2 複数Smart Linkグループの負荷分散の設定例 2-16

2章 Smart Link

2.1 概要

ネットワークの信頼性を保障するために、図 2-1に示すようにアップリンクの装置とダウンリンクの装置を 2 重で接続する冗長構成のネットワークを築きます。

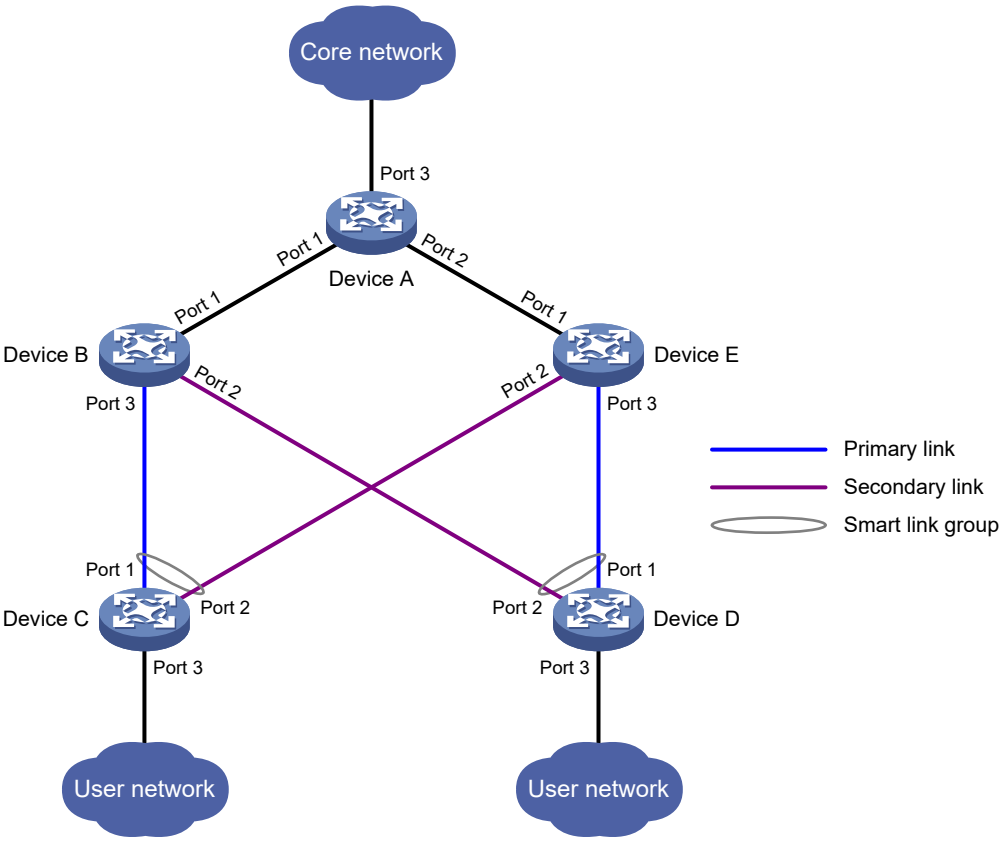


図 2-1 2 つのアップリンクを持つネットワーク

冗長構成のネットワークでループを回避するには、スパニングツリープロトコルを使用します。しかし、スパニングツリープロトコルは収束時間が長く、収束速度に高い要求を持つユーザに適していないという問題があります。

スパニングツリープロトコルの詳細は、オペレーションマニュアルのセクション 2 *アクセス "STP"*を参照してください。

Smart Link は、STP の収束が遅いという問題に対処するために開発された機能です。プライマリリンクで障害が発生した場合に、ただちにバックアップリンクに切り替えるため、ネットワークの高速な収束を提供します。

装置は Flush メッセージを転送するため、Smart link グループと制御 VLAN を転送するように Smart link の設定を行います。図 2-1の Device C、Device D は Smart link の装置です。

関連装置は Smart link をサポートし、指定された制御 VLAN から Flush メッセージを受信します。図 2-1の Device A、Device B、Device E は関連装置です。

2.1.1 基本概念

I. Smart link グループ

Smart link グループは、primary と secondary の 2 つのポートで構成されています。1 つのポートだけが active になり転送可能になります。もう一方のポートはブロックされ、standby 状態になります。リンク障害や片方向リンクで active ポートがシャットダウンした場合、active ポートがブロックされた状態になり、standby ポートが active になります。

図 2-1では、Device C の Port1 と Port2 が、Smart Link グループを形成し、Device D の Port1 と Port2 が、別の Smart Link グループを形成します。Port1 が active で、Port2 は standby 状態です。

II. Primary/secondary ポート

Smart link グループには primary ポートと secondary ポートの 2 種類のポートがあります。Smart Link グループの両方のポートが UP している場合には、primary ポートが優先的に転送状態になり、secondary ポートは standby 状態になります。primary ポートで障害が発生した場合、secondary ポートは、トラフィックを転送するために active になります。

図 2-1では、Device C の Port1 と Device D の Port1 を primary ポートとして、Device C の Port2 と Device D の Port2 を secondary ポートとして設定しています。

III. Primary/secondary リンク

Smart link グループの primary ポートをつなぐリンクが primary リンクです。secondary ポートをつなぐリンクが secondary リンクです。

IV. Flush メッセージ

Flush メッセージは、リンクの切り替えが Smart link グループで発生した場合に、MAC アドレスエントリと ARP/ND エントリをリフレッシュするよう他の装置に通知するために使用されます。Flush メッセージは、共通のマルチキャストデータパケットであり、ブロックされた受信ポートによって廃棄されます。

V. プロテクト VLAN

Smart link グループは、プロテクト VLAN の転送状態を制御します。異なる Smart link グループのポートは、異なるプロテクト VLAN を制御します。プロテクト VLAN のポートの状態は、Smart link グループのポートの状態によって決まります。

VI. 送信制御 VLAN

送信制御 VLAN は、Flush メッセージの送信を制御します。リンクの切り替えが発生した場合、装置（図 2-1では Device C と Device D）は送信制御 VLAN を使用して Flush メッセージを送信します。

VII. 受信制御 VLAN

受信制御 VLAN は Flush メッセージを受信し、処理します。リンクの切り替えが発生した場合、装置（図 2-1では、Device A、Device B、Device E）は受信制御 VLAN の Flush メッセージの処理を行い、MAC アドレスエントリと ARP/ND エントリをリフレッシュさせます。

2.1.2 Smart Link の動作メカニズム

I. リンクバックアップ

図 2-1で示すように、Device C の Port1 のリンクは primary link です。Device C の Port2 のリンクは secondary link です。通常、Port1 が active 状態の時、Port2 は standby 状態になります。primary link で障害が発声した場合、Port2 がトラフィックを転送するために standby から active に切り替わります。Port1 はブロックされ、standby 状態になります。

ポートの状態が変化した際にポートの状態変化をユーザに通知するために、ログを出力します。

II. トポロジー変更

リンク切り替えは、すべての装置の MAC アドレスエントリと ARP/ND エントリを無効化してしまうため、正常な通信を保証するために転送エントリアップデートメカニズムを必要とします。以下のアップデートメカニズムが提供されます。

- **アップリンクのトラフィックをトリガとした MAC アドレスの学習**－アップデートはアップリンクトラフィックによって発生します。このメカニズムは、他のベンダの装置など、Smart Link をサポートしていない装置を使用する環境に適切です。
- **フラッシュアップデート**－Smart Link 対応装置がアップリンクの装置へバックアップリンク上の flush メッセージを送信することで、flush の情報をアップデートします。このメカニズムは、アップリンクの装置が MAC アドレスエントリと ARP/ND エントリをアップデートする Smart Link flush メッセージを認識できる必要があります。

III. preemption モード

図 2-1では、Device C の Port1 のリンクは primary link です。Device C の Port2 のリンクは secondary link です。primary link で障害が発生すると、Port1 は自動的にブロッキングされ standby 状態になります。そして、Port2 がトラフィックを転送するよう standby から active に切り替わります。primary link が復旧するとシステムは、以下の 1 つの動作を行います。

- Smart Link グループに Role preemption が設定されない場合、トラフィック転送状態を維持するために、リンク障害でブロッキングされた port1 は、active に切り替わりません。port2 でリンク障害が発生した場合に、port1 は active に切り替わります。
- Smart Link グループに Role preemption を設定した場合、port1 のリンクが復旧するとすぐに active に切り替わります。port2 は自動的にブロッキングされ standby 状態になります。

IV. 負荷分散

リング構成のネットワークは複数の VLAN のトラフィックを転送します。Smart Link は、Smart Link グループ毎に異なる VLAN でトラフィックを転送させ、負荷分散を行います。

負荷分散を行うために、ポートを複数の Smart Link グループに割り当てます。それぞれ異なるプロテクト VLAN の各グループに設定してください。Smart Link グループからのトラフィックが異なる経路で転送できるように、Smart Link グループでポートが異なることを確認してください。

MSTI（Multiple Spanning Tree Instances）を参照することで、Smart Link グループのプロテクト VLAN を設定することができます。MSTI の詳細は、オペレーションマニュアルのセクション 2 *アクセス* "*STP*"を参照してください。

2.1.3 Smart Link と Monitor Link のコラボレーション

Smart Link は、アップリンクで障害が発生した場合や障害が復旧した場合、リンクの状態変化を検出できません。アップリンクのリンク状態を監視するために、アップリンクポートを監視する Monitor Link を設定することができます。Monitor Link は、ダウンリンクの装置上でリンクの切り替えを実行する Smart Link をトリガにし、ダウンリンクポートのアップ/ダウンの状態をアップリンクポートのアップ/ダウン状態に適応させます。Monitor Link の詳細は、オペレーションマニュアルのセクション 8 *高可用性 ” Monitor Link*"を参照してください。

2.2 Smart LinK 設定作業リスト

作業リスト
Smart Link装置の設定： ● （必須設定項目） Smart Linkグループのプロテクトvlanの設定 ● （必須設定項目） Smart Linkグループのメンバポートの設定 ● （オプション設定項目） Smart Linkグループのrole preemptionの設定 ● （オプション設定項目） flushメッセージの送信の有効化
関連装置の設定 ● （必須設定項目） flushメッセージの受信の有効化

2.3 Smart Link装置の設定

2.3.1 設定要件

Smart link 装置の設定を行う前に、以下の作業を完了してください。

- ループを防ぐため、Smart Link グループのメンバポートの設定をする前に、ポートをシャットダウンしてください。Smart Link グループの設定を完了したのち、ポートをリンクアップさせてください。
- Smart Link グループに追加するポートは、スパニングツリー機能を無効にしてください。

🕮 **メモ：**

- スパニングツリー機能を無効にした場合、Smart Link 機能をポートで有効するまではネットワークでループが発生する可能性があります。
- アグリゲーショングループメンバと Smart Link メンバの両方を設定した場合、アグリゲーショングループの設定が適用されます。ポートは **display smart-link group** コマンドで表示することができません。Smart Link グループの設定は、アグリゲーショングループからポートを削除したのち、適用されます。

2.3.2 Smart Link グループのプロテクト VLAN の設定

MSTI を参照することにより、Smart Link グループにプロテクト VLAN を設定できます。プロテクト VLAN 設定は、スパニングツリープロトコルによります。

STP、RSTP あるいは MSTP モードでは、VALN と MSTI 間のマッピングを手動で設定しなければなりません。

PVST モードでは、VLAN と MSTI のマッピングを自動で行います。スパニングツリープロトコルが無効の場合は、VLAN は MSTI0 にマッピングされます。

以下に Smart Link グループのプロテクト VLAN の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． MST region view に移行する	**stp region-configuration**	PVSTモードで動作する場合省略します。 コマンドの詳細は、コマンドマニュアルのセクション2 *アクセス* "*STP*"を参照してください。
3． VLAN-インスタンスマッピングテーブルを設定する	● 方法1： **instance** *instance-id* **vlan** *vlan-id-list* ● 方法2： **vlan-mapping modulo** *modulo*	PVSTモードで動作する場合省略します。 デフォルト：MST regionのすべてのVLANはCIST（MSTI0）にマッピングされます。 コマンドの詳細は、コマンドマニュアルのセクション2 *アクセス* "*STP*"を参照してください。
4． MST region 設定を手動でアクティブにする	**active region-configuration**	PVSTモードで動作する場合省略します。 コマンドの詳細は、コマンドマニュアルのセクション2 *アクセス* "*STP*"を参照してください。

操作	コマンド	補足
5.　（オプション設定項目）現在のアクティブな MST region の設定情報を表示する	**display stp region-configuration**	すべてのviewで実行できます。 コマンドの出力はVLAN-インスタンスマッピング情報が含まれます。 コマンドの詳細はコマンドマニュアルの、セクション2 *アクセス "STP"*を参照してください。
6.　system view に戻る	**quit**	PVSTモードで動作する場合省略します。
7.　Smart Link グループを作成し、smart link group view に移行する	**smart-link group** *group-id*	ー
8.　Smart Link グループのプロテクト VLAN を設定する	**protected-vlan reference-instance** *instance-id-list*	デフォルト：設定なし

重要：

pvst mode を設定している装置で Smart Link を使用する場合は、以下の通りに **protected-vlan reference-instance** コマンドを指定してください。**reference-instance** の値が正しく指定されていない場合は、Smart Link の STANDBY ポートがパケットを転送します。

・**stp global enable** コマンド設定なし
　protected-vlan reference-instance 0 コマンドを設定します。
・**stp global enable** コマンド設定あり

VLAN の個数が 128 個までは、VLAN ID＝インスタンス ID でマッピングされます。129 個目以降の VLAN は全て、インスタンス 0 にマッピングされます。

例）vlan 1, 3, 5, 200 を定義している場合、以下のように自動的にマッピングされます。

Instance　VLANs Mapped
0　2, 4, 6 to 199, 201 to 4094
（未定義の VLAN、または、129 個目以降の VLAN は 0 にマッピングされる）
1　1
3　3
5　5
200　200

注）**display stp region-configuration** は、MSTP モード時しか利用できず、PVST モード時は、実際の MSTI マッピング状態を確認できません。

Smart Link の対象となる vlan の ID が、VLAN ID＝インスタンス ID でマッピングされた vlan の場合は、protected-vlan reference-instance に該当する vlan と同じ ID を instance に設定します。Smart Link の対象となる vlan の ID が、インスタンス 0 にマッピングされている場合は、**protected-vlan reference-instance 0** を設定します。

たとえば、VLAN 100 を使用する場合は、**protected-vlan reference-instance 100** を設定します。しかし、VLAN 200 を使用する場合は、定義された VLAN の数により、vlan と同じ ID または 0 のどちらを指定すべきか判断する必要があります。

2.3.3 Smart Link グループのメンバポートの設定

Smart Link グループのメンバポートを smart link group view か interface view のどちらかで設定できます。2 つの view で行った設定は同じ効果を持ちます。

I. smart link group view でメンバポートの設定

以下に smart link group view で Smart Link グループのメンバポートの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Smart Link グループを作成し、smart link group view に移行する	**smart-link group** *group-id*	―
3. Smart Link グループのメンバポートを設定する	**port** *interface-type interface-number* { **primary** | **secondary** }	デフォルト：設定なし

II. interface view でメンバポートの設定

以下に interface view で Smart Link グループのメンバポートの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. interface view または aggregate interface view に移行する	**interface** *interface-type interface-number*	ー
3. Smart Link グループのメンバポートを設定する	**port smart-link group** *group-id* { **primary** | **secondary** }	デフォルト：設定なし

2.3.4 Smart Link グループの role preemption の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. smart link group view に移行する	**smart-link group** *group-id*	ー
3. role preemption を有効にする	**preemption mode role**	デフォルト：無効
4. preemption delay を設定する	**preemption delay** *delay*	デフォルト：1秒 preemption delayの設定は、role preemptionを有効にした後にのみ適用されます。

2.3.5 flush メッセージの送信の有効化

Flush メッセージの送信を有効にする設定を行う場合、以下のガイドラインに従ってください。

- Smart link グループで設定された制御 VLAN は、他の smart link グループに設定された制御 VLAN と異なるようにしてください。
- 制御 VLAN がすでに存在することを確認し、Smart link グループのメンバポートを制御 VLAN に割り当ててください。
- Smart Link グループの制御 VLAN は、プロテクト VLAN にしてください。制御 VLAN を削除しないでください。制御 VLAN を削除すると、flush メッセージを正しく送信できなくなります。

以下に Flush メッセージの送信を有効にする設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. smart link group view に移行する	**smart-link group** *group-id*	ー
3. Flush メッセージの送信を有効にする	**flush enable** [**control-vlan** *vlan-id*]	デフォルト：有効 VLAN 1は制御VLANです。

2.4 関連装置の設定

2.4.1 設定要件

Smart Link グループのメンバポートに接続している、関連する装置のポートのスパニングツリー機能を無効にしてください。スパニングツリーが有効になっている場合、トポロジーが変更された場合に転送ステートにいない場合、ポートは flush メッセージを破棄します。

2.4.2 flush メッセージの受信の有効化

flush メッセージを受信するため、関連づけられた装置ですべてのポートを有効にする必要はありません。Smart Link 装置と宛先装置間の primary と secondary のリンク上のポートのすべての制御 VLAN でのみ、有効にする必要があります。

Flush メッセージの受信を有効にする設定を行う前に、以下の作業を完了してください。

- flush メッセージを処理する制御 VLAN を指定していない場合、装置は flush メッセージを処理せずに転送します。
- Smart Link 装置において、受信制御 VLAN と送信制御 VLAN が同じ VLAN であることを確認してください。 送受信する制御 VLAN が同じでない場合、関連装置は、受信した flush メッセージを処理せずに転送します。
- 制御 VLAN を削除しないでください。制御 VLAN を削除すると、flush メッセージを正しく送信できなくなります。
- 制御 VLAN が既存の VLAN であることを確認してください。制御 VLAN に flush メッセージが受信できるポートを割り当ててください。

以下に Flush メッセージの受信を有効にする設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. interface view または aggregate interface view に移行する	**interface** *interface-type interface-number*	―
3. Flush メッセージを受信する制御 VLAN を設定する	**smart-link flush enable** [**control-vlan** *vlan-id-list*]	デフォルト：設定なし

2.5 Smart Linkの表示と維持

すべての view で **display** コマンドを実行でき、user view で **reset** コマンドを実行できます。

操作	コマンド
受信したFlushメッセージの情報を表示する	**display smart-link flush**
Smart linkグループの情報を表示する	**display smart-link group** { *group-id* | **all** }

操作	コマンド
Flushメッセージの統計情報をクリアする	**reset smart-link statistics**

2.6 Smart Linkの設定例

2.6.1 単一 Smart Link group グループの設定例

I. ネットワーク要件

図 2-2に示すようなネットワークで設定します。

- Device C、Device D は Smart link 装置です。Device A、Device B、Device E は関連装置です。Device C の VLAN 1～VLAN 30 のトラフィックが Device A に 2 重アップリンクされます。
- 2 重アップリンクのバックアップ用に Device C と Device D で Smart link を設定します。

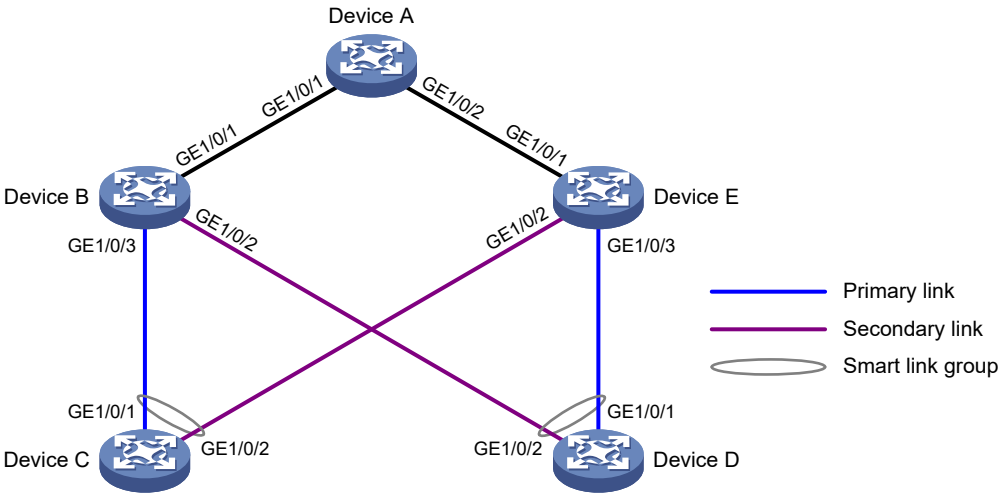


図 2-2 ネットワーク図

II. 設定手順

1)　Device C を設定します。

VLAN 1～VLAN 30 を作成します。MSTI1 にマッピングし、MST region 設定を動作させます。

```
<DeviceC> system-view
[DeviceC] vlan 1 to 30
[DeviceC] stp region-configuration
[DeviceC-mst-region] instance 1 vlan 1 to 30
```

```
[DeviceC-mst-region] active region-configuration
[DeviceC-mst-region] quit
```

GigabitEthernet 1/0/1 と GigabitEthernet 1/0/2 をシャットダウンします。GigabitEthernet 1/0/1 と GigabitEthernet 1/0/2 上のスパニングツリー機能を無効にします。トランクポートとして設定し、VLAN 1～VLAN 30 に割り当てます。

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] shutdown
[DeviceC-GigabitEthernet1/0/1] undo stp enable
[DeviceC-GigabitEthernet1/0/1] port link-type trunk
[DeviceC-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceC-GigabitEthernet1/0/1] quit
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] shutdown
[DeviceC-GigabitEthernet1/0/2] undo stp enable
[DeviceC-GigabitEthernet1/0/2] port link-type trunk
[DeviceC-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
[DeviceC-GigabitEthernet1/0/2] quit
```

Smart Link グループ 1 を作成し、すべての VLAN をプロテクト VLAN として MSTI 1 にマッピングします。

```
[DeviceC] smart-link group 1
[DeviceC-smlk-group1] protected-vlan reference-instance 1
```

Smart Link グループ 1 の primary ポートとして GigabitEthernet 1/0/1 を設定し、secondary ポートとして GigabitEthernet 1/0/2 を設定します。

```
[DeviceC-smlk-group1] port gigabitethernet 1/0/1 primary
[DeviceC-smlk-group1] port gigabitethernet 1/0/2 secondary
```

Smart Link グループ 1 で flush メッセージの送信を有効にし、送信制御 VLAN として VLAN 10 を設定します。

```
[DeviceC-smlk-group1] flush enable control-vlan 10
[DeviceC-smlk-group1] quit
```

GigabitEthernet 1/0/1 と GigabitEthernet 1/0/2 を再度アップにします。

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] undo shutdown
[DeviceC-GigabitEthernet1/0/1] quit
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] undo shutdown
```

```
[DeviceC-GigabitEthernet1/0/2] quit
```

2) Device D を設定します。

VLAN 1～VLAN 30 を作成します。MSTI1 にマッピングし、MST region 設定を動作させます。

```
<DeviceD> system-view
[DeviceD] vlan 1 to 30
[DeviceD] stp region-configuration
[DeviceD-mst-region] instance 1 vlan 1 to 30
[DeviceD-mst-region] active region-configuration
[DeviceD-mst-region] quit
```

GigabitEthernet 1/0/1 と GigabitEthernet 1/0/2 をシャットダウンします。GigabitEthernet 1/0/1 と GigabitEthernet 1/0/2 上のスパニングツリー機能を無効にします。トランクポートとして設定し、VLAN 1～VLAN 30 に割り当てます。

```
[DeviceD] interface gigabitethernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] shutdown
[DeviceD-GigabitEthernet1/0/1] undo stp enable
[DeviceD-GigabitEthernet1/0/1] port link-type trunk
[DeviceD-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceD-GigabitEthernet1/0/1] quit
[DeviceD] interface gigabitethernet 1/0/2
[DeviceD-GigabitEthernet1/0/2] shutdown
[DeviceD-GigabitEthernet1/0/2] undo stp enable
[DeviceD-GigabitEthernet1/0/2] port link-type trunk
[DeviceD-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
[DeviceD-GigabitEthernet1/0/2] quit
```

Smart Link グループ 1 を作成し、すべての VLAN をプロテクト VLAN として MSTI 1 にマッピングします。

```
[DeviceD] smart-link group 1
[DeviceD-smlk-group1] protected-vlan reference-instance 1
```

Smart Link グループ 1 の primary ポートとして GigabitEthernet 1/0/1 を設定し、secondary ポートとして GigabitEthernet 1/0/2 を設定します。

```
[DeviceD-smlk-group1] port gigabitethernet 1/0/1 primary
[DeviceD-smlk-group1] port gigabitethernet 1/0/2 secondary
```

Smart Link グループ 1 で flush メッセージの送信を有効にし、送信制御 VLAN として VLAN20 を設定します。

```
[DeviceD-smlk-group1] flush enable control-vlan 20
[DeviceD-smlk-group1] quit
```

GigabitEthernet 1/0/1 と GigabitEthernet 1/0/2 を再度アップにします。

```
[DeviceD] interface gigabitethernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] undo shutdown
[DeviceD-GigabitEthernet1/0/1] quit
[DeviceD] interface gigabitethernet 1/0/2
[DeviceD-GigabitEthernet1/0/2] undo shutdown
[DeviceD-GigabitEthernet1/0/2] quit
```

3)　Device B を設定します。

VLAN 1～VLAN 30 を作成します。

```
<DeviceB> system-view
[DeviceB] vlan 1 to 30
```

GigabitEthernet 1/0/1 をトランクポートとして設定し、VLAN 1～VLAN 30 に割り付けます。flush メッセージの受信を有効にし、VLAN 10 と VLAN 20 を受信制御 VLAN として設定します。

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port link-type trunk
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceB-GigabitEthernet1/0/1] smart-link flush enable control-vlan 10 20
[DeviceB-GigabitEthernet1/0/1] quit
```

GigabitEthernet 1/0/2 をトランクポートとして設定し、VLAN 1～VLAN 30 に割り付けます。スパニングツリー機能を無効にします。flush メッセージの受信を有効にします。VLAN 20 を受信制御 VLAN として設定します。

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] port link-type trunk
[DeviceB-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
[DeviceB-GigabitEthernet1/0/2] undo stp enable
[DeviceB-GigabitEthernet1/0/2] smart-link flush enable control-vlan 20
[DeviceB-GigabitEthernet1/0/2] quit
```

GigabitEthernet 1/0/3 をトランクポートとして設定し、VLAN 1～VLAN 30 に割り付けます。スパニングツリー機能を無効にします。flush メッセージの受信を有効にします。VLAN 10 を受信制御 VLAN として設定します。

```
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] port link-type trunk
[DeviceB-GigabitEthernet1/0/3] port trunk permit vlan 1 to 30
```

```
[DeviceB-GigabitEthernet1/0/3] undo stp enable
[DeviceB-GigabitEthernet1/0/3] smart-link flush enable control-vlan 10
[DeviceB-GigabitEthernet1/0/3] quit
```

4) Device E を設定します。

VLAN 1～VLAN 30 を作成します。

```
<DeviceE> system-view
[DeviceE] vlan 1 to 30
```

GigabitEthernet 1/0/1 をトランクポートとして設定し、VLAN 1～VLAN 30 に割り付けます。スパニングツリー機能を無効にします。flush メッセージの受信を有効にします。VLAN 10 と VLAN20 を受信制御 VLAN として設定します。

```
[DeviceE] interface gigabitethernet 1/0/1
[DeviceE-GigabitEthernet1/0/1] port link-type trunk
[DeviceE-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceE-GigabitEthernet1/0/1] smart-link flush enable control-vlan 10 20
[DeviceE-GigabitEthernet1/0/1] quit
```

GigabitEthernet 1/0/2 をトランクポートとして設定し、VLAN 1～VLAN 30 に割り付けます。スパニングツリー機能を無効にします。flush メッセージの受信を有効にします。VLAN 10 を受信制御 VLAN として設定します。

```
[DeviceE] interface gigabitethernet 1/0/2
[DeviceE-GigabitEthernet1/0/2] port link-type trunk
[DeviceE-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
[DeviceE-GigabitEthernet1/0/2] undo stp enable
[DeviceE-GigabitEthernet1/0/2] smart-link flush enable control-vlan 10
[DeviceE-GigabitEthernet1/0/2] quit
```

GigabitEthernet 1/0/3 をトランクポートとして設定し、VLAN 1～VLAN 30 に割り付けます。スパニングツリー機能を無効にします。flush メッセージの受信を有効にします。VLAN 20 を受信制御 VLAN として設定します。

```
[DeviceE] interface gigabitethernet 1/0/3
[DeviceE-GigabitEthernet1/0/3] port link-type trunk
[DeviceE-GigabitEthernet1/0/3] port trunk permit vlan 1 to 30
[DeviceE-GigabitEthernet1/0/3] undo stp enable
[DeviceE-GigabitEthernet1/0/3] smart-link flush enable control-vlan 20
[DeviceE-GigabitEthernet1/0/3] quit
```

5) Device A を設定します。

VLAN 1～VLAN 30 を作成します。

```
<DeviceA> system-view
[DeviceA] vlan 1 to 30
```

GigabitEthernet 1/0/1 と GigabitEthernet 1/0/2 をトランクポートとして設定し、VLAN 1～VLAN 30 に割り付けます。flush メッセージの受信を有効にし、VLAN 10 と VLAN 20 を受信制御 VLAN として設定します。

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-type trunk
[DeviceA-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceA-GigabitEthernet1/0/1] smart-link flush enable control-vlan 10 20
[DeviceA-GigabitEthernet1/0/1] quit
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port link-type trunk
[DeviceA-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
[DeviceA-GigabitEthernet1/0/2] smart-link flush enable control-vlan 10 20
[DeviceA-GigabitEthernet1/0/2] quit
```

III. 設定の確認

display smart-link group コマンドを使用し、装置上の Smart Link グループの設定を表示します。

Device C 上の Smart Link グループの設定を表示します。

```
[DeviceC] display smart-link group 1
Smart link group 1 information:
  Device ID       : 000f-e23d-5af0
  Preemption mode : NONE
  Preemption delay: 1(s)
  Control VLAN    : 10
  Protected VLAN  : Reference Instance 1

  Member                  Role      State   Flush-count     Last-flush-time

--------------------------------------------------------------------------------
  GE1/0/1                PRIMARY   ACTIVE  5               16:45:20 2014/04/21

  GE1/0/2                SECONDARY STANDBY 1               16:37:20 2014/04/21
```

display smart-link flush コマンドを使用し、装置が受信した flush メッセージを表示します。

Device B 上で受信した flush メッセージを表示します。

```
[DeviceB] display smart-link flush
 Received flush packets                              : 5
 Receiving interface of the last flush packet        : GigabitEthernet1/0/3
 Receiving time of the last flush packet             : 16:50:21 2014/04/21
 Device ID of the last flush packet                  : 000f-e23d-5af0
 Control VLAN of the last flush packet               : 10
```

2.6.2 複数 Smart Link グループの負荷分散の設定例

I. ネットワーク要件

図 2-3に示すようなネットワークで設定します。

- Device C は Smart Link 装置です。Device A、Device B、Device D は関連装置です。Device C 上の VLAN 1～VLAN 200 のトラフィックは、Device B と Device D によって Device A に 2 重にアップリンクされています。
- Device C のアップリンクのバックアップと負荷分散を実装します。VLAN 1～VLAN 100 のトラフィックは、Device B によって Device A にアップリンクされ、VLAN 101～VLAN 200 のトラフィックは、Device D によって Device A にアップリンクされています。

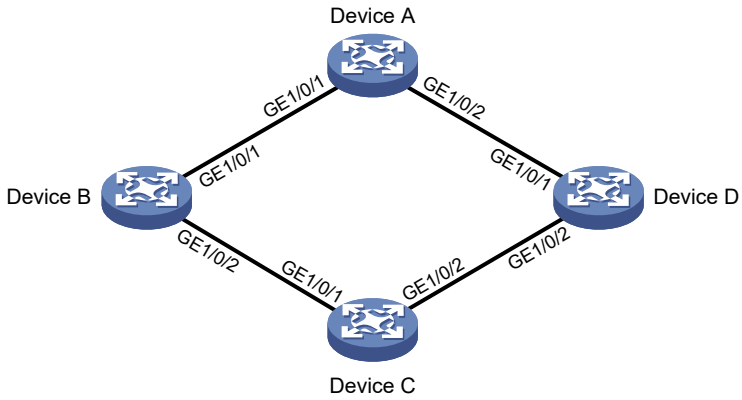


図 2-3 ネットワーク図

II. 設定手順

1)　Device C を設定します。

VLAN 1～VLAN 200 を作成します。VLAN 1～ VLAN 100 を MSTI 1 にマッピングします。VLAN 101～VLAN 200 を MSTI 2 にマッピングします。MST region 設定をアクティブにします。

```
<DeviceC> system-view
[DeviceC] vlan 1 to 200
[DeviceC] stp region-configuration
[DeviceC-mst-region] instance 1 vlan 1 to 100
[DeviceC-mst-region] instance 2 vlan 101 to 200
[DeviceC-mst-region] active region-configuration
[DeviceC-mst-region] quit
```

GigabitEthernet 1/0/1 と GigabitEthernet 1/0/2 をシャットダウンします。GigabitEthernet 1/0/1 と GigabitEthernet 1/0/2 上のスパニングツリー機能を無効にします。トランクポートとして設定し、VLAN 1～VLAN 200 に割り当てます。

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] shutdown
[DeviceC-GigabitEthernet1/0/1] undo stp enable
[DeviceC-GigabitEthernet1/0/1] port link-type trunk
[DeviceC-GigabitEthernet1/0/1] port trunk permit vlan 1 to 200
[DeviceC-GigabitEthernet1/0/1] quit
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] shutdown
[DeviceC-GigabitEthernet1/0/2] undo stp enable
[DeviceC-GigabitEthernet1/0/2] port link-type trunk
[DeviceC-GigabitEthernet1/0/2] port trunk permit vlan 1 to 200
[DeviceC-GigabitEthernet1/0/2] quit
```

Smart Link グループ 1 を作成し、すべての VLAN を Smart Link グループ 1 のプロテクト VLAN として MSTI 1 にマッピングします。

```
[DeviceC] smart-link group 1
[DeviceC-smlk-group1] protected-vlan reference-instance 1
```

Smart Link グループ 1 の primary ポートとして GigabitEthernet 1/0/1 を設定し、secondary ポートとして GigabitEthernet 1/0/2 を設定します。

```
[DeviceC-smlk-group1] port gigabitethernet 1/0/1 primary
[DeviceC-smlk-group1] port gigabitethernet 1/0/2 secondary
```

Smart Link グループ 1 で role preemption を有効にし、flush メッセージの送信を有効にします。送信制御 VLAN として VLAN 10 を設定します。

```
[DeviceC-smlk-group1] preemption mode role
[DeviceC-smlk-group1] flush enable control-vlan 10
[DeviceC-smlk-group1] quit
```

Smart Link グループ 2 を作成し、すべての VLAN を Smart Link グループ 2 のプロテクト VLAN として MSTI 2 にマッピングします。

```
[DeviceC] smart-link group 2
[DeviceC-smlk-group2] protected-vlan reference-instance 2
```

Smart Link グループ 2 の secondary ポートとして GigabitEthernet 1/0/1 を設定し、primary ポートとして GigabitEthernet 1/0/2 を設定します。

```
[DeviceC-smlk-group2] port gigabitethernet 1/0/2 primary
[DeviceC-smlk-group2] port gigabitethernet 1/0/1 secondary
```

Smart Link グループ 2 で role preemption を有効にします。flush メッセージの送信を有効にします。送信制御 VLAN として VLAN 110 を設定します。

```
[DeviceC-smlk-group2] preemption mode role
[DeviceC-smlk-group2] flush enable control-vlan 110
[DeviceC-smlk-group2] quit
```

GigabitEthernet 1/0/1 と GigabitEthernet 1/0/2 を再度アップにします。

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] undo shutdown
[DeviceC-GigabitEthernet1/0/1] quit
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] undo shutdown
[DeviceC-GigabitEthernet1/0/2] quit
```

2) Device B を設定します。

VLAN 1～VLAN 200 を作成します。

```
<DeviceB> system-view
[DeviceB] vlan 1 to 200
```

GigabitEthernet 1/0/1 をトランクポートとして設定し、VLAN 1～VLAN 200 に割り付けます。flush メッセージの受信を有効にし、VLAN 10 と VLAN 110 を GigabitEthernet 1/0/1 の受信制御 VLAN として設定します。

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port link-type trunk
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 1 to 200
[DeviceB-GigabitEthernet1/0/1] smart-link flush enable control-vlan 10 110
[DeviceB-GigabitEthernet1/0/1] quit
```

GigabitEthernet 1/0/2 をトランクポートとして設定し、VLAN 1～VLAN 200 に割り付けます。スパニングツリー機能を無効にします。flush メッセージの受信を有効にします。VLAN 10 と VLAN 110 を受信制御 VLAN として設定します。

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] port link-type trunk
[DeviceB-GigabitEthernet1/0/2] port trunk permit vlan 1 to 200
[DeviceB-GigabitEthernet1/0/2] undo stp enable
[DeviceB-GigabitEthernet1/0/2] smart-link flush enable control-vlan 10 110
[DeviceB-GigabitEthernet1/0/2] quit
```

3) Device D を設定します。

VLAN 1～VLAN 200 を作成します。

```
<DeviceD> system-view
[DeviceD] vlan 1 to 200
```

GigabitEthernet 1/0/1 をトランクポートとして設定し、VLAN 1～VLAN 200 に割り付けます。flush メッセージの受信を有効にし、VLAN 10 と VLAN 110 を GigabitEthernet 1/0/1 の受信制御 VLAN として設定します。

```
[DeviceD] interface gigabitethernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] port link-type trunk
[DeviceD-GigabitEthernet1/0/1] port trunk permit vlan 1 to 200
[DeviceD-GigabitEthernet1/0/1] smart-link flush enable control-vlan 10 110
[DeviceD-GigabitEthernet1/0/1] quit
```

GigabitEthernet 1/0/2 をトランクポートとして設定し、VLAN 1～VLAN 200 に割り付けます。スパニングツリー機能を無効にします。flush メッセージの受信を有効にします。VLAN 10 と VLAN 110 を受信制御 VLAN として設定します。

```
[DeviceD] interface gigabitethernet 1/0/2
[DeviceD-GigabitEthernet1/0/2] port link-type trunk
[DeviceD-GigabitEthernet1/0/2] port trunk permit vlan 1 to 200
[DeviceD-GigabitEthernet1/0/2] undo stp enable
[DeviceD-GigabitEthernet1/0/2] smart-link flush enable control-vlan 10 110
[DeviceD-GigabitEthernet1/0/2] quit
```

4)　Device A を設定します。

VLAN 1～VLAN 200 を作成します。

```
<DeviceA> system-view
[DeviceA] vlan 1 to 200
```

GigabitEthernet 1/0/1 と GigabitEthernet 1/0/2 をトランクポートとして設定し、VLAN 1～VLAN 200 に割り付けます。flush メッセージの受信を有効にし、VLAN 10 と VLAN 110 をポートの受信制御 VLAN として設定します。

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-type trunk
[DeviceA-GigabitEthernet1/0/1] port trunk permit vlan 1 to 200
[DeviceA-GigabitEthernet1/0/1] smart-link flush enable control-vlan 10 110
[DeviceA-GigabitEthernet1/0/1] quit
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port link-type trunk
[DeviceA-GigabitEthernet1/0/2] port trunk permit vlan 1 to 200
[DeviceA-GigabitEthernet1/0/2] smart-link flush enable control-vlan 10 110
[DeviceA-GigabitEthernet1/0/2] quit
```

III. 設定の確認

display smart-link group コマンドを使用し、装置上の Smart Link グループの設定を表示します。

Device C 上の Smart Link グループの設定を表示します。

```
[DeviceC] display smart-link group all
Smart link group 1 information:
  Device ID       : 000f-e23d-5af0
  Preemption mode : ROLE
  Preemption delay: 1(s)
  Control VLAN    : 10
  Protected VLAN  : Reference Instance 1

  Member                   Role      State   Flush-count     Last-flush-time

--------------------------------------------------------------------------------
  GE1/0/1                PRIMARY   ACTIVE  5               16:45:20 2014/04/21

  GE1/0/2                SECONDARY STANDBY 1               16:37:20 2014/04/21

Smart link group 2 information:
  Device ID       : 000f-e23d-5af0
  Preemption mode : ROLE
  Preemption delay: 1(s)
  Control VLAN    : 110
  Protected VLAN  : Reference Instance 2

  Member                   Role      State   Flush-count     Last-flush-time

--------------------------------------------------------------------------------
  GE1/0/2                PRIMARY   ACTIVE  5               16:45:20 2014/04/21

  GE1/0/1                SECONDARY STANDBY 1               16:37:20 2014/04/21
```

display smart-link flush コマンドを使用し、装置が受信した flush メッセージを表示することができます。

Device B 上で受信した flush メッセージを表示します。

```
[DeviceB] display smart-link flush
 Received flush packets                              : 5
 Receiving interface of the last flush packet        : GigabitEthernet1/0/2
 Receiving time of the last flush packet             : 16:25:21 2014/04/21
 Device ID of the last flush packet                  : 000f-e23d-5af0
 Control VLAN of the last flush packet               : 10
```

目次

このセクションのページは**8-x-x** です。

3 章 Monitor Link..... 3-1
3.1 概要..... 3-1
3.2 設定の制限とガイドライン..... 3-2
3.3 Monitor Link の設定作業リスト..... 3-2
3.4 Monitor Link グループの作成..... 3-2
3.5 Monitor Link グループメンバインタフェースの設定..... 3-2
3.5.1 monitor link group view での設定..... 3-3
3.5.2 interface view での設定..... 3-3
3.6 Monitor Link の表示と維持..... 3-3
3.7 Monitor Link の設定例..... 3-4

3章 Monitor Link

3.1 概要

Monitor Link はダウンリンクインタフェースの状態を Monitor Link グループのアップリンクインタフェースの状態に関連づけます。アップリンクが故障したため、Monitor Link がダウンリンクインタフェースをシャットダウンする場合、下流の装置が別のリンクに接続を変更します。

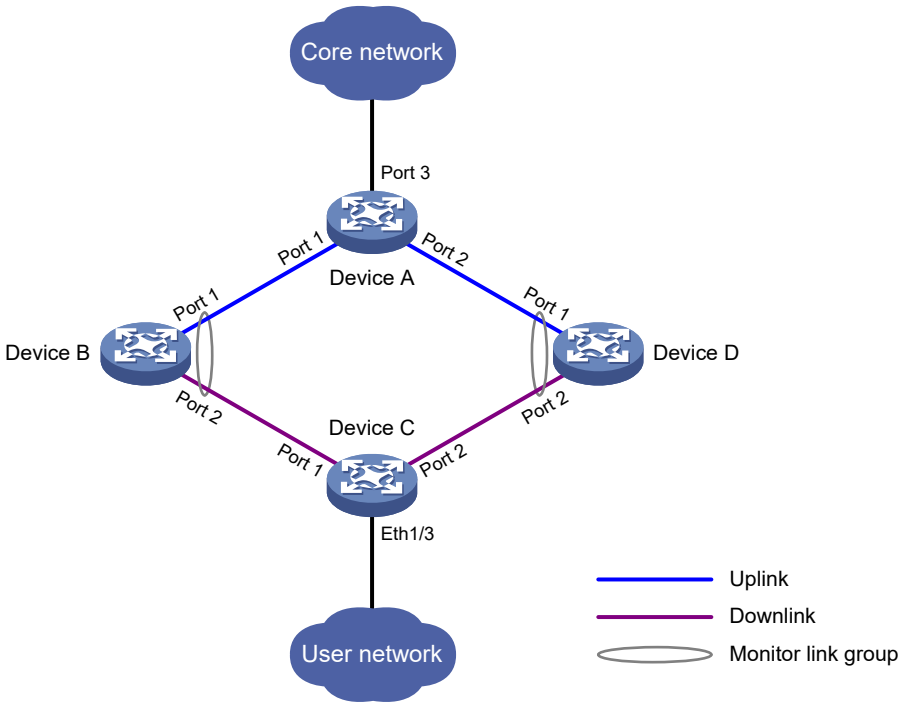


図 3-1 Monitor Link アプリケーションシナリオ

Monitor Link グループはアップリンクインタフェースとダウンリンクインタフェースが含まれます。インタフェースは 1 つの Monitor Link グループにのみ所属します。

- アップリンクインタフェースは監視されるインタフェースです。Monitor Link グループの状態は、そのメンバアップリンクインタフェースの状態と関連します。Monitor Link グループ内のアップ状態にあるアップリンクインタフェースの数が指定されたしきい値より小さい場合、Monitor Link グループはダウンとなりダウンリンクインタフェースはシャットダウンします。アップ状態にあるアップリンクインタフェースの数がしきい値に戻ると、Monitor Link グループはアップしダウンリンクインタフェースもアップになります。
- ダウンリンクインタフェースは監視するインタフェースです。ダウンインタフェースの状態は Monitor Link グループの状態と関連します。Monitor Link グループの状態が変化すると、メンバダウンリンクインタフェースの状態がグループ状態に一致するように変更します。

図 3-1は以下のような構成となります。

- Device B の Port 1 と Port 2 が Monitor Link グループとなります。
- Device D の Port 1 と Port 2 が別の Monitor Link グループとなります。
- Port 1 は両方の Device のアップリンクインタフェースで、Port 2 は両方の Device のダウンリンクインタフェースです。

Monitor Link グループの動作は、他の Monitor Link グループの動作と独立しています。Monitor Link グループ内のアップ状態にあるアップリンクインタフェースの数が指定されたしきい値より小さい場合、Monitor Link グループはダウンとなりダウンリンクインタフェースはシャットダウンします。アップ状態にあるアップリンクインタフェースの数がしきい値に戻ると、Monitor Link グループはアップしダウンリンクインタフェースもアップになります。

3.2 設定の制限とガイドライン

Monitor Link を設定する場合、以下の制限とガイドラインに従ってください。

- Monitor Link グループのダウンリンクインタフェースを手動でシャットダウンあるいはアップさせないでください。

3.3 Monitor Linkの設定作業リスト

作業リスト
（必須設定項目）Monitor Linkグループの作成
（必須設定項目）Monitor Linkグループメンバインタフェースの設定

3.4 Monitor Linkグループの作成

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． Monitor Link グループを作成し monitor link group view に移行する	**monitor-link group** *group-id*	デフォルト：設定なし

3.5 Monitor Linkグループメンバインタフェースの設定

Monitor Link グループのメンバインタフェースを monitor link group view か interface view のどちらかで設定することができます。2 つの view で行った設定は同じ効果を持ちます。以下のインタフェースは Monitor Link グループのメンバインタフェースの設定として設定することができます。

- レイヤ 2 イーサネットインタフェース、アグリゲートインタフェース
- アグリゲーショングループのメンバポート

Monitor Link グループメンバインタフェースを設定する場合、以下のガイドラインに従ってください。

- ダウンリンクインタフェースでダウン/アップ状態が頻繁に変更することをさけるため、ダウンリンクインタフェースを設定する前にアップリンクインタフェースを設定してください。
- Monitor link による中断を防ぐため、同じ Monitor link グループにアグリゲートインタフェース、アグリゲーショングループのメンバポートを割り当てないでください。
- インタフェースは 1 つの Monitor link グループのみ割り当てることができます。

3.5.1 monitor link group view での設定

以下に monitor link group view で Monitor Link グループのメンバインタフェースの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. monitor link group view に移行する	**monitor-link group** *group-id*	ー
3. Monitor Link グループのメンバインタフェースを設定する	**port** *interface-type interface-number* { **downlink** | **uplink** }	デフォルト：設定なし

3.5.2 interface view での設定

以下に interface view で Monitor Link グループのメンバインタフェースの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. interface view に移行する	**interface** *interface-type interface-number*	ー
3. Monitor Link グループのメンバとして現在のインタフェースを設定する	**port monitor-link group** *group-id* { **downlink** | **uplink** }	デフォルト：設定なし

3.6 Monitor Linkの表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
Monitor linkグループの情報を表示する	**display monitor-link group** { *group-id* | **all** }

3.7 Monitor Linkの設定例

I. ネットワーク要件

図 3-2に示すようなネットワークで設定します。

- Device C は Smart link 装置で、Device A、Device B、Device D は関連装置です。Device C 上の VLAN 1～VLAN 30 のトラフィックは Smart Link グループを介して Device A にデュアルアップリンクされます。
- Device C はデュアルアップリンクのバックアップを実装します。Device A と Device B（または Device D）間でリンク障害が発生した際に、Device C はリンク障害を察知し、Smart Link グループ内でリンク切り替えを行います。

Smart Link の詳細は、オペレーションマニュアルのセクション 8 *高可用性* "*Smart Link*"を参照してください。

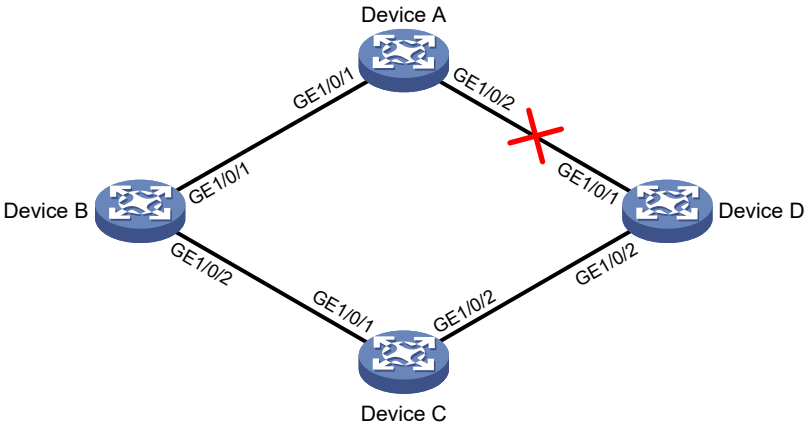


図 3-2 ネットワーク図

II. 設定手順

1)　Device C を設定します。

VLAN 1～VLAN 30 を作成します。

```
<DeviceC> system-view
[DeviceC] vlan 1 to 30
```

MSTI 1 に VLAN をマッピングします。

```
[DeviceC] stp region-configuration
[DeviceC-mst-region] instance 1 vlan 1 to 30
```

MST region 設定を動作させます。

```
[DeviceC-mst-region] active region-configuration
[DeviceC-mst-region] quit
```

GigabitEthernet 1/0/1 をシャットダウンします。

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] shutdown
```

インタフェースでスパニングツリー機能を無効にします。

```
[DeviceC-GigabitEthernet1/0/1] undo stp enable
```

トランクポートとしてインタフェースを設定します。

```
[DeviceC-GigabitEthernet1/0/1] port link-type trunk
```

インタフェースを VLAN 1～VLAN 30 に割り当てます。

```
[DeviceC-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
[DeviceC-GigabitEthernet1/0/1] quit
```

GigabitEthernet 1/0/1 の設定と同様に GigabitEthernet 1/0/2 を設定します。

```
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] shutdown
[DeviceC-GigabitEthernet1/0/2] undo stp enable
[DeviceC-GigabitEthernet1/0/2] port link-type trunk
[DeviceC-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
[DeviceC-GigabitEthernet1/0/2] quit
```

Smart Link グループ 1 を作成し、プロテクト VLAN として MSTI 1 にすべての VLAN をマッピングします。

```
[DeviceC] smart-link group 1
[DeviceC-smlk-group1] protected-vlan reference-instance 1
```

Smart Link グループ 1 の primary ポートとして GigabitEthernet 1/0/1 を設定し、secondary ポートとして GigabitEthernet 1/0/2 を設定します。

```
[DeviceC-smlk-group1] port gigabitethernet 1/0/1 primary
[DeviceC-smlk-group1] port gigabitethernet 1/0/2 secondary
```

Smart Link グループで flush メッセージの送信を有効にします。

```
[DeviceC-smlk-group1] flush enable
[DeviceC-smlk-group1] quit
```

GigabitEthernet 1/0/1 と GigabitEthernet 1/0/2 を再度リンクアップにします。

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] undo shutdown
[DeviceC-GigabitEthernet1/0/1] quit
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] undo shutdown
[DeviceC-GigabitEthernet1/0/2] quit
```

2)　Device A を設定します。

VLAN 1～VLAN 30 を作成します。

```
<DeviceA> system-view
[DeviceA] vlan 1 to 30
```

GigabitEthernet 1/0/1 を設定します。

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-type trunk
```

インタフェースに VLAN 1～VLAN 30 を割り当てます。

```
[DeviceA-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
```

インタフェースで flush メッセージの受信を有効にします。

```
[DeviceA-GigabitEthernet1/0/1] smart-link flush enable
[DeviceA-GigabitEthernet1/0/1] quit
```

GigabitEthernet 1/0/1 の設定と同様に GigabitEthernet 1/0/2 を設定します。

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port link-type trunk
[DeviceA-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
[DeviceA-GigabitEthernet1/0/2] smart-link flush enable
[DeviceA-GigabitEthernet1/0/2] quit
```

3)　Device B を設定します。

VLAN 1～VLAN 30 を作成します。

```
<DeviceB> system-view
[DeviceB] vlan 1 to 30
```

トランクポートとして GigabitEthernet 1/0/1 を設定します。

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port link-type trunk
```

インタフェースに VLAN 1～VLAN 30 を割り当てます。

```
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
```

インタフェースで flush メッセージの受信を有効にします。

```
[DeviceB-GigabitEthernet1/0/1] smart-link flush enable
[DeviceB-GigabitEthernet1/0/1] quit
```

GigabitEthernet 1/0/2 でスパニングツリー機能を無効にします。

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] undo stp enable
```

トランクポートとしてインタフェースを設定します。

```
[DeviceB-GigabitEthernet1/0/2] port link-type trunk
```

インタフェースに VLAN 1～VLAN 30 を割り当てます。

```
[DeviceB-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
```

インタフェースで flush メッセージの受信を有効にします。

```
[DeviceB-GigabitEthernet1/0/2] smart-link flush enable
[DeviceB-GigabitEthernet1/0/2] quit
```

Monitor Link グループ 1 を作成します。

```
[DeviceB] monitor-link group 1
```

Monitor Link グループ 1 のアップリンクインタフェースとして GigabitEthernet 1/0/1 を設定します。

```
[DeviceB-mtlk-group1] port gigabitethernet 1/0/1 uplink
```

Monitor Link グループ 1 のダウンリンクインタフェースとして GigabitEthernet 1/0/2 を設定します。

```
[DeviceB-mtlk-group1] port gigabitethernet 1/0/2 downlink
[DeviceB-mtlk-group1] quit
```

4)　Device D を設定します。

VLAN 1～VLAN 30 を作成します。

```
<DeviceD> system-view
[DeviceD] vlan 1 to 30
```

トランクポートとして GigabitEthernet 1/0/1 を設定します。

```
[DeviceD] interface gigabitethernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] port link-type trunk
```

インタフェースに VLAN 1～VLAN 30 を割り当てます。

```
[DeviceD-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30
```

インタフェースで flush メッセージの受信を有効にします。

```
[DeviceD-GigabitEthernet1/0/1] smart-link flush enable
[DeviceD-GigabitEthernet1/0/1] quit
```

GigabitEthernet 1/0/2 でスパニングツリー機能を無効にします。

```
[DeviceD] interface gigabitethernet 1/0/2
[DeviceD-GigabitEthernet1/0/2] undo stp enable
```

トランクポートとしてインタフェースを設定します。

```
[DeviceD-GigabitEthernet1/0/2] port link-type trunk
```

インタフェースに VLAN 1～VLAN 30 を割り当てます。

```
[DeviceD-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30
```

インタフェースで flush メッセージの受信を有効にします。

```
[DeviceD-GigabitEthernet1/0/2] smart-link flush enable
[DeviceD-GigabitEthernet1/0/2] quit
```

Monitor Link グループ 1 を作成します。

```
[DeviceD] monitor-link group 1
```

Monitor Link グループ 1 のアップリンクインタフェースとして GigabitEthernet 1/0/1 を設定します。

```
[DeviceD-mtlk-group1] port gigabitethernet 1/0/1 uplink
```

Monitor Link グループ 1 のダウンリンクインタフェースとして GigabitEthernet 1/0/2 を設定します。

```
[DeviceD-mtlk-group1] port gigabitethernet 1/0/2 downlink
[DeviceD-mtlk-group1] quit
```

III. 設定の確認

リンク障害のため、Device A 上の GigabitEthernet 1/0/2 がダウンした場合、Device B の Monitor Link グループ 1 の情報を確認します。

```
[DeviceB] display monitor-link group 1
 Monitor link group 1 information:
  Group status     : UP
  Downlink up-delay: 0(s)
  Last-up-time     : 16:38:26 2014/4/21
  Last-down-time   : 16:37:20 2014/4/21
  Up-port-threshold: 1

  Member                    Role       Status
  ------------------------------------------------
  GE1/0/1                  UPLINK     UP
  GE1/0/2                  DOWNLINK   UP
```

Device D の Monitor Link グループ 1 の情報を確認します。

```
[DeviceD] display monitor-link group 1
Monitor link group 1 information:
  Group status     : DOWN
  Downlink up-delay: 0(s)
  Last-up-time     : 16:37:20 2014/4/21
  Last-down-time   : 16:38:26 2014/4/21
  Up-port-threshold: 1

  Member                    Role       Status
  ------------------------------------------------
  GE1/0/1                  UPLINK     DOWN
  GE1/0/2                  DOWNLINK   DOWN
```

目次

このセクションのページは**8-x-x** です。

4章 Track..... 4-1
4.1 概要..... 4-1
4.1.1 コラボレーションメカニズム..... 4-1
4.1.2 サポート検出モジュール..... 4-2
4.1.3 サポートアプリケーションモジュール..... 4-2
4.2 制限とガイドライン..... 4-2
4.3 コラボレーションアプリケーション例..... 4-2
4.4 Track設定作業リスト..... 4-3
4.5 Trackモジュールと検出モジュールの関連づけ..... 4-3
4.5.1 TrackとNQAの関連づけ..... 4-3
4.5.2 TrackとPoEの関連づけ..... 4-4
4.6 Trackモジュールとアプリケーションモジュールの関連づけ..... 4-5
4.6.1 設定要件..... 4-5
4.6.2 Trackとデフォルトルーティングの関連づけ..... 4-5
4.7 Trackの表示と維持..... 4-6

4章 Track

4.1 概要

トラックモジュールはアプリケーションと検出モジュール間で動作します。アプリケーションモジュールから、さまざまな検出モジュール間の相違点を保護します。

4.1.1 コラボレーションメカニズム

トラックモジュールはアプリケーションと検出モジュールと連携します。

図 4-1に示すように検出モジュールとアプリケーションモジュールの Track モジュールを連携した後、コラボレーションが有効となります。以下のことを行います。

1) 検出モジュールは、インタフェース状態、リンク状態、ネットワークの接続性、ネットワーク性能のような指定したオブジェクトを調査し、検出結果を Track モジュールに通知します。
2) Track モジュールは関連したアプリケーションモジュールに検出結果を送信します。
3) Track オブジェクトの変更を通知した場合、アプリケーションモジュールは通信の中断とネットワーク性能の低下を防ぐため、結果に対して対応することができます。

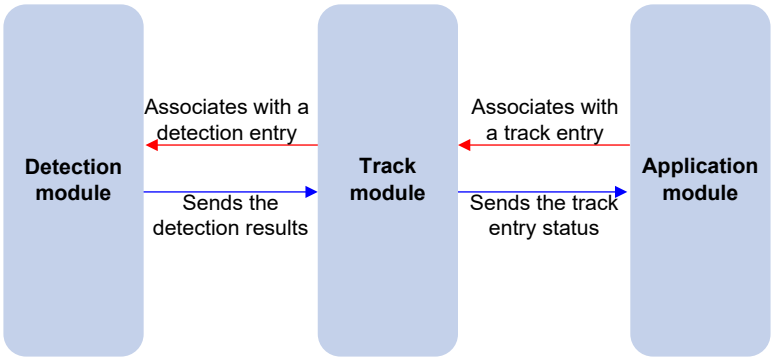


図 4-1 Track モジュールを介したコラボレーション

II. Track モジュールと検出モジュール間のコラボレーション

検出モジュールは、関連した Track 対象オブジェクトの検出結果を Track 対象モジュールに送信します。Track モジュールは以下のように Track エントリの状態を変更します。

- Track 対象オブジェクト機能が正常の場合、Track エントリの状態は Positive になります。たとえば、以下のいずれかの状況の Track エントリの状態は Positive です。
  - ターゲットインタフェースがアップです。
  - ターゲットネットワークが到達可能です。
- Track 対象オブジェクト機能が正常の場合、Track エントリの状態は Negative になります。たとえば、以下のいずれかの状況の Track エントリの状態は Negative です。
  - ターゲットインタフェースがダウンです。
  - ターゲットネットワークが到達不可能です。

- 検出結果が有効でない場合、Track エントリの状態は、NotReady になります。たとえば Track エントリに関連した NQA テストグループが存在しない場合、NotReady になります。

III. Track モジュールとアプリケーションモジュール間のコラボレーション

トラックモジュールはアプリケーションモジュールにトラックエントリの状態変化を報告します。そして、アプリケーションモジュールは通信の中断とネットワークの性能低下を防ぐため、正しいアクションを行うことができます。

4.1.2 サポート検出モジュール

以下の検出モジュールが Track モジュールに関連づけることができます。

- NQA
- インタフェース管理モジュール
- ルート管理モジュール
- LLDP

4.1.3 サポートアプリケーションモジュール

以下のアプリケーションモジュールが Track モジュールに関連づけることができます。

- EAA

4.2 制限とガイドライン

アプリケーションモジュールの Track エントリを設定する場合、状態の変化をすぐに通知することを防ぐため、通知する前に遅延時間を設定することができます。

遅延時間を設定することで、ルートの収束がリンク状態の変更通知よりも遅い場合、通信が失敗することを防ぎます。

4.3 コラボレーションアプリケーション例

以下に NQA、Track、デフォルトルーティング間のコラボレーションの例を示します。

装置でネクストホップ 192.168.0.88 のデフォルトルートを設定します。ネクストホップが到達可能な場合、デフォルトルートは有効です。ネクストホップが到達不可能となった場合、デフォルトルートは無効となります。このため、NQA、Track、デフォルトルーティングモジュール間のコラボレーションを設定します。

1) IP アドレス 192.168.0.88 の到達可能性を監視するため、NQA テストグループを作成します。
2) Track エントリを作成し、NQA テストグループに関連づけます。
   - □ ネクストホップ 192.168.0.88 が到達可能である場合、Track エントリは Positive 状態となります。
   - □ ネクストホップが到達不能になった場合、Track エントリは Negative 状態となります。
3) デフォルトルートに Track エントリを関連づけます。
   - □ Track エントリが Positive 状態になった場合、デフォルトルートが有効となります。

- Track エントリが Negative 状態になった場合、デフォルトルートが無効となります。

4.4 Track設定作業リスト

コラボレーション機能を動作させるため、Track モジュールと検出モジュール、および Track モジュールとアプリケーションモジュールを関連づけます。

作業リスト
(必須設定項目) Trackモジュールと検出モジュールの関連づけ • TrackとNQAの関連づけ • TrackとPoEの関連づけ
(必須設定項目) Trackモジュールとアプリケーションモジュールの関連づけ • Trackとデフォルトルーティングの関連づけ

4.5 Trackモジュールと検出モジュールの関連づけ

4.5.1 Track と NQA の関連づけ

I. Track と NQA の関連づけ

NQA は、ネットワークのパフォーマンス、サービス、サービス品質を解析するために複数のテストタイプをサポートしています。たとえば、NQA テストでは、宛先へ到達可能かどうか、あるいは TCP サーバへ TCP 接続がアップであるかどうかを定期的に検出することができます。

NQA テストグループは、Track エントリに関連づけられている場合、以下のように機能します。

- エラーが連続して指定のしきい値に達した場合、NQA モジュールは、Track モジュールに Track 対象オブジェクトの異常を通知します。その後、Track モジュールは、Track エントリの状態を Negative に変更します。
- 指定したしきい値に達していない場合、NQA モジュールは、Track 対象オブジェクトが正常に機能していることを Track モジュールに通知します。Track モジュールは、Track エントリの状態を Positive に変更します。

NQA の詳細は、オペレーションマニュアルのセクション 9 *システム管理* "*NQA*"を参照してください。

II. 制限とガイドライン

指定した NQA テストグループあるいは Track エントリのリアクションエントリが存在しない場合、Track エントリの状態は NotReady となります。

III. 設定手順

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

操作	コマンド	補足
2． NQA リアクションエントリに関連づけられた Track エントリを作成し、Track view に入る	**track** *track-entry-number* **nqa entry** *admin-name operation-tag* **reaction** *item-number*	―

4.5.2 Track と PoE の関連づけ

メモ：

Track と PoE の関連づけは、Version 7.4.61 を含む以降のソフトウェアからサポートしています。

Track と PoE の関連づけ

PoE モジュールは Track モジュールと連携して、デバイスと PD 間のリンクステータスを監視できます。たとえば、PD が NQA ICMP エコーテストをサポートしている場合、NQA に関連付けられた Track エントリを指定して、PD の到達可能性をテストできます。NQA ICMP エコーテストは、レイヤ 3 インタフェースで設定する必要があります。PI はレイヤ 2 インタフェースです。ICMP エコーテスト用の VLAN インタフェースを作成し、その VLAN に PI を割り当てる必要があります。

Track モジュールは、次のモニタリング結果を PoE モジュールに通知します。

- Positive:監視対象オブジェクトに到達可能です。
- Negative:監視対象オブジェクトに到達不能です。
- NotReady:トラックエントリに関連付けられた NQA グループが存在しないなどの理由により、監視結果の準備ができていません。

トラックモジュールはリンクの障害を検出すると、トラックエントリの状態を正から負に変更します。これにより、PoE モジュールは次のアクションを実行します。

- alarm-only:SNMP 通知とログを出力します。
- alarm-reboot-pd:SNMP 通知とログを出力し、PI に接続されている PD を再起動します。
- NotReady:トラックエントリに関連付けられた NQA グループが存在しないなどの理由により、監視結果の準備ができていません。

I. 設定手順

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． PI view に移行する	**interface** *interface-type interface-number*	―
3． PI とトラックエントリを関連付ける	**poe track** *track-entry-number* **action** { **alarm** | **alarm-reboot-pd** }	デフォルト：PIはトラックエントリに関連付けられていません。

4.6 Trackモジュールとアプリケーションモジュールの関連づけ

Track モジュールとアプリケーションモジュールを関連づける前に、Track エントリが作成されていることを確認してください。

4.6.1 設定要件

アプリケーションモジュールと関連付ける前に Track エントリを作成してください。

関連づけられた Track エントリが存在しない場合、アプリケーションモジュールは間違った Track エントリ状態の情報を取得する可能性があります。

4.6.2 Track とデフォルトルーティングの関連づけ

I. Track とデフォルトルーティングの関連づけ

デフォルトルートは手動でルートを設定します。デフォルトルートについての詳細は、オペレーションマニュアルのセクション 4 *ルーティングプロトコル* を参照してください。

デフォルトルートの欠点は、ネットワークトポロジの変化に適応できないことです。そのため、ネットワークの障害やトポロジの変化が発生すると、ターゲットとの通信ができなくなることがあります。

この問題を回避するために、デフォルトルートのバックアップをする別のルートを設定します。デフォルトルートが到達可能であるとき、場合パケットはデフォルトルートを通して転送されます。デフォルトルートが到達不可能であるとき、場合パケットはバックアップルートを通して転送されます。

リアルタイムでデフォルトルートの到達可能性をチェックする場合、Track とデフォルトルート間の関連づけを行います。

デフォルトルートを設定するとき場合に、出力インタフェースでなくネクストホップを指定すると、デフォルトルート、Track モジュール、宛先モジュール間でのコラボレーションを確立することができます。これにより、Track エントリの状態でデフォルトルートの到達可能性をチェックすることができます。

- Track エントリの状態が Positive の場合、以下の状況となります。
  - デフォルトルートのネクストホップが到達可能です。
  - 設定されたデフォルトルートが有効です。
- Track エントリの状態が Negative の場合、以下の状況となります。
  - デフォルトルートのネクストホップが到達不可能です。
  - 設定されたデフォルトルートが無効です。
- Track エントリの状態が NotReady の場合、以下の状況となります。
  - デフォルトルートのネクストホップの到達可能性が不明です。
  - デフォルトルートが有効です。

II. 制限とガイドライン

デフォルトルート、Track モジュール、宛先モジュール間でのコラボレーションを行う場合、NQA 用に同一のデフォルトルートのネクストホップを設定してください。そうでない場合アクセス検出は正しく動作しません。

デフォルトルートのルートを復旧させる場合、関連する Track エントリはデフォルトルートではなく復旧ルートのネクストホップを監視させる必要があります。そうでなければルートは無効とみなされます。

III. 設定手順

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． ネクストホップの到達可能性をチェックするためにデフォルトルーティングと Track エントリを関連づける	**ip route-static** 0.0.0.0 { 0.0.0.0 | 0 } { *interface-type interface-number* [*next-hop-address* [**nexthop-index** *index-string*]] | *next-hop-address* [**nexthop-index** *index-string*] [**permanent**] } [**preference** *preference*] [**description** *text*]	デフォルト：設定なし

4.7 Trackの表示と維持

すべての view で **display** コマンドを表示することができます。

操作	コマンド
Trackエントリの情報を表示する	**display track** { *track-entry-number* | **all** [**negative** | **positive**] } [**brief**]

QX-S1100G シリーズ Ethernet スイッチ

オペレーションマニュアル

9. システム管理

本マニュアルは以下に示す章で構成されています。

01-システムの保守とデバッグ

02-NTP

03-Information Center

04-SNMP

05-RMON

06-NQA

07-ポートミラーリング

08-トラフィックミラーリング

09-プロセスモニタリングとメンテナンス

10-PoE

11-NetMeister

目次

このセクションのページは **9-x-x** です。

1 章 システムの保守とデバッグ 1-1
1.1 Ping 1-1
1.1.1 ping コマンドを使用したネットワークの接続試験 1-1
1.1.2 Ping 設定例 1-1
1.2 Tracert 1-3
1.2.1 設定要件 1-4
1.2.2 tracert コマンドを使用した故障の検出、ルートにあるすべてのノードの確認 1-4
1.2.3 Tracert 設定例 1-4
1.3 システムのデバッグ 1-6
1.3.1 スイッチのデバッグ情報の制御 1-6
1.3.2 システムデバッグの設定 1-7

1章 システムの保守とデバッグ

この章は ping、tracert を使用したシステムのデバッグ情報について記載します。

1.1 Ping

ping コマンドで、指定したアドレスに到達可能かどうかを確認したり、ネットワーク接続を試験したりすることができます。

ping は ICMP エコーリクエスト（ECHO-REQUEST）を宛先装置に送信します。リクエストを受信した、宛先リクエストは ICMP のリクエストに応答して送信元装置に ICMP エコーリプライ（ECHO-REPLY）を送信します。送信元装置は、パケット送信数、受信したパケットリプライ数、ラウンドトリップタイムの ping の統計情報を表示します。これらの統計情報を解析することによってネットワークの性能を測定することができます。

ping - **r** コマンドを使用して、ICMP エコーリクエストが通過したルーターを表示できます。

1.1.1 ping コマンドを使用したネットワークの接続試験

すべての view で **ping** コマンドを実行できます。

操作	コマンド	補足
指定したアドレスに到達可能かどうかを確認する	• IPv4ネットワーク：**ping** [**ip**] [**-a** *source-ip* | **-c** *count* | **-f** | **-h** *ttl* | **-i** *interface-type interface-number* | **-m** *interval* | **-n** | **-p** *pad* | **-q** | **-r** | **-s** *packet-size* | **-t** *timeout* | **-tos** *tos* | **-v**] * *host* • IPv6ネットワーク：**ping ipv6** [**-a** *source-ipv6* | **-c** *count* | **-i** *interface-type interface-number* | **-m** *interval* | **-q** | **-s** *packet-size* | **-t** *timeout* | **-v**] * *host*	低速ネットワークで**ping**コマンドを使用する場合、タイムアウトタイマの値を大きな値に設定してください。（コマンドの**-t**キーワードで示されます。）

1.1.2 Ping 設定例

I. ネットワーク要件

図 1-1に示すように、Device A と Device C 間で通信可能かどうか確認します。互いに通信可能である場合、Device A から Device C のルートについての詳細な情報を取得します。

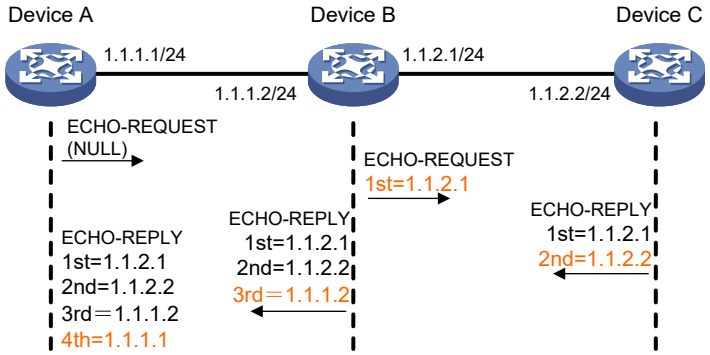


図 1-1 ネットワーク図

II. 設定手順

Device A で **ping** コマンドを使用し、Device C と通信可能かどうか確認します。

```
Ping 1.1.2.2 (1.1.2.2): 56 data bytes, press CTRL_C to break
56 bytes from 1.1.2.2: icmp_seq=0 ttl=254 time=2.137 ms
56 bytes from 1.1.2.2: icmp_seq=1 ttl=254 time=2.051 ms
56 bytes from 1.1.2.2: icmp_seq=2 ttl=254 time=1.996 ms
56 bytes from 1.1.2.2: icmp_seq=3 ttl=254 time=1.963 ms
56 bytes from 1.1.2.2: icmp_seq=4 ttl=254 time=1.991 ms

--- Ping statistics for 1.1.2.2 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.963/2.028/2.137/0.062 ms
```

出力は、以下の状態を示します。

- Device A が Device C に 5 つの ICMP パケットを送信し、Device A は ICMP パケットを受信します。
- パケットの送信失敗がありません。
- ルートが到達可能です。

Device A から Device C の詳細なルート情報を取得します。

```
<DeviceA> ping -r 1.1.2.2
Ping 1.1.2.2 (1.1.2.2): 56 data bytes, press CTRL_C to break
56 bytes from 1.1.2.2: icmp_seq=0 ttl=254 time=4.685 ms
RR:     1.1.2.1
        1.1.2.2
        1.1.1.2
        1.1.1.1
56 bytes from 1.1.2.2: icmp_seq=1 ttl=254 time=4.834 ms  (same route)
56 bytes from 1.1.2.2: icmp_seq=2 ttl=254 time=4.770 ms  (same route)
56 bytes from 1.1.2.2: icmp_seq=3 ttl=254 time=4.812 ms  (same route)
56 bytes from 1.1.2.2: icmp_seq=4 ttl=254 time=4.704 ms  (same route)

--- Ping statistics for 1.1.2.2 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 4.685/4.761/4.834/0.058 ms
```

図 1-1に示すように **ping - r** のテスト手順は以下となります。

1) 送信元（Device A）は RR オプションを空で ICMP エコーリクエストを宛先（Device C）に対して送信します。
2) 中間装置（Device B）は ICMP エコーリクエストの RR オプションに出力インタフェースの IP アドレス（1.1.2.1）を追加し、転送します。

3) リクエストを受信した宛先装置はリクエストの RR オプションをコピーし、RR オプションに出力インタフェースの IP アドレス（1.1.2.2）を追加します。ICMP エコーリプライを送信します。
4) 中間装置は ICMP エコーリプライの RR オプションに出力インタフェースの IP アドレス（1.1.1.2）を追加し、リプライを転送します。
5) リプライを受信した送信元装置は RR オプションにインタフェースの IP アドレス（1.1.1.1）を追加します。最後に、1.1.1.1 <-> {1.1.1.2; 1.1.2.1} <-> 1.1.2.2 という Device A～Device C 間の詳細な情報を取得します。

1.2 Tracert

Tracert（traceroute と呼ばれます）は、ネットワークが有効かどうか確認するために、送信元から宛先にパケットを伝送するレイヤ 3 装置の IP アドレスの追跡を行います。ネットワークに不具合があった場合に、tracert コマンドを使用して機能しなくなったノードを特定するのに有用です。

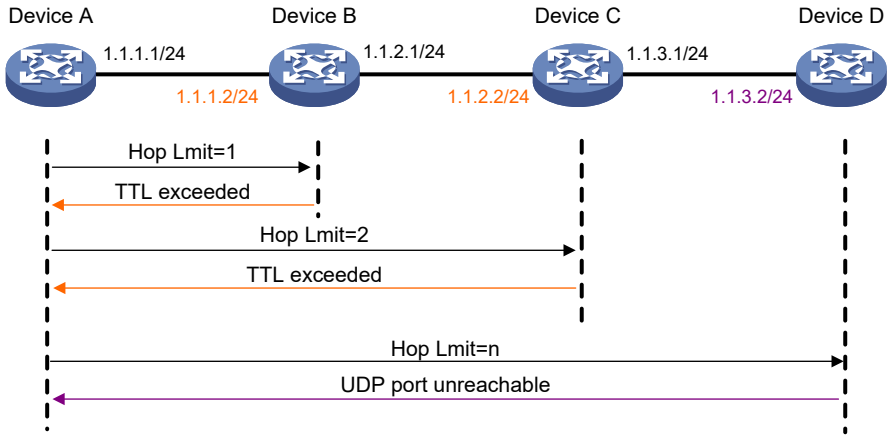


図 1-2 Tracert の動作

Tracert は装置の IP アドレスを取得するため、受信した ICMP エラーメッセージを使用します。図 1-2に示すように、tracert が動作します。

1) 送信元装置（Device A）が宛先装置（Device D）に TTL 値が 1 のパケットを送信します。パケットの UDP 番号は宛先のアプリケーションで使用されないポート番号です。
2) 最初のホップ（Device B）（パケットを最初に受信するレイヤ 3 装置）は、1.1.1.2 の IP アドレスがカプセル化された TTL-expired ICMP エラーメッセージを送信元に返します。このように、送信元装置は最初のレイヤ 3 装置のアドレス（1.1.1.2）を受信します。
3) 送信元装置が宛先の装置に TTL 値が 2 のパケットを送信します。
4) 2 番目のホップ（Device C）が TTL-expired ICMP エラーメッセージで応答し、これで送信元装置は 2 番目のレイヤ 3 装置のアドレス（1.1.2.2）を取得します。
5) このプロセスは、最終宛先の装置に到達するまで続きます。宛先のアプリケーションは UDP ポートを使用していません。宛先は IP アドレス 1.1.3.2 の到達不能 ICMP エラーメッセージのリプライをします。
6) 送信元装置は以下のことを認識します。

- 到達不能 ICMP エラーメッセージを受信した場合、宛先に届いたことを認識します。
- 宛先装置までのパスは 1.1.1.2 から、1.1.2.2 から、1.1.3.2 であると認識します。

1.2.1 設定要件

tracert コマンドを使用する前に、以下の作業を行ってください。

IPv4 ネットワーク：

- 中間装置（送信元装置と宛先装置の間の装置）で ICMP タイムアウトパケットの送信を有効にします。中間デバイスが QX シリーズの場合、装置で **ip ttl-expires enable** コマンドを実行してください。このコマンドの詳細は、コマンドマニュアルのセクション 3 *IP サービス* "*IP パフォーマンスの最適化*"を参照してください。
- 中間装置（送信元装置と宛先装置の間の装置）で ICMP 宛先到達不能パケットの送信を有効にします。中間デバイスが QX シリーズの場合、装置で **ip unreachables enable** コマンドを実行してください。このコマンドの詳細は、コマンドマニュアルのセクション 3 *IP サービス* "*IP パフォーマンスの最適化*"を参照してください。

IPv6 ネットワーク：

- 中間装置（送信元装置と宛先装置の間の装置）で ICMPv6 タイムアウトパケットの送信を有効にします。中間装置が QX シリーズの場合、装置で **ipv6 hoplimit-expires enable** コマンドを実行してください。このコマンドの詳細は、コマンドマニュアルのセクション 3 *IP サービス* "*IPv6 の基本*"を参照してください。
- 中間装置（送信元装置と宛先装置の間の装置）で ICMPv6 宛先到達不能パケットの送信を有効にします。中間装置が QX シリーズの場合、装置で **ipv6 unreachables enable** コマンドを実行してください。このコマンドの詳細は、コマンドマニュアルのセクション 3 *IP サービス* "*IPv6 の基本* "を参照してください。

1.2.2 tracert コマンドを使用した故障の検出、ルートにあるすべてのノードの確認

すべての view で **tracert** コマンドを実行できます。

操作	コマンド
送信元から宛先のルートを表示する	• IPv4ネットワーク： **tracert** [**-a** *source-ip* | **-f** *first-ttl* | **-m** *max-ttl* | **-p** *port* | **-q** *packet-number* | **-w** *timeout*] * *host* • IPv6ネットワーク： **tracert ipv6** [**-f** *first-hop* | **-m** *max-hops* | **-p** *port* | **-q** *packet-number* | **-w** *timeout*] * *host*

1.2.3 Tracert 設定例

I. ネットワーク要件

図 1-3に示すように、Device A は Device C への Telnet が失敗しています。

Device A と Device C 間でネットワークの接続性を確認します。互いに通信できない場合、ネットワークの故障したノードを特定できます。

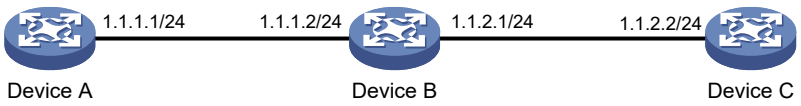


図 1-3 ネットワーク図

II. 設定手順

1) 図 1-3に示すように Device に IP アドレスを設定します。
2) Device A でデフォルトルートを設定します。

```
<DeviceA> system-view
[DeviceA] ip route-static 0.0.0.0 0.0.0.0 1.1.1.2
[DeviceA] quit
```

3) Device A と Device C 間の接続性を確認します。

```
<DeviceA> ping 1.1.2.2
Ping 1.1.2.2(1.1.2.2): 56 -data bytes, press CTRL_C to break
Request time out
Request time out
Request time out
Request time out
Request time out

--- Ping statistics for 1.1.2.2 ---
5 packet(s) transmitted,0 packet(s) received,100.0% packet loss
```

出力は、Device A と Device C が通信不可能であることを示します。

4) 故障したノードを特定します。

Device B で ICMP タイムアウトパケットの送信を有効にします。

```
<DeviceB> system-view
[DeviceB] ip ttl-expires enable
```

Device C で ICMP 到達不可能パケットの送信を有効にします。

```
<DeviceC> system-view
[DeviceC] ip unreachables enable
```

故障したノードを特定します。

```
<DeviceA> tracert 1.1.2.2
traceroute to 1.1.2.2 (1.1.2.2) 30 hops at most,40 bytes each packet, press CTRL_C
to break
 1  1.1.1.2 (1.1.1.2) 1 ms 2 ms 1 ms
 2  * * *
 3  * * *
 4  * * *
 5
<DeviceA>
```

出力は、Device A と Device C が互いに到達できず、Device A と Device B が到達でき、Device B と Device C 間の通信でエラーが発生していることを示します。

5) 問題を確認するため Device A と Device C で以下のコマンドを実行します。

- **debugging ip icmp** コマンドを使用して Device A と Device C で ICMP パケットの送受信ができるか確認を行います。

- **display ip routing-table** コマンドを使用して Device A と Device C のルートがあるか確認します。

1.3 システムのデバッグ

装置は、さまざまなデバッグ機能があります。サポートしているプロトコルおよび機能の大半に対し、システムはユーザのエラー診断に役立つデバッグ情報を提供しています。

1.3.1 スイッチのデバッグ情報の制御

次の 2 つのスイッチがデバッグ情報の表示を制御します。

- **モジュールデバッグスイッチ** － モジュール特有のデバッグ情報を制御します。
- **画面出力スイッチ** － 所定の画面にデバッグ情報を表示するかを制御します。出力する画面上で **terminal monitor** コマンド、**terminal logging level** コマンドを使用します。これらのコマンドの詳細は、コマンドマニュアルのセクション 9 *システム管理* "*Information center*"を参照してください。

図 1-4に示すように、モジュールデバッグスイッチと画面出力スイッチの関係を示したものです。装置は、デバッグ情報をモジュール 1、2、3 に出力できると仮定します。両方に電源が入っている場合のみ情報は端末に出力されます。

デバッグ情報は通常、コンソールに表示されます。他の宛先にデバッグ情報を送信することができます。詳細はオペレーションマニュアルのセクション 9 *システム管理* "*Information center*"を参照してください。

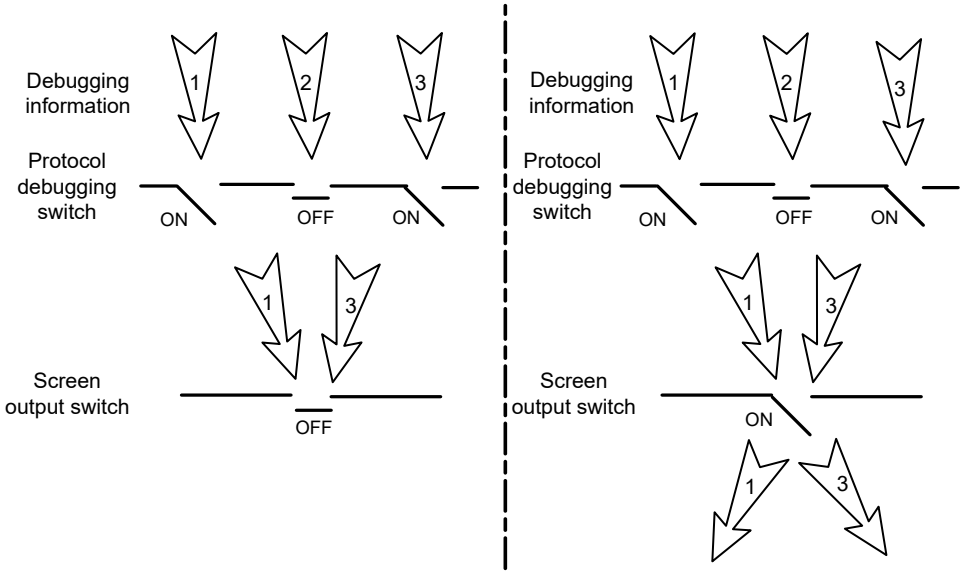


図 1-4 モジュールデバッグスイッチと画面出力スイッチの関係

1.3.2 システムデバッグの設定

デバッグコマンドの出力は、メモリ容量に影響します。システム性能を保証するため、異常な状況にあるプロトコルに関連したデバッグのみ有効にしてください。デバッグを行った後、**undo debugging all** コマンドを使用してすべてのデバッグ機能を無効にしてください。

以下にデバッグ機能の設定を示します。

操作	コマンド	補足
1. user view でプロトコルのデバッグを有効にする	**debugging** *module-name* [*option*]	デフォルト：無効
2. （オプション設定項目）すべての view で有効なデバッグ機能を表示する	**display debugging** [*module-name*]	—

目次

このセクションのページは **9-x-x** です。

2 章 NTP 2-1
2.1 概要 2-1
2.1.1 NTP の動作 2-1
2.1.2 NTP アーキテクチャ 2-2
2.1.3 運用モード 2-3
2.1.4 NTP セキュリティ 2-5
2.1.5 プロトコルと標準 2-7
2.2 設定の制限とガイドライン 2-7
2.3 設定作業リスト 2-7
2.4 NTP サービスの有効化 2-7
2.5 NTP 運用モードの設定 2-7
2.5.1 NTP クライアント/サーバモードの設定 2-7
2.5.2 NTP シンメトリックアクティブ/パッシブモードの設定 2-8
2.5.3 NTP ブロードキャストモードの設定 2-8
2.5.4 NTP マルチキャストモードの設定 2-9
2.6 NTP サービスアクセス制御権の設定 2-9
2.7 NTP 認証の設定 2-10
2.7.1 クライアント/サーバモードの NTP 認証の設定 2-10
2.7.2 シンメトリックアクティブ/パッシブモードの NTP 認証の設定 2-11
2.7.3 ブロードキャストモードの NTP 認証の設定 2-13
2.7.4 マルチキャストモードの NTP 認証の設定 2-14
2.8 NTP オプションパラメータの設定 2-16
2.8.1 NTP メッセージの送信元アドレスの設定 2-16
2.8.2 インタフェースでの NTP メッセージ受信の無効化 2-17
2.8.3 ダイナミックアソシエーションの最大数の設定 2-17
2.8.4 NTP パケットの DSCP 値の設定 2-18
2.9 NTP の表示と維持 2-18
2.10 NTP 設定例 2-18
2.10.1 NTP クライアント/サーバモードの設定例 2-18
2.10.2 NTP シンメトリックアクティブ/パッシブモードの設定例 2-20
2.10.3 NTP ブロードキャストモードの設定例 2-21
2.10.4 NTP マルチキャストモードの設定例 2-22
2.10.5 NTP 認証を使用したクライアント/サーバモードの設定例 2-25
2.10.6 NTP 認証を使用したブロードキャストモードの設定例 2-26

2章 NTP

NTP（Network Time Protocol）を使用して、ネットワークを介して信頼されたシステムクロックと同期を取ることが可能になります。システムメッセージのタイムスタンプとログは、システム時刻を使用しているため、ネットワーク管理、チャージシステム、監査、分散コンピューティングなどの、さまざまなアプリケーションでは正確なシステムクロックが必要となります。

2.1 概要

NTP はネットワーク装置間のシステムクロックを動的に同期させるため、一般的に大規模ネットワークで使用されます。手動でシステムクロックを設定するよりも、高いクロック精度が保証されます。NTP を有効に利用することで、装置間のシステムクロックを同期させ続けることができます。

NTP は UDP プロトコルで、UDP ポート 123 を使用します。

🕮 **メモ：**

NTP は、レイヤ 3 イーサネットインタフェースでサポートします。

2.1.1 NTP の動作

図 2-1に示すように、Device A と Device B の 2 つの Device 間でシステム時間を同期させる NTP の基本的なワークフローを示します。以下のように仮定します。

- システムクロックの同期を行う前に、Device A の時刻は 10:00:00 am で Device B の時刻は 11:00:00 am と設定されています。
- Device B は NTP サーバとして使用されます。Device A は Device B に同期化されます。
- NTP メッセージが Device A から Device B あるいは Device B から Device A に送信されるまで 1 秒かかります。

Device B で NTP メッセージを処理するのに 1 秒かかります。

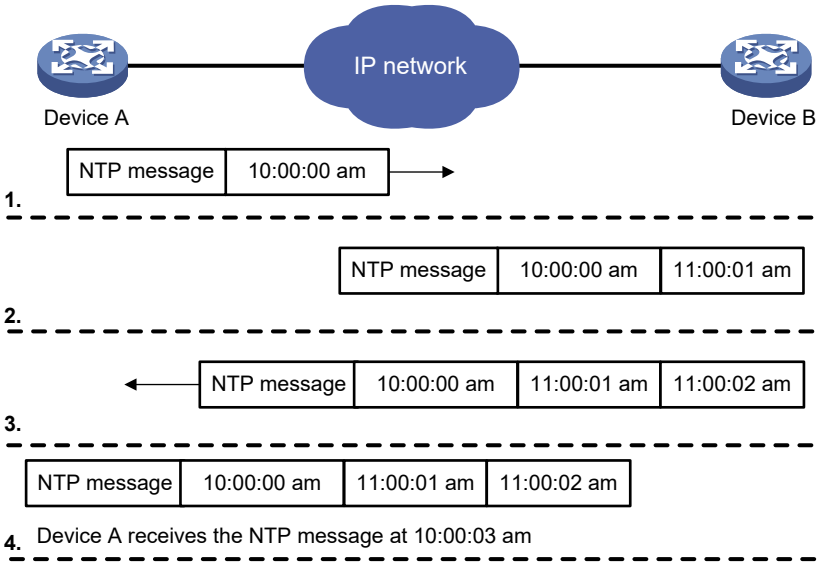


図 2-1 基本ワークフロー

以下に同期プロセスを示します。

1) Device A から Device B に NTP メッセージを送信します。メッセージは、Device A から発信される場合にタイムスタンプが与えられます。タイムスタンプは 10:00:00 am （T1） です。
2) NTP メッセージが Device B に届くと、Device B によってタイムスタンプが与えられます。タイムスタンプは 11:00:01 am （T2） です。
3) NTP メッセージが Device B から発信される場合に、Device B はメッセージにタイムスタンプを与えます。タイムスタンプは 11:00:02 am （T3）です。
4) Device A が NTP メッセージを受信した場合、Device A の現地時刻は 10:00:03 am （T4）です。

Device A には以下の 2 つの重要なパラメータを計算するための情報があります。

- **NTP メッセージのラウンドトリップ遅延**：遅延＝（T4 － T1）－（T3 － T2）＝2 秒
- **Device A と Device B の間の時差**：オフセット＝（（T2 － T1）＋（T3 － T4））/2 ＝1 時間

これらのパラメータにもとづき、Device A の時計を Device B の時計に同期することができます。

上記は、NTP の動作メカニズムについての概要です。詳細については、関連するプロトコルと標準を参照してください。

2.1.2 NTP アーキテクチャ

NTP はクロックの正確さを定義するため、図 2-2に示すように 1 から 16 の stratum（層）を使用します。stratum の値が小さいほど高い精度を持ちます。stratum 1 から 15 レベルのクロックは同期された時間で、stratum のレベル 16 のクロックは同期化されていないことを示します。

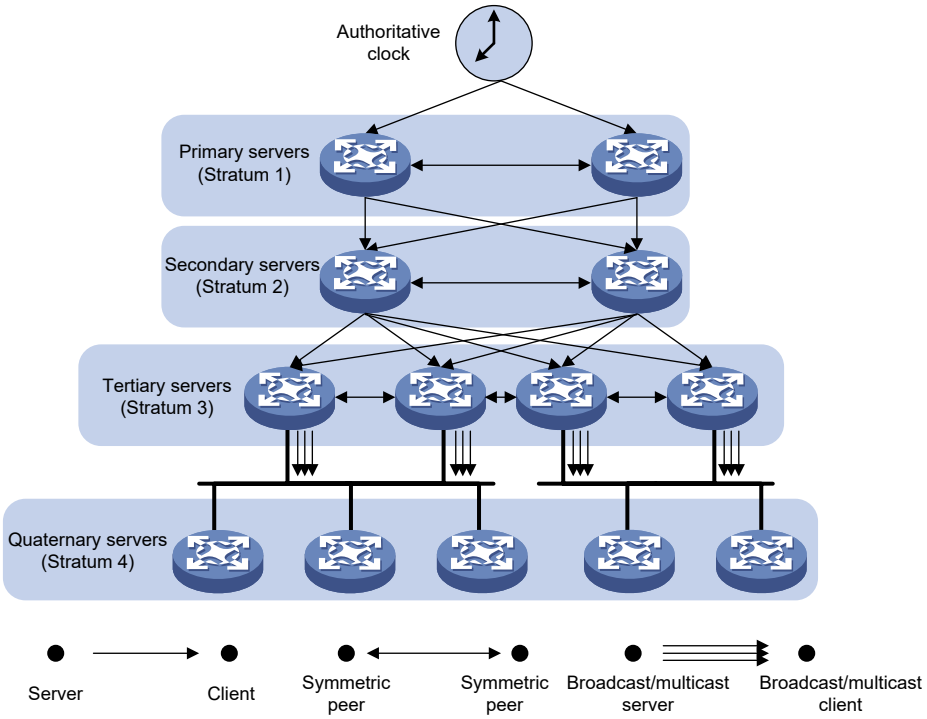


図 2-2 NTP アーキテクチャ

stratum レベル 1 の NTP サーバは、原子時計のような基準となるソースから時間を取得し、NTP サーバとして他の装置に時間を提供します。stratum レベル 2 のサーバは stratum レベル 1 のサーバなどから時間を取得します。

時間の正確性と有効性を保証するため、装置は複数の NTP サーバを指定できます。装置は stratum のようなパラメータをもとにしてクロックソースとして最適な NTP サーバを選択します。装置が選択するクロックは参照ソースと呼ばれます。クロック選択の詳細は関連するプロトコルと標準を参照してください。

ネットワークの装置がもっとも権威のあるサーバに同期することができない場合、以下の処理を行うことができます。

- ネットワークから相対的に精度のあるクロックを持つ装置を選択します。
- ネットワークのほかの装置と同期させるため、参照クロックとして相対的に精度のある装置のローカルクロックを使用します。

2.1.3 運用モード

NTP は以下の運用モードをサポートします。

- クライアント/サーバモード
- シンメトリックアクティブ/パッシブモード
- ブロードキャストモード
- マルチキャストモード

表 2-1 NTP 運用モード

モード	作業処理	原則	アプリケーションシナリオ
クライアント/サーバ	クライアントではNTPサーバのIPアドレスを指定します。 クライアントはクロック同期メッセージをNTPサーバに送信します。 メッセージを受信したサーバは自動的にサーバのモードで動作し、応答を返します。 クライアントはサーバに複数同期した場合、サーバからの応答を受信した後、最適なクロックを選択し、ローカルクロックを最適な参照ソースと同期させます。	クライアントはサーバと同期することができますが、サーバはクライアントと同期することができません。	図 2-2に示すように、このモードは高いstratumの装置が低いstratumの装置に同期します。
シンメトリックアクティブ/パッシブ	シンメトリックアクティブピア上で、シンメトリックパッシブピアのIPアドレスを指定します。 シンメトリックアクティブピアは周期的にシンメトリックパッシブピアにクロック同期メッセージを送信します。 シンメトリックパッシブピアは自動的にシンメトリックパッシブモードで動作し、応答を送信します。 シンメトリックアクティブピアがサーバに複数同期した場合、サーバからの応答を受信した後、最適なクロックを選択し、ローカルクロックを最適な参照ソースと同期させます。	シンメトリックアクティブピアとシンメトリックパッシブピアは互いに同期することができます。両方が同期された場合、低いstratumのピアが高いstratumのピアに同期します。	図 2-2に示すように、このモードはバックアップとして動作させるため、同じstratumの2つ以上のサーバ間で使われます。 高いstratumのすべてのサーバと通信できない場合、サーバは同じstratumのサーバと同期します。
ブロードキャスト	サーバは周期的にブロードキャストアドレス255.255.255.255にクロック同期メッセージを送信します。 クライアントはサーバと同期するため、ブロードキャストメッセージに応答したサーバからブロードキャストメッセージを待ちます。 最初にブロードキャストメッセージを受信した場合、クライアントとサーバはネットワーク遅延を計算するため、メッセージの交換を開始します。ブロードキャストサーバのみがクロック同期メッセージを送信します。	ブロードキャストクライアントはブロードキャストサーバに同期することができますが、ブロードキャストサーバはブロードキャストクライアントに同期することができません。	ブロードキャストサーバはクロック同期メッセージを同じサブネットのクライアントに送信します。 図 2-2に示すように、このモードは潜在的に1つあるいは少ないサーバで、多くのクライアントがある環境で使われます。 ブロードキャストモードは、ブロードキャストサーバのみがクロック同期メッセージを送信するため、クライアント/サーバモードやシンメトリックアクティブ/パッシブよりも精度が低くなります。

モード	作業処理	原則	アプリケーションシナリオ
マルチキャスト	マルチキャストサーバは周期的にユーザが設定したマルチキャストアドレスにクロック同期メッセージを送信します。クライアントはマルチキャストメッセージに応答したサーバからマルチキャストメッセージを待ちます。	マルチキャストクライアントはマルチキャストサーバに同期することができますが、マルチキャストサーバはマルチキャストクライアントに同期することができません。	マルチキャストサーバはクロック同期メッセージを同じあるいは異なるサブネットのクライアントに送信します マルチキャストモードは、クライアント/サーバモードやシンメトリックアクティブ/パッシブよりも精度が低くなります。

この章では、NTP サーバあるいはサーバとは、クライアント/サーバモードの NTP サーバとして動作する装置を示します。タイムサーバとは、NTP サーバ、NTP シンメトリックピア、ブロードキャストサーバ、マルチキャストサーバを含んだ、クロック同期を行うことができるすべての装置を示します。

2.1.4 NTP セキュリティ

クロック同期のセキュリティを向上させるため、装置は NTP サービスアクセス制御権と認証機能をサポートします。

I. NTP サービスアクセス制御権の設定

ACL を用いて NTP サービスアクセス制御権を設定することができます。アクセス制御権は以下となります。

- **Peer**ー時刻要求と NTP コントロールクエリ（アラーム、認証ステータス、時間サーバなどの情報）を受信し、ローカル装置が隣接装置に自身を同期させることを可能とします。
- **Server**ー時刻要求と NTP コントロールクエリを受信するが、ローカル装置がピアの装置に自身を同期させることを可能としません。
- **Synchronization**ーアドレスリストを通過したアドレスを持つシステムからの時刻要求のみ受信します。
- **Query**ーピアの装置からローカル装置への NTP コントロールクエリのみ受信します。

装置が NTP 要求を受信した場合、もっとも制限の少ないアクセス制御権からもっとも制御されているアクセス制御権の順番（peer、server、synchronization、query）でアクセス制御権に対する要求にマッチします。

- アクセス制御権が設定されていない場合、**peer** はローカル装置とビアの装置に与えられます。
- ビアの装置の IP アドレスが複数のアクセス制御権のための ACL にマッチし、**Permit** となる場合、もっとも制限の少ないアクセス制御権がビアの装置に与えられます。ACL にマッチしない、または **deny** となった場合、アクセス制御権は与えられません。
- アクセス制御権のために指定された ACL に条件が作成されない場合、アクセス制御権は与えられません。
- アクセス制御権のために指定された ACL が 1 つも作成されない場合、**peer** が与えられます。

- アクセス制御権で指定された ACL にルールが含まれていない場合、アクセス制御権は与えられません。

この機能は、NTP を運用するシステムに最低限のセキュリティを提供します。より安全な方法としては NTP 認証があります。

II. NTP 認証

NTP 認証は、セキュリティのため、NTP メッセージを認証します。NTP メッセージが認証をパスした場合、装置は、メッセージを受信し、クロック同期情報を取得します。パスしない場合、メッセージを廃棄します。この機能は、許可されていないサーバに同期をしないようにするために使われます。

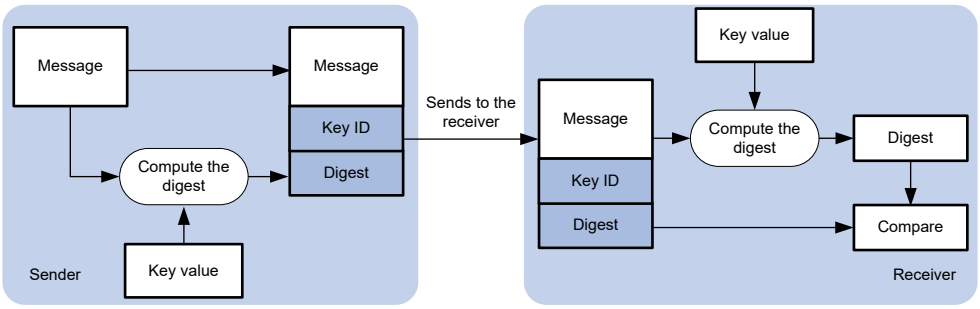


図 2-3 NTP 認証

図 2-3に示すように NTP 認証は以下のように動作します。

1) Sender は、キーID によって識別されたキーに従って NTP メッセージを計算するため MD5 アルゴリズムを使用します。NTP メッセージを計算したダイジェストとキーID を Receiver に送信します。
2) メッセージを受信すると Receiver は以下の処理を行います。

a) メッセージのキーIDに応じてキーを確認します。

b) ダイジェストを計算するため、キー、キーと同一の認証アルゴリズムを使用します。

c) NTPメッセージの計算したダイジェストとNTPメッセージに含まれているダイジェストと比較します。

- 計算したダイジェストと NTP メッセージに含まれているダイジェストが異なる場合、Receiver はメッセージを廃棄します。
- 計算したダイジェストと NTP メッセージに含まれているダイジェストが同一ですが作成の要求がない場合、Receiver はメッセージに応答します。NTP メッセージの詳細は、オペレーションマニュアルのセッション *9 システム管理*“*NTP*”の“*ダイナミックアソシエーションの最大数の設定*”を参照してください。
- 計算したダイジェストと NTP メッセージに含まれているダイジェストが同一で、NTP セッションが作成されている場合、ローカル装置は Sender が認証 ID の使用を許可するか決定します。Sender が認証 ID の使用を許可されている場合、Receiver はメッセージを受信します。Sender が認証 ID の使用を許可されていない場合、Receiver はメッセージを廃棄します。

2.1.5 プロトコルと標準

- RFC 1305, *Network Time Protocol (Version 3) Specification, Implementation and Analysis*
- RFC 5905, *Network Time Protocol Version 4: Protocol and Algorithms Specification*

2.2 設定の制限とガイドライン

以下の設定の制限とガイドラインに従って NTP を設定してください。

- アグリゲートメンバーポートで NTP と SNTP を同時に設定することはできません。
- 頻繁にクロックが変更する、あるいは同期の失敗が発生することを防ぐため、ネットワークの参照クロックを複数指定しないでください。
- NTP としてシステムクロックソースを指定するため、**clock protocol** コマンドを使用してください。**clock protocol** コマンドの詳細は、コマンドマニュアルのセクション 1 *はじめに*“*装置管理*”を参照してください。

2.3 設定作業リスト

作業リスト
（必須設定項目） NTPサービスの有効化
（必須設定項目） 以下のうちの1つを実行します。 • NTP運用モードの設定 • 参照ソース用ローカルクロックの設定
（オプション設定項目） NTP認証の設定
（オプション設定項目） NTPオプションパラメータの設定

2.4 NTPサービスの有効化

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． NTP サービスを有効にする	**ntp-service enable**	デフォルト：無効

2.5 NTP運用モードの設定

この章は NTP 運用モードの設定方法について記載します。

2.5.1 NTP クライアント/サーバモードの設定

NTP クライアントを設定する場合、以下のガイドラインに従います。

- サーバは他の装置によって同期させる必要があります。あるいは NTP クライアントを同期する前に参照ソースとしてローカルクロックを使用する必要があります。そうでなければクライアントは NTP サーバに同期することができません。
- サーバの stratum レベルがクライアントと等しいあるいは高いレベルである場合クライアントはサーバに同期しません。
- **ntp-service unicast-server** コマンドを繰り返して設定することで複数のサーバを設定することができます。
- 装置がクライアント/サーバモードで動作する場合、クライアントの IP アドレスを指定します。

以下に NTP クライアントの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. 装置の NTP サーバを指定する	**ntp-service unicast-server** { *server-name* | *ip-address* } [**authentication-keyid** *keyid* | **maxpoll** *maxpoll-interval* | **minpoll** *minpoll-interval* | **priority** | **source** *interface-type interface-number* | **version** *number*] *	デフォルト：指定なし

2.5.2 NTP シンメトリックアクティブ/パッシブモードの設定

NTP シンメトリックアクティブピアを設定する場合、以下のガイドラインに従います。

- NTP を有効にするため、シンメトリックパッシブピアで **ntp-service enable** コマンドを実行してください。そうでなければシンメトリックパッシブピアはシンメトリックアクティブピアから NTP メッセージを処理しません。
- シンメトリックアクティブピアあるいはシンメトリックパッシブピアのどちらかあるいは、その両方は同期化された状態にする必要があります。そうでなければ同期化することができません。
- **ntp-service unicast-peer** コマンドを繰り返して設定することで複数のシンメトリックパッシブピアを設定することができます。
- シンメトリックアクティブ/パッシブモードで装置が動作する場合、シンメトリックパッシブピア用にシンメトリックアクティブピアの IP アドレスを指定します。

以下に NTP シンメトリックアクティブピアの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. シンメトリックパッシブピアを指定する	**ntp-service unicast-peer** { *peer-name* | *ip-address* } [**authentication-keyid** *keyid* | **maxpoll** *maxpoll-interval* | **minpoll** *minpoll-interval* | **priority** | **source** *interface-type interface-number* | **version** *number*] *	デフォルト：指定なし

2.5.3 NTP ブロードキャストモードの設定

ブロードキャストサーバは、ブロードキャストクライアントを同期する前に、他の装置によって同期させる必要があります。あるいは参照ソースとしてローカルクロックを使用す

る必要があります。そうでなければブロードキャストクライアントはブロードキャストサーバに同期させることができません。

ブロードキャストサーバとクライアントの両方でブロードキャストモードの NTP を設定します。QX-S1100G シリーズはブロードキャストサーバ機能をサポートしていません。

I. ブロードキャストクライアントの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． interface view に移行する	**interface** *interface-type interface-number*	NTPブロードキャストメッセージを受信するインタフェースに移行します。
3． NTP ブロードキャストクライアントモードで動作するように装置を設定する	**ntp-service broadcast-client**	デフォルト：設定なし コマンドを実行した後、装置は指定したインタフェースからNTPブロードキャストメッセージを受信します。

2.5.4 NTP マルチキャストモードの設定

マルチキャストサーバは、マルチキャストクライアントを同期する前に、他の装置によって同期させる必要があります。あるいは参照ソースとしてローカルクロックを使用する必要があります。そうでなければマルチキャストクライアントはマルチキャストサーバに同期させることができません。

マルチキャストサーバとクライアントの両方でマルチキャストモードの NTP を設定します。QX-S1100G シリーズはマルチキャストサーバ機能をサポートしていません。

I. マルチキャストクライアントの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． interface view に移行する	**interface** *interface-type interface-number*	NTPマルチキャストメッセージを受信するインタフェースに移行します。
3． NTP マルチキャストクライアントモードで動作するように装置を設定する	**ntp-service multicast-client** [*ip-address*]	デフォルト：設定なし コマンドを実行した後、装置は指定したインタフェースからNTPマルチキャストメッセージを受信します。

2.6 NTPサービスアクセス制御権の設定

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

操作	コマンド	補足
2． 隣接装置がローカル装置にアクセスするための NTP サービスアクセス制御権を設定する	**ntp-service** { **peer** | **query** | **server** | **synchronization** } **acl** *ipv4-acl-number*	デフォルト：peer

NTP サービスアクセス制御権をローカル装置に設定する前にアクセス制御権に関連した ACL を作成、設定してください。詳細はコマンドマニュアルのセクション 6 *ACL and QoS*”*ACL*”を参照してください。

2.7 NTP認証の設定

この章は NTP 認証の設定手順について記載します。

2.7.1 クライアント/サーバモードの NTP 認証の設定

サーバとクライアントで設定されたキーID とキーの値は同一にする必要があります。そうでなければ NTP 認証は失敗します。ピアの装置がローカル装置でキーID を使用することができることを確認してください。

以下にクライアントの NTP 認証の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． NTP 認証を有効にする	**ntp-service authentication enable**	デフォルト：無効
3． NTP 認証キーを設定する	**ntp-service authentication-keyid** *keyid* **authentication-mode md5** { **cipher** | **simple** } *string* *	デフォルト：設定なし
4． 認証キーをトラステッドキーとして設定する	**ntp-service reliable authentication-keyid** *keyid*	デフォルト：設定なし
5． NTP サーバとキーを関連づける	**ntp-service unicast-server** { *server-name* | *ip-address* } **authentication-keyid** *keyid*	―

以下にサーバの NTP 認証の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． NTP 認証を有効にする	**ntp-service authentication enable**	デフォルト：無効
3． NTP 認証キーを設定する	**ntp-service authentication-keyid** *keyid* **authentication-mode md5** { **cipher** | **simple** } *string* *	デフォルト：設定なし
4． 認証キーをトラステッドキーとして設定する	**ntp-service reliable authentication-keyid** *keyid*	デフォルト：設定なし

クライアントとサーバで異なる設定が実行されると、NTP 認証の結果は異なります。詳細を表 2-2に示します。（ーは相違がないことを示します。）

以下に NTP 認証の結果を示します。

表 2-2 NTP 認証の結果

クライアント			サーバ		認証結果
NTP 認証を有効にする	キーをトラステッドキーとして設定する	NTP サーバにキーを関連づける	NTP 認証を有効にする	キーをトラステッドキーとして設定する	
Yes	Yes	Yes	Yes	Yes	認証は成功します。NTPメッセージは正常に送受信することができます。
Yes	Yes	Yes	Yes	No	認証は失敗します。NTPメッセージは正常に送受信することができません。
Yes	Yes	Yes	No	ー	認証は失敗します。NTPメッセージは正常に送受信することができません。
Yes	No	Yes	ー	ー	認証は失敗します。NTPメッセージは正常に送受信することができません。
Yes	ー	No	ー	ー	認証はありません。NTPメッセージは正常に送受信することができます。
No	ー	ー	ー	ー	認証はありません。NTPメッセージは正常に送受信することができます。

2.7.2 シンメトリックアクティブ/パッシブモードの NTP 認証の設定

アクティブピアとパッシブピアで設定されたキーID とキーの値は同一にする必要があります。そうでなければ NTP 認証は失敗します。ピアの装置がローカル装置でキーID を使用することができることを確認してください。

以下にアクティブピアの NTP 認証の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． NTP 認証を有効にする	**ntp-service authentication enable**	デフォルト：無効
3． NTP 認証キーを設定する	**ntp-service authentication-keyid** *keyid* **authentication-mode md5** { **cipher** | **simple** } *string* *	デフォルト：設定なし
4． 認証キーをトラステッドキーとして設定する	**ntp-service reliable authentication-keyid** *keyid*	デフォルト：設定なし

操作	コマンド	補足
5． パッシブピアとキーを関連づける	**ntp-service unicast-peer** { *ip-address* | *peer-name* } **authentication-keyid** *keyid*	―

以下にパッシブピアの NTP 認証の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． NTP 認証を有効にする	**ntp-service authentication enable**	デフォルト：無効
3． NTP 認証キーを設定する	**ntp-service authentication-keyid** *keyid* **authentication-mode md5** { **cipher** | **simple** } *string* *	デフォルト：設定なし
4． 認証キーをトラステッドキーとして設定する	**ntp-service reliable authentication-keyid** *keyid*	デフォルト：設定なし

アクティブピアとパッシブピアで異なる設定が実行されると、NTP 認証の結果は異なります。詳細を表 2-3に示します。（ーは相違がないことを示します。）

以下に NTP 認証の結果を示します。

表 2-3 NTP 認証の結果

アクティブピア			パッシブピア		認証結果
NTP 認証を有効にする	キーをトラステッドキーとして設定する	パッシブピアにキーを関連づける	NTP 認証を有効にする	キーをトラステッドキーとして設定する	
アクティブピアとパッシブピアのstratumレベルは考慮しません。					
Yes	Yes	Yes	Yes	Yes	認証は成功します。NTPメッセージは正常に送受信することができます。
Yes	Yes	Yes	Yes	No	認証は失敗します。NTPメッセージは正常に送受信することができません。
Yes	Yes	Yes	No	―	認証は失敗します。NTPメッセージは正常に送受信することができません。
Yes	―	No	Yes	―	認証は失敗します。NTPメッセージは正常に送受信することができません。
Yes	―	No	No	―	認証はありません。NTPメッセージは正常に送受信することができます。
No	―	―	Yes	―	認証は失敗します。NTPメッセージは正常に送受信することができません。

アクティブピア			パッシブピア		認証結果
NTP 認証を有効にする	キーをトラステッドキーとして設定する	パッシブピアにキーを関連づける	NTP 認証を有効にする	キーをトラステッドキーとして設定する	
No	ー	ー	No	ー	認証はありません。NTPメッセージは正常に送受信することができます。
アクティブピアはパッシブピアよりも高いstratumを持ちます。					
Yes	No	Yes	ー	ー	認証は失敗します。NTPメッセージは正常に送受信することができません。
パッシブピアはアクティブピアよりも高いstratumを持ちます。					
Yes	No	Yes	Yes	ー	認証は失敗します。NTPメッセージは正常に送受信することができません。
Yes	No	Yes	No	ー	認証はありません。NTPメッセージは正常に送受信することができます。

2.7.3 ブロードキャストモードの NTP 認証の設定

ブロードキャストクライアントとブロードキャストサーバで設定されたキーID とキーの値は同一にする必要があります。そうでなければ NTP 認証は失敗します。ピアの装置がローカル装置でキーID を使用することができることを確認してください。QX-S1100G シリーズはブロードキャストサーバ機能をサポートしていません。

以下にブロードキャストクライアントの NTP 認証の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． NTP 認証を有効にする	**ntp-service authentication enable**	デフォルト：無効
3． NTP 認証キーを設定する	**ntp-service authentication-keyid** *keyid* **authentication-mode md5** { **cipher** | **simple** } *string* *	デフォルト：設定なし
4． 認証キーをトラステッドキーとして設定する	**ntp-service reliable authentication-keyid** *keyid*	デフォルト：設定なし

ブロードキャストクライアントとブロードキャストサーバで異なる設定が実行されると、NTP 認証の結果は異なります。詳細を表 2-4に示します。（ーは相違がないことを示します。）

以下に NTP 認証の結果を示します。

表 2-4 NTP 認証の結果

ブロードキャストサーバ			ブロードキャストクライアント		認証の結果
NTP 認証を有効にする	キーをトラステッドキーとして設定する	ブロードキャストサーバとキーを関連づける	NTP 認証を有効にする	キーをトラステッドキーとして設定する	
Yes	Yes	Yes	Yes	Yes	認証は成功します。NTPメッセージは正常に送受信することができます。
Yes	Yes	Yes	Yes	No	認証は失敗します。NTPメッセージは正常に送受信することができません。
Yes	Yes	Yes	No	ー	認証は失敗します。NTPメッセージは正常に送受信することができません。
Yes	No	Yes	Yes	ー	認証は失敗します。NTPメッセージは正常に送受信することができません。
Yes	No	Yes	No	ー	認証はありません。NTPメッセージは正常に送受信することができます。
Yes	ー	No	Yes	ー	認証は失敗します。NTPメッセージは正常に送受信することができません。
Yes	ー	No	No	ー	認証はありません。NTPメッセージは正常に送受信することができます。
No	ー	ー	Yes	ー	認証は失敗します。NTPメッセージは正常に送受信することができません。
No	ー	ー	No	ー	認証はありません。NTPメッセージは正常に送受信することができます。

2.7.4 マルチキャストモードの NTP 認証の設定

マルチキャストクライアントとマルチキャストサーバで設定されたキーID とキーの値は同じにする必要があります。そうでなければ NTP 認証は失敗します。ピアの装置がローカル装置でキーID を使用することができることを確認してください。QX-S1100G シリーズはマルチキャストサーバ機能をサポートしていません。

以下にマルチキャストクライアントの NTP 認証の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． NTP 認証を有効にする	**ntp-service authentication enable**	デフォルト：無効
3． NTP 認証キーを設定する	**ntp-service authentication-keyid** *keyid* **authentication-mode md5** { **cipher** | **simple** } *string* *	デフォルト：設定なし
4． 認証キーをトラステッドキーとして設定する	**ntp-service reliable authentication-keyid** *keyid*	デフォルト：設定なし

マルチキャストクライアントとマルチキャストサーバで異なる設定が実行されると、NTP 認証の結果は異なります。詳細を表 2-5に示します。（ーは相違がないことを示します。）

以下に NTP 認証の結果を示します。

表 2-5 NTP 認証の結果

マルチキャストサーバ			マルチキャストクライアント		認証の結果
NTP 認証を有効にする	キーをトラステッドキーとして設定する	マルチキャストサーバにキーを関連づける	NTP 認証を有効にする	キーをトラステッドキーとして設定する	
Yes	Yes	Yes	Yes	Yes	認証は成功します。NTPメッセージは正常に送受信することができます。
Yes	Yes	Yes	Yes	No	認証は失敗します。NTPメッセージは正常に送受信することができません。
Yes	Yes	Yes	No	ー	認証は失敗します。NTPメッセージは正常に送受信することができません。
Yes	No	Yes	Yes	ー	認証は失敗します。NTPメッセージは正常に送受信することができません。
Yes	No	Yes	No	ー	認証はありません。NTPメッセージは正常に送受信することができます。
Yes	ー	No	Yes	ー	認証は失敗します。NTPメッセージは正常に送受信することができません。
Yes	ー	No	No	ー	認証はありません。NTPメッセージは正常に送受信することができます。
No	ー	ー	Yes	ー	認証は失敗します。NTPメッセージは正常に送受信することができません。

マルチキャストサーバ			マルチキャストクライアント		認証の結果
NTP 認証を有効にする	キーをトラステッドキーとして設定する	マルチキャストサーバにキーを関連づける	NTP 認証を有効にする	キーをトラステッドキーとして設定する	
No	―	―	No	―	認証はありません。NTPメッセージは正常に送受信することができます。

2.8 NTPオプションパラメータの設定

この章はオプション作業設定項目について記載します。NTP セキュリティ、性能、信頼性を改善するために設定します。

2.8.1 NTP メッセージの送信元アドレスの設定

NTP メッセージの送信元アドレスまたは送信元インタフェースを指定できます。NTP メッセージの送信元インタフェースを指定すると、装置は指定されたインタフェースの IP アドレスを送信元アドレスとして使用して、NTP メッセージを送信します。

インタフェースの状態の変更によって、NTP 通信の失敗を引き起こすことを防ぐため、常にアップ状態であるインタフェースの IP アドレスを使用するように設定します。たとえば常にアップ状態であるインタフェースはループバックインタフェースです。装置のインタフェースの状態の変更によって、NTP メッセージを受信できるようにするため、送信元インタフェースとしてループバックインタフェースを設定します。

装置が NTP リクエストに応答する場合、NTP 応答の送信元 IP アドレスは、NTP リクエストを受信したインタフェースの IP アドレスです。

以下に NTP メッセージの送信元インタフェースを指定する場合のガイドラインを示します。

- **ntp-service unicast-server** コマンドあるいは **ntp-service unicast-peer** コマンドで、NTP メッセージの送信元インタフェースを指定した場合、指定したインタフェースの IP アドレス NTP メッセージの送信元 IP アドレスとして使用されます。

以下に NTP メッセージの送信元インタフェースの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． NTP メッセージの送信元アドレスを指定する	**ntp-service source** { *interface-type interface-number* | *ip-address* }	デフォルト：設定なし

2.8.2 インタフェースでの NTP メッセージ受信の無効化

NTP が有効な場合、デフォルトですべてのインタフェースは NTP メッセージを受信することができます。セキュリティのため、インタフェースで NTP メッセージを受信しないようにすることができます。

以下に NTP メッセージの受信をインタフェースで無効にする設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． interface view に移行する	**interface** *interface-type interface-number*	―
3． インタフェースで NTP メッセージの受信を無効にする	**undo ntp-service inbound enable**	デフォルト：有効

2.8.3 ダイナミックアソシエーションの最大数の設定

NTP は以下のアソシエーションタイプがあります。

- **スタティックアソシエーション** ― 手動で作成したアソシエーションです。
- **ダイナミックアソシエーション** ― NTP を動作する間、システムによって作成された一時的なアソシエーションです。12 分以内にメッセージの交換が行われない場合、ダイナミックアソシエーションは削除されます。

以下に設定される異なるアソシエーションモードを示します。

- **クライアント/サーバモード** ― NTP サーバを指定した後、システムはクライアントでスタティックアソシエーションを作成します。サーバはアソシエーション（スタティックあるいはダイナミック）を作成するのではなく、単に受信したメッセージに対して、受動的に応答します。
- **シンメトリックアクティブ/パッシブモード** ― シンメトリックアクティブピアでシンメトリックパッシブピアを指定した後、シンメトリックアクティブピア上でスタティックアソシエーションが作成され、シンメトリックパッシブピアでダイナミックアソシエーションが作成されます。
- **ブロードキャスト/マルチキャストモード** ― サーバでスタティックアソシエーションが作成され、クライアントでダイナミックアソシエーションが作成されます。

1 つの装置で、スタティックアソシエーション、ダイナミックアソシエーションを含み、共通で最大 128 のアソシエーションを作成することができます。

ダイナミックアソシエーションが多くのシステムリソースを占有しないように、制限させるため、ダイナミックアソシエーションの最大数を制限します。

以下にダイナミックアソシエーションの最大数の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． ダイナミックアソシエーションの最大数を設定する	**ntp-service max-dynamic-sessions** *number*	デフォルト：100

2.8.4 NTP パケットの DSCP 値の設定

パケットの DSCP 値は、パケットの優先度レベルを指定し、パケットの優先度に影響します。

以下に NTP パケットの DSCP 値の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． NTP パケットの DSCP 値を設定する	**ntp-service dscp** *dscp-value*	デフォルト：48

2.9 NTPの表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
IPv4 NTPアソシエーションを表示する	**display ntp-service sessions** [**verbose**]
NTPサービスステータスの情報を表示する	**display ntp-service status**
ローカル装置からプライマリNTPサーバに戻ったNTPサーバの概要情報を表示する	**display ntp-service trace**

2.10 NTP設定例

2.10.1 NTP クライアント/サーバモードの設定例

I. ネットワーク要件

図 2-4に示すように設定します。

- Device A の stratum レベル 2 のローカルクロックを参照ソースとして設定します。
- Device B をクライアントモードで動作し、Device A を Device B の NTP サーバとして設定します。

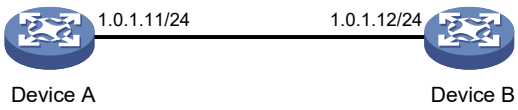


図 2-4 ネットワーク図

II. 設定手順

1) 図 2-4に示すように各インタフェースの IP アドレスを設定します。（詳細は省略します。）
2) Device B を設定します。

NTP サービスを有効にします。

```
<DeviceB> system-view
[DeviceB] ntp-service enable
```

Device B が Device A に同期されるように、Device B の NTP サーバとして Device A を指定します。

```
[DeviceB] ntp-service unicast-server 1.0.1.11
```

III. 設定の確認

Device B が時刻を Device A と同期させ、Device B の stratum レベルが 3 であることを確認します。

```
[DeviceB] display ntp-service status
 Clock status: synchronized
 Clock stratum: 3
 System peer: 1.0.1.11
 Local mode: client
 Reference clock ID: 1.0.1.11
 Leap indicator: 00
 Clock jitter: 0.000977 s
 Stability: 0.000 pps
 Clock precision: 2^-19
 Root delay: 0.00383 ms
 Root dispersion: 16.26572 ms
 Reference time: d0c6033f.b9923965  Wed, Dec 29 2010 18:58:07.724
System poll interval: 64 s
```

Device B と Device A 間で NTP アソシエーションが確立されていることを確認します。

```
[DeviceB] display ntp-service sessions
       source          reference       stra reach poll  now offset  delay disper
**************************************************************************
[12345]1.0.1.11        127.127.1.0        2     1   64   15   -4.0 0.0038 16.262
Notes: 1 source(master), 2 source(peer), 3 selected, 4 candidate, 5 configured.
 Total sessions: 1
```

2.10.2 NTP シンメトリックアクティブ/パッシブモードの設定例

I. ネットワーク要件

図 2-5に示すように、設定します。

- 参照ソースとして Device A のローカルクロックを stratum レベル 2 に設定します。
- シンメトリックアクティブモードで動作するように Device B を設定し、Device B のパッシブピアとして Device A を指定します。



図 2-5 ネットワーク図

II. 設定手順

1) 図 2-5に示すように各インタフェースの IP アドレスを設定します。（詳細は省略します。）
2) Device B を設定します。

NTP サービスを有効にします。

```
<DeviceB> system-view
[DeviceB] ntp-service enable
```

III. 設定の確認

Device B が時刻を Device A と同期させたことを確認します。

```
[DeviceB] display ntp-service status
 Clock status: synchronized
 Clock stratum: 3
 System peer: 3.0.1.31
 Local mode: sym_passive
 Reference clock ID: 3.0.1.31
 Leap indicator: 00
 Clock jitter: 0.000916 s
 Stability: 0.000 pps
 Clock precision: 2^-19
 Root delay: 0.00609 ms
 Root dispersion: 1.95859 ms
 Reference time: 83aec681.deb6d3e5  Wed, Jan  8 2014 14:33:11.081
 System poll interval: 64 s
```

Device B と Device A 間の IPv4 NTP アソシエーションが確立されていることを確認します。

```
[DeviceB] display ntp-service sessions
       source          reference       stra reach poll  now offset  delay disper
**************************************************************************
   [12]3.0.1.31       127.127.1.0        2    62   64   34 0.4251 6.0882 1392.1
Notes: 1 source(master), 2 source(peer), 3 selected, 4 candidate, 5 configured.
 Total sessions: 1
```

2.10.3 NTP ブロードキャストモードの設定例

I. ネットワーク要件

図 2-6に示すように、同一ネットワークセグメントで複数の装置用の NTP サーバとして Switch C が動作し、装置の時刻を同期させます。

- Switch C のローカルクロックは参照ソースとして使用され、stratum レベル 2 です。
- Switch C はブロードキャストサーバモードで動作し、VLAN インタフェース 2 からブロードキャストメッセージを送信します。
- Switch A と Switch B はブロードキャストクライアントモードで動作し、VLAN インタフェース 2 でブロードキャストメッセージを受信します。

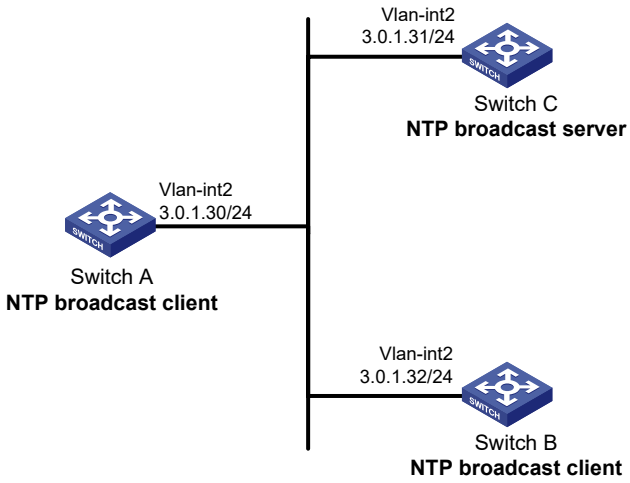


図 2-6 ネットワーク図

II. 設定手順

1) 図 2-6に示すように各インタフェースの IP アドレスを設定します。（詳細は省略します。）
2) Switch A を設定します。

NTP サービスを有効にします。

```
<SwitchA> system-view
[SwitchA] ntp-service enable
```

ブロードキャストクライアントモードで動作するように Switch A を設定し、VLAN インタフェース 2 からブロードキャストメッセージを受信します。

```
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ntp-service broadcast-client
```

3)　Switch B を設定します。

NTP サービスを有効にします。

```
<SwitchB> system-view
[SwitchB] ntp-service enable
```

ブロードキャストクライアントモードで動作するように Switch B を設定し、VLAN インタフェース 2 からブロードキャストメッセージを受信します。

```
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] ntp-service broadcast-client
```

III. 設定の確認

次の手順では、例として Switch A を使用して設定を確認します。

Switch A が Switch C と同期して、Switch A の stratum レベルが 3 で、Switch C の stratum レベルが 2 であることを確認します。

```
[SwitchA-Vlan-interface2] display ntp-service status
 Clock status: synchronized
 Clock stratum: 3
 System peer: 3.0.1.31
 Local mode: bclient
 Reference clock ID: 3.0.1.31
 Leap indicator: 00
 Clock jitter: 0.044281 s
 Stability: 0.000 pps
 Clock precision: 2^-19
 Root delay: 0.00229 ms
 Root dispersion: 4.12572 ms
 Reference time: d0d289fe.ec43c720  Sat, Jan  8 2011  7:00:14.922
 System poll interval: 64 s
```

Switch A と Switch C 間で NTP アソシエーションが確立されていることを確認します。

```
[SwitchA-Vlan-interface2] display ntp-service sessions
       source          reference       stra reach poll  now offset  delay disper
**************************************************************************
 [1245]3.0.1.31       127.127.1.0        2     1   64  519   -0.0 0.0022 4.1257
Notes: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured.
 Total sessions: 1
```

2.10.4 NTP マルチキャストモードの設定例

I. ネットワーク要件

図 2-7に示すように、異なるネットワークセグメントで複数の装置用の NTP サーバとして Switch C が動作し、装置の時刻を同期させます。

- Switch C のローカルクロックは参照ソースとして使用され、stratum レベル 2 です。

- Switch C はマルチキャストサーバモードで動作し、VLAN インタフェース 2 からマルチキャストメッセージを送信します。
- Switch A と Switch D はマルチキャストクライアントモードで動作し、それぞれ VLAN インタフェース 2 と VLAN インタフェース 3 を通してマルチキャストメッセージを受信します。

メモ：

- この例では、Switch B は IPv4 マルチキャストルーティングをサポートする必要があります。
- QX-S1100G シリーズはマルチキャストルーティングをサポートしていません。

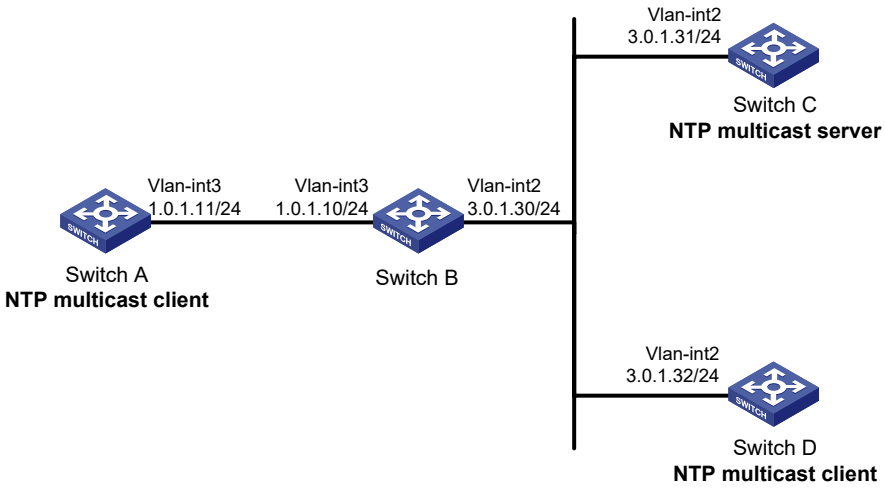


図 2-7 ネットワーク図

II. 設定手順

1)　図 2-7に示すように各インタフェースの IP アドレスを設定します。

QX-S1100G シリーズは、NTP サーバ、マルチキャストルーティングをサポートしていないため SwitchB と SwitchC の設定は省略します。

2)　Switch D を設定します。

NTP サービスを有効にします。

```
<SwitchD> system-view
[SwitchD] ntp-service enable
```

マルチキャストクライアントモードで動作するように Switch D を設定し、VLAN インタフェース 2 からマルチキャストメッセージを送信します。

```
[SwitchD] interface vlan-interface 2
[SwitchD-Vlan-interface2] ntp-service multicast-client
```

3)　設定を確認します。

Switch D が Switch C に同期化され、Switch D の stratum レベルが 3 で、Switch C の stratum レベルが 2 であることを確認します。

Switch D と Switch C は同じサブネット上にあるため、Switch D はマルチキャスト機能を有効にせずに Switch C からマルチキャストメッセージを受信できます。

```
[SwitchD-Vlan-interface2] display ntp-service status
 Clock status: synchronized
 Clock stratum: 3
 System peer: 3.0.1.31
 Local mode: bclient
 Reference clock ID: 3.0.1.31
 Leap indicator: 00
 Clock jitter: 0.044281 s
 Stability: 0.000 pps
 Clock precision: 2^-19
 Root delay: 0.00229 ms
 Root dispersion: 4.12572 ms
 Reference time: d0d289fe.ec43c720  Sat, Jan  8 2011  7:00:14.922
 System poll interval: 64 s
```

Switch D と Switch C 間で NTP アソシエーションが確立されていることを確認します。

```
[SwitchD-Vlan-interface2] display ntp-service sessions
       source          reference       stra reach poll  now offset  delay disper
**************************************************************************
 [1245]3.0.1.31       127.127.1.0       2     1   64  519   -0.0 0.0022 4.1257
Notes: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured.
 Total sessions: 1
```

4)　Switch A を設定します。

NTP サービスを有効にします。

```
<SwitchA> system-view
[SwitchA] ntp-service enable
```

マルチキャストクライアントモードで動作するように Switch A を設定し、VLAN インタフェース 3 からマルチキャストメッセージを受信します。

```
[SwitchA] interface vlan-interface 3
[SwitchA-Vlan-interface3] ntp-service multicast-client
```

III. 設定の確認

Switch A が時刻を Switch C と同期し、Switch A の stratum レベルが 3 であることを確認します。

```
[SwitchA-Vlan-interface3] display ntp-service status
 Clock status: synchronized
 Clock stratum: 3
 System peer: 3.0.1.31
 Local mode: bclient
 Reference clock ID: 3.0.1.31
 Leap indicator: 00
 Clock jitter: 0.165741 s
 Stability: 0.000 pps
 Clock precision: 2^-19
 Root delay: 0.00534 ms
 Root dispersion: 4.51282 ms
 Reference time: d0c61289.10b1193f  Wed, Dec 29 2010 20:03:21.065
 System poll interval: 64 s
```

Switch A と Switch C 間で NTP アソシエーションが確立されていることを確認します。

```
[SwitchA-Vlan-interface3] display ntp-service sessions
      source          reference       stra reach poll  now offset  delay disper
**************************************************************************
 [1234]3.0.1.31       127.127.1.0        2   247   64  381   -0.0 0.0053 4.5128
Notes: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured.
 Total sessions: 1
```

2.10.5 NTP 認証を使用したクライアント/サーバモードの設定例

I. ネットワーク要件

- 図 2-8に示すように、Device A の stratum レベル 2 のローカルクロックは参照ソースとして使われます。
- Device B はクライアントモードで動作し、Device A は Device B の NTP サーバとして使用されます。
- Device A と Device B の両方で NTP 認証を設定します。

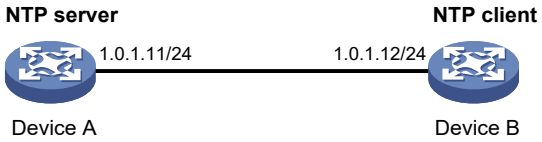


図 2-8 ネットワーク図

II. 設定手順

1) 図 2-8に示すように各インタフェースの IP アドレスを設定します。（詳細は省略します。）
2) Device B を設定します。

NTP サービスを有効にします。

```
<DeviceB> system-view
[DeviceB] ntp-service enable
```

Device B で NTP 認証を有効にします。

```
[DeviceB] ntp-service authentication enable
```

キーID 42 とキー値 **aNiceKey** でプレーンテキスト認証キーを作成します。

```
[DeviceB] ntp-service authentication-keyid 42 authentication-mode md5 simple aNiceKey
```

キーをトラステッドキーとして指定します。

```
[DeviceB] ntp-service reliable authentication-keyid 42
```

Device B の NTP サーバとして Device A を指定し、キーID を 42 としてサーバと関連づけます。

```
[DeviceB] ntp-service unicast-server 1.0.1.11 authentication-keyid 42
```

Device B が Device A のクロックの同期を行う前に、Device A の NTP 認証を有効にします。

III. 設定の確認

Device B が時刻を Device A と同期させ、Device B の stratum レベルが 3 であることを確認します。

```
[DeviceB] display ntp-service status
 Clock status: synchronized
 Clock stratum: 3
 System peer: 1.0.1.11
 Local mode: client
 Reference clock ID: 1.0.1.11
 Leap indicator: 00
 Clock jitter: 0.005096 s
 Stability: 0.000 pps
 Clock precision: 2^-19
 Root delay: 0.00655 ms
 Root dispersion: 1.15869 ms
 Reference time: d0c62687.ab1bba7d  Wed, Dec 29 2010 21:28:39.668
 System poll interval: 64 s
```

Device B と Device A 間で NTP アソシエーションが確立されていることを確認します。

```
[DeviceB] display ntp-service sessions
       source          reference       stra reach poll  now offset  delay disper
**************************************************************************
 [1245]1.0.1.11        127.127.1.0        2     1   64  519   -0.0 0.0065    0.0
Notes: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured.
 Total sessions: 1
```

2.10.6 NTP 認証を使用したブロードキャストモードの設定例

I. ネットワーク要件

図 2-9に示すように、同一ネットワークセグメントで複数の装置用の NTP サーバとして Switch C が動作し、装置の時刻を同期させます。NTP サーバを認証するように Switch A と Switch B を設定します。

- Switch C のローカルクロックは参照ソースとして使用され、stratum レベル 3 です。
- Switch C はブロードキャストサーバモードで動作し、VLAN インタフェース 2 からブロードキャストメッセージを送信します。
- Switch A と Switch B はブロードキャストクライアントモードで動作し、VLAN インタフェース 2 を通してブロードキャストメッセージを受信します。
- Switch A、Switch B、Switch C で NTP 認証を設定します。

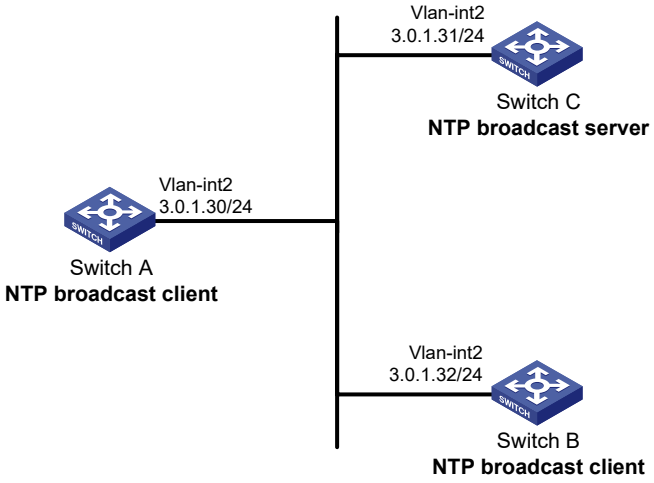


図 2-9 ネットワーク図

II. 設定手順

1) 図 2-9に示すように各インタフェースの IP アドレスを設定します。（詳細は省略します。）
2) Switch A を設定します。

NTP サービスを有効にします。

```
<SwitchA> system-view
[SwitchA] ntp-service enable
```

Switch A で NTP 認証を有効にします。認証キーID を 88 とし、キーの値を 123456 として、NTP 認証キーを設定します。プレーンテキストで入力し、キーをトラステッドキーとして指定します。

```
[SwitchA] ntp-service authentication enable
[SwitchA] ntp-service authentication-keyid 88 authentication-mode md5 simple 123456
[SwitchA] ntp-service reliable authentication-keyid 88
```

NTP ブロードキャストクライアントモードで動作するように Switch A を設定し、VLAN インタフェース 2 からブロードキャストメッセージを受信します。

```
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ntp-service broadcast-client
```

3) Switch B を設定します。

NTP サービスを有効にします。

```
<SwitchB> system-view
[SwitchB] ntp-service enable
```

Switch B で NTP 認証を有効にします。認証キーID を 88 とし、キーの値を 123456 として、NTP 認証キーを設定します。プレーンテキストで入力し、キーをトラステッドキーとして指定します。

```
[SwitchB] ntp-service authentication enable
[SwitchB] ntp-service authentication-keyid 88 authentication-mode md5 simple 123456
[SwitchB] ntp-service reliable authentication-keyid 88
```

NTP ブロードキャストクライアントモードで動作するように Switch B を設定し、VLAN インタフェース 2 からブロードキャストメッセージを受信します。

```
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] ntp-service broadcast-client
```

III. 設定の確認

Device B が時刻を Switch C と同期し、Device B の stratum レベルが 4 であることを確認します。

```
[SwitchB-Vlan-interface2] display ntp-service status
 Clock status: synchronized
 Clock stratum: 4
 System peer: 3.0.1.31
 Local mode: bclient
 Reference clock ID: 3.0.1.31
 Leap indicator: 00
 Clock jitter: 0.006683 s
 Stability: 0.000 pps
 Clock precision: 2^-19
 Root delay: 0.00127 ms
 Root dispersion: 2.89877 ms
 Reference time: d0d287a7.3119666f  Sat, Jan  8 2011  6:50:15.191
 System poll interval: 64 s
```

Switch B と Switch C 間で NTP アソシエーションが確立されていることを確認します。

```
[SwitchB-Vlan-interface2] display ntp-service sessions
       source          reference       stra reach poll  now offset  delay disper
**************************************************************************
 [1245]3.0.1.31        127.127.1.0        3     3   64   68   -0.0 0.0000    0.0
Notes: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured.
 Total sessions: 1
```

目次

このセクションのページは **9-x-x** です。

3 章 Information Center 3-1
3.1 概要 3-1
3.1.1 ログタイプ 3-1
3.1.2 ログレベル 3-1
3.1.3 ログの出力先 3-2
3.1.4 デフォルト出力ルール 3-2
3.1.5 Diagnostic ログのデフォルト出力ルール 3-2
3.1.6 hidden ログのデフォルト出力ルール 3-3
3.1.7 ログフォーマット 3-3
3.2 Information Center 設定作業リスト 3-5
3.3 コンソールへのログの出力 3-6
3.4 モニタ端末へのログの出力 3-6
3.5 ログホストへのログの出力 3-7
3.6 ログバッファへのログの出力 3-7
3.7 ログの最小記録期間の設定 3-8
3.8 情報の同期出力の設定 3-8
3.9 インタフェースでのリンクアップ/ダウンのログ情報生成の無効化 3-9
3.10 ログメッセージの SNMP notification の送信の有効化 3-9
3.11 Information Center の表示と維持 3-10
3.12 設定例 3-10
3.12.1 コンソールへのログ出力の設定例 3-10
3.12.2 UNIX ログホストへのログ出力の設定例 3-11
3.12.3 Linux ログホストへのログ出力の設定例 3-12

3章 Information Center

3.1 概要

Information Center は、送信元モジュールによって作成されたログを受信し、ユーザが定義した出力ルールに従って、異なる宛先にログを出力します。送信元モジュールにもとづいて、分類、フィルタリング、出力することができます。サポートされる送信元を表示するには、**info-center source ?**コマンドを使用します。

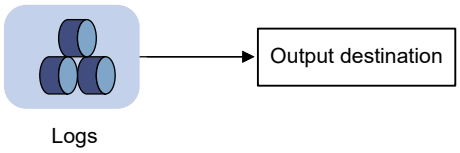


図 3-1 Information center の図

デフォルトで Information Center は有効です。Information Center が有効な場合、情報の分類や出力のため、システム性能にある程度影響を与えます。システムリソースが不十分である場合、リソースの消費を防ぐため Information Center を無効にしてください。

3.1.1 ログタイプ

ログは以下のタイプに分類されます。

- **Common ログ** － 共通なシステム情報の記録です。本章では、特に指定がない場合、ログは Common ログを示します。
- **Diagnostic ログ** － デバッグメッセージ記録です。
- **Hidden ログ** － 入力コマンドのような端末で表示されないログ情報です。

3.1.2 ログレベル

ログは重要度により 0～7 の 8 つのレベルに分類されます。装置は指定されたレベル以上の重要度レベルを出力します。たとえば出力ルールを 6（informational）と設定した場合、0～6 までの重要度のログが出力されます。

表 3-1 ログレベル

重要度	レベル	説明
0	Emergency	システムが使用できません。たとえば、システムの許可が終了しました。
1	Alert	即急に対応が必要です。たとえば、インタフェースのトラフィックが上限を超えました。
2	Critical	深刻な状態です。たとえば、装置の温度が上限を超えました、電源モジュールが故障しました、FANトレイが故障しました。
3	Error	エラー状態です。たとえば、リンク状態が変更しました。

重要度	レベル	説明
4	Warning	警告状態です。たとえば、インタフェースが切断されました、あるいはメモリリソースが上限まで使われました。
5	Notification	通常通りですが、注意状態です。たとえば、装置にログインしました、あるいは装置が再起動しました。
6	Informational	情報メッセージです。たとえば、コマンドあるいはpingが実行されました。
7	Debug	デバッグメッセージです。

3.1.3 ログの出力先

システムは、コンソール、モニタ端末、ログバッファ、ログホスト、ログファイルの宛先にログを出力します。ログの出力先は独立しており、Information Center を有効にした後、設定することができます。1 つのログを複数の宛先に送る事が可能です。

3.1.4 デフォルト出力ルール

デフォルト出力ルールはログの送信元モジュールと出力先の重要度レベルを定義しています。出力ルールにマッチしたログが、出力先に出力されます。表 3-2にデフォルト出力ルールを示します。

表 3-2 デフォルト出力ルール

出力先	ログ送信元モジュール	出力装置	重要度
コンソール	サポートされるすべてのモジュール	有効	Debugging
モニタ端末	サポートされるすべてのモジュール	無効	Debugging
ログホスト	サポートされるすべてのモジュール	有効	Informational
ログバッファ	サポートされるすべてのモジュール	有効	Informational
ログファイル	サポートされるすべてのモジュール	有効	Informational

3.1.5 Diagnostic ログのデフォルト出力ルール

Diagnostic ログは Diagnostic ログファイルにのみ出力することができます。送信元モジュールと重要度でフィルタすることはできません。表 3-3に Diagnostic ログのデフォルト出力ルールを示します。

表 3-3 Diagnostic ログのデフォルト出力ルール

出力先	ログ送信元モジュール	出力装置	重要度
Diagnosticログファイル	サポートされるすべてのモジュール	有効	Debugging

3.1.6 hidden ログのデフォルト出力ルール

Hidden ログはログホスト、ログバッファ、ログファイルに出力することができます。表 3-4 に hidden ログのデフォルト出力ルールを示します。

表 3-4 hidden ログのデフォルト出力ルール

出力先	ログ送信元モジュール	出力装置	重要度
ログホスト	サポートされるすべてのモジュール	有効	Informational
ログバッファ	サポートされるすべてのモジュール	有効	Informational
ログファイル	サポートされるすべてのモジュール	有効	Informational

3.1.7 ログフォーマット

ログのフォーマットは出力先で異なります。表 3-5にログ情報の標準のログフォーマットを示します。このフォーマットは使用するツールによって異なります。

表 3-5 ログフォーマット

出力先	フォーマット	例
コンソール、モニタ端末、ログバッファ、ログファイル	Prefix Timestamp Sysname Module/Level/Mnemonic: Content	%Nov 24 14:21:43:502 2010 Sysname SHELL/5/SHELL_LOGIN: VTY logged in from 192.168.1.26
ログホスト	<PRI>Timestamp Sysname %%vvModule/Level/Mnemonic: Source; Content	<190>Nov 24 16:22:21 2010 Sysname %%10 SHELL/5/SHELL_LOGIN: -DevIP=1.1.1.1; VTY logged in from 192.168.1.26

表 3-6にログメッセージのフィールドの説明を示します。

表 3-6 ログフィールドの説明

フィールド	説明
Prefix (information type)	ログホスト以外の宛先へのログはタイムスタンプの前識別子があります。 ● パーセントの識別子（%）はinformational以上のレベルのログを示しています。 ● アスタリスク（*）の識別子はデバッグログを示します。 ● アスタリスク（^）の識別子はdiagnosticログを示します。

フィールド	説明
PRI (priority)	ログホストへのログはタイムスタンプの前にプライオリティの識別子があります。プライオリティは、facility*8+levelという式で計算されます。 ● **facility**はロギングファシリティ名です。16～23の値に対応したファシリティ名はlocal0～local7です。**info-center loghost**コマンドで設定されます。ログホストでログのソースを識別するのに使われます。対応するログソースのログをクエリやフィルタするのに使用します。 ● **level**は重要度（Severity）の範囲で0～7です。表 3-1に詳細を示します。
Timestamp	ログが作成された場合の時間を記録します。 ログホストとほかの宛先に送信したログは、異なる精度のタイムスタンプを持ちます。タイムスタンプのフォーマットは異なるコマンドで設定されます。詳細を表 3-7と表 3-8に示します。
Sysname （ホスト名あるいはホストのIPアドレス）	Sysnameはログが作成された装置のホスト名あるいはIPアドレスです。装置の名前を修正する場合は**sysname**コマンドを使用します。
%% (vendor ID)	このフィールドは、ベンダを識別するために使用します。出力先がログホストである場合のみ表示されます。
vv (version information)	このフィールドは、ログのバージョン識別子で、値は10です。出力先がログホストである場合のみ表示されます。
Module	このフィールドは、システム情報を作成するモジュールの名前を示します。system viewで**info-center source ?** コマンドを入力すると、モジュールの一覧を参照できます。
Level	ログのレベルを識別します。表 3-1に重要度のレベルの詳細を示します。
Mnemonic	ログの概要が記載されます。最大32文字の文字列です。
Source	ログ送信者を識別します。このフィールドは、unicomまたは標準形式でログホストに送信されるログにのみ存在します。このフィールドには次の情報が含まれています。 ● **DevIp** – ログ送信者のIPアドレス
Content	ログの内容が記載されます。

表 3-7 タイムスタンプの精度と設定コマンド

アイテム	ログホスト	コンソール、モニタ端末、ログバッファ、ログファイル
精度	秒（デフォルト）またはミリ秒	ミリ秒
設定コマンド	**info-center timestamp loghost**	**info-center timestamp**

表 3-8 タイムスタンプパラメータの内容

パラメータ	内容	例
boot	時間はシステムが開始してからのミリ秒で記載された経過時間です。フォーマットはxxx.yyyです。xxxは上位32ビットでyyyは下位32ビットです。 ログホストを除いたすべての宛先に送信される出力先のログでサポートされます。	%0.109391473 Sysname FTPD/5/FTPD_LOGIN: User ftp (192.168.1.23) has logged in successfully. 0.109391473は**boot**フォーマットのタイムスタンプです。

パラメータ	内容	例
date	現在の日付と時刻です。 ● ログホストに出力されるログの場合、タイムスタンプはMMM DD hh：mm：ss YYYY（秒に正確）またはMMM DD hh : mm : ss.ms YYYY（ミリ秒に正確）のフォーマットにすることができます。 ● 他の宛先に出力されるログの場合、タイムスタンプはMMM DD hh : mm : ss : ms YYYY のフォーマットです。 すべてのログでサポートされます。	%May 30 05:36:29:579 2003 Sysname FTPD/5/FTPD_LOGIN: User ftp (192.168.1.23) has logged in successfully. May 30 05:36:29:579 2018は、コンソールに送信されるログの**date**フォーマットのタイムスタンプです。
iso	ISO 8601で規定されたタイムスタンプで、秒単位（デフォルト）またはミリ秒単位まで正確です。 ログホストへ送付するログのみサポートします。	<189>2003-05-30T06:42:44 Sysname %%10FTPD/5/FTPD_LOGIN: User ftp (192.168.1.23) has logged in successfully. 2018-05-30T06:42:44は、秒に正確な**iso**フォーマットのタイムスタンプです。ミリ秒まで正確なタイムスタンプは、2018-05-30T06:42:44.708のようなものです。
none	タイムスタンプが含まれていません。 すべてのログでサポートされます。	% Sysname FTPD/5/FTPD_LOGIN: User ftp (192.168.1.23) has logged in successfully. タイムスタンプが含まれません
no-year-date	年またはミリ秒を除いた現在の日付と時間です。MMMDD hh：mm：ssのフォーマットです。 ログホストに送信されるログのみでサポートされます。	<189>May 30 06:44:22 Sysname %%10FTPD/5/FTPD_LOGIN(l): User ftp (192.168.1.23) has logged in successfully. May 30 06:44:22は**no-year-date**フォーマットのタイムスタンプです。

3.2 Information Center設定作業リスト

作業リスト
以下の少なくとも1つの作業を実行します。 ● コンソールへのログの出力 ● モニタ端末へのログの出力 ● ログホストへのログの出力 ● ログバッファへのログの出力
（オプション設定項目） 情報の同期出力の設定
（オプション設定項目） インタフェースでのリンクアップ/ダウンのログ情報生成の無効化
（オプション設定項目） ログの最小記録期間の設定

3.3 コンソールへのログの出力

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. Information Center を有効にする	**info-center enable**	デフォルト：有効
3. （オプション設定項目）コンソールへのログの出力ルールを設定する	**info-center source** { *module-name* | **default** } { **console** | **logbuffer** | **logfile** | **loghost** | **monitor** } { **deny** | **level** *severity* }	デフォルト出力ルールについての詳細は、オペレーションマニュアルのセクション9 *システム管理” Information Center”の”概要”の”デフォルト出力ルール”*を参照してください。
4. （オプション設定項目）タイムスタンプのフォーマットを設定する	**info-center timestamp** { **boot** | **date** | **none** }	デフォルト：**date**
5. user view に戻る	**quit**	ー
6. （オプション設定項目）コンソールへのログの出力を有効にする	**terminal monitor**	デフォルト：コンソールでは有効、モニタ端末では無効です。
7. 現在の端末でデバッグ情報の表示を有効にする	**terminal debugging**	デフォルト：無効
8. （オプション設定項目）コンソールに出力されるログの重要度を設定する	**terminal logging level** *severity*	デフォルト：6（informational）

3.4 モニタ端末へのログの出力

AUX、VTY、VTY line を通して装置にログインしているモニタ端末です。

以下にモニタ端末へのログ出力の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. Information Center を有効にする	**info-center enable**	デフォルト：有効
3. （オプション設定項目）モニタ端末へのログの出力ルールを設定する	**info-center source** { *module-name* | **default** } { **console** | **logbuffer** | **logfile** | **loghost** | **monitor** } { **deny** | **level** *severity* }	デフォルト出力ルールについての詳細は、オペレーションマニュアルのセクション9 *システム管理” Information Center”の”概要”の”デフォルト出力ルール”*を参照してください。
4. （オプション設定項目）タイムスタンプのフォーマットを設定する	**info-center timestamp** { **boot** | **date** | **none** }	デフォルト：**date**
5. user view に戻る	**quit**	ー

操作	コマンド	補足
6． モニタ端末へのログの出力を有効にする	**terminal monitor**	デフォルト：コンソールでは有効、モニタ端末では無効です。
7． 現在の端末でデバッグ情報の表示を有効にする	**terminal debugging**	デフォルト：無効
8． （オプション設定項目）モニタ端末に出力されるログの重要度を設定する	**terminal logging level** *severity*	デフォルト：6（informational）

3.5 ログホストへのログの出力

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． Information Center を有効にする	**info-center enable**	デフォルト：有効
3． ログホストへのログの出力ルールを設定する	**info-center source** { *module-name* | **default** } { **console** | **logbuffer** | **logfile** | **loghost** | **monitor** } { **deny** | **level** *severity* }	デフォルト出力ルールについての詳細は、オペレーションマニュアルのセクション9 *システム管理” Information Center”の”概要”の” デフォルト出力ルール”*を参照してください。
4． （オプション設定項目）出力ログの送信元 IP アドレスを指定する	**info-center loghost source** *interface-type interface-number*	デフォルト：ルータの出力インタフェースにマッチするプライマリIPアドレスです。
5． （オプション設定項目）タイムスタンプのフォーマットを設定する	**info-center timestamp loghost** { **date** [**with-milliseconds**] | **iso** [**with-milliseconds**] * | **no-year-date** | **none** }	デフォルト：**date**
6． ログホストを指定し、関連するパラメータを設定する	**info-center loghost** { *hostname* | *ipv4-address* | **ipv6** *ipv6-address* } [**port** *port-number*] [**facility** *local-number*] [**filter** *filter-name*]	デフォルト：設定なし *port-number*引数はログホストで設定された値と同じにする必要があります。異なる場合ログを受信できません。装置は最大20のログホストをサポートします。

3.6 ログバッファへのログの出力

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． Information Center を有効にする	**info-center enable**	デフォルト：有効
3． ログバッファへの出力を有効にする	**info-center logbuffer**	デフォルト：有効

操作	コマンド	補足
4.　（オプション設定項目）最大ログバッファサイズを設定する	**info-center logbuffer size** *buffersize*	デフォルト：512
5.　（オプション設定項目）ログバッファの出力ルールを設定する	**info-center source** { *module-name* | **default** } { **console** | **logbuffer** | **logfile** | **loghost** | **monitor** } { **deny** | **level** *severity* }	デフォルト出力ルールについての詳細は、オペレーションマニュアルのセクション9 *システム管理”Information Center”の”概要”の”デフォルト出力ルール”*を参照してください。
6.　（オプション設定項目）タイムスタンプのフォーマットを設定する	**info-center timestamp** { **boot** | **date** | **none** }	デフォルト：**date**

3.7 ログの最小記録期間の設定

ログバッファにあるログの記録期間の最小値を設定することができます。この機能はログが指定した時間内に新しいログによって上書きしてしまうことを防ぎます。

ログバッファあるいはログファイルが一杯になった場合、新しいログはデフォルトでもっとも古いログに新しいログを上書きします。最小記録期間を設定した後、システムはログを削除するかどうか決定するため、ログの最小記録期間を確認します。システムクロックからログが作成された時間を引いた時間はログの記録期間となります。

- ログの記録期間が最小記録期間以下である場合、システムはログを削除しません。新しいログは保存されません。
- ログの記録期間が最小記録期間より長い場合、システムは新しいログを保存するため、ログを削除します。

以下にログの最小記録期間の設定を示します。

操作	コマンド	補足
1.　system view に移行する	**system-view**	―
2.　ログの最小記録期間を設定する	**info-center syslog min-age** *min-age*	デフォルト：設定なし

3.8 情報の同期出力の設定

システムログの出力が行われると、設定の操作が中断されてしまいます。ログが出力される前に、以前に入力されたコマンドを見つける必要があります。

情報の同期出力とは、システムログの出力によりユーザの入力が中断された場合、中断されたところから操作を継続できるようにするため、ログの出力後、以前に入力されたコマンドおよび、コマンドプロンプト（編集モードのコマンドプロンプト、あるいは対話モードの[Y/N]の文字列）を表示させることができます。

以下に情報の同期出力の設定を示します。

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

操作	コマンド	補足
2． 情報の同期出力を設定する	**info-center synchronous**	デフォルト：無効

3.9 インタフェースでのリンクアップ/ダウンのログ情報生成の無効化

デフォルトでは、インタフェースのリンク状態が変わる場合に、装置のすべてのインタフェースはリンクアップ/ダウンのログ情報を生成します。そのため、以下のような場合、指定したインタフェースの情報生成を無効にすることができます。

インタフェースの情報を監視するため、通常はデフォルトの有効にすることを推奨します。

- あるインタフェースの状態にのみ関係している場合です。この場合、ほかのインタフェースのリンクアップ/ダウンのログ情報を生成できないようにします。
- インタフェースのリンク状態が安定せず、不必要なログ情報が連続して生成される場合です。この場合、ほかのインタフェースのリンクアップ/ダウンのログ情報を生成できないようにします。

以下にインタフェースのリンクアップ/ダウンのログ情報の生成を無効の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． interface view に移行する	**interface** *interface-type interface-number*	―
3． インタフェースのリンクアップ/ダウンのログ情報の生成を無効にする	**undo enable log updown**	デフォルト : すべてのインタフェースは、インタフェースの状態が変化した場合、リンクアップ/ダウンのログ情報を生成します。

3.10 ログメッセージのSNMP notificationの送信の有効化

snmp-agent trap enable syslog コマンドを有効にすると、装置はシスログメッセージによる SNMP notification の送信を有効にします。

装置は SNMP notification をカプセル化し、SNMP モジュールとログバッファに送信します。

SNMP モジュールが受信した SNMP notification を正常に送信するため、装置で SNMP の設定を行ってください。SNMP の設定については、オペレーションマニュアルのセクション *9 システム管理*“*SNMP*”を参照してください。

以下にシスログメッセージによる SNMP notification の送信を有効化の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． ログメッセージの SNMP notification の送信を有効にする	**snmp-agent trap enable syslog**	デフォルト：無効

3.11 Information Centerの表示と維持

すべての view で **display** コマンドを実行でき、user view で **reset** コマンドを実行できます。

操作	コマンド
Information Centerの設定を表示する	**display info-center**
ログバッファの状態とログ情報を表示する	**display logbuffer** [**reverse**] [**level** *severity* | **size** *buffersize* | **slot** *slot-number*] *
ログバッファの概要を表示する	**display logbuffer summary** [**level** *severity* | **slot** *slot-number*] *
ログファイルの設定を表示する	**display logfile summary**
ログバッファを削除する	**reset logbuffer**

3.12 設定例

3.12.1 コンソールへのログ出力の設定例

I. ネットワーク要件

Device は warning 以上の重要度のレベルの FTP ログをコンソールに出力するように設定します。

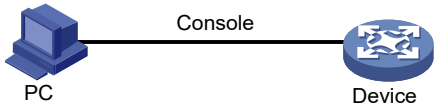


図 3-2 ネットワーク図

II. 設定手順

Information Center を有効にします。

```
<Device> system-view
[Device] info-center enable
```

コンソールへのログ出力を無効にします。

```
[Device] info-center source default console deny
```

それぞれのチャネルのデフォルトのシステム設定が異なるため、特定のチャネル（この例では **console**）では、必要に応じて、すべてのモジュールのログ情報の出力を無効にし、不要な情報が出力されないように出力ルールを設定します。

warning レベル以上の重要度の FTP ログをコンソールに出力するように設定します。

```
[Device] info-center source ftp console level warning
[Device] quit
```

コンソールでログの表示を有効にします。（この機能はデフォルトで有効です。）

```
<Device> terminal logging level 6
<Device> terminal monitor
The current terminal is enabled to display logs.
```

設定を行った後、FTP モジュールがログを生成した場合、Information Center は自動的にコンソールにログを送信し、ログを表示します。

3.12.2 UNIX ログホストへのログ出力の設定例

I. ネットワーク要件

Device が informational 以上の重要度のレベルの FTP ログを UNIX ログホストに出力するように設定します。



図 3-3 ネットワーク図

II. 設定手順

Device とログホストが互いに通信可能であることを確認してください。（詳細は省略します。）

1)　Device を設定します。

Information Center を有効にします。

```
<Device> system-view
[Device] info-center enable
```

ログホスト 1.2.0.1/16 を指定し、ロギングファシリティを **local4** に指定します。

```
[Device] info-center loghost 1.2.0.1 facility local4
```

ログホストにログの出力を無効にします。

```
[Device] info-center source default loghost deny
```

不要な情報が出力されないようにするため、出力ルールを設定する前に、ログを出力するすべてのモジュールが、指定した宛先（この例では **loghost**）に出力しないようにします。

informational レベル以上の重要度の FTP ログをロゴホストに出力するように設定します。

```
[Device] info-center source ftp loghost level informational
```

2)　ログホストを設定します。

ログホストの設定手順は、UNIX システムのベンダによって異なります。以下に例を示します。

a)　rootユーザとしてログホストにログインします。

b)　ディレクトリ/**var**/**log**/にサブディレクトリ**Device**を作成し、ディレクトリ**Device**にファイル**info.log**を作成し、**Device**からログを保存します。

```
# mkdir /var/log/Device
# touch /var/log/Device/info.log
```

c)　ディレクトリ/**etc**/のファイル**syslog.conf**を編集し、以下の内容を追加します。

```
# Device configuration messages
local4.info /var/log/Device/info.log
```

この設定で、ホストがログを受信するために使用する **local4** はロギングファシリティの名前です。**info** は重要度のレベルです。UNIX システムは、**informational** の重要度のログ情報をファイル/**var**/**log**/**Device**/**info.log** に記録します。

🕮 **メモ：**

ファイル/**etc**/**syslog.conf** を編集する場合のガイドラインを以下に示します。

- コメントは個別の行に記入し、# 記号で始めてください。
- ファイル名に不要なスペース等をいれないでください。
- ロギングファシリティ名とファイル/**etc**/**syslog.conf** が指定するログ情報の重要度は、**info-center loghost** コマンドと **info-center source** コマンドで Device に設定したものと一致しなければなりません。一致しないと、ログ情報は正しくログホストに出力されないことがあります。

---

d)　**syslogd**のプロセスIDを表示します。**syslogd**プロセスを削除し、**syslogd**の使用を再開するコマンド（**-r**オプション変更された構成を実施させる）を実行してください。

```
# ps -ae | grep syslogd
147
# kill -HUP 147
# syslogd -r &
```

上記設定後は、Device は関連するファイルに FTP ログ情報を保存できるようになります。

3.12.3 Linux ログホストへのログ出力の設定例

I. ネットワーク要件

Device が informational の重要度のレベルの FTP ログを Linux ログホスト 1.2.0.1/16 に出力するように設定します。



図 3-4 ネットワーク図

II. 設定手順

Device とログホストが互いに通信可能であることを確認してください。（詳細は省略します。）

1)　Device を設定します。

Information Center を有効にします。

```
<Device> system-view
[Device] info-center enable
```

ログホスト 1.2.0.1/16 を指定し、ロギングファシリティを **local5** に指定します。

```
[Device] info-center loghost 1.2.0.1 facility local5
```

ログホストにログの出力を無効にします。

```
[Device] info-center source default loghost deny
```

不要な情報が出力されないようにするため、出力ルールを設定する前に、ログを出力するすべてのモジュールが、指定した宛先（この例では **loghost**）に出力しないようにします。

informational レベル以上の重要度の FTP ログをロゴホストに出力するように設定します。

```
[Device] info-center source ftp loghost level informational
```

2)　ログホストを設定します。

ログホストの設定手順は、Linux システムのベンダによって異なります。以下に例を示します。

a)　rootユーザとしてログホストにログインします。

b)　ディレクトリ/**var**/**log**/にサブディレクトリ**Device**を作成します。ディレクトリ**Device**にファイル**info.log**を作成し、**Device**からログを保存します。

```
# mkdir /var/log/Device
# touch /var/log/Device/info.log
```

c)　ディレクトリ/**etc**/のファイル**syslog.conf**を編集し、以下の内容を追加します。

Device configuration messages

```
local5.info /var/log/Device/info.log
```

この設定で、ホストがログを受信するために使用する **local5** はロギングファシリティの名前です。**info** は重要度のレベルです。Linux システムは、**informational** の重要度のログ情報をファイル/**var**/**log**/**Device**/**info.log** に記録します。

🕮 **メモ：**

ファイル/**etc/syslog.conf** を編集する場合のガイドラインを以下に示します。

- コメントは個別の行に記入し、# 記号で始めてください。
- ファイル名に不要なスペース等をいれないでください。
- ロギングファシリティ名とファイル/**etc/syslog.conf** が指定するログ情報の重要度は、**info-center loghost** コマンドと **info-center source** コマンドで Device に設定したものと一致しなければなりません。一致しないと、ログ情報は正しくログホストに出力されないことがあります。

d) **syslogd**のプロセスIDを表示し、**syslogd**プロセスを削除、**syslogd**の使用を再開するコマンド（**-r**オプション変更された構成を実施させる）を実行してください。

Linux ログホストで **syslogd** プロセスに**-r** のオプションが付けられていることを確認してください。

```
# ps -ae | grep syslogd
147
# kill -9 147
# syslogd -r &
```

上記設定後は、Device は関連するファイルにログ情報を保存できるようになります。

目次

このセクションのページは **9-x-x** です。

4 章 SNMP 4-1
4.1 概要 4-1
4.1.1 SNMP の構造 4-1
4.1.2 MIB と view ベースの MIB アクセス管理 4-1
4.1.3 SNMP の動作 4-2
4.1.4 プロトコルバージョン 4-2
4.1.5 アクセスコントロールモード 4-3
4.2 SNMP 基本パラメータの設定 4-3
4.2.1 SNMPv1 あるいは SNMPv2c 基本パラメータの設定 4-3
4.2.2 SNMPv3 基本パラメータの設定 4-5
4.3 SNMP ロギングの設定 4-7
4.4 SNMP 通知の設定 4-7
4.4.1 SNMP notification の有効化 4-8
4.4.2 ホストへ notification を送信する SNMP エージェントの設定 4-8
4.5 SNMP の表示と維持 4-10
4.6 設定例 4-10
4.6.1 SNMPv1/SNMPv2c の設定例 4-10
4.6.2 SNMPv3 の設定例 4-12

4章 SNMP

4.1 概要

SNMP（Simple Network Management Protocol）はネットワークで装置にアクセスし、操作させるための管理システムとして、ベンダ、物理的な特徴、相互接続技術に関係なく、広く使われているインタネット標準プロトコルです。

SNMP を使用することで、装置の状態のモニタリング、トラブルシューティング、コリジョンの統計情報やほかの情報の管理を行うため、ネットワーク管理者が、装置の情報を確認し、設定することができます。

4.1.1 SNMP の構造

SNMP は以下の機能で構成されています。

- **SNMP マネジャー** － NMS（network management system）上で動作し、ネットワーク内の SNMP 対応装置をモニタし管理します。エージェント上の MIB オブジェクトの値を取得および設定できます。
- **SNMP エージェント** － 管理対象装置上で動作し、SNMP マネジャーからのリクエストを受信し操作します。インタフェースの状態の変化などのイベント発生時に SNMP マネジャーに Trap を送信します。
- **MIB（Management Information Base）** － SNMP マネジャーが読み取り、設定するために、SNMP エージェントによって保持されているインタフェース状態や CPU 使用率などの変数を指定します。

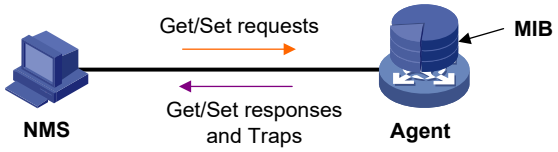


図 4-1 NMS、エージェント、MIB の関係

4.1.2 MIB と view ベースの MIB アクセス管理

MIB はツリー構造の「ノード」「オブジェクト」と呼ばれる変数を保存し、各ノードを固有の OID で区別します。OID はルートノードからリーフノードへのパスを示す番号列です。図 4-2では、オブジェクト B は OID {1.2.1.1}で区別されます。

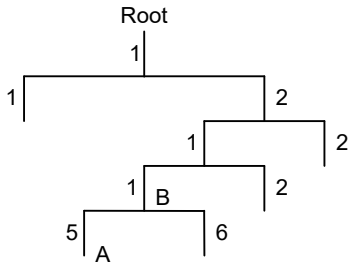


図 4-2 MIB ツリー

MIB view は、アクセス制限のある MIB オブジェクトの集合（あるいは MIB オブジェクト階層）を表し、view 名によって識別されます。MIB view に含まれる MIB オブジェクトはアクセス可能ですが、MIB view から除外されている MIB オブジェクトはアクセスできません。

MIB view は複数の view を持つことができます。複数の view は、*view-name oid-tree* の組み合わせで識別されます。

SNMP グループあるいはコミュニティに MIB view を割り当てることによって、MIB のアクセスを管理することができます。

4.1.3 SNMP の動作

SNMP は以下の基本的な動作を提供します。

- **Get** – エージェント MIB の SNMP オブジェクトノードを取得します。
- **Set** – エージェント MIB のオブジェクトノードの値を変更します。
- **Notification** – SNMP エージェントが NMS にイベントを通知するため、trap あるいは inform があります。Notification の 2 つのタイプの違いは、inform では ack（確認応答）が必要ですが、trap では必要ありません。trap は SNMPv1、SNMPv2c、SNMPv3 で有効ですが、inform は SNMPv2c、SNMPv3 でのみ有効です。

4.1.4 プロトコルバージョン

QX シリーズは、SNMPv1、SNMPv2c、SNMPv3 をサポートします。NMS と SNMP エージェントは相互に通信するため、同じ SNMP バージョンを使用する必要があります。

- **SNMPv1** – コミュニティ名で認証を行います。SNMP エージェントにアクセスするために、NMS は SNMP エージェントでセットしたものと同じコミュニティ名を使わなければなりません。NMS が使用するコミュニティ名がエージェントでセットしたものと違う場合、NMS はエージェントにアクセスするための SNMP セッションを構築することができない、もしくはエージェントからの Trap と Notification を受信することができません。
- **SNMPv2c** – コミュニティ名で認証を行います。SNMPv1 と互換を取り、より多くの動作モード、データ タイプ、エラーコードをサポートします。
- **SNMPv3** – USM （User-Based Security Model） を使ってセキュアな SNMP 通信を実現します。整合性、信頼性、および機密保持のために SNMP パケットを認証し暗号化する、認証とプライバシーのメカニズムを設定できます。

4.1.5 アクセスコントロールモード

SNMP は MIB オブジェクトにアクセスするため、以下のモードを使用します。

- VACM（View-based Access Control Model）モデルーVACM モードは MIB view を SNMP コミュニティやユーザに割り当てることで、MIB オブジェクトへのアクセスを制御します。

同じ SNMP コミュニティやユーザに複数回割り当てた場合、最後に作成した設定が適用されます。

VACM モードは NMS から MIB オブジェクトにアクセスする権限のみ必要です。

4.2 SNMP基本パラメータの設定

SNMPv3 は SNMPv1、SNMPv2c と多くの点で異なります。章を分けて設定方法について説明します。

4.2.1 SNMPv1 あるいは SNMPv2c 基本パラメータの設定

ユーザロールが network-admin あるいは level-15 のユーザのみ SNMPv1 あるいは SNMPv2c コミュニティ、ユーザ、グループを作成することができます。ほかのユーザロールのユーザは関連コマンド、SNMPv1 あるいは SNMPv2c 機能のコマンドへのアクセスが許可されていたとしても、SNMPv1 あるいは SNMPv2c コミュニティ、ユーザ、グループを作成することができません。

SNMP エージェントは、エージェントのリスニングポートが別のサービスによって使用されている場合、有効にできません。UDP ポートの使用情報を表示するには、**display udp verbose** コマンドを実行します。**display udp verbose** コマンドの詳細については、オペレーションマニュアルのセクション 3 *IP サービス*“*IP パフォーマンスの最適化*”のコマンドを参照してください。

SNMP エージェントを無効にすると、SNMP 設定は有効になりません。**display current-configuration** コマンドは、SNMP 設定を表示しません。SNMP 設定は構成ファイルに保存されません。SNMP 設定を有効にするには、SNMP エージェントを有効にします。

以下に SNMPv1 あるいは SNMPv2c 基本パラメータの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. （オプション設定項目） SNMP エージェントを有効にする	**snmp-agent**	デフォルト：無効 **snmp-agent calculate-password** コマンドを除いた**snmp-agent** で始まるいずれかのコマンドで SNMP エージェントを有効にできます。 IPアドレスを設定するまで SNMPポートは開きません。

操作	コマンド	補足
3.　（オプション設定項目） システム連絡先を設定する	**snmp-agent sys-info contact** *sys-contact*	デフォルト：設定なし
4.　（オプション設定項目） システム所在地を設定する	**snmp-agent sys-info location** *sys-location*	デフォルト：設定なし
5.　SNMPv1 あるいは SNMPv2c を有効にする	**snmp-agent sys-info version** { **all** | { **v1** | **v2c** | **v3** } * }	デフォルト：SNMPv3が有効
6.　（オプション設定項目） ローカルエンジン ID を変更する	**snmp-agent local-engineid** *engineid*	デフォルト：ローカルエンジン ID はCompany ID＋ device ID
7.　（オプション設定項目） MIB view を作成または更新する	**snmp-agent mib-view** { **excluded** | **included** } *view-name oid-tree* [**mask** *mask-value*]	デフォルト：**ViewDefault** このviewは**iso**サブツリーのすべてのオブジェクトが対象ですが、**snmpUsmMIB**と**snmpVacmMIB**と**snmpModules.18**はアクセス可能です。 *view-name*、*old-tree*のペアはそれぞれviewのレコードを表します。別のMIBサブツリーマスクに同じレコード名を複数回指定した場合、最後の設定が有効です。
8.　SNMP アクセス権を設定する	• （アプローチ1） SNMPコミュニティを作成する： **snmp-agent community** { **read** | **write** } [**simple** | **cipher**] *community-name* [**mib-view** *view-name*] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } | **acl ipv6** { *ipv6-acl-number* | **name** *ipv6-acl-name* }] * • （アプローチ2） SNMPv1/SNMPv2cグループを作成し、グループにユーザを追加する： – **snmp-agent group** { **v1** | **v2c** } *group-name* [**notify-view** *view-name* | **read-view** *view-name* | **write-view** *view-name*] * [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } | **acl ipv6** { *ipv6-acl-number* | **name** *ipv6-acl-name* }] * – **snmp-agent usm-user** { **v1** | **v2c** } *user-name group-name* [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } | **acl ipv6** { *ipv6-acl-number* | **name** *ipv6-acl-name* }] *	いずれか一方のアプローチを使用します。 デフォルト：SNMPグループあるいはSNMPコミュニティは設定なし アプローチ2の*user-name*はアプローチ1のコミュニティ名と同じで、NMBで設定されるコミュニティ名と同じでなければなりません。

操作	コマンド	補足
9.　（オプション設定項目） SNMP エージェントが送受信できる SNMP パケットの最大バイトサイズ（バイト）を設定する	**snmp-agent packet max-size** *byte-count*	デフォルト：1500バイト
10.（オプション設定項目） SNMP レスポンスパケットの DSCP 値を設定する	**snmp-agent packet response dscp** *dscp-value*	デフォルト：0 Version 7.2.30を含む以降のソフトウェアからサポートしています。

4.2.2 SNMPv3 基本パラメータの設定

ユーザロールが network-admin あるいは level-15 のユーザのみ SNMPv3 コミュニティ、ユーザ、グループを作成することができます。ほかのユーザロールのユーザは関連コマンド、SNMPv3 機能のコマンドへのアクセスが許可されていたとしても、SNMPv3 コミュニティ、ユーザ、グループを作成することができません。

SNMPv3 ユーザはグループで管理されます。グループのすべての SNMPv3 ユーザは同じセキュリティモデルを共有しますが、異なる認証、プライバシーキーの設定を使用することができます。ユーザのセキュリティモデルを設定し、SNMP 間の通信が失敗しないようにするため、グループのセキュリティモデルの設定とセキュリティキーは、表 4-1に従い、NMS の設定に合わせる必要があります。

表 4-1 異なるセキュリティモデルの基本セキュリティの設定要件

セキュリティモデル	グループのセキュリティモデルキーワード	ユーザのセキュリティキー設定	補足
プライバシーあり、認証あり	privacy	認証キー、 プライバシーキー	認証キーあるいはプライバシーキーが設定されていない場合、SNMP 間の通信は失敗します。
プライバシーなし、認証あり	authentication	認証キー	認証キーが設定されていない場合、SNMP間の通信は失敗します。 ユーザのプライバシーキー（ある場合）は影響しません。
認証なし、プライバシーなし	authentication あるいはprivacyのいずれもありません。	なし	認証キー、プライバシーキーが設定されても適用されません。

以下に SNMPv3 基本パラメータの設定を示します。

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

操作	コマンド	補足
2.　（オプション設定項目） SNMP エージェントを有効にする	**snmp-agent**	デフォルト：無効 **snmp-agent calculate-password** コマンドを除いた**snmp-agent** で始まるいずれかのコマンドで SNMP エージェントを有効にできます。
3.　（オプション設定項目） システム連絡先を設定する	**snmp-agent sys-info contact** *sys-contact*	デフォルト：設定なし
4.　（オプション設定項目） システム所在地を設定する	**snmp-agent sys-info location** *sys-location*	デフォルト：設定なし
5.　SNMPv3 を有効にする	**snmp-agent sys-info version** { **all** | { **v1** | **v2c** | **v3** } * }	デフォルト：SNMPv3が有効です。
6.　（オプション設定項目） ローカルエンジン ID を設定する	**snmp-agent local-engineid** *engineid*	デフォルト：ローカルエンジン ID はCompany ID＋ device ID です。 ⚠ **重要：** ローカルエンジンIDの変更後、既存のSNMPv3ユーザと暗号キーは無効になります。SNMPv3ユーザと暗号キーを再設定してください。
7.　（オプション設定項目） MIB view を作成または更新する	**snmp-agent mib-view** { **excluded** | **included** } *view-name oid-tree* [**mask** *mask-value*]	デフォルト：**ViewDefault** このviewは**iso**サブツリーのすべてのオブジェクトが対象ですが、**snmpUsmMIB**と**snmpVacmMIB**と**snmpModules.18**はアクセス可能です。 *view-name*、*old-tree*のペアはそれぞれviewのレコードを表します。別のMIBサブツリーマスクに同じレコード名を複数回指定した場合、最後の設定が有効です。
8.　（オプション設定項目）SNMPv3 グループを作成する	**snmp-agent group v3** *group-name* [**authentication** | **privacy**] [**notify-view** *read-view* | **read-view** *view-name* | **write-view** *view-name*] * [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } | **acl ipv6** { *ipv6-acl-number* | **name** *ipv6-acl-name* }] *	デフォルト：設定なし
9.　（オプション設定項目） 平文テキストキーを暗号キーに変換する	**snmp-agent calculate-password** *plain-password* **mode** { **3desmd5** | **3dessha** | **md5** | **sha** } { **local-engineid** | **specified-engineid** *engineid* }	—
10. SNMPv3 ユーザを作成する	**snmp-agent usm-user v3** *user-name group-name* [{ **cipher** | **simple** } **authentication-mode** { **md5** | **sha** } *auth-password* [**privacy-mode** { **3des** | **aes128** | **des56** } *priv-password*]] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } | **acl ipv6** { *ipv6-acl-number* | **name** *ipv6-acl-name* }] *	

操作	コマンド	補足
11.（オプション設定項目）SNMP エージェントが送受信できる SNMP パケットの最大バイトサイズ（バイト）を設定する	**snmp-agent packet max-size** *byte-count*	デフォルト：1500バイト

4.3 SNMPロギングの設定

必要な場合のみ SNMP ロギングを設定してください。SNMP ロギングを設定するとメモリに負担をかけ、装置の性能に影響を与える可能性があります。

SNMP エージェントは、GET リクエスト、SET リクエスト、SET 応答、SNMP 通知、SNMP 認証失敗をロギングしますが、GET 応答はロギングしません。

- **GET オペレーション** － エージェントは NMS の IP アドレス、アクセスノード名、ノード OID をロギングします。
- **SET オペレーション** － エージェントは NMS の IP アドレス、アクセスノード名、ノード OID、変数値、エラーコード、エラーインデックスをロギングします
- **通知トラッキング** － NMS に SNMP 通知を送信したのち、エージェントをロギングします。
- **SNMP 認証失敗** ー エージェントは SNMP 認証の失敗をロギングします。

SNMP モジュールは Information Center にログを送信します。

コンソールやログバッファなどの特定の宛先にメッセージを出力するため、Information Center を設定することができます。各ログエントリのノードフィールド（MIB ノード名）と値フィールド（MIB ノードの値）の合計最大サイズは 1024 バイトです。最大サイズを超過した場合、Information Center はフィールドのデータを切り捨てます。Information Center の詳細は、オペレーションマニュアルのセクション *9 システム管理 “Information Center”* を参照してください。

以下に SNMP ロギングの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2.（オプション設定項目）SNMP ロギングを有効にする	**snmp-agent log** { **all** | **authfail** | **get-operation** | **set-operation** }	デフォルト：無効
3.（オプション設定項目）SNMP 通知ロギングを有効にする	**snmp-agent trap log**	デフォルト：無効

4.4 SNMP通知の設定

SNMP エージェントはリンク状態の変更やユーザログイン、ログアウトなどの重要なイベントの notification （trap、inform）を NMS に通知します。特に説明がない限り、コマンドラインの **trap** キーワードは trap と inform を含みます。

4.4.1 SNMP notification の有効化

必要な場合のみ SNMP notification を有効にしてください。SNMP notification はメモリに負担をかけ、装置の性能に影響を与える可能性があります。

インタフェースのリンク状態が変更した場合、次のタスクを実行する必要があります。

- **snmp-agent trap enable standard** [**linkdown** | **linkup**] *コマンドを設定し、グローバルで linkUp あるいは linkDown notification を有効にしてください。
- **enable snmp trap updown** コマンドをインタフェースで設定し、linkUp あるいは linkDown notification を有効にしてください。

モジュールで notification を有効にした後、notification がモジュールの設定に依存して作成されます。詳細は、各モジュールの設定ガイドを参照してください。

IPv6 で notification を使用するには、SNMPv2c または SNMPv3 を有効にします。

以下に SNMP notification を有効にする設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． notification を有効にする	**snmp-agent trap enable** [**configuration** | *protocol* | **standard** [**authentication** | **coldstart** | **linkdown** | **linkup** | **warmstart**] * | **system**]	デフォルト：**configuration**、**standard**、**system**が有効です。ほかのSNMP notificationはモジュールによって変わります。装置がプロトコルのnotificationを送信するには、まずプロトコルを有効にします。
3． interface view に移行する	**interface** *interface-type interface-number*	―
4． リンク状態の notification を有効にする	**enable snmp trap updown**	デフォルト：有効

4.4.2 ホストへ notification を送信する SNMP エージェントの設定

ホストに trap あるいは inform する notification を送信する SNMP エージェントを設定することができます。一般的にホストは NMS で、解析や管理に使われます。trap を受信した場合、NMS は trap を受信する場合確認応答を送信しないため、trap は inform よりも少ないリソースで使用することができます。

I. 設定ガイドライン

ネットワークの輻輳が発生する、あるいは宛先に到達できない場合、SNMP エージェントはキューに notification をバッファします。キューのサイズと notification の保持時間（キューに保持できる最大時間）を設定することができます。notification は保持時間が満了した場合削除されます。notification のキューが一杯になった場合、もっとも古い notification が自動的に削除されます。

インタフェースの説明やインタフェースタイプを追加させるため、標準 linkUp/linkDown notification を拡張することができますが、NMS が拡張 SNMP メッセージをサポートしていることを確認する必要があります。

inform を送信するために、以下を確認してください。

- SNMP エージェントと NMS は SNMPv2c あるいは SNMPv3 を使用します。
- SNMPv3 が使用される場合、SNMPv3 基本設定を行う際に NMS の SNMP エンジン ID を設定してください。また SNMPv3 ユーザを作成する場合、SNMP エンジンの IP アドレスを指定してください。

II. 設定要件

- NMS として基本 SNMP の設定と同じように SNMP エージェントを設定してください。SNMPv1 あるいは SNMPv2c を使用する場合、コミュニティ名を設定してください。SNMPv3 を使用する場合、notification の SNMPv3 ユーザ、MIB view を設定してください。
- SNMP エージェントと NMS が互いに到達可能であるようにしてください。

III. 設定手順

以下にホストに notification を送信する SNMP エージェントの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． 宛先ホストを設定する	• （アプローチ1）宛先ホストにtrapを送信する： **snmp-agent target-host trap address udp-domain** { *ipv4-target-host* | **ipv6** *ipv6- target-host* } [**udp-port** *port-number*] **params securityname** *security-string* [**v1** | **v2c** | **v3** [**authentication** | **privacy**]] • （アプローチ2）宛先ホストにinformを送信する： **snmp-agent target-host inform address udp-domain** { *ipv4-target-host* | **ipv6** *ipv6- target-host* } [**udp-port** *port-number*] **params securityname** *security-string* { **v2c** | **v3** [**authentication** | **privacy**] }	いずれか一方を使用します。 デフォルト：設定なし
3． （オプション設定項目） notification の送信元アドレスを設定する	**snmp-agent** { **inform** | **trap** } **source** *interface-type interface-number*	デフォルト: SNMPは送信元IPアドレスとして出力インタフェースのIPアドレスを使用します。
4． （オプション設定項目） 拡張 linkUp/linkDown notification を有効にする	**snmp-agent trap if-mib link extended**	デフォルト：標準 linkUp/linkDown notificationを使用します
5． （オプション設定項目） notification キューサイズを設定する	**snmp-agent trap queue-size** *size*	デフォルト：100
6． （オプション設定項目） notification ライフタイムを設定する	**snmp-agent trap life** *seconds*	デフォルト：120秒

4.5 SNMPの表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
連絡先、所在地、SNMP のバージョンを含むSNMPエージェントのシステム情報を表示する	**display snmp-agent sys-info** [**contact** | **location** | **version**] *
SNMPエージェント統計情報を表示する	**display snmp-agent statistics**
ローカルエンジンIDを表示する	**display snmp-agent local-engineid**
SNMPグループ情報を表示する	**display snmp-agent group** [*group-name*]
notificationキューの基本情報を表示する	**display snmp-agent trap queue**
notificationを送信できるモジュールおよびnotificationの状態（有効あるいは無効）を表示する	**display snmp-agent trap-list**
SNMPv3ユーザ情報を表示する	**display snmp-agent usm-user** [**engineid** *engineid* | **group** *group-name* | **username** *user-name*] *
SNMP v1または SNMP v2c のコミュニティ情報を表示する	**display snmp-agent community** [**read** | **write**]
MIB view情報を表示する	**display snmp-agent mib-view** [**exclude** | **include** | **viewname** *view-name*]

4.6 設定例

4.6.1 SNMPv1/SNMPv2c の設定例

SNMPv1 の設定手順は SNMPv2c 設定手順と同一です。この設定例は SNMPv1 を使用します。

I. ネットワーク要件

図 4-3に示すように、NMS（1.1.1.2/24）は SNMPv1 で SNMP エージェント（1.1.1.1/24）を管理します。エージェントはイベントを報告する notification を NMS に自動的に送信します。

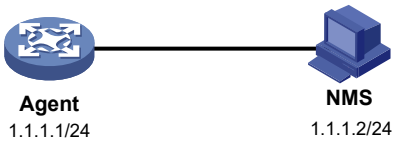


図 4-3 ネットワーク図

II. 設定手順

1)　SNMP エージェントを設定します。

エージェントの IP アドレスを設定し、NMS と通信可能であることを確認します。（詳細は省略します。）

SNMPv1 を指定し、読み込みのみのコミュニティ **public** と読み書き可能なコミュニティ **private** を生成します。

```
<Agent> system-view
[Agent] snmp-agent sys-info version v1
[Agent] snmp-agent community read public
[Agent] snmp-agent community write private
```

エージェントの連絡先と所在地情報を設定します。

```
[Agent] snmp-agent sys-info contact NEC
[Agent] snmp-agent sys-info location Tokyo
```

SNMP notification を有効にし、SNMP trap の宛先として IP アドレスが 1.1.1.2 の NMS を設定し、コミュニティ名として **public** を使用します。（NMS が trap を受信できること確認するため、**snmp-agent target-host** コマンドで設定されている SNMP のバージョンを NMS と同一に指定します。）

```
[Agent] snmp-agent trap enable
[Agent] snmp-agent target-host trap address udp-domain 1.1.1.2 params securityname public v1
```

2)　SNMP NMS を設定します。

- SNMPv1 を指定します。
- 読み込みのみのコミュニティ **public** と読み書き可能なコミュニティ **private** を作成します。
- 必要に応じて、タイムアウト時間と再トライを行う最大数を設定します。

NMS の設定についての詳細は、NMS のマニュアルを参照してください。

メモ：

エージェントと NMS の SNMP 設定は同一にする必要があります。

III. 設定の確認

エージェントから Null0 インタフェースの MTU 値を取得します。取得に成功します。

```
Send request to 1.1.1.1/161 ...
Protocol version: SNMPv1
Operation: Get
Request binding:
1: 1.3.6.1.2.1.2.2.1.4.135471
Response binding:
1: Oid=ifMtu.135471 Syntax=INT Value=1500
Get finished
```

エージェントの MIB ノードの値を取得するため、wrong コミュニティ名を使用します。NMS で trap の認証に失敗していることがわかります。

```
1.1.1.1/2934 V1 Trap = authenticationFailure
SNMP Version = V1
Community = public
Command = Trap
Enterprise = 1.3.6.1.4.1.43.1.16.4.3.50
GenericID = 4
SpecificID = 0
Time Stamp = 8:35:25.68
```

4.6.2 SNMPv3 の設定例

I. ネットワーク要件

図 4-4に示すように、NMS（1.1.1.2/24）は SNMPv3 でエージェント（1.1.1.1/24）のインタフェース状態をモニタし管理します。エージェントはイベントを通知する notification を NMS に自動的に送信します。

NMS とエージェントは SNMP セッションを構成する場合に認証を行います。認証アルゴリズムは SHA-1 で、認証キーは **123456TESTauth&!**です。NMS とエージェント間のパケットは、AES アルゴリズム、プライバシーキー**123456TESTencr&!**で暗号化されます。

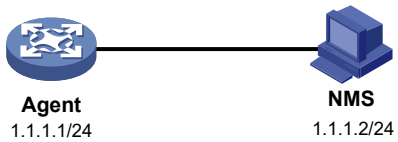


図 4-4 ネットワーク図

II. 設定手順

1)　SNMP エージェントを設定します。

エージェントの IP アドレス 1.1.1.1/24 を設定し、NMS と通信可能であることを確認します。（詳細は省略します。）

SNMPv3 グループ **managev3group** を作成します。test view の SNMPv3 グループ **managev3group** に、アクセス権限を設定します。snmpMIB ノード（OID : 1.3.6.1.6.3.1）下のオブジェクト（linkUp オブジェ気宇と、linkDown オブジェクトを含みます。）を読み

込みのみできるように設定し、ほかの MIB オブジェクトはアクセスできないようにします。

```
<Agent> system-view
[Agent] undo snmp-agent mib-view ViewDefault
[Agent] snmp-agent mib-view included test snmpMIB
[Agent] snmp-agent group v3 managev3group privacy read-view test
```

SNMPv3 グループ **managev3group** にアクセス権限を設定します。test view のシステムノード（OID：1.3.6.1.2.1.1）とインタフェースノード（OID：1.3.6.1.2.1.2）下のオブジェクトを読み書きできるように設定します。

```
[Agent] snmp-agent mib-view included test 1.3.6.1.2.1.1
[Agent] snmp-agent mib-view included test 1.3.6.1.2.1.2
[Agent] snmp-agent group v3 managev3group privacy read-view test write-view test
```

ユーザ **VACMtest** を、SNMPv3 グループ **managev3group** に追加し、認証アルゴリズム **sha**、認証キー**123456TESTauth&!**、暗号化アルゴリズム **aes128**、プライバシーキー**123456TESTencr&!**を設定します。

```
[Agent] snmp-agent usm-user v3 VACMtest managev3group simple authentication-mode sha 123456TESTauth&! privacy-mode aes128 123456TESTencr&!
```

エージェントの連絡先と所在地情報を設定します。

```
[Agent] snmp-agent sys-info contact NEC
[Agent] snmp-agent sys-info location Tokyo
```

エージェントで notifications を有効にします。Trap の宛先として 1.1.1.2 の NMS を指定し、Trap のユーザ名を **VACMtest** に設定します。

```
[Agent] snmp-agent trap enable
[Agent] snmp-agent target-host trap address udp-domain 1.1.1.2 params VACMtest v3 privacy
```

2)　SNMP NMS を設定します。
- □　SNMPv3 を指定します。
- □　SNMPv3 ユーザ **VACMtest** を作成します。
- □　認証機能とプライバシー機能の両方を有効にしてください。
- □　認証に **SHA-1** を使用し、暗号化に **AES** を設定してください。
- □　認証キー**123456TESTauth&!**とプライバシーキー**123456TESTencr&!**を設定してください。
- □　必要に応じて、タイムアウト時間と再トライを行う最大数を設定します。

NMS の設定についての詳細は、NMS のマニュアルを参照してください。

🕮 メモ：

エージェントと NMS の SNMP 設定は同一にする必要があります。

III. 設定の確認

エージェントにアクセスするためユーザ名 VACMtest を使用します。

sysName ノードの値を回復します。値 Agent が戻ります。

Sysname に sysName ノードの値を設定します。取得に成功します。

エージェントでインタフェースをシャットダウンあるいはアップにします。NMS は linkUP （OID：1.3.6.1.6.3.1.1.5.4） あるいは linkDown （OID：1.3.6.1.6.3.1.1.5.3）の notification を受信します。

目次

このセクションのページは **9-x-x** です。

5 章 RMON 5-1
5.1 概要 5-1
5.1.1 RMON グループ 5-1
5.1.2 アラームグループとプライベートアラームグループのサンプルタイプ 5-3
5.1.3 プロトコルと標準 5-4
5.2 RMON 統計機能の設定 5-4
5.2.1 RMON イーサネット統計機能エントリの作成 5-4
5.2.2 RMON 履歴管理エントリの作成 5-4
5.2.3 RMON アラーム機能の設定 5-5
5.3 RMON の表示と維持 5-6
5.4 RMON 設定例 5-7
5.4.1 イーサネット統計情報の設定例 5-7
5.4.2 履歴統計情報の設定例 5-7
5.4.3 アラーム機能の設定例 5-8

5章 RMON

5.1 概要

RMON（Remote Monitoring）は、SNMP を拡張した機能です。リモートモニタリングとネットワーク装置とサブネットの管理を行います。RMON モニタ（ネットワーク装置に組み込まれた RMON エージェント）は定期的に、または継続的に、ポートに接続されたネットワークのトラフィック統計情報を収集します。統計情報がアラームのしきい値を超えたとき、管理対象装置は、自動的にトラップを送信することができます。NMS は、常に MIB 変数をポーリングし結果を比較する必要はありません。

RMON は、例外条件の NMS を通知するために SNMP トラップを使用しています。RMON SNMP トラップは、ブロードキャストトラフィックのしきい値を超過したトラフィックイベントなど、様々なイベントを報告します。対照的に、SNMP 標準トラップは、リンクアップ、リンクダウン、モジュールの障害などの装置の動作状態の変化を報告します。

SNMP の詳細は、オペレーションマニュアルのセクション 9 *システム管理*"*SNMP*"を参照してください。

NEC は、RMON モニタとして、組み込み RMON エージェントの機能を提供しています。NMS は RMON MIB にアクセスすることで基本的な SNMP の動作を行うことができます。

5.1.1 RMON グループ

標準 RMON グループのうち、NEC では、統計情報グループ、履歴グループ、イベントグループ、アラームグループ、プローブ設定グループ、およびユーザ履歴グループをサポートします。プローブ設定グループとユーザ履歴グループは CLI から設定できません。設定を行うために MIB にアクセスする必要があります。

I. 統計情報グループ

統計情報グループは、モニタされたイーサネットインタフェースのトラフィック情報の統計情報を取得し、Ethernet 統計情報テーブル（ethernetStatsTable）の統計情報を記録します。統計情報は以下があります。

- ネットワークの衝突数
- CRC アライメントエラー
- アンダーサイズ/オーバーサイズパケット
- ブロードキャスト数
- マルチキャスト数
- 受信バイト数
- 受信パケット数

Ethernet 統計情報テーブルの統計情報は統計情報の総数です。

II. 履歴グループ

履歴グループは、定期的にインタフェース上のトラフィック情報の統計情報を収集し、履歴レコードテーブル（ethernetHistoryTable）の統計情報を記録します。統計情報は以下があります。

- 帯域幅使用率
- エラーパケット数
- パケットの合計数

履歴レコードテーブルは各サンプリング間隔でインタフェースに受信されたトラフィックの統計情報を記録します。

III. イベントグループ

イベントグループは、アラームグループとプライベートアラームグループで定義されているアラームによって発生したイベントの作成と通知を制御します。RMON アラームイベントは以下の方法で処理されます。

- **Log**－イベントログテーブル内のイベント情報（発生したイベント時間、イベントの内容を含みます。）をロギングします。管理装置は、SNMP Get 操作によってログを収集することができます。
- **Trap**－イベントが発生したとき、NMS に SNMP 通知を送信します。
- **Log-Trap**－イベントログテーブルのイベント情報をロギングし、イベントが発生したときに、SNMP 通知を送信します。
- **None**－処理を行いません。

IV. アラームグループ

RMON アラームグループは、インタフェース上の受信パケット（etherStatsPkts）のカウントなどのアラーム変数をモニタします。アラームエントリを作成したのち、RMON エージェントは指定した間隔でモニタアラーム変数の値を取得します。モニタ対象の変数の値が増加方向のしきい値を超えると、増加方向のイベントが発生します。変数の値が減少方向のしきい値を下回ると、減少方向のイベントが発生します。その後イベントは、イベントグループで定義したように処理されます。

アラームエントリがしきい値を連続して複数回交差する場合、RMON エージェントは、最初のしきい値が交差したときにアラームイベントを発生します。サンプリングされた値が増加方向あるいは減少方向のしきい値を超えた時点で 1 つのイベントが発生します。反対方向のしきい値を超えるまで次のイベントは発生しません。たとえば、図 5-1に示すように、増加方向のしきい値を超えると 1 つのイベントが発生し、減少方向のしきい値を超えるまで次のイベントは発生しません。

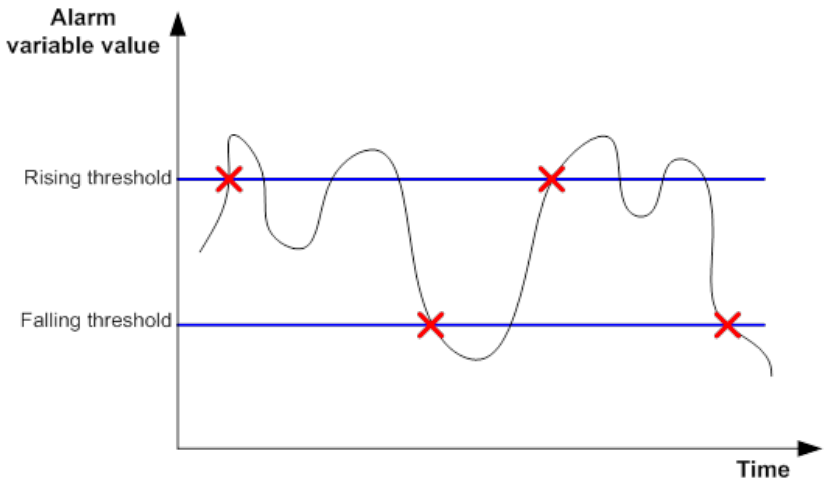


図 5-1 増加方向と減少方向のアラームイベント

V. プライベートアラームグループ

プライベートアラームグループは複数のアラーム変数の値を計算し、計算結果を定義済みの増加方向と減少方向のしきい値と比較します。

RMON エージェントは変数をサンプリングし、プライベートアラームにもとづいたアラームアクションを以下のように行います。

1) ユーザ定義した形式のプライベートアラーム変数をサンプリングします。
2) 定義した形式にもとづいてサンプリングした値を計算します。
3) 定義されたしきい値と計算した値を比較し、以下のいずれかのアクションを行います。
   - 比較結果が増加方向のしきい値以上である場合、増加方向のアラームイベントに関するイベントをトリガします。
   - 比較結果が減少方向のしきい値以下である場合、減少方向のアラームイベントに関するイベントをトリガします。

アラームエントリがしきい値を連続して複数回交差する場合、RMON エージェントは、最初のしきい値が交差したときにアラームイベントを発生します。サンプリングされた値が増加方向あるいは減少方向のしきい値を超えた時点で 1 つのイベントが発生します。反対方向のしきい値を超えるまで次のイベントは発生しません。たとえば、増加方向のしきい値を超えると 1 つのイベントが発生し、減少方向のしきい値を超えるまで次のイベントは発生しません。

5.1.2 アラームグループとプライベートアラームグループのサンプルタイプ

RMON エージェントは以下のサンプルタイプをサポートします。

- **absolute**– RMON は、サンプル値をしきい値と直接比較します。増加方向のしきい値と減少方向のしきい値の変数を、サンプリングした後に比較します。
- **delta**– RMON は現在のサンプル値を最後に取得したサンプル値から引き、その差を増加方向のしきい値と減少方向のしきい値と比較します。

5.1.3 プロトコルと標準

- RFC 4502, *Remote Network Monitoring Management Information Base Version 2*
- RFC 2819, *Remote Network Monitoring Management Information Base Status of this Memo*

5.2 RMON統計機能の設定

RMON 統計機能はイーサネット統計グループと履歴グループによって実装されます。

イーサネット統計グループはイーサネット統計情報テーブルで定義された変数であり、記録されたコンテンツは、統計エントリが現在時刻に作成された時点からの変数の合計です。設定の詳細は、オペレーションマニュアルのセクション 9 *システム管理* "*RMON*"の"*RMON イーサネット統計機能エントリの作成*"を参照してください。

ヒストリグループは、各サンプリング間隔の変数で収集された統計情報を提供します。ヒストリグループは収集を管理するため、履歴管理テーブルを使用し、履歴テーブルに収集された統計情報を記録します。設定の詳細は、オペレーションマニュアルのセクション 9 *システム管理* "*RMON*"の"*RMON 履歴管理エントリの作成*"を参照してください。

5.2.1 RMON イーサネット統計機能エントリの作成

I. 設定ガイドライン

RMON 統計エントリのインデックスは、グローバルに一意である必要があります。インデックスが別のインタフェースで使用されている場合、作成操作は失敗します。

Ethernet インタフェースに対して作成できる RMON 統計エントリは 1 つだけです。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. interface view に移行する	**interface** *interface-type interface-number*	—
3. RMON 統計情報テーブルにインタフェースのエントリを作成する	**rmon statistics** *entry-number* [**owner** *text*]	—

5.2.2 RMON 履歴管理エントリの作成

1 つのインタフェースに複数の履歴管理エントリを設定することができますが、エントリ数とサンプリング間隔は同一にしてはいけません。

指定したバケットサイズが有効な履歴テーブルサイズを超過しても、履歴管理エントリを作成することができます。RMON はバケットサイズを可能な限り予期したサイズに設定します。

以下に RMON 履歴管理エントリの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． interface view に移行する	**interface** *interface-type interface-number*	―
3． RMON 履歴管理テーブルにインタフェースのエントリを作成する	**rmon history** *entry-number* **buckets** *number* **interval** *sampling-interval* [**owner** *text*]	デフォルト：設定なし

5.2.3 RMON アラーム機能の設定

RMON アラーム機能を設定するときに、以下のガイドラインに従ってください。

- RMON アラーム機能の設定を行う前、アラームが発生したとき NMS に通知するため、SNMP エージェントを設定してください。SNMP エージェントについては、オペレーションマニュアルのセクション 9 *システム管理* "*SNMP*"を参照してください。
- 新しいイベント、アラーム、プライベートアラームを作成するために以下の条件が必要です。
  - □ 新しいエントリのパラメータは、すでに存在するエントリと同じにすることはできません。
  - □ エントリ数が最大になっていないこと。

表 5-1に比較されるパラメータとエントリの制限を示します。

表 5-1 RMON の設定制限

エントリ	比較パラメータ	エントリの最大数
イベント	● イベント記述（**description** *string*） ● イベントタイプ（**log**、**trap**、**logtrap**、**none**） ● コミュニティ名（*security-string*）	60
アラーム	● アラーム変数（*alarm-variable*） ● サンプリング間隔（*sampling-interval*） ● サンプルタイプ（**absolute**、**delta**） ● 増加方向のしきい値（*threshold-value1*） ● 減少方向のしきい値 （*threshold-value2*）	60
プライベートアラーム	● アラーム変数式（*prialarm-formula*） ● サンプリング間隔（*sampling-interval*） ● サンプルタイプ（**absolute**、**delta**） ● 増加方向のしきい値（*threshold-value1*） ● 減少方向のしきい値 （*threshold-value2*）	50

以下に RMON アラーム機能の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. （オプション設定項目）イベントテーブルにイベントエントリを作成する	**rmon event** *entry-number* [**description** *string*] { **log** | **log-trap** *security-string* | **none** | **trap** *security-string* } [**owner** *text*]	デフォルト：設定なし
3. アラームテーブルあるいはプライベートアラームテーブルにエントリを作成する	• アラームテーブルにエントリを作成する： **rmon alarm** *entry-number alarm-variable sampling-interval* { **absolute** | **delta** } [**startup-alarm** { **falling** | **rising** | **rising-falling** }] **rising-threshold** *threshold-value1 event-entry1* **falling-threshold** *threshold-value2 event-entry2* [**owner** *text*] • プライベートアラームテーブルにエントリを作成する： **rmon prialarm** *entry-number prialarm-formula prialarm-des sampling-interval* { **absolute** | **delta** } [**startup-alarm** { **falling** | **rising** | **rising-falling** }] **rising-threshold** *threshold-value1 event-entry1* **falling-threshold** *threshold-value2 event-entry2* **entrytype** { **forever** | **cycle** *cycle-period* } [**owner** *text*]	デフォルト：設定なし アラームを作成されていないイベントと関連付けることができますが、イベントを設定したのち、アラームが動作します。

5.3 RMONの表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
RMON統計情報を表示する	**display rmon statistics** [*interface-type interface-number*]
RMON履歴管理エントリと履歴サンプルを表示する	**display rmon history** [*interface-type interface-number*]
RMONアラームエントリを表示する	**display rmon alarm** [*entry-number*]
RMONプライベートアラームエントリを表示する	**display rmon prialarm** [*entry-number*]
RMONイベントエントリを表示する	**display rmon event** [*entry-number*]
イベントエントリのログ情報を表示する	**display rmon eventlog** [*entry-number*]

5.4 RMON設定例

5.4.1 イーサネット統計情報の設定例

I. ネットワーク要件

図 5-2に示すように、GigabitEthernet 1/0/1 のトラフィックの統計情報の合計を収集するため、Device 上で RMON Ethernet 統計情報グループエントリを作成します。

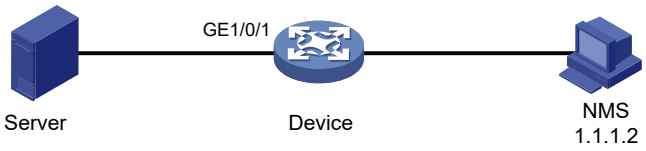


図 5-2 ネットワーク図

II. 設定手順

GigabitEthernet 1/0/1 の RMON イーサネット統計情報エントリを作成します。

```
<Device> system-view
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] rmon statistics 1 owner user1
```

GigabitEthernet 1/0/1 の RMON エージェントで収集された統計情報を表示します。

```
<Device> display rmon statistics gigabitethernet 1/0/1
EtherStatsEntry 1 owned by user1 is VALID.
  Interface : GigabitEthernet1/0/1<ifIndex.3>
  etherStatsOctets          : 21657     , etherStatsPkts          : 307
  etherStatsBroadcastPkts   : 56        , etherStatsMulticastPkts : 34
  etherStatsUndersizePkts   : 0         , etherStatsOversizePkts  : 0
  etherStatsFragments       : 0         , etherStatsJabbers       : 0
  etherStatsCRCAlignErrors  : 0         , etherStatsCollisions    : 0
  etherStatsDropEvents (insufficient resources): 0
  Incoming packets by size:
  64      : 235       ,   65-127   : 67        ,   128-255   : 4
  256-511: 1          ,   512-1023: 0          ,   1024-1518: 0
```

NMS から SNMP Get 操作を行いトラフィックの統計情報を取得します。(詳細は省略します。)

5.4.2 履歴統計情報の設定例

I. ネットワーク要件

図 5-3に示すように、1 分ごとの GigabitEthernet 1/0/1 のトラフィックの統計情報をサンプリングするため、Device 上で RMON 履歴管理エントリを作成します。

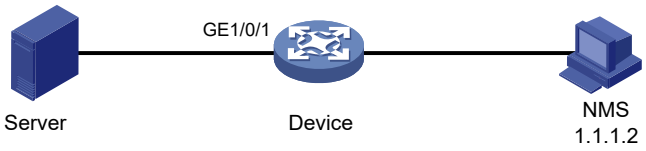


図 5-3 ネットワーク図

II. 設定手順

1 分ごとの GigabitEthernet 1/0/1 のトラフィックの統計情報をサンプリングするため、RMON 履歴管理エントリを作成します。履歴統計テーブルに最大 8 つのインタフェース用のサンプルを記録します。

```
<Device> system-view
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] rmon history 1 buckets 8 interval 60 owner user1
```

GigabitEthernet 1/0/1 で収集された履歴統計情報を表示します。

```
[Device-GigabitEthernet1/0/1] display rmon history
HistoryControlEntry 1 owned by user1 is VALID
  Sampled interface     : GigabitEthernet1/0/1<ifIndex.3>
  Sampling interval     : 60(sec) with 8 buckets max
  Sampling record 1 :
    dropevents        : 0         , octets               : 834
    packets           : 8         , broadcast packets    : 1
    multicast packets : 6         , CRC alignment errors : 0
    undersize packets : 0         , oversize packets     : 0
    fragments         : 0         , jabbers              : 0
    collisions        : 0         , utilization          : 0
  Sampling record 2 :
    dropevents        : 0         , octets               : 962
    packets           : 10        , broadcast packets    : 3
    multicast packets : 6         , CRC alignment errors : 0
    undersize packets : 0         , oversize packets     : 0
    fragments         : 0         , jabbers              : 0
    collisions        : 0         , utilization          : 0
```

NMS から SNMP Get 操作を行いトラフィックの統計情報を取得します。（詳細は省略します。）

5.4.3 アラーム機能の設定例

I. ネットワーク要件

図 5-4に示すように、GigabitEthernet 1/0/1 の入力トラフィックの入力トラフィックの統計情報をモニタし、以下のイベントが発生するとき、SNMP でアラームを送信します。

- サンプリング間隔の値が 5 秒で、増加方向のしきい値（100）を超えます。
- サンプリング間隔の値が 5 秒で、減少方向のしきい値（50）を下回ります。

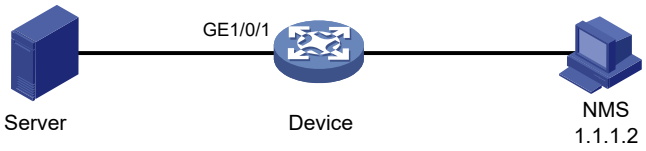


図 5-4 ネットワーク図

II. 設定手順

1.1.1.2 の NMS の SNMP 設定と同様に、SNMP エージェント（Device）の設定を行います。この例では SNMPv1、public コミュニティの読み込み、プライベートコミュニティの書き込みの設定を使用します。

```
<Device> system-view
[Device] snmp-agent
[Device] snmp-agent community read public
[Device] snmp-agent community write private
[Device] snmp-agent sys-info version v1
[Device] snmp-agent trap enable
[Device] snmp-agent trap log
[Device] snmp-agent target-host trap address udp-domain 1.1.1.2 params securityname public
```

GigabitEthernet 1/0/1 の RMON イーサネット統計情報エントリを作成します。

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] rmon statistics 1 owner user1
[Device-GigabitEthernet1/0/1] quit
```

ノード 1.3.6.1.2.1.16.1.1.1.4.1 の delta サンプル値が 100 を超えた場合、あるいは 50 を下回った場合、SNMP 通知を送信するために RMON イベントエントリ、RMON アラームエントリを作成します。

```
[Device] rmon event 1 trap public owner user1
[Device] rmon alarm 1 1.3.6.1.2.1.16.1.1.1.4.1 5 delta rising-threshold 100 1 falling-threshold 50 1 owner user1
```

メモ：

1.3.6.1.2.1.16.1.1.1.4.1 は GigabitEthernet 1/0/1 のオブジェクトインスタンスです。ここで 1.3.6.1.2.1.16.1.1.1.4 は入力トラフィックの合計オブジェクトを示し、1 は GigabitEthernet 1/0/1 の RMON イーサネット統計情報エントリインデックスです。

RMON アラームエントリを表示します。

```
<Device> display rmon alarm 1
AlarmEntry 1 owned by user1 is VALID.
  Sample type                    : delta
  Sampled variable              : 1.3.6.1.2.1.16.1.1.1.4.1<etherStatsOctets.1>
  Sampling interval (in seconds) : 5
  Rising threshold               : 100(associated with event 1)
  Falling threshold              : 50(associated with event 1)
  Alarm sent upon entry startup  : risingOrFallingAlarm
  Latest value                   : 0
```

GigabitEthernet 1/0/1 の統計情報を表示します。

```
<Device> display rmon statistics gigabitethernet 1/0/1
EtherStatsEntry 1 owned by user1 is VALID.
  Interface : GigabitEthernet1/0/1<ifIndex.3>
  etherStatsOctets          : 57329     , etherStatsPkts          : 455
  etherStatsBroadcastPkts   : 53        , etherStatsMulticastPkts : 353
  etherStatsUndersizePkts   : 0         , etherStatsOversizePkts  : 0
  etherStatsFragments       : 0         , etherStatsJabbers       : 0
  etherStatsCRCAlignErrors : 0          , etherStatsCollisions    : 0
  etherStatsDropEvents (insufficient resources): 0
  Incoming packets by size :
  64     : 7         ,  65-127  : 413       ,  128-255  : 35
  256-511: 0         ,  512-1023: 0         ,  1024-1518: 0
```

アラームが開始したとき、NMS は notification を受信します。

目次

このセクションのページは **9-x-x** です。

6 章 NQA 6-1
6.1 概要 6-1
6.1.1 NQA のテストタイプ 6-1
6.1.2 しきい値監視機能 6-2
6.2 NQA 設定作業リスト 6-2
6.3 NQA サーバの設定 6-2
6.4 NQA クライアントの有効化 6-3
6.5 NQA クライアントの NQA テストの設定 6-4
6.5.1 NQA テストの設定作業リスト 6-4
6.5.2 ICMP エコーテストの設定 6-4
6.5.3 DHCP テストの設定 6-5
6.5.4 DNS テストの設定 6-6
6.5.5 FTP テストの設定 6-7
6.5.6 HTTP テストの設定 6-8
6.5.7 UDP ジッタテストの設定 6-9
6.5.8 SNMP テストの設定 6-10
6.5.9 TCP テストの設定 6-11
6.5.10 UDP エコーテストの設定 6-12
6.5.11 音声テストの設定 6-13
6.5.12 DLSw テストの設定 6-16
6.5.13 NQA テストのオプションパラメータの設定 6-16
6.5.14 しきい値監視機能の設定 6-17
6.5.15 NQA 統計情報収集機能の設定 6-19
6.5.16 NQA 履歴記録保存の設定 6-19
6.5.17 NQA クライアントにおける NQA テストのスケジューリング 6-20
6.6 NQA の表示と維持 6-20
6.7 NQA 設定例 6-21
6.7.1 ICMP エコーテスト設定例 6-21
6.7.2 DHCP テスト設定例 6-23
6.7.3 DNS テスト設定例 6-24
6.7.4 FTP テスト設定例 6-25
6.7.5 HTTP テスト設定例 6-27
6.7.6 UDP ジッタテスト設定例 6-28
6.7.7 SNMP テスト設定例 6-30
6.7.8 TCP テスト設定例 6-32
6.7.9 UDP エコーテスト設定例 6-34
6.7.10 音声テスト設定例 6-35
6.7.11 DLSw テスト設定例 6-37

6章 NQA

6.1 概要

NQA（Network quality analyzer）は、ネットワークの性能、IP サービスのサービスレベルとアプリケーションを確認し、ネットワークの問題を診断することができます。以下のタイプのテストをサポートしています。

- ICMP エコーテスト
- DHCP
- DLSw
- DNS
- FTP
- HTTP
- SNMP
- TCP
- UDP エコーテスト
- Voice
- UDP ジッタ

図 6-1に示すように、NQA 送信元装置（NQA クライアント）は、ネットワークパフォーマンスを測定するため、NQA 宛先装置に IP サービスとアプリケーションのシミュレーションを行うデータを送信します。取得した性能の測定基準は、1 方向の遅延、ジッタ、音声品質、アプリケーション性能、サーバ応答時間が含まれます。

NQA のすべてのタイプは NQA クライアントが必要ですが、TCP、UDP エコー、UDP ジッタ、音声は NQA サーバのみ必要です。FTP のように、すでに宛先装置でサービスが提供されている場合、NQA サーバは必要ではありません。

さまざまなテストのニーズを満たすため、特定の IP アドレスとポートをリスニングし、応答する NQA サーバを設定することができます。



図 6-1 ネットワーク図

6.1.1 NQA のテストタイプ

以下に異なる NQA テストタイプを示します。

- TCP あるいは DLSw テストは接続をセットアップします。
- UDP ジッタや音声テストは指定した数のプローブパケットを送信します。プローブパケット数は **probe packet-number** コマンドで設定可能です。
- FTP テストはファイルのアップロードあるいはダウンロードを行います。
- HTTP テストは Web ページを取得します。
- DHCP テストは DHCP を通して IP アドレスを取得します。

- DNS テストは IP アドレスにドメイン名を変換します。
- ICMP エコーテストは ICMP エコーリクエストを送信します。
- UDP エコーテストは UDP ペットを送信します。
- SNMP テストは SNMPv1 パケット、SNMPv2c パケット、SNMPv3 パケットを送信します。

6.1.2 しきい値監視機能

しきい値監視機能は、NQA が指定したしきい値を越えた場合、指定されたアクションを実行します。

表 6-1に監視対象とサポートするテストタイプの関係について示します。

表 6-1 監視対象とサポートするテストタイプの関係

監視対象	サポートするテストタイプ
プローブ期間	UDPジッタ、音声を除くすべてのNQAテスト
検査失敗回数	UDPジッタ、音声を除くすべてのNQAテスト
廃棄パケット数	UDPジッタ、音声テスト
1方向のジッタ（送信元から宛先、宛先から送信元）	UDPジッタ、音声テスト
1方向の遅延（送信元から宛先、宛先から送信元）	UDPジッタ、音声テスト
ICPIF（Calculated Planning Impairment Factor）（詳細はオペレーションマニュアルの *セクション9 システム管理"NQA"の"音声テストの設定"* を参照してください。）	音声テスト
MOS（Mean Opinion Scores）（詳細はオペレーションマニュアルの *セクション9 システム管理"NQA"の"音声テストの設定"* を参照してください。）	音声テスト

6.2 NQA設定作業リスト

作業リスト	補足
NQAサーバの設定	TCP、UDP、UDPジッタ、音声テストでは必須設定項目
（必須設定項目）NQAクライアントの有効化	ー
（必須設定項目） NQAクライアントのNQAテストの設定	ー

6.3 NQAサーバの設定

TCP、UDP エコー、UDP ジッタ、音声テストを実行するため、宛先装置で NQA サーバを有効にする必要があります。NQA サーバは。指定されたアドレスとポート番号で NQA クライアントからの要求に応答します。IP アドレスとポート番号は NQA クライアントが設定したものと一致する必要があります。また現在リスニングしているものとは別にする必要があります。

NQA サーバ上で、各 IP アドレスとポート番号に対応した複数の TCP、UDP リスニングサービスを設定することができます。リスニングサービスは NQA サーバで固有にする必要があります。IP アドレスとポート番号は NQA クライアントで設定された IP アドレスとポート番号と同一にする必要があります。

以下に NQA サーバの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． NQA サーバを有効にする	**nqa server enable**	デフォルト：無効
3． TCP、UDP リスニングサービスを設定する	● TCPリスニングサービスを設定する： **nqa server tcp-connect** *ip-address port-number* [**tos** *tos*] ● UDPリスニングサービスを設定する： **nqa server udp-echo** *ip-address port-number* [**tos** *tos*]	NQAサーバによって送信された応答パケットのIPパケットヘッダのToS値を指定することができます。 デフォルトのToS値：0

6.4 NQAクライアントの有効化

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． NQA クライアントを有効にする	**nqa agent enable**	デフォルト：有効 NQAクライアントを有効にしたのちNQAの設定が適用されます。

6.5 NQAクライアントのNQAテストの設定

6.5.1 NQA テストの設定作業リスト

作業リスト
（必須設定項目） 少なくとも1つを設定してください。 • ICMPエコーテストの設定 • DHCPテストの設定 • DNSテストの設定 • FTPテストの設定 • HTTPテストの設定 • UDPジッタテストの設定 • SNMPテストの設定 • TCPテストの設定 • UDPエコーテストの設定 • 音声テストの設定 • DLSwテストの設定
（オプション設定項目） NQAテストのオプションパラメータの設定
（オプション設定項目） しきい値監視機能の設定
（オプション設定項目） NQA統計情報収集機能の設定
（オプション設定項目） NQA履歴記録保存の設定
（必須設定項目） NQAクライアントにおけるNQAスケジューリング

6.5.2 ICMP エコーテストの設定

ICMP エコーテストは宛先装置の到達可能性をテストします。ICMP エコーテストは **ping** コマンドと同等の機能ですが、さらに詳細な情報が得られます。送信元と宛先間で複数のパスがある場合、ICMP エコーテストでネクストホップを指定できます。

IPv6 ネットワークでは NQA ICMP エコーテストはサポートしていません。IPv6 アドレスの到達可能性をテストする場合には、**ping ipv6** コマンドを使用してください。詳細はコマンドマニュアルのセクション 9 *システム管理* "*システムの保守とデバッグ*"を参照してください。

以下に ICMP エコーテストの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. NQA テストを作成し、NQA operation view に移行する	**nqa entry** *admin-name operation-tag*	デフォルト：設定なし
3. ICMP エコータイプを指定し、その view に移行する	**type icmp-echo**	—
4. ICMP エコーリクエストの宛先アドレスを指定する	**destination ip** *ip-address*	デフォルト：設定なし

操作	コマンド	補足
5.　（オプション設定項目）各 ICMP エコーリクエストのペイロードサイズを指定する	**data-size** *size*	デフォルト：100バイト
6.　（オプション設定項目）各 ICMP エコーリクエストのペイロードに入る文字列を指定する	**data-fill** *string*	デフォルト：0010203040506070809（16進数表示）
7.　（オプション設定項目）ICMP エコーリクエストの送信元 IP アドレスを指定する	● 送信元インタフェースを指定する： **source interface** *interface-type interface-number* ● 送信元IPアドレスを指定する： **source ip** *ip-address*	デフォルト：設定なし ICMPエコー要求パケットは送信元IPアドレスとして送信インタフェースのプライマリIPアドレスを使用します。 指定されていない場合、送信元IPアドレスとして出力インタフェースのプライマリIPアドレスが適用されます。 **source ip**コマンドと**source interface**コマンドの両方が設定された場合、最後に設定したコマンドが適用されます。 指定した送信元インタフェースはアップ状態でなくてはいけません。 送信元IPアドレスはローカルインタフェースのIPアドレスで、アップ状態でなくてはいけません。そうでなければICMPエコーテストに失敗します。
8.　（オプション設定項目）ICMP エコーリクエストのネクストホップを指定する	**next-hop** *ip-address*	デフォルト：設定なし

6.5.3 DHCP テストの設定

DHCP テストは、DHCP サーバが DHCP クライアントリクエストに応答できるかどうかをテストします。また DHCP サーバから IP アドレスを取得する時間を計測することができます。

NQA クライアントは、DHCP サーバから IP アドレスを取得するために DHCP リクエストを転送する DHCP リレーエージェントをテストします。DHCP テストを実行するインタフェースはインタフェースの IP アドレスを変更しません。DHCP テストを完了した場合、取得した IP アドレスを解放するため、NQA クライアントはパケットを送信します。

以下に DHCP テストの設定を示します。

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

操作	コマンド	補足
2． NQA テストを作成し、NQA operation view に移行する	**nqa entry** *admin-name operation-tag*	デフォルト：設定なし
3． DHCP タイプを指定し、その view に移行する	**type dhcp**	―
4． DHCP パケットの宛先 IP アドレスとして DHCP サーバの IP アドレスを指定する	**destination ip** *ip-address*	デフォルト：設定なし
5． （オプション設定項目）DHCP リクエストパケットの送信元 IP アドレスを指定する	**source ip** *ip-address*	デフォルト：設定なし ICMPエコー要求パケットは送信元IPアドレスとして送信インタフェースのプライマリIPアドレスを使用します。 指定する送信元IPアドレスはローカルインタフェースのIPアドレスにする必要があります。またローカルインタフェースはアップ状態にする必要があります。そうでない場合、プローブパケットを送信できません。 NQAクライアントはDHCPサーバに送信するDHCP要求の**giaddr**フィールドに送信元IPアドレスを追加します。

6.5.4 DNS テストの設定

DNS テストは DNS クライアントが DNS サーバを通してドメイン名を IP アドレスに変換する時間を測定します。

DNS テストは DNS 解決をテストします。取得した DNS エントリは保存しません。

以下に DNS テストの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． NQA テストを作成し、NQA operation view に移行する	**nqa entry** *admin-name operation-tag*	デフォルト：設定なし
3． DNS タイプを指定し、その view に移行する	**type dns**	―
4． DNS パケットの宛先アドレスとして DNS サーバの IP アドレスを指定する	**destination ip** *ip-address*	デフォルト：設定なし
5． 変換に必要なドメイン名を指定する	**resolve-target** *domain-name*	デフォルト：設定なし

6.5.5 FTP テストの設定

FTP テストは NQA クライアントが FTP サーバからファイルを転送するかダウンロードする時間をテストします。

FTP テストを設定する場合、以下の制限とガイドラインに従ってください。

- **filename** コマンドが設定され、**put** オペレーションが行われる場合、NQA クライアントにファイルが存在することを確認してください。
- FTP サーバからファイルを取得するために **get** オペレーションを行う場合、FTP サーバの指定した URL にファイルが存在することを確認してください。
- NQA クライアントは FTP サーバから取得したファイルを保存しません。
- FTP テストを行う場合、小さいサイズのファイルを使用してください。大きいサイズのファイルは、タイムアウトでテストが失敗したり、ネットワークの帯域幅以上を独占して他のサービスに影響を与えたりする可能性があります。

以下に FTP テストの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. NQA テストを作成し、NQA operation view に移行する	**nqa entry** *admin-name operation-tag*	デフォルト：設定なし
3. FTP タイプを指定し、その view に移行する	**type ftp**	―
4. 宛先の FTP サーバの URL を指定する	**url** *url*	デフォルト：指定なし 以下のいずれかのフォーマットでURLを入力します。 ● ftp://*host*/*filename* ● ftp://*host*:*port*/*filename* **get**オペレーションを行う場合、ファイル名が必要です。
5. （オプション設定項目）FTP リクエストパケットの送信元 IP アドレスを指定する	**source ip** *ip-address*	デフォルト：設定なし ICMPエコー要求パケットは送信元IPアドレスとして送信インタフェースのプライマリIPアドレスを使用します。 送信元IPアドレスはローカルインタフェースのIPアドレスにする必要があります。またローカルインタフェースはアップ状態にする必要があります。そうでない場合、FTPは送信できません。
6. FTP のオペレーションタイプを指定する	**operation** { **get** | **put** }	デフォルト：**get** FTPサーバからファイルを取得します。
7. FTP ログインユーザ名を指定する	**username** *username*	デフォルト：設定なし
8. FTP ログインパスワードを指定する	**password** { **cipher** | **simple** } *string*	デフォルト：設定なし

操作	コマンド	補足
9.　（オプション設定項目）転送されるファイル名を指定する	**filename** *file-name*	デフォルト：設定なし この操作は**put**オペレーションが行われる場合に必要です。

6.5.6 HTTP テストの設定

HTTP テストは NQA クライアントが HTTP サーバからデータを取得する時間をテストします。

以下に HTTP テストの設定を示します。

操作	コマンド	補足
1.　system view に移行する	**system-view**	―
2.　NQA テストを作成し、NQA operation view に移行する	**nqa entry** *admin-name operation-tag*	デフォルト：設定なし
3.　HTTP タイプを指定し、その view に移行する	**type http**	―
4.　宛先の HTTP サーバの URL を指定する	**url** *url*	デフォルト：指定なし 以下のいずれかのフォーマットでURLを入力します。 ● http://*host*/*resource* ● http://*host*:*port*/*resource*
5.　HTTP ログインユーザ名を指定する	**username** *username*	デフォルト：設定なし
6.　HTTP ログインパスワードを指定する	**password** { **cipher** | **simple** } *password*	デフォルト：設定なし
7.　（オプション設定項目）リクエストパケットの送信元 IP アドレスを指定する	**source ip** *ip-address*	デフォルト：設定なし ICMPエコー要求パケットは送信元IPアドレスとして送信インタフェースのプライマリIPアドレスを使用します。 送信元IPアドレスはローカルインタフェースのIPアドレスにする必要があります。またローカルインタフェースはアップ状態にする必要があります。そうでない場合、リクエストは送信できません。
8.　（オプション設定項目）HTTP オペレーションタイプを指定する	**operation** { **get** | **post** }	デフォルト：**get** HTTPサーバからファイルを取得します。
9.　（オプション設定項目）HTTP バージョンを指定する	**version** { **v1.0** | **v1.1** }	デフォルト：HTTP 1.0

6.5.7 UDP ジッタテストの設定

⚠ **注意：**
UDP ジッタテストをポート番号 1～1023 で行わないでください。1～1023 を使用した場合 NQA テストは失敗するか、このポートに該当するサービスが動作しなくなります。

ジッタは相互のパケット遅延の変動値を意味します。UDP ジッタテストはネットワークで音声サービスやビデオサービスなどのジッタに敏感なリアルタイムサービスを行えるかどうか確認するため、片方向、双方向のジッタをテストします。

UDP ジッタテストは以下のように動作します。

1) NQA クライアントは通常の間隔で宛先ポートに UDP パケットを送信します。
2) 宛先装置は、受信した各パケットにタイムスタンプを追加し、NQA クライアントにパケットを送り返します。
3) 応答を受信すると、NQA クライアントは、タイムスタンプに従ってジッタを計算します。

UDP ジッタテストは、NQA サーバと NQA クライアントの両方が必要です。UDP ジッタテストを実行する前に、NQA サーバで UDP リスニングサービスの設定を行う必要があります。UDP リスニングサービスの詳細は、コマンドマニュアルのセクション 9 *システム管理* "*NQA*"の"*NQA サーバの設定*"を参照してください。

以下に UDP ジッタテストの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. NQA テストを作成し、NQA operation view に移行する	**nqa entry** *admin-name operation-tag*	デフォルト：設定なし
3. UDP ジッタタイプを指定し、その view に移行する	**type udp-jitter**	―
4. UDP パケットの宛先アドレスを指定する	**destination ip** *ip-address*	デフォルト：設定なし 宛先アドレスはNQAサーバでリスニングサービスを行っているIPアドレスと同一です。サーバでUDPリスニングサービスを設定するには、**nqa server udp-echo**コマンドを使用します。
5. UDP パケットの宛先ポートを指定する	**destination port** *port-number*	デフォルト：設定なし 宛先ポートはNQAサーバでリスニングサービスを行っているポート番号と同一です。サーバでUDPリスニングサービスを設定するには、**nqa server udp-echo**コマンドを使用します。

操作	コマンド	補足
6.　（オプション設定項目）UDP パケットの送信元 IP アドレスを指定する	**source ip** *ip-address*	デフォルト：l設定なし CMPエコー要求パケットは送信元IPアドレスとして送信インタフェースのプライマリIPアドレスを使用します。 送信元IPアドレスはローカルインタフェースのIPアドレスにする必要があります。またローカルインタフェースはアップ状態にする必要があります。そうでない場合、UDPパケットは送信できません。
7.　（オプション設定項目）UDP パケットの送信元ポート番号を指定する	**source port** *port-number*	デフォルト：設定なし
8.　（オプション設定項目）各 UDP パケットのペイロードサイズを指定する	**data-size** *size*	デフォルト：100バイト
9.　（オプション設定項目）各 UDP パケットのペイロードで使われる文字列を指定する	**data-fill** *string*	デフォルト：0001020304050607080 9（16進数表示）
10.　（オプション設定項目）UDP ジッタテストで送信する UDP パケット数を指定する	**probe packet-number** *packet-number*	デフォルト：10
11.　（オプション設定項目）UDP パケットを送信する間隔を設定する	**probe packet-interval** *interval*	デフォルト：20ミリ秒
12.　（オプション設定項目）NQA クライアントの UDP パケットの受信待ち時間を指定する	**probe packet-timeout** *timeout*	デフォルト：3000ミリ秒

🕮 **メモ：**

display nqa result コマンドあるいは **display nqa statistics** コマンドを使用して UDP ジッタテストを確認してください。**display nqa history** コマンドは、UDP ジッタテストの結果や統計情報を表示しません。

6.5.8 SNMP テストの設定

SNMP テストは NQA クライアントが SNMP パケットを SNMP エージェントに送信し、SNMP エージェントから応答パケットを受信する時間を測定します。

以下に SNMP テストの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. NQA テストを作成し、NQA operation view に移行する	**nqa entry** *admin-name operation-tag*	デフォルト：設定なし
3. SNMP タイプを指定し、その view に移行する	**type snmp**	―
4. SNMP パケットの宛先アドレスを指定する	**destination ip** *ip-address*	デフォルト：設定なし
5. （オプション設定項目）SNMP パケットの送信元ポート番号を指定する	**source port** *port-number*	デフォルト：設定なし
6. （オプション設定項目）SNMP パケットの送信元 IP アドレスを指定する	**source ip** *ip-address*	デフォルト：設定なし ICMPエコー要求パケットは送信元IPアドレスとして送信インタフェースのプライマリIPアドレスを使用します。 送信元IPアドレスはローカルインタフェースのIPアドレスにする必要があります。またローカルインタフェースはアップ状態にする必要があります。そうでない場合、SNMPパケットは送信できません。

6.5.9 TCP テストの設定

TCP テストは、NQA クライアントと NQA サーバ上のポート間で TCP 接続が確立される時間を測定するために使われます。これにより指定したサーバのポートの有効性と能力を判断します。

TCP テストは NQA サーバと NQA クライアントの両方が必要です。TCP テストを実行する前に、NQA サーバで TCP リスニングサービスの設定を行う必要があります。TCP リスニングサービスの詳細は、オペレーションマニュアルのセクション 9 *システム管理*"*NQA*"の"*NQA サーバの設定*"を参照してください。

以下に TCP テストの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. NQA テストを作成し、NQA operation view に移行する	**nqa entry** *admin-name operation-tag*	デフォルト：設定なし
3. TCP タイプを指定し、その view に移行する	**type tcp**	―

操作	コマンド	補足
4. TCP パケットの宛先アドレスを指定する	**destination ip** *ip-address*	デフォルト：設定なし 宛先アドレスはNQAサーバでリスニングサービスを行っているIPアドレスです。サーバでTCPリスニングサービスを設定するには、**nqa server tcp-connect**コマンドを使用します。
5. TCP パケットの宛先ポート番号を指定する	**destination port** *port-number*	デフォルト：設定なし 宛先ポート番号はNQAサーバでリスニングサービスを行っているポート番号です。サーバでTCPリスニングサービスを設定するには、**nqa server tcp-connect**コマンドを使用します。
6. （オプション設定項目）TCP パケットの送信元 IP アドレスを指定する	**source ip** *ip-address*	デフォルト：設定なし ICMPエコー要求パケットは送信元IPアドレスとして送信インタフェースのプライマリIPアドレスを使用します。 送信元IPアドレスはローカルインタフェースのIPアドレスにする必要があります。またローカルインタフェースはアップ状態にする必要があります。そうでない場合、TCPパケットは送信できません。

6.5.10 UDP エコーテストの設定

UDP エコーテストはクライアントと NQA サーバの UDP ポート間のラウンドトリップ時間をテストします。

UDP エコーテストは、NQA サーバと NQA クライアントの両方が必要です。UDP エコーテストを行う前に、NQA サーバで UDP をリスニングするサービスを設定してください。UDP リスニングサービスの詳細は、コマンドマニュアルのセクション 9 *システム管理* "*NQA*"の"*NQA サーバの設定*"を参照してください。

以下に UDP エコーテストの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. NQA テストを作成し、NQA operation view に移行する	**nqa entry** *admin-name operation-tag*	デフォルト：設定なし
3. UDP エコータイプを指定し、その view に移行する	**type udp-echo**	―

操作	コマンド	補足
4. UDP パケットの宛先アドレスを指定する	**destination ip** *ip-address*	デフォルト：設定なし 宛先アドレスは、NQAサーバでリスニングサービスが設定されたIPアドレスと同一でなくてはいけません。サーバでUDPリスニングサービスを設定するには、**nqa server udp-echo**コマンドを使用します。
5. UDP パケットの宛先ポートを指定する	**destination port** *port-number*	デフォルト：設定なし 宛先ポート番号は、NQAサーバでリスニングサービスが設定されたポート番号と同一でなくてはいけません。サーバでUDPリスニングサービスを設定するには、**nqa server udp-echo**コマンドを使用します。
6. （オプション設定項目）各 UDP パケットのペイロードサイズを指定する	**data-size** *size*	デフォルト：100バイト
7. （オプション設定項目）各 UDP パケットのペイロードに入る文字列を指定する	**data-fill** *string*	デフォルト：0010203040506070809（16進数表示
8. （オプション設定項目）UDP パケットの送信元ポートを指定する	**source port** *port-number*	デフォルト：設定なし
9. （オプション設定項目）UDP パケットの送信元 IP アドレスを指定する	**source ip** *ip-address*	デフォルト：設定なし ICMPエコー要求パケットは送信元IPアドレスとして送信インタフェースのプライマリIPアドレスを使用します。 送信元IPアドレスは、ローカルインタフェースのIPアドレスで、アップ状態でなくてはいけません。 そうでなければUDPパケットが送信できません。

6.5.11 音声テストの設定

注意：
音声テストでポート 1～1023 を使用しないでください。1～1023 を使用した場合、このポートに関連したサービスが使えなくなります。

音声テストは VoIP ネットワーク性能を測定します。

音声テストは以下のように動作します。

1) NQA クライアントは指定した間隔で音声パケットを宛先装置（NQA サーバ）に送信します。

   音声パケットは以下のコーデックタイプがあります。

   - G.711 A-law
   - G.711 μ-law
   - G.729 A-law

2) 宛先装置は、受信した各音声パケットにタイムスタンプを追加し、NQA クライアントにパケットを送り返します。
3) 応答を受信すると、NQA クライアントは、タイムスタンプに従ってジッタと 1 方向遅延を計算します。

VoIP ネットワーク性能に反映される以下のパラメータは、音声テストによって収集されたメトリックを使用して計算することができます。

- **ICPIF（Calculated Planning Impairment Factor）**－パケットのロスや遅延による VoIP ネットワークの音声データの減衰を測定します。高い値は低いサービス品質を表します。
- **MOS（Mean Opinion Scores）**－ICPIF を使用して得られた 1～5 の MOS の値です。高い値は高いサービス品質を表します。

音声品質の評価は、ユーザの音声品質の許容度に依存します。音声品質に高い許容度を持つユーザの場合、アドバンテージファクタの設定を行う **advantage-factor** コマンドを使用します。システムが ICPIF 値を計算する場合、音声品質の評価用に ICPIF と MOS の値を修正するため、アドバンテージファクタが取りはずされます。

音声テストは、NQA サーバと NQA クライアントの両方が必要です。音声テストを実行する前に、NQA サーバで UDP リスニングサービスの設定を行う必要があります。UDP リスニングサービスの詳細は、コマンドマニュアルのセクション 9 *システム管理* "*NQA*"の "*NQA サーバの設定*"を参照してください。

1 回の音声テストで 1 回のテストが行われます。

以下に音声テストの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	－
2． NQA テストを作成し、NQA operation view に移行する	**nqa entry** *admin-name operation-tag*	デフォルト：設定なし
3． 音声タイプを指定し、その view に移行する	**type voice**	－
4． 音声パケットの宛先 IP アドレスを指定する	**destination ip** *ip-address*	デフォルト：設定なし 宛先アドレスは、NQAサーバでリスニングサービスが設定されたIPアドレスと同一でなくてはいけません。サーバでUDPリスニングサービスを設定するには、**nqa server udp-echo**コマンドを使用します。

操作	コマンド	補足
5. 音声パケットの宛先ポートを指定する	**destination port** *port-number*	デフォルト：設定なし 宛先ポートはNQAサーバでリスニングサービスを行っているポート番号です。サーバでUDPリスニングサービスを設定するには、**nqa server udp-echo**コマンドを使用します。
6. （オプション設定項目）コーデックタイプを指定する	**codec-type** { **g711a** | **g711u** | **g729a** }	デフォルト：G.711 A-law
7. （オプション設定項目）計算される MOS と ICPIF 値のアドバンテージファクタを設定する	**advantage-factor** *factor*	デフォルト：0
8. （オプション設定項目）音声パケットの送信元 IP アドレスを指定する	**source ip** *ip-address*	デフォルト： ICMPエコー要求パケットは送信元IPアドレスとして送信インタフェースのプライマリIPアドレスを使用します。 送信元IPアドレスはローカルインタフェースのIPアドレスにする必要があります。またローカルインタフェースはアップ状態にする必要があります。そうでない場合、音声パケットは送信できません。
9. （オプション設定項目）音声パケットの送信元ポート番号を指定する	**source port** *port-number*	デフォルト：設定なし
10. （オプション設定項目）音声パケットのペイロードサイズを指定する	**data-size** *size*	デフォルト：コーデックタイプによって異なります。 G.711A-law、G.711 μ-lawは172バイト、G.729 A-lawは32バイトです。
11. （オプション設定項目）各 UDP パケットのペイロードで使われる文字列を指定する	**data-fill** *string*	デフォルト： 00010203040506070809（16進数表示）
12. （オプション設定項目）音声テストで送信する UDP パケット数を指定する	**probe packet-number** *packet-number*	デフォルト：1000
13. （オプション設定項目）音声パケットを送信する間隔を設定する	**probe packet-interval** *interval*	デフォルト：20ミリ秒
14. （オプション設定項目）NQA クライアントの音声パケットの受信待ち時間を指定する	**probe packet-timeout** *timeout*	デフォルト：5000ミリ秒

🕮 **メモ：**

display nqa result コマンドあるいは **display nqa statistics** コマンドを使用して音声テストを確認してください。**display nqa history** コマンドは、音声テストの結果や統計情報を表示しません。

6.5.12 DLSw テストの設定

DLSw テストは DLSw 装置の応答時間を測定します。

以下に DLSw テストの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． NQA テストを作成し、NQA operation view に移行する	**nqa entry** *admin-name operation-tag*	デフォルト：設定なし
3． DLSw タイプを指定し、その view に移行する	**type dlsw**	―
4． プローブパケットの宛先 IP アドレスを指定する	**destination ip** *ip-address*	デフォルト：設定なし
5． （オプション設定項目）プローブパケットの送信元 IP アドレスを指定する	**source ip** *ip-address*	デフォルト : ICMPエコー要求パケットは送信元IPアドレスとして送信インタフェースのプライマリIPアドレスを使用します。 送信元IPアドレスはローカルインタフェースのIPアドレスにする必要があります。またローカルインタフェースはアップ状態にする必要があります。そうでない場合、プローブパケットは送信できません。

6.5.13 NQA テストのオプションパラメータの設定

テストグループを指定しない場合、パラメータはすべてのテストタイプに適用されます。

NQA テストのオプションパラメータは 1 回のテストのみ有効です。

以下に NQA テストのオプションパラメータの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． NQA テストを作成し、NQA operation view に移行する	**nqa entry** *admin-name operation-tag*	デフォルト：設定なし

操作	コマンド	補足
3． NQA テストタイプを指定し、その view に移行する	**type** { **dhcp** | **dlsw** | **dns** | **ftp** | **http** | **icmp-echo** | **snmp** | **tcp** | **udp-echo** | **udp-jitter** | **voice** }	ー
4． 説明を設定する	**description** *text*	デフォルト：設定なし
5． NQA テストを連続して行う間隔を指定する	**frequency** *interval*	デフォルト： 音声テストは6000ミリ秒、他のテストは0msです。 1回のテストで1回のテストが実行されます。 間隔が終了したとき、テストが完了していない場合、次のテストは開始しません。
6． 1 回の NQA テストの検査回数を指定する	**probe count** *times*	デフォルト：1回 音声テストでは無効です。1回のテストで1回のテストが実行されます。
7． NQA テストのタイムアウト時間を指定する	**probe timeout** *timeout*	デフォルト：3000ms UDPジッタテストと音声テストでは無効です。
8． テストパケットの TTL を指定する	**ttl** *value*	デフォルト：20 DHCPテストでは無効です。
9． NQA テストパケットの IP パケットヘッダの ToS 値を設定する	**tos** *value*	デフォルト：0
10．ルーティングテーブルバイパス機能を有効にする	**route-option bypass-route**	デフォルト：無効 DHCPテストでは無効です。

6.5.14 しきい値監視機能の設定

I. しきい値タイプ

NQA テストは以下のしきい値タイプをサポートします。

- **average** – モニタリングされた性能の平均値が、上限あるいは下限を超えた場合、しきい値違反が発生します。
- **accumulate** – テストのモニタデータがしきい値を違反した回数の合計を監視します。回数の合計数が特定の値に達するか超えた場合、しきい値違反が発生します。
- **consecutive** – テストグループを開始してからのモニタデータのしきい値違反の連続回数を監視します。モニタデータのしきい値違反の連続回数が特定の回数になった場合、しきい値違反が発生します。

average、accumulate のしきい値タイプは NQA テストごとにカウントされますが、**consecutive** タイプはテストグループが開始されてからの時間となります。

II. トリガー動作

以下のアクションがトリガー動作となります。

- **none** － NQA は端末画面にのみ結果を表示します。NMS にトラップを送信しません。
- **trap-only** － NQA は端末画面に結果を表示します。NMS にトラップを送信します。
- **trigger-only** － NQA は端末画面に結果を表示します。コラボレーションに関連づけられたほかのモジュールにトラップを送信します。

QX シリーズはトリガー動作 **trigger-only** をサポートしていません。

III. リアクションエントリ

リアクションエントリでは、しきい値監視を行うため、監視対象、しきい値タイプ、トリガー動作を実装します。

リアクションエントリの状態には、無効、しきい値超過、しきい値未満があります。

- NQA のテストグループが開始する前は、リアクションエントリは無効の状態です。
- しきい値が違反している場合、エントリの状態はしきい値超過に設定されます。それ以外の場合、エントリの状態はしきい値未満に設定されています。

IV. 設定手順

しきい値監視の設定を行う前に、**snmp-agent target-host** コマンドを使用してトラップメッセージの宛先アドレスを設定してください。このコマンドの詳細は、コマンドマニュアルのセクション 9 *システム管理* "*SNMP*"を参照してください。

以下にしきい値監視機能の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	－
2． NQA テストを作成し、NQA operation view に移行する	**nqa entry** *admin-name operation-tag*	デフォルト：設定なし
3． NQA operation view に移行する	**type** { **dhcp** | **dlsw** | **dns** | **ftp** | **http** | **icmp-echo** | **snmp** | **tcp** | **udp-echo** | **udp-jitter** | **voice** }	－
4． 指定状況下になった場合ネットワーク管理サーバにトラップを送信する	**reaction trap** { **probe-failure** *consecutive-probe-failures* | **test-complete** | **test-failure** [*accumulate-probe-failures*] }	デフォルト：設定なし UDPジッタテストと音声テストは**test-complete**キーワードのみサポートしています。
5． しきい値監視機能を設定する	● 故障回数を監視する（UDPジッタテストと音声テストは未サポート）： **reaction** *item-number* **checked-element probe-fail threshold-type** { **accumulate** *accumulate-occurrences* | **consecutive** *consecutive-occurrences* } [**action-type none**]	－

6.5.15 NQA 統計情報収集機能の設定

NQA は統計情報グループとして同一の収集間隔で統計情報を収集します。統計情報グループについて情報を表示するには、**display nqa statistics** コマンドを使用します。

NQA は、1 回のみの NQA テストの統計情報グループを作成しません。**frequency** コマンドを使用し、テスト間隔を 0 に設定した場合、NQA は統計情報グループを作成しません。

以下に NQA 統計情報収集機能の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. NQA テストを作成し、NQA operation view に移行する	**nqa entry** *admin-name operation-tag*	デフォルト：設定なし
3. NQA テストタイプを指定し、その view に移行する	**type** { **dhcp** | **dlsw** | **dns** | **ftp** | **http** | **icmp-echo** | **snmp** | **tcp** | **udp-echo** | **udp-jitter** | **voice** }	ー
4. （オプション設定項目）統計情報を収集する間隔を指定する	**statistics interval** *interval*	デフォルト：60分
5. （オプション設定項目）保持する統計情報グループ数の最大値を設定する	**statistics max-group** *number*	デフォルト：2グループ 最大値を0に設定すると統計情報を収集しません。 統計グループが最大数となった場合、新しい統計情報グループを保存するため、一番古い統計情報グループが削除されます。
6. （オプション設定項目）統計情報グループの保持時間を指定する	**statistics hold-time** *hold-time*	デフォルト：120分 保持時間が終了した場合、統計グループは削除されます。

6.5.16 NQA 履歴記録保存の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. NQA テストを作成し、NQA operation view に移行する	**nqa entry** *admin-name operation-tag*	デフォルト：設定なし
3. NQA operation type view に移行する	**type** { **dhcp** | **dlsw** | **dns** | **ftp** | **http** | **icmp-echo** | **snmp** | **tcp** | **udp-echo** }	UDPジッタテストと音声テストは無効です。
4. NQA テストの履歴記録の保存を有効にする	**history-record enable**	デフォルト：無効
5. （オプション設定項目）履歴記録の保存期間を設定する	**history-record keep-time** *keep-time*	デフォルト：120分 保存期間が満了した場合記録が削除されます。
6. （オプション設定項目）履歴記録を保存できる最大数を指定する	**history-record number** *number*	デフォルト：50 最大数を超過した場合、一番古い履歴が削除されます。

操作	コマンド	補足
7.　（オプション設定項目）履歴記録を表示する	**display nqa history**	―

6.5.17 NQA クライアントにおける NQA テストのスケジューリング

指定した開始時間と終了時間（開始時間＋テスト間隔）を設定することにより、NQA テストグループをスケジューリングできます。指定した開始時間がシステム時間を過ぎていた場合、NQA テストはただちに開始します。開始時間と終了時間が共にシステム時間を過ぎていた場合、NQA テストは行われません。**display clock** コマンドにより現在のシステム時間を確認することができます。

以下に NQA テストのスケジューリングを設定する場合の制限とガイドラインを示します。

- NQA operation view あるいはスケジュールされた NQA テストの view に移行することはできません。
- システム時間を調整しても、開始されたあるいは終了した NQA テストには影響しません。開始する前の NQA テストはシステム時間の調整のみが適用されます。

以下に NQA クライアントにおける NQA テストをスケジューリングする設定を示します。

操作	コマンド
1.　system view に移行する	**system-view**
2.　NQA テストのスケジューリングのパラメータを指定する	**nqa schedule** *admin-name operation-tag* **start-time** { *hh:mm:ss* [*yyyy/mm/dd* | *mm/dd/yyyy*] | **now** } **lifetime** { *lifetime* | **forever** } [**recurring**]

6.6 NQAの表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
NQAテストの履歴記録を表示する	**display nqa history** [*admin-name operation-tag*]
NQAテストの最新の結果を表示する	**display nqa result** [*admin-name operation-tag*]
NQAテストの統計情報を表示する	**display nqa statistics** [*admin-name operation-tag*]
NQAサーバ状態を表示する	**display nqa server**

6.7 NQA設定例

6.7.1 ICMP エコーテスト設定例

I. ネットワーク要件

図 6-2に示すように、Device A から Device C を通して Device B へのラウンドトリップ時間をテストするため、NQA クライアントから ICMP エコーテストを設定します。Device A のネクストホップは Device C です。

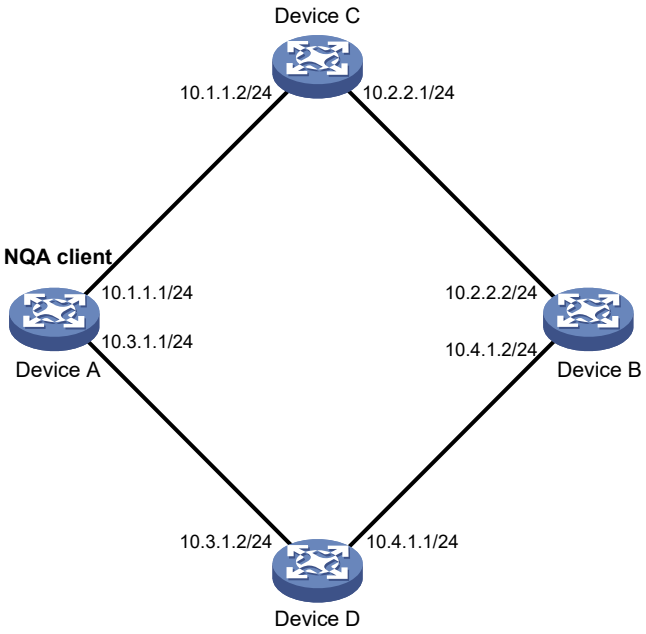


図 6-2 ネットワーク図

II. 設定手順

各インタフェースに IP アドレスを割り当てます。（詳細は省略します。）

Device が互いに通信できるようにスタティックルートあるいはルーティングプロトコルを設定します。（詳細は省略します。）

ICMP エコーテストを作成します。

```
<DeviceA> system-view
[DeviceA] nqa entry admin test1
[DeviceA-nqa-admin-test1] type icmp-echo
```

ICMP エコーリクエストの宛先 IP アドレスとして 10.2.2.2 を指定します。

```
[DeviceA-nqa-admin-test1-icmp-echo] destination ip 10.2.2.2
```

ネクストホップとして 10.1.1.2 を設定します。ICMP エコーリクエストは Device C から Device B に送信されます。

```
[DeviceA-nqa-admin-test1-icmp-echo] next-hop ip 10.1.1.2
```

ICMP エコーテストの検査回数を 10 回実行します。

```
[DeviceA-nqa-admin-test1-icmp-echo] probe count 10
```

ICMP エコーテストのタイムアウト時間を 500ms に指定します。

```
[DeviceA-nqa-admin-test1-icmp-echo] probe timeout 500
```

NQA テストを連続して行う間隔を 5000ms に設定します。

```
[DeviceA-nqa-admin-test1-icmp-echo] frequency 5000
```

NQA 履歴記録の保存を有効にします。

```
[DeviceA-nqa-admin-test1-icmp-echo] history-record enable
```

NQA 履歴記録の保存できる最大数を 10 に設定します。

```
[DeviceA-nqa-admin-test1-icmp-echo] history-record number 10
[DeviceA-nqa-admin-test1-icmp-echo] quit
```

ICMP エコーテストを開始します。

```
[DeviceA] nqa schedule admin test1 start-time now lifetime forever
```

ICMP エコーテスト開始から一定の時間が経過した後、テストを停止します。

```
[DeviceA] undo nqa schedule admin test1
```

ICMP エコーテストの最新の結果を表示します。

```
[DeviceA] display nqa result admin test1
NQA entry (admin admin, tag test1) test results:
    Send operation times: 10             Receive response times: 10
    Min/Max/Average round trip time: 2/5/3
    Square-Sum of round trip time: 96
    Last succeeded probe time: 2011-08-23 15:00:01.2
  Extended results:
    Packet loss ratio: 0%
    Failures due to timeout: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
```

ICMP エコーテストの履歴記録を表示します。

```
[DeviceA] display nqa history admin test1
NQA entry (admin admin, tag test) history records:
  Index      Response     Status           Time
  370        3            Succeeded        2007-08-23 15:00:01.2
  369        3            Succeeded        2007-08-23 15:00:01.2
  368        3            Succeeded        2007-08-23 15:00:01.2
  367        5            Succeeded        2007-08-23 15:00:01.2
  366        3            Succeeded        2007-08-23 15:00:01.2
  365        3            Succeeded        2007-08-23 15:00:01.2
  364        3            Succeeded        2007-08-23 15:00:01.1
  363        2            Succeeded        2007-08-23 15:00:01.1
  362        3            Succeeded        2007-08-23 15:00:01.1
  361        2            Succeeded        2007-08-23 15:00:01.1
```

出力では、Device A からのパケットが Device C を通して Device B に送信できることを示しています。NQA テスト中のパケットロスはありません。最小、最大、平均ラウンドトリップ時間はそれぞれ、2、5、3ms です。

6.7.2 DHCP テスト設定例

I. ネットワーク要件

図 6-3に示すように、Switch A が DHCP サーバ（Switch B）から IP アドレスを取得する時間をテストするため DHCP テストを設定します。

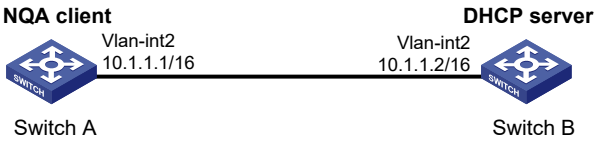


図 6-3 ネットワーク図

II. 設定手順

DHCP テストを作成します。

```
<SwitchA> system-view
[SwitchA] nqa entry admin test1
[SwitchA-nqa-admin-test1] type dhcp
```

宛先アドレスとして DHCP サーバの IP アドレス 10.1.1.2 を指定します。

```
[SwitchA-nqa-admin-test1-dhcp] destination ip 10.1.1.2
```

履歴記録を保存するように設定します。

```
[SwitchA-nqa-admin-test1-dhcp] history-record enable
[SwitchA-nqa-admin-test1-dhcp] quit
```

DHCP テストを開始します。

```
[SwitchA] nqa schedule admin test1 start-time now lifetime forever
```

DHCP テストを一定の期間実行したのち、テストを停止します。

```
[SwitchA] undo nqa schedule admin test1
```

DHCP テストの最新の結果を表示します。

```
[SwitchA] display nqa result admin test1
NQA entry (admin admin, tag test1) test results:
    Send operation times: 1              Receive response times: 1
    Min/Max/Average round trip time: 512/512/512
    Square-Sum of round trip time: 262144
    Last succeeded probe time: 2011-11-22 09:56:03.2
  Extended results:
    Packet loss ratio: 0%
    Failures due to timeout: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
```

DHCP テストの履歴記録を表示します。

```
[SwitchA] display nqa history admin test1
NQA entry (admin admin, tag test1) history records:
  Index      Response     Status           Time
  1          512          Succeeded        2011-11-22 09:56:03.2
```

出力では、Switch A が DHCP サーバから IP アドレスを取得するのに 512 ミリ秒かかることを示します。

6.7.3 DNS テスト設定例

I. ネットワーク要件

図 6-4に示すように、Device A が DHCP サーバから IP アドレスを取得するため DNS 解決時間の測定を行う DNS テストを設定します。



図 6-4 ネットワーク図

II. 設定手順

各インタフェースに IP アドレスを割り当てます。（詳細は省略します。）

Device が互いに通信できるようにスタティックルートあるいはルーティングプロトコルを設定します。（詳細は省略します。）

DNS テストを作成します。

```
<DeviceA> system-view
[DeviceA] nqa entry admin test1
[DeviceA-nqa-admin-test1] type dns
```

宛先アドレスとして DNS サーバの IP アドレス 10.2.2.2 を指定します。

```
[DeviceA-nqa-admin-test1-dns] destination ip 10.2.2.2
```

host.com のドメイン名に変換されるように指定します。

```
[DeviceA-nqa-admin-test1-dns] resolve-target host.com
```

履歴記録を保存するように設定します。

```
[DeviceA-nqa-admin-test1-dns] history-record enable
[DeviceA-nqa-admin-test1-dns] quit
```

DNS テストを開始します。

```
[DeviceA] nqa schedule admin test1 start-time now lifetime forever
```

DNS テストを一定の期間実行したのち、テストを停止します。

```
[DeviceA] undo nqa schedule admin test1
```

DNS テストの最新の結果を表示します。

```
[DeviceA] display nqa result admin test1
NQA entry (admin admin, tag test1) test results:
    Send operation times: 1              Receive response times: 1
    Min/Max/Average round trip time: 62/62/62
    Square-Sum of round trip time: 3844
    Last succeeded probe time: 2011-11-10 10:49:37.3
  Extended results:
    Packet loss ratio: 0%
    Failures due to timeout: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
```

DNS テストの履歴記録を表示します。

```
[DeviceA] display nqa history admin test1
NQA entry (admin admin, tag test) history records:
  Index      Response     Status           Time
  1          62           Succeeded        2011-11-10 10:49:37.3
```

出力では、Device A がドメイン名 host.com を IP アドレスに変換するのに 62 ミリ秒かかることを示します。

6.7.4 FTP テスト設定例

I. ネットワーク要件

図 6-5に示すように、Device A が FTP サーバにファイルをアップロードする時間を測定するために FTP テストを設定します。ログインユーザ名は admin、ログインパスワードは systemtest、FTP サーバに転送されるファイルは config.txt とします。



図 6-5 ネットワーク図

II. 設定手順

各インタフェースに IP アドレスを割り当てます。（詳細は省略します。）

Device が互いに通信できるようにスタティックルートあるいはルーティングプロトコルを設定します。（詳細は省略します。）

FTP テストを作成します。

```
<DeviceA> system-view
[DeviceA] nqa entry admin test1
[DeviceA-nqa-admin-test1] type ftp
```

FTP サーバの URL を指定します。

```
[DeviceA-nqa-admin-test-ftp] url ftp://10.2.2.2
```

送信元 IP アドレス 10.1.1.1 を指定します。

```
[DeviceA-nqa-admin-test1-ftp] source ip 10.1.1.1
```

Device が FTP サーバにファイル config.txt をアップロードするように設定します。

```
[DeviceA-nqa-admin-test1-ftp] operation put
[DeviceA-nqa-admin-test1-ftp] filename config.txt
```

FTP テストのユーザ名 admin を指定します。

```
[DeviceA-nqa-admin-test1-ftp] username admin
```

FTP テストのパスワード systemtest を指定します。

```
[DeviceA-nqa-admin-test1-ftp] password simple systemtest
```

履歴記録を保存するように設定します。

```
[DeviceA-nqa-admin-test1-ftp] history-record enable
[DeviceA-nqa-admin-test1-ftp] quit
```

FTP テストを開始します。

```
[DeviceA] nqa schedule admin test1 start-time now lifetime forever
```

FTP テストを一定期間実行したのち、テストを停止します。

```
[DeviceA] undo nqa schedule admin test1
```

FTP テストの最新の結果を表示します。

```
[DeviceA] display nqa result admin test1
NQA entry (admin admin, tag test1) test results:
    Send operation times: 1              Receive response times: 1
    Min/Max/Average round trip time: 173/173/173
    Square-Sum of round trip time: 29929
    Last succeeded probe time: 2011-11-22 10:07:28.6
  Extended results:
    Packet loss ratio: 0%
    Failures due to timeout: 0
    Failures due to disconnect: 0
    Failures due to no connection: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
```

FTP テストの履歴記録を表示します。

```
[DeviceA] display nqa history admin test1
NQA entry (admin admin, tag test1) history records:
  Index      Response     Status           Time
  1          173          Succeeded        2011-11-22 10:07:28.6
```

出力では、Device A が FTP サーバにファイルをアップロードするのに 173 ミリ秒かかることを示しています。

6.7.5 HTTP テスト設定例

I. ネットワーク要件

図 6-6に示すように HTTP サーバからデータを取得する時間をテストするため、NQA クライアントに HTTP テストを設定します。



図 6-6 ネットワーク図

II. 設定手順

各インタフェースに IP アドレスを割り当てます。（詳細は省略します。）

Device が互いに通信できるようにスタティックルートあるいはルーティングプロトコルを設定します。（詳細は省略します。）

HTTP テストを作成します。

```
<DeviceA> system-view
[DeviceA] nqa entry admin test1
[DeviceA-nqa-admin-test1] type http
```

HTTP サーバの URL を指定します。

```
[DeviceA-nqa-admin-test-http] url http://10.2.2.2/index.htm
```

HTTP サーバからデータを取得するように HTTP テストを設定します。

```
[DeviceA-nqa-admin-test1-http] operation get
```

HTTP version 1.0 を使用するように設定します。

```
[DeviceA-nqa-admin-test1-http] version v1.0
```

履歴記録を保存するように設定します。

```
[DeviceA-nqa-admin-test1-http] history-record enable
[DeviceA-nqa-admin-test1-http] quit
```

HTTP テストを開始します。

```
[DeviceA] nqa schedule admin test1 start-time now lifetime forever
```

HTTP テストを一定期間実行したのち、テストを停止します。

```
[DeviceA] undo nqa schedule admin test1
```

HTTP テストの最新の結果を表示します。

```
[DeviceA] display nqa result admin test1
NQA entry (admin admin, tag test1) test results:
    Send operation times: 1              Receive response times: 1
    Min/Max/Average round trip time: 64/64/64
    Square-Sum of round trip time: 4096
    Last succeeded probe time: 2011-11-22 10:12:47.9
  Extended results:
    Packet loss ratio: 0%
    Failures due to timeout: 0
    Failures due to disconnect: 0
    Failures due to no connection: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
```

HTTP テストの履歴記録を表示します。

```
[DeviceA] display nqa history admin test1
NQA entry (admin admin, tag test1) history records:
  Index      Response     Status           Time
  1          64           Succeeded        2011-11-22 10:12:47.9
```

出力では、Device A が HTTP サーバからデータを取得するのに 64 ミリ秒かかることを示します。

6.7.6 UDP ジッタテスト設定例

I. ネットワーク要件

図 6-7に示すように、Device A と Device B 間のジッタ、遅延、ラウンドトリップ時間を測定するため、UDP ジッタテストを設定します。



図 6-7 ネットワーク図

II. 設定手順

1) 各インタフェースに IP アドレスを割り当てます。（詳細は省略します。）
2) 各装置間で通信可能になるように、スタティックルートあるいはルーティングテーブルを設定します。（詳細は省略します。）
3) Device B を設定します。

NQA サーバを有効にします。

```
<DeviceB> system-view
[DeviceB] nqa server enable
```

IP アドレス 10.2.2.2、UDP ポート 9000 でリスニングサービスを設定します。

```
[DeviceB] nqa server udp-echo 10.2.2.2 9000
```

4)　Device A を設定します。

UDP ジッタテストを作成します。

```
<DeviceA> system-view
[DeviceA] nqa entry admin test1
[DeviceA-nqa-admin-test1] type udp-jitter
```

UDP ジッタテストの宛先 IP アドレス 10.2.2.2 を設定します。

```
[DeviceA-nqa-admin-test1-udp-jitter] destination ip 10.2.2.2
```

宛先ポート 9000 を設定します。

```
[DeviceA-nqa-admin-test1-udp-jitter] destination port 9000
```

1000 ミリ秒の間隔で UDP ジッタテストを繰り返すように設定します。

```
[DeviceA-nqa-admin-test1-udp-jitter] frequency 1000
[DeviceA-nqa-admin-test1-udp-jitter] quit
```

UDP ジッタテストを開始します。

```
[DeviceA] nqa schedule admin test1 start-time now lifetime forever
```

UDP ジッタテストを一定期間実行したのち、テストを停止します。

```
[DeviceA] undo nqa schedule admin test1
```

UDP ジッタテストの最新の結果を表示します。

```
[DeviceA] display nqa result admin test1
NQA entry (admin admin, tag test1) test results:
    Send operation times: 10              Receive response times: 10
    Min/Max/Average round trip time: 15/32/17
    Square-Sum of round trip time: 3235
    Last packet received time: 2011-05-29 13:56:17.6
  Extended results:
    Packet loss ratio: 0%
    Failures due to timeout: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
    Packets out of sequence: 0
    Packets arrived late: 0
  UDP-jitter results:
   RTT number: 10
    Min positive SD: 4                    Min positive DS: 1
    Max positive SD: 21                   Max positive DS: 28
    Positive SD number: 5                 Positive DS number: 4
    Positive SD sum: 52                   Positive DS sum: 38
    Positive SD average: 10               Positive DS average: 10
    Positive SD square-sum: 754           Positive DS square-sum: 460
    Min negative SD: 1                    Min negative DS: 6
    Max negative SD: 13                   Max negative DS: 22
    Negative SD number: 4                 Negative DS number: 5
    Negative SD sum: 38                   Negative DS sum: 52
    Negative SD average: 10               Negative DS average: 10
    Negative SD square-sum: 460           Negative DS square-sum: 754
    SD average: 10                         DS average: 10
  One way results:
```

```
    Max SD delay: 15                        Max DS delay: 16
    Min SD delay: 7                         Min DS delay: 7
    Number of SD delay: 10                  Number of DS delay: 10
    Sum of SD delay: 78                     Sum of DS delay: 85
    Square-Sum of SD delay: 666             Square-Sum of DS delay: 787
    SD lost packets: 0                    DS lost packets: 0
    Lost packets for unknown reason: 0
```

UDP ジッタテストの履歴記録を表示します。

```
[DeviceA] display nqa statistics admin test1
NQA entry (admin admin, tag test1) test statistics:
  NO. : 1
    Start time: 2011-05-29 13:56:14.0
    Life time: 47 seconds
    Send operation times: 410            Receive response times: 410
    Min/Max/Average round trip time: 1/93/19
    Square-Sum of round trip time: 206176
  Extended results:
    Packet loss ratio: 0%
    Failures due to timeout: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
    Packets out of sequence: 0
    Packets arrived late: 0
  UDP-jitter results:
   RTT number: 410
    Min positive SD: 3                      Min positive DS: 1
    Max positive SD: 30                     Max positive DS: 79
    Positive SD number: 186                 Positive DS number: 158
    Positive SD sum: 2602                   Positive DS sum: 1928
    Positive SD average: 13                 Positive DS average: 12
    Positive SD square-sum: 45304           Positive DS square-sum: 31682
    Min negative SD: 1                      Min negative DS: 1
    Max negative SD: 30                     Max negative DS: 78
    Negative SD number: 181                 Negative DS number: 209
    Negative SD sum: 181                    Negative DS sum: 209
    Negative SD average: 13                 Negative DS average: 14
    Negative SD square-sum: 46994           Negative DS square-sum: 3030
    SD average: 9                            DS average: 1
  One way results:
    Max SD delay: 46                        Max DS delay: 46
    Min SD delay: 7                         Min DS delay: 7
    Number of SD delay: 410                 Number of DS delay: 410
    Sum of SD delay: 3705                   Sum of DS delay: 3891
    Square-Sum of SD delay: 45987           Square-Sum of DS delay: 49393
    SD lost packets: 0                    DS lost packets: 0
    Lost packets for unknown reason: 0
```

6.7.7 SNMP テスト設定例

I. ネットワーク要件

図 6-8に示すように、NQA クライアントが SNMP エージェントから応答を取得する時間を測定するため、SNMP テストを設定します。



図 6-8 ネットワーク図

II. 設定手順

1) 各インタフェースに IP アドレスを割り当てます。（詳細は省略します。）
2) 各装置間で通信可能になるように、スタティックルートあるいはルーティングテーブルを設定します。（詳細は省略します。）
3) SNMP エージェント（Device B）を設定します。

SNMP のバージョンを all に設定します。

```
<DeviceB> system-view
[DeviceB] snmp-agent sys-info version all
```

read コミュニティを public に設定します。

```
[DeviceB] snmp-agent community read public
```

write コミュニティを private に設定します。

```
[DeviceB] snmp-agent community write private
```

4) Device A を設定します。

SNMP テストを作成します。

```
<DeviceA> system-view
[DeviceA] nqa entry admin test1
[DeviceA-nqa-admin-test1] type snmp
```

SNMP テストの宛先 IP アドレスを 10.2.2.2 に設定します。

```
[DeviceA-nqa-admin-test1-snmp] destination ip 10.2.2.2
```

履歴記録を保存するように設定します。

```
[DeviceA-nqa-admin-test1-snmp] history-record enable
[DeviceA-nqa-admin-test1-snmp] quit
```

SNMP テストを開始します。

```
[DeviceA] nqa schedule admin test1 start-time now lifetime forever
```

SNMP テストを一定期間実行したのち、テストを停止します。

```
[DeviceA] undo nqa schedule admin test1
```

SNMP テストの最新の結果を表示します。

```
[DeviceA] display nqa result admin test1
NQA entry (admin admin, tag test1) test results:
    Send operation times: 1              Receive response times: 1
    Min/Max/Average round trip time: 50/50/50
    Square-Sum of round trip time: 2500
    Last succeeded probe time: 2011-11-22 10:24:41.1
  Extended results:
    Packet loss ratio: 0%
    Failures due to timeout: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
```

SNMP テストの履歴記録を表示します。

```
[DeviceA] display nqa history admin test1
NQA entry (admin admin, tag test1) history records:
  Index      Response     Status           Time
  1          50           Succeeded        2011-11-22 10:24:41.1
```

出力では、Device A が SNMP エージェントから応答を受信するのに 50 ミリ秒かかることを示します。

6.7.8 TCP テスト設定例

I. ネットワーク要件

図 6-9に示すように、NQA クライアントが Device B の NQA サーバに TCP 接続を確立するまでの時間を測定するために TCP テストを設定します。



図 6-9 ネットワーク図

II. 設定手順

1) 各インタフェースに IP アドレスを割り当てます。（詳細は省略します。）
2) 各装置間で通信可能になるように、スタティックルートあるいはルーティングテーブルを設定します。（詳細は省略します。）
3) Device B を設定します。

NQA サーバを有効にします。

```
<DeviceB> system-view
[DeviceB] nqa server enable
```

IP アドレス 10.2.2.2、TCP ポート 9000 でリスニングサービスを設定します。

```
[DeviceB] nqa server tcp-connect 10.2.2.2 9000
```

4) Device A を設定します。

TCP テストを作成します。

```
<DeviceA> system-view
[DeviceA] nqa entry admin test1
[DeviceA-nqa-admin-test1] type tcp
```

宛先 IP アドレスを 10.2.2.2 に設定します。

```
[DeviceA-nqa-admin-test1-tcp] destination ip 10.2.2.2
```

宛先ポート番号を 9000 に設定します。

```
[DeviceA-nqa-admin-test1-tcp] destination port 9000
```

履歴記録を保存するように設定します。

```
[DeviceA-nqa-admin-test1-tcp] history-record enable
[DeviceA-nqa-admin-test1-tcp] quit
```

TCP テストを開始します。

```
[DeviceA] nqa schedule admin test1 start-time now lifetime forever
```

TCP テストを一定期間実行したのち、テストを停止します。

```
[DeviceA] undo nqa schedule admin test1
```

TCP テストの最新の結果を表示します。

```
[DeviceA] display nqa result admin test1
NQA entry (admin admin, tag test1) test results:
    Send operation times: 1              Receive response times: 1
    Min/Max/Average round trip time: 13/13/13
    Square-Sum of round trip time: 169
    Last succeeded probe time: 2011-11-22 10:27:25.1
  Extended results:
    Packet loss ratio: 0%
    Failures due to timeout: 0
    Failures due to disconnect: 0
    Failures due to no connection: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
```

TCP テストの履歴記録を表示します。

```
[DeviceA] display nqa history admin test1
NQA entry (admin admin, tag test1) history records:
  Index      Response     Status           Time
  1          13           Succeeded        2011-11-22 10:27:25.1
```

出力では、Device A が NQA サーバのポート 9000 と TCP 接続を確立するのに 13 ミリ秒かかることを示します。

6.7.9 UDP エコーテスト設定例

I. ネットワーク要件

図 6-10に示すように、Device A と Device B 間のラウンドトリップ時間をテストするように、UDP エコーテストを設定します。宛先ポート番号は 8000 番です。



図 6-10 ネットワーク図

II. 設定手順

1) 各インタフェースに IP アドレスを割り当てます。（詳細は省略します。）
2) Device が互いに通信できるようにスタティックルートあるいはルーティングプロトコルを設定します。（詳細は省略します。）
3) Device B を設定します。

NQA サーバを有効にします。

```
<DeviceB> system-view
[DeviceB] nqa server enable
```

IP アドレス 10.2.2.2、UDP ポート 8000 をリスニングするように設定します。

```
[DeviceB] nqa server udp-echo 10.2.2.2 8000
```

4) Device A を設定します。

UDP エコーテストを作成します。

```
<DeviceA> system-view
[DeviceA] nqa entry admin test1
[DeviceA-nqa-admin-test1] type udp-echo
```

宛先 IP アドレスを 10.2.2.2 に設定します。

```
[DeviceA-nqa-admin-test1-udp-echo] destination ip 10.2.2.2
```

宛先ポート番号を 8000 に設定します。

```
[DeviceA-nqa-admin-test1-udp-echo] destination port 8000
```

履歴記録を保存するように設定します。

```
[DeviceA-nqa-admin-test1-udp-echo] history-record enable
[DeviceA-nqa-admin-test1-udp-echo] quit
```

UDP エコーテストを開始します。

```
[DeviceA] nqa schedule admin test1 start-time now lifetime forever
```

UDP エコーテストを一定期間実行したのち、テストを停止します。

```
[DeviceA] undo nqa schedule admin test1
```

UDP エコーテストの最新の結果を表示します。

```
[DeviceA] display nqa result admin test1
NQA entry (admin admin, tag test1) test results:
    Send operation times: 1              Receive response times: 1
    Min/Max/Average round trip time: 25/25/25
    Square-Sum of round trip time: 625
    Last succeeded probe time: 2011-11-22 10:36:17.9
  Extended results:
    Packet loss ratio: 0%
    Failures due to timeout: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
```

UDP エコーテストの履歴記録を表示します。

```
[DeviceA] display nqa history admin test1
NQA entry (admin admin, tag test1) history records:
  Index      Response     Status           Time
  1          25           Succeeded        2011-11-22 10:36:17.9
```

出力は、Device A と Device B のポート 8000 番の間のラウンドトリップ時間が 25ms であることを示します。

6.7.10 音声テスト設定例

I. ネットワーク要件

図 6-11に示すように、Device A と Device B 間のジッタ、遅延、MOS、ICPIF をテストするため音声テストを設定します。



図 6-11 ネットワーク図

II. 設定手順

1) 各インタフェースに IP アドレスを割り当てます。（詳細は省略します。）
2) 各装置間で通信可能になるように、スタティックルートあるいはルーティングテーブルを設定します。（詳細は省略します。）
3) Device B を設定します。

NQA サーバを有効にします。

```
<DeviceB> system-view
[DeviceB] nqa server enable
```

IP アドレス 10.2.2.2、UDP ポート 9000 でリスニングサービスを設定します。

```
[DeviceB] nqa server udp-echo 10.2.2.2 9000
```

4)　Device A を設定します。

音声テストを作成します。

```
<DeviceA> system-view
[DeviceA] nqa entry admin test1
[DeviceA-nqa-admin-test1] type voice
```

宛先 IP アドレスを 10.2.2.2 に設定します。

```
[DeviceA-nqa-admin-test1-voice] destination ip 10.2.2.2
```

宛先ポート番号を 9000 に設定します。

```
[DeviceA-nqa-admin-test1-voice] destination port 9000
[DeviceA-nqa-admin-test1-voice] quit
```

音声テストを開始します。

```
[DeviceA] nqa schedule admin test1 start-time now lifetime forever
```

音声テストを一定期間実行したのち、テストを停止します。

```
[DeviceA] undo nqa schedule admin test1
```

音声テストの最新の結果を表示します。

```
[DeviceA] display nqa result admin test1
NQA entry (admin admin, tag test1) test results:
    Send operation times: 1000          Receive response times: 1000
    Min/Max/Average round trip time: 31/1328/33
    Square-Sum of round trip time: 2844813
    Last packet received time: 2011-06-13 09:49:31.1
  Extended results:
    Packet loss ratio: 0%
    Failures due to timeout: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
Packets out of sequence: 0
    Packets arrived late: 0
  Voice results:
   RTT number: 1000
    Min positive SD: 1                   Min positive DS: 1
    Max positive SD: 204                 Max positive DS: 1297
    Positive SD number: 257              Positive DS number: 259
    Positive SD sum: 759                 Positive DS sum: 1797
    Positive SD average: 2               Positive DS average: 6
    Positive SD square-sum: 54127        Positive DS square-sum: 1691967
    Min negative SD: 1                   Min negative DS: 1
    Max negative SD: 203                 Max negative DS: 1297
    Negative SD number: 255              Negative DS number: 259
    Negative SD sum: 759                 Negative DS sum: 1796
    Negative SD average: 2               Negative DS average: 6
    Negative SD square-sum: 53655        Negative DS square-sum: 1691776
    SD average: 2                         DS average: 6
  One way results:
    Max SD delay: 343                    Max DS delay: 985
    Min SD delay: 343                    Min DS delay: 985
    Number of SD delay: 1                Number of DS delay: 1
    Sum of SD delay: 343                 Sum of DS delay: 985
    Square-Sum of SD delay: 117649       Square-Sum of DS delay: 970225
    SD lost packets: 0                  DS lost packets: 0
```

```
    Lost packets for unknown reason: 0
  Voice scores:
    MOS value: 4.38                          ICPIF value: 0
```

音声テストの統計情報を表示します。

```
[DeviceA] display nqa statistics admin test1
NQA entry (admin admin, tag test1) test statistics:
  NO. : 1

    Start time: 2011-06-13 09:45:37.8
    Life time: 331 seconds
    Send operation times: 4000           Receive response times: 4000
    Min/Max/Average round trip time: 15/1328/32
    Square-Sum of round trip time: 7160528
  Extended results:
    Packet loss ratio: 0%
    Failures due to timeout: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
Packets out of sequence: 0
    Packets arrived late: 0
  Voice results:
   RTT number: 4000
    Min positive SD: 1                     Min positive DS: 1
    Max positive SD: 360                   Max positive DS: 1297
    Positive SD number: 1030               Positive DS number: 1024
    Positive SD sum: 4363                  Positive DS sum: 5423
    Positive SD average: 4                 Positive DS average: 5
    Positive SD square-sum: 497725         Positive DS square-sum: 2254957
    Min negative SD: 1                     Min negative DS: 1
    Max negative SD: 360                   Max negative DS: 1297
    Negative SD number: 1028               Negative DS number: 1022
    Negative SD sum: 1028                  Negative DS sum: 1022
    Negative SD average: 4                 Negative DS average: 5
    Negative SD square-sum: 495901         Negative DS square-sum: 5419
    SD average: 16                          DS average: 2
  One way results:
    Max SD delay: 359                      Max DS delay: 985
    Min SD delay: 0                        Min DS delay: 0
    Number of SD delay: 4                  Number of DS delay: 4
    Sum of SD delay: 1390                  Sum of DS delay: 1079
    Square-Sum of SD delay: 483202         Square-Sum of DS delay: 973651
    SD lost packets: 0                    DS lost packets: 0
    Lost packets for unknown reason: 0
  Voice scores:
    Max MOS value: 4.38                    Min MOS value: 4.38
    Max ICPIF value: 0                     Min ICPIF value: 0
```

6.7.11 DLSw テスト設定例

I. ネットワーク要件

図 6-12に示すように、DLSw 装置の応答時間を測定するため、DLSw テストを設定します。



図 6-12 ネットワーク図

II. 設定手順

各インタフェースに IP アドレスを割り当てます。（詳細は省略します。）

Device が互いに通信できるようにスタティックルートあるいはルーティングプロトコルを設定します。（詳細は省略します。）

DLSw テストを作成します。

```
<DeviceA> system-view
[DeviceA] nqa entry admin test1
[DeviceA-nqa-admin-test1] type dlsw
```

宛先 IP アドレスを 10.2.2.2 に設定します。

```
[DeviceA-nqa-admin-test1-dlsw] destination ip 10.2.2.2
```

履歴記録を保存するように設定します。

```
[DeviceA-nqa-admin-test1-dlsw] history-record enable
[DeviceA-nqa-admin-test1-dlsw] quit
```

DLSw テストを開始します。

```
[DeviceA] nqa schedule admin test1 start-time now lifetime forever
```

DLSw テストを一定期間実行したのち、テストを停止します。

```
[DeviceA] undo nqa schedule admin test1
```

DLSw テストの最新の結果を表示します。

```
[DeviceA] display nqa result admin test1
NQA entry (admin admin, tag test1) test results:
    Send operation times: 1              Receive response times: 1
    Min/Max/Average round trip time: 19/19/19
    Square-Sum of round trip time: 361
    Last succeeded probe time: 2011-11-22 10:40:27.7
  Extended results:
    Packet loss ratio: 0%
    Failures due to timeout: 0
    Failures due to disconnect: 0
    Failures due to no connection: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
```

DLSw テストの履歴記録を表示します。

```
[DeviceA] display nqa history admin test1
NQA entry (admin admin, tag test1) history records:
  Index      Response     Status           Time
  1          19           Succeeded        2011-11-22 10:40:27.7
```

出力では、DLSw 装置の応答時間が 19 ミリ秒であることを示します。

目次

このセクションのページは **9-x-x** です。

7 章 ポートミラーリング 7-1
7.1 概要 7-1
7.1.1 用語 7-1
7.1.2 ポートミラーリングの分類と実行 7-2
7.2 ローカルポートミラーリングの設定 7-5
7.2.1 ローカルポートミラーリング設定作業リスト 7-5
7.2.2 ローカルミラーリンググループの作成 7-6
7.2.3 ローカルミラーリンググループのソースポートの作成 7-6
7.2.4 ローカルミラーリンググループのモニタポートの作成 7-7
7.3 レイヤ 2 リモートポートミラーリングの設定 7-7
7.3.1 リフレクタポートを使用したレイヤ 2 リモートポートミラーリングの設定作業リスト 7-8
7.3.2 出力ポートを使用したレイヤ 2 リモートポートミラーリングの設定作業リスト 7-8
7.3.3 ディスティネーション装置のリモートディスティネーショングループの設定 7-9
7.3.4 ソース装置のリモートソースグループの設定 7-11
7.4 複数モニタポートのローカルミラーリングの設定 7-14
7.4.1 設定の制限とガイドライン 7-14
7.4.2 設定手順 7-15
7.5 ポートミラーリングの表示と維持 7-15
7.6 ポートミラーリングの設定例 7-16
7.6.1 ローカルポートミラーリングの設定例 7-16
7.6.2 レイヤ 2 リモートポートミラーリングの設定例（リフレクタポート） 7-17
7.6.3 レイヤ 2 リモートポートミラーリングの設定例（出力ポート） 7-20
7.6.4 複数のモニタポートのローカルポートミラーリングの設定例 7-23

7章 ポートミラーリング

7.1 概要

ポートミラーリングはポートを通過したパケットを分析するために、データ監視端末が接続されているモニタポートへパケットをコピーします。

7.1.1 用語

以下にポートミラーリングの設定で使用する用語を示します。

I. ミラーリングソース

1 つのモニタ対象ポートをミラーリングソースにすることができます。モニタ対象ポートはソースポートと呼ばれます。ミラーリングソースを通過するパケットはパケットを解析するデータをモニタリングする装置に接続するポートにコピーされます。コピーはミラーパケットと呼ばれます。

II. ソース装置

ミラーリングソースが存在する装置は”送信元装置”あるいは”ソース装置”と呼ばれます。

III. ミラーリング宛先

ミラーリング宛先は、ミラーリングされたパケットの宛先ポート（別名モニタポートとも呼ばれます）であり、データ監視装置に接続します。モニタポートが存在する装置は"宛先装置"あるいは”ディスティネーション装置”と呼ばれます。モニタポートは、接続されている監視装置にミラーリングされたパケットを転送します。

モニタポートは複数のポートをモニタすることができ、場合によっては複数の重複したパケットを受信する可能性があります。たとえば、以下の状況が存在する場合、2 つのパケットのコピーはポート 1 で受信されます。

- ポート 1 は同一装置上のポート 2 とポート 3 の送受信トラフィックをモニタします。
- パケットがポート 2 からポート 3 へ転送されます。

IV. ミラーリング方向

ミラーリング方向は、受信トラフィック、送信トラフィック、送受信トラフィックがあり、モニタリングソースでコピーされます。

- **受信** – ミラーリングソースで受信したパケットをコピーします。

- **送信** – ミラーリングソースに送信したパケットをコピーします。
- **送受信** – ミラーリングソースで送受信したパケットをコピーします。

🕮 **メモ：**

- 受信トラフィックミラーリングでは、もとのパケットの VLAN タグもミラーリングされるパケットにコピーされます。
- 送信トラフィックミラーリングでは、ミラーリングされるパケットは送信インタフェースの VLAN タグを送信します。

V. ミラーリンググループ

ポートミラーリングはポートミラーリンググループによって実行されます。ミラーリンググループには 3 つのタイプ（ローカル、リモートソース、リモート宛先ミラーリング）があります。ミラーリンググループの詳細は、オペレーションマニュアルのセクション *9 システム管理*”*ポートミラーリング*”の”*ポートミラーリングの分類と実行*”を参照してください。

VI. リフレクタポート、出力ポート、リモートプローブ VLAN

リフレクタポート、リモートプローブ VLAN、および出力ポートは、レイヤ 2 リモートポートミラーリングに使用されます。リモートプローブ VLAN は、ミラーリングされたパケットを宛先装置に送信するための専用の VLAN です。

リフレクタポートと出力ポートのどちらも、送信元装置上に存在し、ミラーリングされたパケットをリモートプローブ VLAN に送信します。

出力ポートは、リモートプローブ VLAN に属している必要がありますが、リフレクタポートはそうでなくても構いません。リフレクタポート、出力ポート、リモートプローブ VLAN、レイヤ 2 リモートポートミラーリングの詳細については、オペレーションマニュアルのセクション *9 システム管理*”*ポートミラーリング*”の”*ポートミラーリングの分類と実行*”を参照してください。

🕮 **メモ：**

ポートミラーリングの装置でソースポート、宛先ポート、リフレクタポート、出力ポートを除くすべてのポートは共通ポートと呼ばれます。

7.1.2 ポートミラーリングの分類と実行

ポートミラーリングは、ローカルポートミラーリングとリモートポートミラーリングに分類されます。

- **ローカルポートミラーリング**－ミラーリングソースとミラーリング宛先が同一装置にあります。

- **リモートポートミラーリング**－ミラーリングソースとミラーリング宛先が異なる装置にあります。

I. ローカルポートミラーリング

ローカルポートミラーリングでは、以下の状況となります。

- ソース装置は、データをモニタリングする装置に直接接続されています。
- ソース装置は、データをモニタリングする装置にミラーリングしたパケットを転送する宛先装置として動作できます。

ローカルミラーリンググループは、同一装置上のミラーリングソースとミラーリング宛先を含むミラーリンググループです。

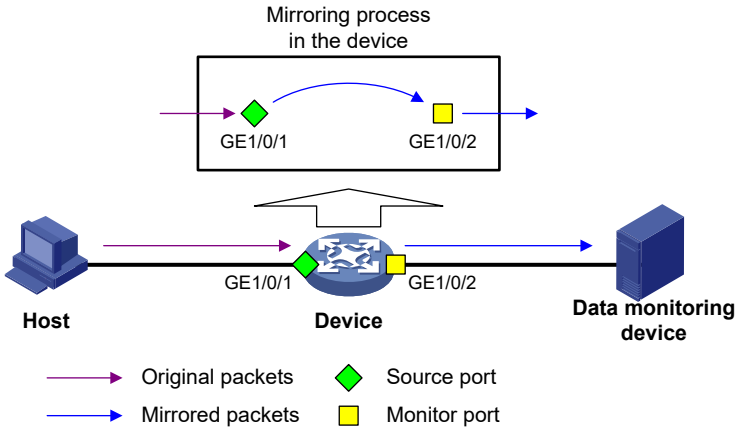


図 7-1 ローカルポートミラーリングの実行

図 7-1に示すように、ソースポート GigabitEthernet 1/0/1 とモニタポート GigabitEthernet 1/0/2 は同じ装置上にあります。GigabitEthernet 1/0/1 のパケットは GigabitEthernet 1/0/2 にコピーされ、解析を行うためデータ監視装置に転送されます。

II. リモートポートミラーリング

リモートポートミラーリングでは、以下の状況となります。

- ミラーリングソースとミラーリング宛先は別の装置上に配置され、別のミラーリンググループに属します。
- ソース装置はモニタリング装置に直接接続されていません。
- ソース装置は宛先装置にミラーしたパケットをコピーします。宛先装置ではデータをモニタリングする装置に転送します。

リモートソースグループはミラーリングソースを含むミラーリンググループです。リモート宛先グループはそれぞれミラーリングディスティネーションを含むミラーリンググループです。送信元装置と宛先装置の間の装置は、中間装置です。

ミラーリングソースとミラーリング宛先は同一レイヤ 2 ネットワークの異なる装置に存在するため、リモートポートミラーリングは、レイヤ 2 リモートポートミラーリングとも呼ばれます。

ソース装置上でリフレクタポートあるいは出力ポートが有効である場合、レイヤ 2 リモートポートミラーリングを動作させることができます。リフレクタポートを使用する方式はリフレクタポート方式と呼ばれます。出力ポートを使用する方式は出力ポート方式と呼ばれます。

- **リフレクタポート方式**－パケットは以下のようにミラーリングされます。
  - ソース装置はミラーリングソースで受信されたパケットをリフレクタポートにコピーします。
  - リフレクタポートはリモートプローブ VLAN のミラーリングされたパケットをブロードキャストします。
  - 中間装置はリモートプローブ VLAN を通して宛先装置にミラーリングされたパケットを転送します。
  - ミラーリングされたパケットを受信すると、宛先装置はミラーリングされたパケットの ID がリモートプローブ VLAN ID と同一かどうか確認します。2 つの VLAN ID が一致する場合、宛先装置はモニタポートを通してデータをモニタする装置にミラーリングされたパケットを転送します。

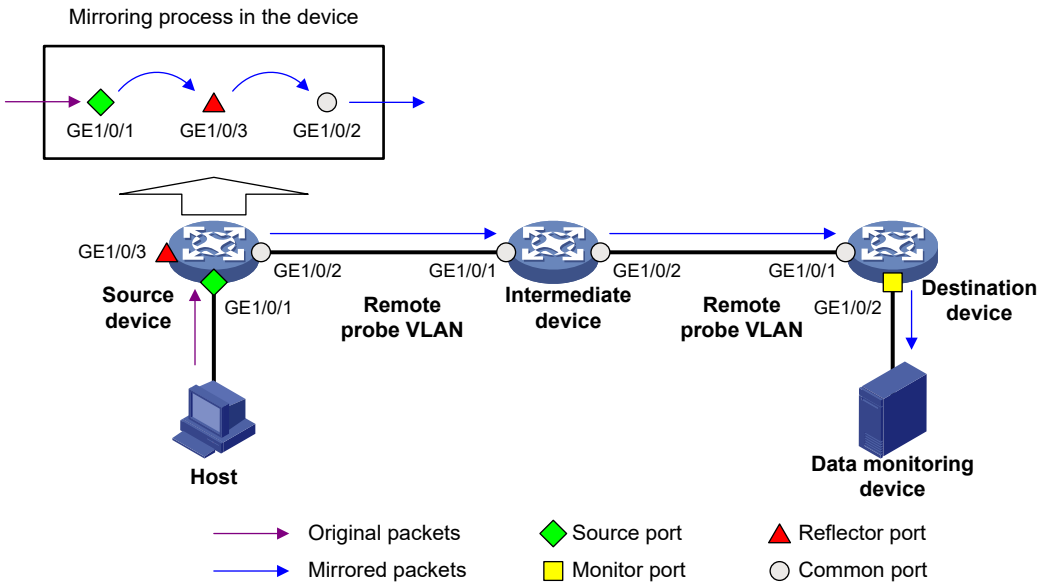


図 7-2 リフレクタポート方式によるレイヤ 2 リモートポートミラーリングの実行

- **出力ポート方式**－パケットは以下のようにミラーリングされます。
  - ソース装置はミラーリングソースで受信されたパケットを出力ポートにコピーします。
  - 出力ポートは中間装置にミラーリングされたパケットを転送します。
  - 中間装置はリモートプローブ VLAN のミラーリングされたパケットをブロードキャストし、宛先装置にミラーリングされたパケットを転送します。
  - ミラーリングされたパケットを受信すると、宛先装置はミラーリングされたパケットの ID がリモートプローブ VLAN ID と同一かどうか確認します。2 つの VLAN ID が一致する場合、宛先装置はモニタポートを通してデータをモニタする装置にミラーリングされたパケットを転送します。

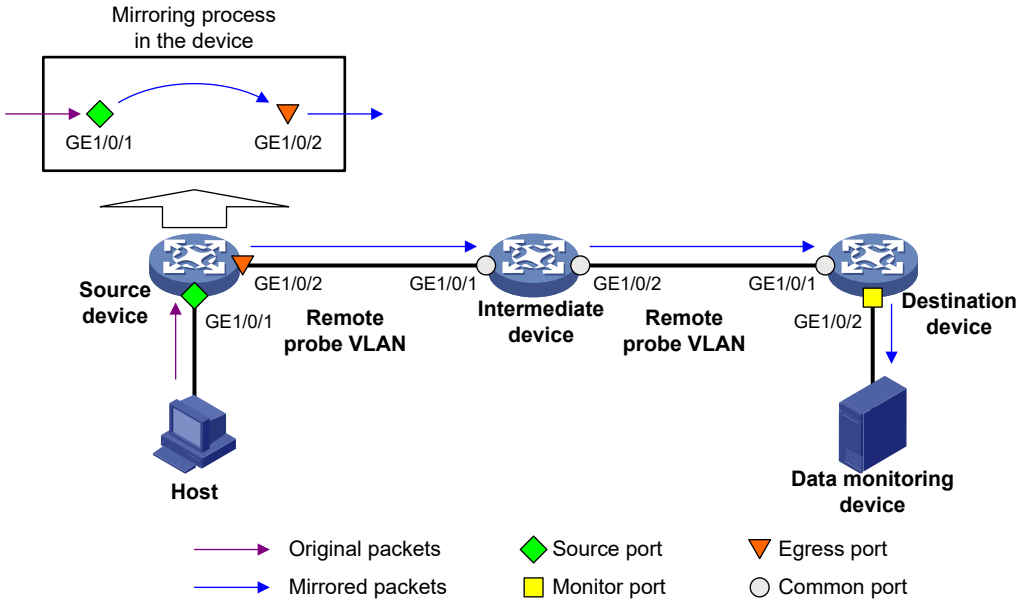


図 7-3 出力ポート方式によるレイヤ 2 リモートポートミラーリングの実行

リフレクタポート方式では、リフレクタポートはリモートプローブ VLAN のミラーリングされたパケットをブロードキャストします。ソース装置のソースポート以外のポートをリモートプローブ VLAN に割り当てることで、ローカルポートミラーリングが動作するリフレクタポート方式を使用することができます。出力ポート方式はこのような方法でローカルポートミラーリングを動作させることはできません。

ミラーされたパケットをレイヤ 2 転送するため、ソース装置と宛先装置に向いている中間装置のポートにリモートプローブ VLAN を割り当てます。

ミラーリンググループのポートの双方向のトラフィックをモニタするため、ソース装置、中間装置、宛先装置のリモートプローブ VLAN の MAC アドレスの学習を無効にする必要があります。MAC アドレスの学習の詳細は、オペレーションマニュアルのセクション 2 *アクセス "MAC アドレステーブル"*を参照してください。

7.2 ローカルポートミラーリングの設定

ローカルポートミラーリングはソースポートとミラーリングポートが設定されている場合のみ適用されます。

7.2.1 ローカルポートミラーリング設定作業リスト

作業リスト
1.　（必須設定項目） ローカルミラーリンググループの作成
2.　（必須設定項目） ローカルミラーリンググループのソースポートの作成
3.　（必須設定項目） ローカルミラーリンググループのモニタポートの作成

7.2.2 ローカルミラーリンググループの作成

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. ローカルミラーリンググループを作成する	**mirroring-group** *group-id* **local**	デフォルト：設定なし

7.2.3 ローカルミラーリンググループのソースポートの作成

ローカルミラーリンググループのソースポートは、以下のいずれかの方法で設定することができます。

- system view でミラーリンググループにソースポートを割り当てます。
- interface view でソースポートとしてミラーリンググループにポートを割り当てます。

  interface view でミラーリンググループに複数のポートを割り当てる場合、上記の方法を繰り返してください。

I. 設定の制限とガイドライン

ローカルミラーリンググループにソースポートを設定する場合、以下の設定の制限とガイドラインに従ってください。

- レイヤ 2 アグリゲートインタフェースはソースポートとして設定することができません。
- ミラーリンググループは複数のソースポートを持つことができます。
- ソースポートはリフレクタポート、出力ポート、モニタポートとして同時に設定できません。
- ミラーリンググループは 1 つの入力トラフィックのミラーリング、1 つの出力トラフィックのミラーリングの最大 2 つの片方向のミラーリンググループを設定することができます。双方向のソースポートは、1 つのミラーリンググループにのみ割り当てることができます。
- 出力トラフィックのミラーリングあるいは双方向トラフィックのミラーリングを行う場合、装置は 1 つのミラーリンググループのみサポートします。

II. system view でのソースポートの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. 指定したローカルミラーリンググループにモニタポートを設定する	**mirroring-group** *group-id* **mirroring-port** *interface-list* { **both** | **inbound** | **outbound** }	デフォルト：設定なし

III. interface view でのソースポートの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. interface view に移行する	**interface** *interface-type interface-number*	―

操作	コマンド	補足
3. 指定したミラーリンググループにモニタポートを設定する	**mirroring-group** *group-id* **mirroring-port** { **both** | **inbound** | **outbound** }	デフォルト：設定なし

7.2.4 ローカルミラーリンググループのモニタポートの作成

ミラーリンググループのモニタポートを設定する場合、以下のいずれかの方法で設定することができます。

- system view でミラーリンググループのモニタポートを設定します。
- interface view でポートをモニタポートとしてミラーリンググループに割り当てることができます。

I. 設定の制限とガイドライン

ローカルミラーリンググループにモニタポートを設定する場合、以下の設定の制限とガイドラインに従ってください。

- モニタポートでスパニングツリー機能を有効にしないでください。
- レイヤ 2 アグリゲートインタフェースはモニタポートとして設定することができません。
- モニタポートは、ポートミラーリングのために使用してください。データをモニタリングする装置がミラーされたトラフィックのみを受信するように、ポートミラーリングのモニタポートを使用してください。

II. system view でのモニタポートの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. 指定したローカルミラーリンググループにモニタポートを設定する	**mirroring-group** *group-id* **monitor-port** *interface-type interface-number*	デフォルト：設定なし

III. interface view でのモニタポートの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. interface view に移行する	**interface** *interface-type interface-number*	―
3. 指定したミラーリンググループにモニタポートを設定する	**mirroring-group** *group-id* **monitor-port**	デフォルト：設定なし

7.3 レイヤ2リモートポートミラーリングの設定

レイヤ 2 リモートポートミラーリングを設定するため、以下の作業を実行してください。

- ソース装置でリモートソースグループを設定してください。
- ディスティネーション装置で連携するリモートディスティネーショングループを設定してください。
- 中間装置がある場合、以下の装置とポートでリモートプローブ VLAN を許可するように設定してください。
  - 中間装置
  - ソース装置と中間装置とディスティネーション装置で中間装置に接続されているポート

レイヤ 2 リモートポートミラーリングを設定する場合、以下の設定の制限とガイドラインに従ってください。

- 出力ポートをリモートプローブ VLAN に割り当ててください。リフレクタポートはリモートプローブ VLAN に割り当てる必要がありません。
- リモートディスティネーション装置にミラーパケットが到達するように、VLAN ID が削除あるいは変更されていないことを確認してください。
- ディスティネーション装置、中間装置、ソース装置の順番で設定することを推奨します。

7.3.1 リフレクタポートを使用したレイヤ 2 リモートポートミラーリングの設定作業リスト

作業リスト
（必須設定項目） ディスティネーション装置のリモートディスティネーショングループの設定
1. リモートディスティネーショングループの作成
2. リモートディスティネーショングループのモニタポートの設定
3. リモートディスティネーショングループのリモートプローブ VLAN の設定
4. リモートプローブ VLAN へのモニタポートの割り当て
（必須設定項目） ソース装置のリモートソースグループの設定
1. リモートソースグループの作成
2. リモートソースグループのソースポートの設定
3. リモートソースグループのリフレクタポートの設定
4. リモートソースグループのリモートプローブ VLAN の設定

7.3.2 出力ポートを使用したレイヤ 2 リモートポートミラーリングの設定作業リスト

作業リスト
（必須設定項目） ディスティネーション装置のリモートディスティネーショングループの設定
1. リモートディスティネーショングループの作成
2. リモートディスティネーショングループのモニタポートの設定
3. リモートディスティネーショングループのリモートプローブ VLAN の設定
4. リモートプローブ VLAN へのモニタポートの割り当て

作業リスト
（必須設定項目） ソース装置のリモートソースグループの設定 1． リモートソースグループの作成 2． リモートソースグループのソースポートの設定 3． リモートソースグループの出力ポートの設定 4． リモートソースグループのリモートプローブ VLAN の設定

7.3.3 ディスティネーション装置のリモートディスティネーショングループの設定

I. リモートディスティネーショングループの作成

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． リモートディスティネーショングループを作成する	**mirroring-group** *group-id* **remote-destination**	デフォルト：設定なし

II. リモートディスティネーショングループのモニタポートの設定

ミラーリンググループのモニタポートを設定する場合、以下のいずれかの方法で設定することができます。

- system view でミラーリンググループのモニタポートを設定します。
- interface view でモニタポートとしてポートをミラーリンググループに割り当てることができます。

リモートディスティネーショングループのモニタポートを設定する場合、以下の設定の制限とガイドラインに従ってください。

- モニタポートでスパニングツリー機能を無効にしてください。
- アグリゲートインタフェースはモニタポートとして設定することができません。
- モニタリング装置が、ミラーリングしたトラフィックのみを受信し、解析できるように、ミラーリングしたトラフィックと通常の転送トラフィックを混在しないで、ポートミラーリングのみモニタポートを使用してください。
- モニタポートは 1 つのミラーリンググループにのみ属することができます。

以下に system view でのリモートディスティネーショングループのモニタポートの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． リモートディスティネーショングループのモニタポートを設定する	**mirroring-group** *group-id* **monitor-port** *interface-type interface-number*	デフォルト：設定なし

以下に interface view でのリモートディスティネーショングループのモニタポートの設定を示します。

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

操作	コマンド	補足
2． interface view に移行する	**interface** *interface-type interface-number*	―
3． ポートをリモートディスティネーショングループのモニタポートに設定する	**mirroring-group** *group-id* **monitor-port**	デフォルト：設定なし

III. リモートディスティネーショングループのリモートプローブ VLAN の設定

リモートディスティネーショングループのリモートプローブ VLAN を設定する場合以下の制限とガイドラインに従ってください。

- リモートプローブ VLAN を設定する前に、最初にスタティック VLAN を作成してください。
- VLAN がリモートプローブ VLAN として設定されている場合、ポートミラーリング専用としてリモートプローブ VLAN を使用してください。VLAN インタフェースを作成、あるいは VLAN のためにほかの機能を設定しないでください。
- ソース装置とディスティネーション装置の、リモートディスティネーショングループのリモートプローブ VLAN を同一に設定してください。
- 装置がサポートするリモートプローブ VLAN は 1 つだけです。

以下にリモートディスティネーショングループのリモートプローブ VLAN の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． リモートディスティネーショングループのリモートプローブ VLAN を設定する	**mirroring-group** *group-id* **remote-probe vlan** *vlan-id*	デフォルト：設定なし

IV. リモートプローブ VLAN へのモニタポートの割り当て

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． モニタポートの interface view に移行する	**interface** *interface-type interface-number*	―
3． プローブ VLAN にポートを割り当てる	• アクセスポート：**port access vlan** *vlan-id* • トランクポート：**port trunk permit vlan** *vlan-id* • ハイブリッドポート：**port hybrid vlan** *vlan-id -list* { **tagged** | **untagged** }	**port access vlan**コマンド、**port trunk permit vlan**コマンド、**port hybrid vlan**コマンドについての詳細は、コマンドマニュアルのセクション2 *アクセス” VLAN*”を参照してください。

7.3.4 ソース装置のリモートソースグループの設定

I. リモートソースグループの作成

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. リモートソースグループを作成する	**mirroring-group** *group-id* **remote-source**	デフォルト：設定なし

II. リモートソースグループのソースポートの設定

リモートソースグループのソースポートを設定する場合、以下のいずれかの設定を行うことができます。

- system view でリモートソースグループにソースポートを割り当てます。
- interface view でリモートソースグループにソースポートを割り当てます。

  interface view でリモートソースグループに複数のポートを割り当てる場合、上記の方法を繰り返してください。

リモートソースグループのソースポートを設定する場合、以下の制限とガイドラインに従ってください。

- ミラーリンググループのソースポートをミラーリンググループのリモートプローブ VLAN に割り当てないでください。
- ミラーリンググループは複数のソースポートを持つことができます。
- ソースポートはリフレクタポート、モニタポート、出力ポートと同時に設定できません。
- ミラーリンググループは 1 つの入力トラフィックのミラーリング、1 つの出力トラフィックのミラーリングの最大 2 つの双方向のミラーリンググループを設定することができます。双方向のソースポートは、1 つのミラーリンググループにのみ割り当てることができます。
- 出力トラフィックのミラーリングあるいは双方向トラフィックのミラーリングを行う場合、装置は 1 つのミラーリンググループのみサポートします。
- レイヤ 2 アグリゲーションインタフェースはソースポートとして設定することができません。

以下に system view でのリモートソースグループのソースポートの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. リモートソースグループのソースポートを設定する	**mirroring-group** *group-id* **mirroring-port** *interface-list* { **both** | **inbound** | **outbound** }	デフォルト：設定なし

以下に interface view でのリモートソースグループのソースポートの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. interface view に移行する	**interface** *interface-type interface-number*	―

操作	コマンド	補足
3. ポートをリモートソースグループのソースポートに設定する	**mirroring-group** *group-id* **mirroring-port** { **both** | **inbound** | **outbound** }	デフォルト：設定なし

III. リモートソースグループのリフレクタポートの

リモートソースグループのリフレクタポートを設定する場合、以下のいずれかの設定を行うことができます。

- system view でリモートソースのリフレクタポートを設定します。
- interface view でポートをリフレクタポートとしてリモートソースグループに割り当てることができます。

リモートソースグループのリフレクタポートを設定する場合、以下の制限とガイドラインに従ってください。

- リフレクタポートとして設定するポートは未使用のポートを設定してください。リフレクタポートにネットワークケーブルを接続しないでください。
- リフレクタポートとして設定された場合、ポートの既存の設定が削除されます。リフレクタポートのほかの機能を設定しないでください。
- ミラーリンググループは 1 つのリフレクタポートのみ含めることができます。
- リフレクタポートの通信モード、MDI、通信速度の設定は変更することができません。

以下に system view でのリモートソースグループのリフレクタポートの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. リモートソースグループのリフレクタポートを設定する	**mirroring-group** *group-id* **reflector-port** *interface-type interface-number*	デフォルト：設定なし

以下に interface view でのリモートソースグループのリフレクタポートの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. interface view に移行する	**interface** *interface-type interface-number*	―
3. ポートをリモートソースグループのリフレクタポートに設定する	**mirroring-group** *group-id* **reflector-port**	デフォルト：設定なし

IV. リモートソースグループの出力ポートの設定

リモートソースグループの出力ポートを設定する場合、以下のいずれかの設定を行うことができます。

- system view でリモートソースグループの出力ポートを設定します。
- interface view でポートを出力ポートとしてリモートソースグループに割り当てることができます。

リモートソースグループの出力ポートを設定する場合、以下のガイドラインに従ってください。

- 出力ポートで以下の機能を無効にしてください。
  - □ スパニングツリー
  - □ 802.1X
  - □ IGMP snooping
  - □ スタティック ARP
  - □ MAC アドレス学習
- ミラーリンググループは 1 つの出力ポートのみ含めることができます。
- 既存のミラーリンググループのソースポートを出力ポートにすることはできません。

以下に system view でのリモートソースグループの出力ポートの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． リモートソースグループの出力ポートを設定する	**mirroring-group** *group-id* **monitor-egress** *interface-type interface-number*	デフォルト：設定なし

以下に interface view でのリモートソースグループの出力ポートの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． interface view に移行する	**interface** *interface-type interface-number*	―
3． ポートをリモートソースグループの出力ポートに設定する	**mirroring-group** *group-id* **monitor-egress**	デフォルト：設定なし

V. リモートソースグループのリモートプローブ VLAN の設定

リモートソースグループのリモートプローブ VLAN を設定する場合、以下の制限とガイドラインに従ってください。

- リモートプローブ VLAN を設定する前に、スタティック VLAN が設定されていることを確認してください。
- リモートプローブ VLAN として VLAN を設定した場合、ポートミラーリング専用としてリモートプローブ VLAN を使用することを推奨します。VLAN インタフェースを作成、あるいは VLAN のためにほかの機能を設定しないでください。
- ソース装置と宛先装置上のリモートミラーリンググループは、同じリモートプローブ VLAN を使用する必要があります。

以下にリモートソースグループのリモートプローブ VLAN の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． リモートソースグループのリモートプローブ VLAN を設定する	**mirroring-group** *group-id* **remote-probe vlan** *vlan-id*	デフォルト：設定なし

7.4 複数モニタポートのローカルミラーリングの設定

通常、ローカルミラーリンググループのモニタポートは 1 つのみ設定できます。複数のデータモニタリング装置のローカル装置のトラフィックをモニタすることができません。複数のモニタポートをサポートするようにローカルポートミラーリングを設定するためレイヤ 2 リモートポートミラーリングのリモートプローブ VLAN を使用します。

レイヤ 2 リモートポートミラーリングで、ミラーパケットリモートプローブ VLAN が設定され、ミラーリングされたパケットがリモートプローブ VLAN にブロードキャストされます。複数のデータのモニタリング装置をリモートプローブ VLAN のメンバポートに接続することで、複数のデータモニタリング装置のローカル装置のトラフィックをモニタすることができます。

設定のフローは以下となります。

1) 装置のリモートソースグループを作成します。
2) ミラーリンググループのソースポートを指定します。
3) リモートソースグループのリモートプローブ VLAN を設定します。
4) データモニタリング装置に接続しているポートをリモートプローブ VLAN に割り当てます。

これによってソースポートのミラーリングされたパケットはリモートプローブ VLAN にブロードキャストされます。そしてデータモニタリング装置に接続しているポートに送信されます。データモニタリング装置はミラーリングされたパケットを受信することができます。

7.4.1 設定の制限とガイドライン

複数のモニタポートでローカルポートミラーリングを設定する場合、以下の制限とガイドラインに従ってください。

- 装置で使用されていないポートをリフレクタポートとして設定してください。リフレクタポートにネットワークケーブルを接続しないでください。
- ポートをリフレクタポートとして設定した場合、工場出荷状態の設定に戻ります。リフレクタポートでほかの機能を設定しないでください。
- ミラーリンググループのソースポートをミラーリンググループのリモートプローブ VLAN に割り当てないでください。
- VLAN は、1 つのリモートソースグループ用のリモートプローブ VLAN として動作することができます。ポートミラーリングのリモートプローブ VLAN と同時に使用しないでください。VLAN の VLAN インタフェースを作成あるいはほかの設定を実行しないでください。
- リモートプローブ VLAN はスタティック VLAN にする必要があります。
- リモートミラーリンググループのリモートプローブ VLAN として設定されている VLAN を削除する場合、最初にミラーリンググループからリモートプローブ VLAN を削除してください。
- 装置がサポートするリモートプローブ VLAN は 1 つだけです。

7.4.2 設定手順

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． リモートソースグループを作成する	**mirroring-group** *group-id* **remote-source**	デフォルト：設定なし
3． リモートソースグループのソースポートを設定する	● system viewで設定する： **mirroring-group** *group-id* **mirroring-port** *interface-list* { **both** | **inbound** | **outbound** } ● interface viewで設定する： 1． interface view に移行する： **interface** *interface-type interface-number* 2． ソースポートとしてミラーリングポートを割り当てる： **mirroring-group** *group-id* **mirroring-port** { **both** | **inbound** | **outbound** } 3． system view に戻る： **quit**	デフォルト：設定なし
4． リモートソースグループのリフレクタポートを設定する	**mirroring-group** *group-id* **reflector-port** *interface-type interface-number*	デフォルト：設定なし
5． リモートプローブ VLAN として設定される VLAN を作成する	**vlan** *vlan-id*	―
6． VLAN にモニタポートを割り当てる	**port** *interface-list*	デフォルト：VLAN1
7． system view に戻る	**quit**	―
8． リモートソースグループのリモートプローブ VLAN として VLAN を設定する	**mirroring-group** *group-id* **remote-probe vlan** *vlan-id*	デフォルト：設定なし

7.5 ポートミラーリングの表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
ミラーリンググループの情報を表示する	**display mirroring-group** { *group-id* | **all** | **local** | **remote-destination** | **remote-source** }

7.6 ポートミラーリングの設定例

7.6.1 ローカルポートミラーリングの設定例

I. ネットワーク要件

図 7-4に示すように、Marketing Department、Technical Department の 2 つの Department で双方向のパケットをモニタリングできるように、ソースポートでのローカルポートミラーリングを設定します。

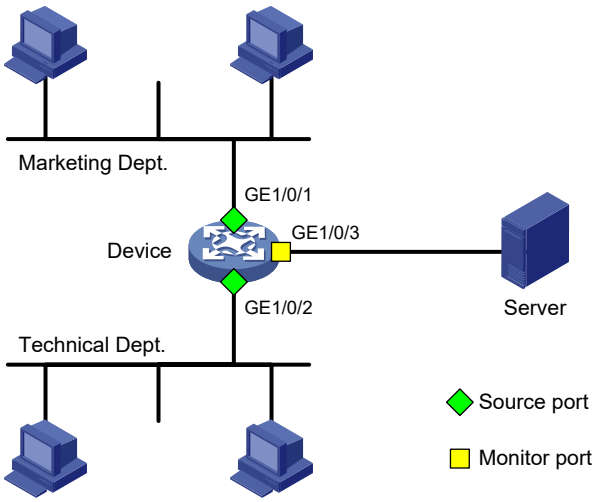


図 7-4 ネットワーク図

II. 設定手順

ローカルミラーリンググループ 1 を作成します。

```
<Device> system-view
[Device] mirroring-group 1 local
```

ローカルミラーリンググループ 1 のソースポートとして GigabitEthernet 1/0/1、GigabitEthernet 1/0/2 を設定します。

```
[Device] mirroring-group 1 mirroring-port gigabitethernet 1/0/1 gigabitethernet 1/0/2 both
```

ローカルミラーリンググループ 1 のモニタポートとして GigabitEthernet 1/0/3 を設定します。

```
[Device] mirroring-group 1 monitor-port gigabitethernet 1/0/3
```

モニタポート GigabitEthernet 1/0/3 のスパニングツリー機能を無効にします。

```
[Device] interface gigabitethernet 1/0/3
[Device-GigabitEthernet1/0/3] undo stp enable
```

```
[Device-GigabitEthernet1/0/3] quit
```

III. 設定の確認

すべてのミラーリンググループの設定を表示します。

```
[Device] display mirroring-group all
Mirroring group 1:
    Type: Local
    Status: Active
    Mirroring port:
        GigabitEthernet1/0/1  Both
        GigabitEthernet1/0/2  Both
    Monitor port: GigabitEthernet1/0/3
```

7.6.2 レイヤ 2 リモートポートミラーリングの設定例（リフレクタポート）

I. ネットワーク要件

図 7-5に示すように、Marketing Department の双方向トラフィックをモニタリングするため、レイヤ 2 リモートポートミラーリングを設定します。

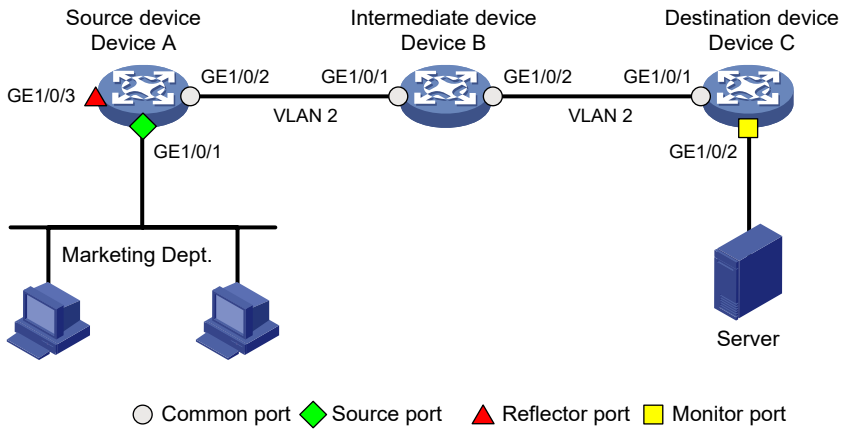


図 7-5 ネットワーク図

II. 設定手順

1)　Device C（ディスティネーション装置）を設定します。

トランクポートして GigabitEthernet 1/0/1 を設定し、VLAN 2 のパケットを許可するように設定します。

```
<DeviceC> system-view
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] port link-type trunk
```

```
[DeviceC-GigabitEthernet1/0/1] port trunk permit vlan 2
[DeviceC-GigabitEthernet1/0/1] quit
```

リモートディスティネーショングループを作成します。

```
[DeviceC] mirroring-group 2 remote-destination
```

VLAN 2 を作成します。

```
[DeviceC] vlan 2
```

VLAN 2 で MAC アドレス学習を無効にします。

```
[DeviceC-vlan2] undo mac-address mac-learning enable
[DeviceC-vlan2] quit
```

ミラーリンググループのリモートプローブ VLAN として設定される VLAN 2 を作成します。

```
[DeviceC] mirroring-group 2 remote-probe vlan 2
```

ミラーリンググループのモニタポートとして GigabitEthernet 1/0/2 を設定します。

```
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] mirroring-group 2 monitor-port
```

GigabitEthernet 1/0/2 のスパニングツリーを無効にします。

```
[DeviceC-GigabitEthernet1/0/2] undo stp enable
```

VLAN 2 に GigabitEthernet 1/0/2 を割り当てます。

```
[DeviceC-GigabitEthernet1/0/2] port access vlan 2
[DeviceC-GigabitEthernet1/0/2] quit
```

2)　Device B （中間装置）を設定します。

VLAN 2 を作成します。

```
<DeviceB> system-view
[DeviceB] vlan 2
```

VLAN 2 で MAC アドレス学習を無効にします。

```
[DeviceB-vlan2] undo mac-address mac-learning enable
[DeviceB-vlan2] quit
```

トランクポートして GigabitEthernet 1/0/1 を設定し、VLAN 2 のパケットを許可するように設定します。

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port link-type trunk
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 2
[DeviceB-GigabitEthernet1/0/1] quit
```

トランクポートして GigabitEthernet 1/0/2 を設定し、VLAN 2 のパケットを許可するように設定します。

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] port link-type trunk
[DeviceB-GigabitEthernet1/0/2] port trunk permit vlan 2
[DeviceB-GigabitEthernet1/0/2] quit
```

3)　Device A （ソース装置）を設定します。

リモートソースグループを作成します。

```
<DeviceA> system-view
[DeviceA] mirroring-group 1 remote-source
```

VLAN 2 を作成します。

```
[DeviceA] vlan 2
```

VLAN 2 で MAC アドレス学習を無効にします。

```
[DeviceA-vlan2] undo mac-address mac-learning enable
[DeviceA-vlan2] quit
```

ミラーリンググループのリモートプローブ VLAN として設定される VLAN 2 を作成します。

```
[DeviceA] mirroring-group 1 remote-probe vlan 2
```

ミラーリンググループのソースポートとして GigabitEthernet 1/0/1 を設定します。

```
[DeviceA] mirroring-group 1 mirroring-port gigabitethernet 1/0/1 both
```

ミラーリンググループのリフレクタポートとして GigabitEthernet 1/0/3 を設定します。

```
[DeviceA] mirroring-group 1 reflector-port gigabitethernet 1/0/3
This operation may delete all settings made on the interface. Continue? [Y/N]:
y
```

トランクポートして GigabitEthernet 1/0/2 を設定し、VLAN 2 のパケットを許可するように設定します。

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port link-type trunk
[DeviceA-GigabitEthernet1/0/2] port trunk permit vlan 2
[DeviceA-GigabitEthernet1/0/2] quit
```

III. 設定の確認

Device C のミラーリンググループの設定を確認します。

```
[DeviceC] display mirroring-group all
Mirroring group 2:
    Type: Remote destination
```

```
    Status: Active
    Monitor port: GigabitEthernet1/0/2
    Remote probe VLAN: 2
```

Device A のミラーリンググループの設定を確認します。

```
[DeviceA] display mirroring-group all
Mirroring group 1:
    Type: Remote source
    Status: Active
    Mirroring port:
        GigabitEthernet1/0/1  Both
    Reflector port: GigabitEthernet1/0/3
    Remote probe VLAN: 2
```

7.6.3 レイヤ 2 リモートポートミラーリングの設定例（出力ポート）

I. ネットワーク要件

図 7-6に示すように、Marketing Department の双方向トラフィックをモニタリングするため、レイヤ 2 リモートポートミラーリングを設定します。

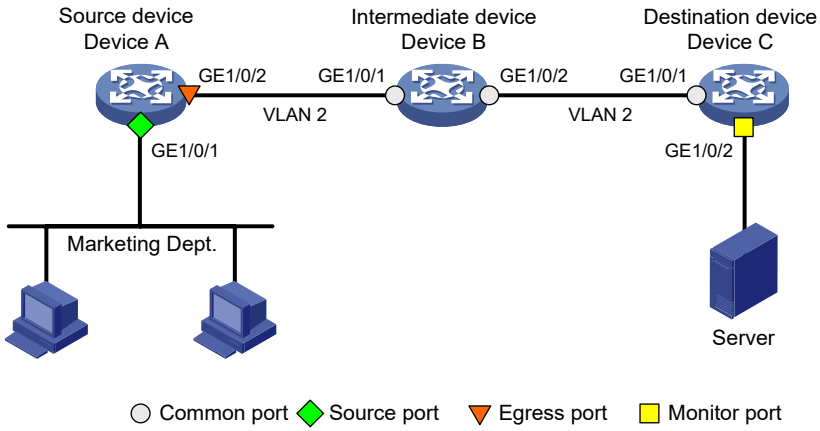


図 7-6 ネットワーク図

II. 設定手順

1)　Device C（ディスティネーション装置）を設定します。

トランクポートして GigabitEthernet 1/0/1 を設定し、VLAN 2 のパケットを許可するように設定します。

```
<DeviceC> system-view
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] port link-type trunk
[DeviceC-GigabitEthernet1/0/1] port trunk permit vlan 2
[DeviceC-GigabitEthernet1/0/1] quit
```

リモートディスティネーショングループを作成します。

```
[DeviceC] mirroring-group 2 remote-destination
```

VLAN 2 を作成します。

```
[DeviceC] vlan 2
```

VLAN 2 で MAC アドレス学習を無効にします。

```
[DeviceC-vlan2] undo mac-address mac-learning enable
[DeviceC-vlan2] quit
```

ミラーリンググループのリモートプローブ VLAN として設定される VLAN 2 を作成します。

```
[DeviceC] mirroring-group 2 remote-probe vlan 2
```

ミラーリンググループのモニタポートとして GigabitEthernet 1/0/2 を設定します。

```
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] mirroring-group 2 monitor-port
```

GigabitEthernet 1/0/2 のスパニングツリーを無効にします。

```
[DeviceC-GigabitEthernet1/0/2] undo stp enable
```

アクセスポートとして VLAN2 に GigabitEthernet 1/0/2 を割り当てます。

```
[DeviceC-GigabitEthernet1/0/2] port access vlan 2
[DeviceC-GigabitEthernet1/0/2] quit
```

2)　Device B （中間装置）を設定します。

VLAN 2 を作成します。

```
<DeviceB> system-view
[DeviceB] vlan 2
```

VLAN 2 で MAC アドレスの学習を無効にします。

```
[DeviceB-vlan2] undo mac-address mac-learning enable
[DeviceB-vlan2] quit
```

トランクポートして GigabitEthernet 1/0/1 を設定し、VLAN 2 のパケットを許可するように設定します。

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port link-type trunk
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 2
[DeviceB-GigabitEthernet1/0/1] quit
```

トランクポートして GigabitEthernet 1/0/2 を設定し、VLAN 2 のパケットを許可するように設定します。

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] port link-type trunk
```

```
[DeviceB-GigabitEthernet1/0/2] port trunk permit vlan 2
[DeviceB-GigabitEthernet1/0/2] quit
```

3)　Device A （ソース装置）を設定します。

リモートソースグループを作成します。

```
<DeviceA> system-view
[DeviceA] mirroring-group 1 remote-source
```

VLAN 2 を作成します。

```
[DeviceA] vlan 2
```

VLAN 2 で MAC アドレスの学習を無効にします。

```
[DeviceA-vlan2] undo mac-address mac-learning enable
[DeviceA-vlan2] quit
```

#ミラーリンググループのリモートプローブ VLAN として VLAN 2 を設定します。

```
[DeviceA] mirroring-group 1 remote-probe vlan 2
```

ミラーリンググループのソースポートとして GigabitEthernet 1/0/1 を設定します。

```
[DeviceA] mirroring-group 1 mirroring-port gigabitethernet 1/0/1 both
```

ミラーリンググループの出力ポートとして GigabitEthernet 1/0/2 を設定します。

```
[DeviceA] mirroring-group 1 monitor-egress gigabitethernet 1/0/2
```

トランクポートして GigabitEthernet 1/0/2 を設定し、VLAN 2 のパケットを許可するように設定します。

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port link-type trunk
[DeviceA-GigabitEthernet1/0/2] port trunk permit vlan 2
```

ポートのスパニングツリーを無効にします。

```
[DeviceA-GigabitEthernet1/0/2] undo stp enable
[DeviceA-GigabitEthernet1/0/2] quit
```

III. 設定の確認

Device C のミラーリンググループの設定を確認します。

```
[DeviceC] display mirroring-group all
Mirroring group 2:
    Type: Remote destination
    Status: Active
    Monitor port: GigabitEthernet1/0/2
    Remote probe VLAN: 2
```

Device A のミラーリンググループの設定を確認します。

```
[DeviceA] display mirroring-group all
Mirroring group 1:
    Type: Remote source
    Status: Active
    Mirroring port:
        GigabitEthernet1/0/1  Both
    Monitor egress port: GigabitEthernet1/0/2
    Remote probe VLAN: 2
```

7.6.4 複数のモニタポートのローカルポートミラーリングの設定例

I. ネットワーク要件

図 7-7に示すように、Department A、Department B、Department C は、GigabitEthernet1/0/1、GigabitEthernet1/0/2、GigabitEthernet1/0/3 を通して、それぞれ Device A と接続されています。3 つの部門の双方向トラフィックを監視できるように、3 つのデータモニタリング装置（Server A、Server B、Server C）を有効にし、ポートミラーリングを設定します。

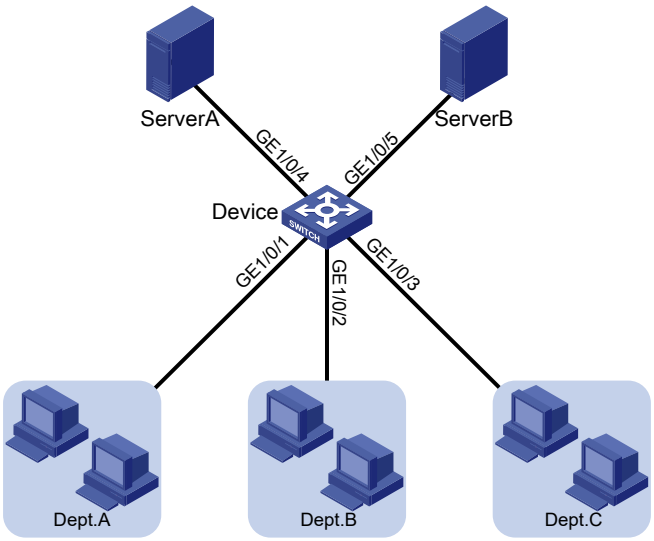


図 7-7 ネットワーク図

II. 設定手順

リモートソースミラーリンググループ 1 を作成します。

```
<Device> system-view
[Device] mirroring-group 1 remote-source
```

リモートソースグループ 1 のソースポートとして GigabitEthernet 1/0/1～GigabitEthernet 1/0/3 を設定します。

```
[Device] mirroring-group 1 mirroring-port gigabitethernet 1/0/1 to gigabitethernet 1/0/3 both
```

Device A の未使用ポート（例：GigabitEthernet 1/0/6）をリモートソースグループ 1 のリフレクタポートとして設定します。

```
[Device] mirroring-group 1 reflector-port gigabitethernet 1/0/6
This operation may delete all settings made on the interface. Continue? [Y/N]:y
```

VLAN 10 を作成します。データモニタリング装置に接続されている GigabitEthernet 1/0/4、GigabitEthernet 1/0/5 を VLAN 10 に割り当てます。

```
[Device] vlan 10
[Device-vlan10] port gigabitethernet 1/0/4 to gigabitethernet 1/0/5
[Device-vlan10] quit
```

リモートソースグループ 1 のリモートプローブ VLAN として VLAN 10 を設定します。

```
[Device] mirroring-group 1 remote-probe vlan 10
```

目次

このセクションのページは **9-x-x** です。

8 章 トラフィックミラーリング 8-1
8.1 トラフィックミラーリングの設定作業リスト 8-1
8.2 一致条件の設定 8-1
8.3 トラフィック動作の設定 8-2
8.4 QoS ポリシーの設定 8-2
8.5 QoS ポリシーの適用 8-2
8.5.1 インタフェースへの QoS ポリシーの適用 8-2
8.5.2 VLAN への QoS ポリシーの適用 8-3
8.5.3 グローバルへの QoS ポリシーの適用 8-3
8.6 トラフィックミラーリングの設定例 8-3
8.6.1 ネットワーク要件 8-3
8.6.2 設定手順 8-4
8.6.3 設定の確認 8-5

8章 トラフィックミラーリング

トラフィックミラーリング（フローミラーリング）は、パケットの監視と解析を行うために、クラスに一致したパケットを指定した宛先にコピーします。これは QoS ポリシーにもとづいて実行されます。

トラフィックミラーリングを設定するため、以下の作業を実行します。

- トラフィッククラスを定義し、ミラーリングされるパケットを分類するために一致条件を設定します。一致基準を定義し、解析されたパケットを柔軟に分類します。
- 指定された宛先に対する一致基準に適合するパケットをミラーリングするようにトラフィックの動作を設定します。

以下のインタフェースにミラーリングされるよう、トラフィックを設定することができます。

- **インタフェース**－インタフェースへのトラフィックをミラーリングすると、宛先インタフェースに一致するパケットをコピーします。データをモニタリングする装置はインタフェースで受信されたパケットを解析します。

QoS ポリシー、トラフィッククラス、トラフィック動作の詳細は、コマンドマニュアルのセクション 6 *ACL and QoS* "*QoS ポリシー*"を参照してください。

8.1 トラフィックミラーリングの設定作業リスト

作業リスト
（必須設定項目） 一致条件の設定
（必須設定項目）トラフィック動作の設定
（必須設定項目） QoSポリシーの設定
（必須設定項目） QoSポリシーの適用 • インタフェースへのQoSポリシーの適用 • VLANへのQoSポリシーの適用 • グローバルへのQoSポリシーの適用

mirror-to コマンドを除いたコマンドの詳細は、コマンドマニュアルのセクション 6 *ACL and QoS* "*QoS ポリシー*"を参照してください。

8.2 一致条件の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． クラスを作成し class view に移行する	**traffic classifier** *classifier-name* [**operator** { **and** | **or** }]	デフォルト：設定なし
3． 一致条件の設定をする	**if-match** *match-criteria*	デフォルト：設定なし

8.3 トラフィック動作の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． トラフィック動作を設定し traffic behavior view に移行する	**traffic behavior** *behavior-name*	デフォルト：設定なし ミラーリングアクションを含むトラフィック動作に最大4つの設定を行うことができます。5つ以上のトラフィック動作を設定した場合、最初の4つのトラフィック動作が適用されます。
3． トラフィック動作のミラーリング宛先を指定する	**mirror-to interface** *interface-type interface-number*	デフォルト：設定なし トラフィック動作において、1つのインタフェースのみトラフィックを監視することができます。複数回コマンドを実行した場合、最後に行った設定が適用されます。
4． （オプション設定項目）トラフィック動作の設定を表示する	**display traffic behavior**	すべてのviewで実行可能です。

8.4 QoSポリシーの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． QoS ポリシーを作成し qos policy view に移行する	**qos policy** *policy-name*	デフォルト：設定なし
3． QoS ポリシーのトラフィック動作とクラスを関連づける	**classifier** *classifier-name* **behavior** *behavior-name*	デフォルト：設定なし
4． （オプション設定項目）QoS ポリシーの設定を表示する	**display qos policy**	すべてのviewで実行可能です。

8.5 QoSポリシーの適用

8.5.1 インタフェースへの QoS ポリシーの適用

インタフェースに QoS ポリシーを適用することで、インタフェース上の指定された方向にトラフィックをミラーリングすることができます。ポリシーは複数のインタフェースに適用することができますが、インタフェースの一つの方向（入力または出力）で、1 つのポリシーだけを適用することができます。

出力方向のトラフィックミラーリングはサポートしていません。

インタフェースに QoS ポリシーを適用するには、以下の手順に従ってください。

操作	コマンド
1． system view に移行する	**system-view**
2． interface view に移行する	**interface** *interface-type interface-number*
3． インタフェースに QoS ポリシーを適用する	**qos apply policy** *policy-name* **inbound**

8.5.2 VLAN への QoS ポリシーの適用

VLAN に QoS ポリシーを適用することで､VLAN 内のすべてのポート上の指定された方向にトラフィックをミラーリングすることができます。

出力方向のトラフィックミラーリングはサポートしていません。

VLAN に QoS ポリシーを適用するには、以下の手順に従ってください。

操作	コマンド
1． system view に移行する	**system-view**
2． VLAN に QoS ポリシーを適用する	**qos vlan-policy** *policy-name* **vlan** *vlan-id-list* **inbound**

8.5.3 グローバルへの QoS ポリシーの適用

グローバルに QoS ポリシーを適用することで、すべてのポートで指定された方向にトラフィックをミラーリングすることができます。

出力方向のトラフィックミラーリングはサポートしていません。

すべてのポートに QoS ポリシーを適用するには、以下の手順に従ってください。

操作	コマンド
1． system view に移行する	**system-view**
2． グローバルに QoS ポリシーを適用する	**qos apply policy** *policy-name* **global inbound**

8.6 トラフィックミラーリングの設定例

8.6.1 ネットワーク要件

図 8-1に示すように、サーバが以下のトラフィックをミラーリングできるようにトラフィックミラーリングを設定します。

- Technical Department がインターネットにアクセスする送信トラフィックを監視します。
- Technical Department が平日の 8:00 から 18:00 までの間に Marketing Department に送信する IP トラフィックを監視します。

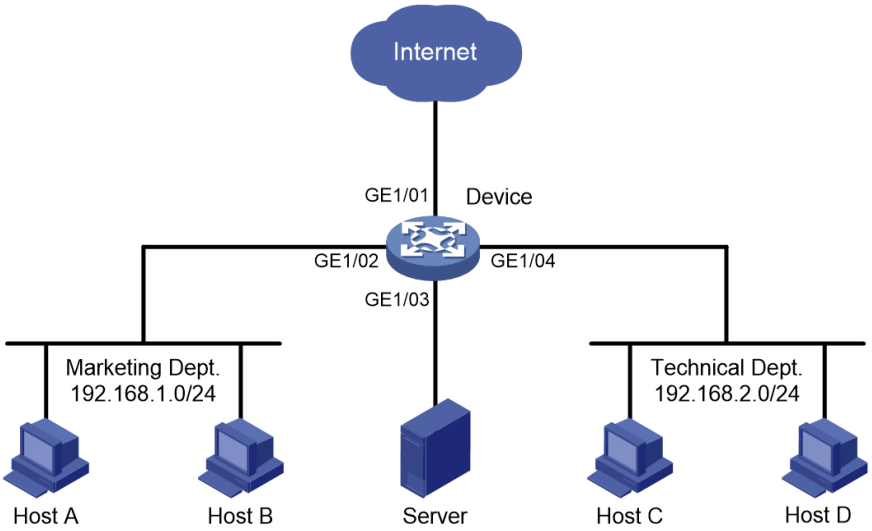


図 8-1 ネットワーク図

8.6.2 設定手順

平日の 8:00 から 18:00 までのタイムレンジを設定します。

```
<DeviceA > system-view
[DeviceA] time-range work 8:00 to 18:00 working-day
```

就業時間内に Technical Department からのパケットがインターネットにアクセスできるよう拡張 IPv4 ACL 3000 を作成します。

```
[DeviceA] acl advanced 3000
[DeviceA-acl-ipv4-adv-3000] rule permit tcp source 192.168.2.0 0.0.0.255 destination-port eq www
[DeviceA-acl-ipv4-adv-3000] rule permit ip source 192.168.2.0 0.0.0.255 destination 192.168.1.0 0.0.0.255 time-range work
[DeviceA-acl-ipv4-adv-3000] quit
```

トラフィッククラス **tech_c** を作成し、ACL 3000 の一致条件を設定します。

```
[DeviceA] traffic classifier tech_c
[DeviceA-classifier-tech_c] if-match acl 3000
[DeviceA-classifier-tech_c] quit
```

トラフィック動作 **tech_b** を作成し、GigabitEthernet 1/0/3 ポートのトラフィックミラーリングの動作を設定します。

```
[DeviceA] traffic behavior tech_b
[DeviceA-behavior-tech_b] mirror-to interface gigabitethernet 1/0/3
[DeviceA-behavior-tech_b] quit
```

QoS ポリシー**tech_p** を作成し、QoS ポリシーのトラフィック動作 **tech_b** とトラフィッククラス **tech_c** を関連づけます。

```
[DeviceA] qos policy tech_p
[DeviceA-qospolicy-tech_p] classifier tech_c behavior tech_b
[DeviceA-qospolicy-tech_p] quit
```

QoS ポリシー**tech_p** を GigabitEthernet 1/0/4 の入力パケットに適用します。

```
[DeviceA] interface gigabitethernet 1/0/4
[DeviceA-GigabitEthernet1/0/4] qos apply policy tech_p inbound
[DeviceA-GigabitEthernet1/0/4] quit
```

8.6.3 設定の確認

設定の完了後、サーバは以下のことができます。

- Technical Department がインターネットにアクセスする送信トラフィックを監視することができます。
- 就業時間内に Technical Department が Marketing Department に送信する IP トラフィックのすべてを監視することができます。

目次

このセクションのページは **9-x-x** です。

9 章 プロセスモニタリングとメンテナンス 9-1
9.1 ユーザプロセスの表示と維持 9-1

9章 プロセスモニタリングとメンテナンス

装置のシステムソフトウェアは、フル機能でモジュラー型の Linux カーネルをベースにした拡張可能なネットワークオペレーティングシステムです。システム（Comware）ソフトウェアは、独立した以下のプロセスがあります。

- **ユーザプロセス**－ユーザ空間で動作します。ユーザプロセスでたいていのシステムソフトウェア機能が動作します。各プロセスは、独立して動作します。あるプロセスが故障しても、その他のプロセスに影響しません。システムは自動的にユーザプロセスをモニタリングします。システムソフトウェアは preemptive マルチスレッティングをサポートしています。プロセスは複数のアクティビティをサポートするために、複数のスレッドを動作することができます。マルチスレッティングの実装は、ソフトウェアのバージョンに依存します。

9.1 ユーザプロセスの表示と維持

すべての view で **display** コマンドを実行でき、user view でその他のコマンドを実行できます。

操作	コマンド
プロセス例外に関する情報を表示する	**display exception context** [**count** *value*] [**slot** *slot-number*]
コアファイルディレクトリを表示する	**display exception filepath** [**slot** *slot-number*]
例外でコアファイルを作成するためのプロセスを有効あるいは無効にし、コアファイルの最大数(デフォルトは 1）を設定する	**process core** { **maxcore** *value* | **off** } { **name** *process-name* } [**slot** *slot-number*]
コアファイルを保存するディレクトリ（デフォルトはマスタ装置のflash:/）を指定する	**exception filepath** *directory*
プロセス例外に関する情報をクリアする	**reset exception context** [**slot** *slot-number*]

目次

このセクションのページは **9-x-x** です。

10章 PoE 10-1
10.1 概要 10-1
10.2 PoE設定作業リスト 10-2
10.3 PIのPoEの有効化 10-2
10.4 PDによる突入電流の許容 10-3
10.5 PIの最大電力の設定 10-4
10.6 PI電力管理の設定 10-4
10.7 PoEモニタリングの設定 10-6
10.8 PoEプロファイルを使用したPIの設定 10-6
10.8.1 PoEプロファイルの設定 10-6
10.8.2 PoEプロファイルの適用 10-7
10.9 動作中でのPSEファームウェアのアップグレード 10-7
10.10 PoEの表示と維持 10-8
10.11 PoE設定例 10-8
10.12 PoEのトラブルシューティング 10-10
10.12.1 PIの優先度をcriticalに設定できない 10-10
10.12.2 PIにPoEプロファイルを適用できない 10-10

10章 PoE

🕮 **メモ:**

- PoE 機能は 10/100/1000 BASE-T イーサネットでサポートしています。PI view は PoE 機能をサポートしているポートの Ethernet interface view を意味します。
- PoE 機能は Version 7.4.61 以降のバージョンでサポートしています。
- poe standard コマンドと poe high-inrush enable コマンドの両機能を設定する場合は、先に poe high-inrush enable コマンドを設定してください。詳細はコマンドマニュアル -システム管理- 10 章 PoE の poe high-inrush enable を参照ください。

10.1 概要

IEEE 802.3at 準拠の PoE＋（Power Over Ethernet）は、ツイストペアケーブルを介して端末に電力を供給するネットワーク装置を有効にします。

図 10-1に示すように、PoE システムは以下の要素があります。

- **PoE 電源**－PoE 電源はすべての PoE システムの電力を供給します。
- **PSE**－PSE（電力供給装置）は PD（電力受電装置）を検出し、分類します。そして PD に電力を供給し、PD 電力と接続状態をモニタします。PSE は endpoint PSE と midspan PSE があります。

QX-S1100G シリーズの PSE は endpoint PSE です。複数の PSE が存在する装置は異なる PSE を識別するために PSE ID を使用します。PSE ID と PSE のスロットあるいはサブスロット番号間のマッピングを表示する場合、**display poe device** コマンドを使用します。

- **PI（電力インタフェース）**– 電力インタフェースは PSE の PoE が有効な Ethernet インタフェースです。
- **PD（電力受電装置）**– PD は PSE から電力を受電します。

PD は IP 電話、AP、ポータブルチャージャ、POS 端末、Web カメラなどがあります。

信頼性を向上させるため、冗長電力ソースに PD を接続することができます。

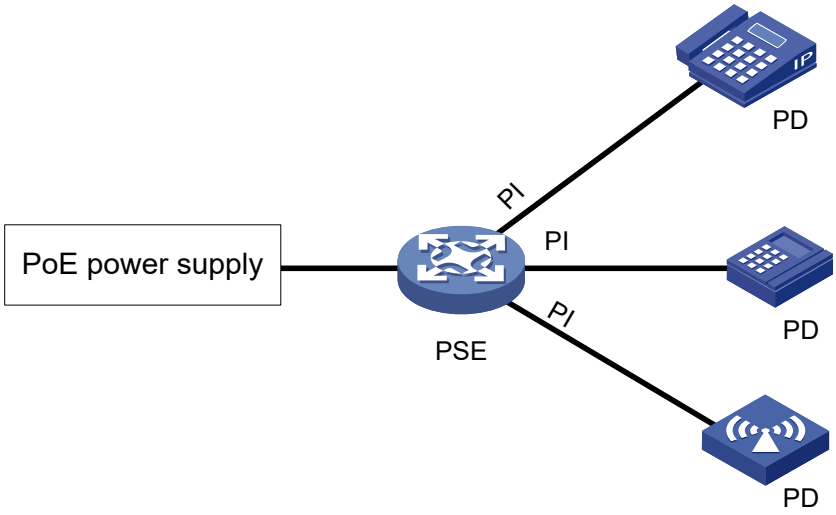


図 10-1 PoE システム図

10.2 PoE設定作業リスト

ポートで直接 PI を設定することができます。あるいは PoE プロファイルを設定し、PI に PoE プロファイルを適用することができます。1 つの PI を設定する場合、ポートに直接設定します。複数の PI を一括して設定する場合、PoE プロファイルを使用します。

PoE を設定する前に、PoE 電源と PSE が正常に動作することを確認してください。そうでない場合、PoE を設定できない、あるいは PoE の設定を適用することができません。

作業リスト
（必須設定項目）PIのPoEの有効化
（オプション設定項目）PIの最大電力の設定
（オプション設定項目）PI電力管理の設定
（オプション設定項目）PoE電力モニタリングの設定
（オプション設定項目）PoEプロファイルを使用したPIの設定 • PoEプロファイルの設定 • PoEプロファイルの適用
（オプション設定項目）動作中でのPSEファームウェアのアップグレード

10.3 PIのPoEの有効化

PI の PoE を有効にした後、PI が PSE 電力過負荷を引き起こさない場合、PI は接続された PD に電力を供給します。PSE の過負荷は、すべての PI の電力消費量の合計が PSE の最大電力を超えると発生します。

PI が PSE 電力の過負荷になる場合、PI 電力管理が有効である場合、PI で PoE を有効にすることができます。PI 電力管理の詳細は、オペレーションマニュアルのセクション 9 *システム管理”PoE”の”PI 電力管理の設定”*を参照してください。

PSE は、PI に接続されたツイストペアを経由して、以下のモードで電力を供給します。

- **signal ペアモード**－ツイストペアケーブルの信号ペア 1、2、3、6 が電力伝送に使用されます。
- **spare ペアモード**－ツイストペアケーブルのスペアペア 4、5、7、8 が電力伝送に使用されます。

🕮 **メモ：**

- QX-S1100G シリーズは signal モードでのみ電力を供給します。
- PI と PD が同じ電力伝送モードを使用する場合にのみ、PI は PD に電力を供給できます。PI と PD が異なる電力伝送モードを使用する場合、電力を供給できません。

以下に PI で PoE を有効にする設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． PI view に移行する	**interface** *interface-type interface-number*	―
3． （オプション設定項目）PI に接続された PD の説明を設定する	**poe pd-description** *text*	デフォルト：設定なし
4． PI で PoE を有効にする	**poe enable**	デフォルト：有効

10.4 PDによる突入電流の許容

🕮 **メモ:**

poe standard コマンドと poe high-inrush enable コマンドの両機能を設定する場合は、先に poe high-inrush enable コマンドを設定してください。詳細はコマンドマニュアル -システム管理- 10 章 PoE の poe high-inrush enable を参照ください。

PD の起動時に突入電流が発生し、PSE の自己保護を引き起こすことがあります。その結果、PSE は PD への電力供給を停止します。PD への電源供給を継続するには、PD が消費する突入電流を許可するようにこの機能を設定します。設定を変更する場合は注意してください。

IEEE 802.3 af および IEEE 802.3 at は、突入電流の仕様を定義します。この装置は、IEEE 802.3 af および IEEE 802.3 at で定義された突入電流の仕様をサポートします。

I. 設定手順

操作	コマンド	補足
5． system view に移行する	**system-view**	―
6． PD による突入電流を許容する	**poe high-inrush enable pse** *pse-id*	デフォルト：無効

10.5 PIの最大電力の設定

PI の最大電力は接続された PD に供給できる最大電力です。PD が PI の最大電力より多くの電力を必要とする場合、PI は PD に電力を供給しません。

以下に PI の最大電力の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． PI view に移行する	**interface** *interface-type interface-number*	ー
3． （オプション設定項目）PI の最大電力を設定する	**poe max-power** *max-power*	デフォルト：30000ミリW

10.6 PI電力管理の設定

PSE 電力が過負荷の状況下において、PI 電力管理機能を有効にすると、PSE は優先度をもとにして PI 電力の管理を行います。PI の電力供給の優先度レベルは critical、high、low の順番で低くなります。PD の優先度は、PD が接続している PI の優先度によって決められます。すべての PSE は同じ PI 電力管理メカニズムを使用します。

PI 電力管理を無効にした場合、PSE が過負荷となる可能性があります。PSE の電力が過負荷になると、最大 PSE 電力の状態にもとづいて動作を実行します。

最大 PSE 電力の状態	過負荷での PSE の動作
設定あり	PSEは新しいPDへの電力を停止します。
設定なし	PoE自己保護メカニズムが開始された場合、PSEはすべてのPDへの電力を停止します。

PI 電力管理を有効にした場合、PSE が過負荷になると、PSE は既存の PD への電力供給を停止する、あるいは優先度をもとにして新しい PD への電力供給を実行します。

新しい PD の優先度	PD の動作
low	PSEは新しいPDに電力を供給しません。
high	• lowの優先度のPDが存在する場合、PSEは既存のlowの優先度のPDへの電力の供給を停止します。そして新しいPDに電力を供給します。 • lowの優先度のPDが存在しない場合、PSEは新しいPDに電力を供給しません。
critical	• lowあるいはhighの優先度のPDが存在する場合、PSEは既存のlowあるいはhighの優先度のPDへの電力の供給を停止します。そして新しいPDに電力を供給します。 • lowあるいはhighの優先度のPDが存在しない場合、PSEは新しいPDに電力を供給しません。

複数の新しい PD が電力供給を必要とする場合、PSE は優先度が高い順で PD に電力を供給します。優先度が同じ場合、もっとも小さい PD の ID を持つ PD が優先されます。

複数の既存の PD が電力供給を停止する必要がある場合、PSE は優先度が低い順で PD への電力を停止します。優先度が同じ場合、もっとも大きい PD の ID を持つ PD から電力を停止します。

PSE は保証された PSE 電力を予約することで、critical の優先度を持つ PI への電力供給を停止しないことを保証します。PI に電力供給を停止しないように割り当てる場合、PI に critical の優先度を設定します。そうでない場合、ほかの PI に電力を供給できるようにするため、PI に high あるいは low の優先度を設定します。

critical の優先度を持つ PI を設定する前に、保証余力電力が、PI の最大電力以上であることを確認してください。保証余力電力は、PSE で供給可能な電力から、PoE が有効および無効な critical の優先度を持つ PI の最大電力の合計を引いた値です。

突然の PD の電力上昇による電力供給の切断を避けるため、装置の各 PoE インタフェースには保証電力が確保されています。PSE の余力電力が保証余力電力未満で PoE インタフェースに優先度が設定されている場合、高い優先度を持つ PoE インタフェースの動作を保証するため、高い優先度を持つ PoE インタフェースへの電力供給は低い優先度の PoE インタフェースよりも優先されます。また、新しい PD を接続する際には、PD を接続する PoE インタフェースの優先度が接続済みの PoE インタフェースよりも低く、PSE の余力電力が保証余力電力よりも小さい場合、PSE は新しい PD に電力を供給しません。

以下に Class 毎の保証余力電力を示します。

装置	Class	保証余力電力
S1108GT-2G-PW	0	17W
	1	4.6W
	2	8W
	3	17W
	4	31W
S1116GT-4G-PW S1124GT-4G-PW	0	16.1W
	1	4W
	2	7.2W
	3	16.1W
	4	31W

以下に PI 電力管理の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． PI 電力管理を有効にする	**poe pd-policy priority**	デフォルト：無効
3． PI view に移行する	**interface** *interface-type interface-number*	―
4． （オプション設定項目）PI の電力供給の優先度を設定する	**poe priority** { **critical** | **high** | **low** }	デフォルト：low

🕮 **メモ：**

電力があらかじめ予約されている PI への設定は変更ありません。

10.7 PoEモニタリングの設定

システムは PSE 電力の使用率をモニタし、PSE 電力供給がしきい値を超過あるいは下回った場合、SNMP notification メッセージを送信します。

PSE 電力の使用率がしきい値を越えたあるいは下回った場合、システムは超過あるいは下回った都度、SNMP notification メッセージを送信します。SNMP notification の詳細は、オペレーションマニュアルのセクション 9 *システム管理*”*SNMP*”を参照してください。

以下に PSE 電力アラームのしきい値の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． PSE の電力アラームのしきい値を設定する	**poe utilization-threshold** *value* **pse** *pse-id*	デフォルト：80%

10.8 PoEプロファイルを使用したPIの設定

PoE プロファイルは複数の PoE の設定を集めたものです。

ポートで PI を設定する、あるいは PoE プロファイルを使用して PI を設定することができます。PI のパラメータを設定する場合以下のガイドラインに従ってください。

- **poe max-power** *max-power* コマンドと **poe priority** { **critical** | **high** | **low** }コマンドは同一の方式になるようにしてください。
- 異なる方式でパラメータを設定した場合、最初の設定が有効となります。設定を変更する場合、最初の設定を削除してから、再度設定を行ってください。

PI の一括設定と PD 固有の PI の設定を行う場合、PoE プロファイルを活用することができます。

- PoE プロファイルを用いて、複数の PI に同じ設定を行うことができます。同じ PoE プロファイルで設定された PI は同じ PoE 機能となります。
- PoE プロファイルで PD の PoE 設定を定義することができます。PD が接続している PI に PoE プロファイルを適用することができます。PD が別の PI に移動した場合、PoE プロファイルを新しい PI に適用することで、再度設定する必要がありません。それによって PoE の設定を簡略化することができます。

10.8.1 PoE プロファイルの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． PoE プロファイルを作成し、PoE profile view に移行する	**poe-profile** *profile-name* [*index*]	デフォルト：設定なし
3． PoE を有効にする	**poe enable**	デフォルト：有効
4． （オプション設定項目）PI の最大電力を設定する	**poe max-power** *max-power*	デフォルト：30000ミリW

操作	コマンド	補足
5.　（オプション設定項目）PI の電力供給の優先度を設定する	**poe priority** { **critical** | **high** | **low** }	デフォルト：low

10.8.2 PoE プロファイルの適用

PoE プロファイルは system view あるいは PI view で適用することができます。system view あるいは PI view の両方の view で設定した場合、後から設定した view の設定が適用されます。PoE プロファイルは、複数の PI に適用できますが、PI は 1 つの PoE プロファイルのみ適用されます。

PoE プロファイルが適用されている場合、PoE プロファイルを変更する前に **undo apply poe-profile** コマンドあるいは **undo apply poe-profile interface** コマンドを使用してください。

I. 複数の PI への PoE プロファイルの適用（system view）

操作	コマンド	補足
1.　system view に移行する	**system-view**	―
2.　1 つ以上の PI に PoE プロファイルを適用する	**apply poe-profile** { **index** *index* | **name** *profile-name* } **interface** *interface-range*	デフォルト：設定なし

II. 1 つの PI への PoE プロファイルの適用（PI view）

操作	コマンド	補足
1.　system view に移行する	**system-view**	―
2.　PI に PoE プロファイルを適用する	**apply poe-profile** { **index** *index* | **name** *profile-name* }	デフォルト：設定なし

10.9 動作中でのPSEファームウェアのアップグレード

装置の動作中に以下のモードで PSE ファームウェアをアップグレードすることができます。

- **refresh モード**– PSE ファームウェアを削除しないで PSE ファームウェアをアップグレードします。通常、refresh モードで PSE ファームウェアをアップグレードします。
- **full モード**– 現在の PSE ファームウェアを削除し、新しい PSE ファームウェアで再起動します。PSE ファームウェアが故障し、PoE コマンドを実行できない場合、full モードを使用します。

装置の再起動による中断によって、PSE ファームウェアのアップグレードに失敗した場合、装置を再起動し、再度 full モードで PSE ファームウェアのアップグレードを行います。アップグレードを行った後、新しい PSE ファームウェアを適用するため、手動で装置を再起動します。

以下に装置の動作中に PSE ファームウェアのアップグレードの方法を示します。

操作	コマンド
1． system view に移行する	**system-view**
2． 装置の動作中に PSE ファームウェアのアップグレードを行う	**poe update** { **full** | **refresh** } *filename* [**pse** *pse-id*]

10.10 PoEの表示と維持

すべての view で display コマンドを実行することができます。

操作	コマンド
PSE情報を表示する	**display poe device** [**slot** *slot-number*]
PIの電力供給の情報を表示する	**display poe interface** [*interface-type interface-number*]
PIの電力情報を表示する	**display poe interface power** [*interface-type interface-number*]
PSEの情報を表示する	**display poe pse** [*pse-id*]
PSEのすべてのPIの電力供給の状態を表示する	**display poe pse** *pse-id* **interface**
PSEのすべてのPIの電力情報を表示する	**display poe pse** *pse-id* **interface power**
PoEプロファイルのすべての情報を表示する	**display poe-profile** [**index** *index* | **name** *profile-name*]
PIに適用されたPoEプロファイルの情報を表示する	**display poe-profile interface** *interface-type interface-number*

10.11 PoE設定例

I. ネットワーク要件

図 10-2に示すように、PoE を次のように設定します。

- IP phone と AP に電力の供給を行います。
- 電力過負荷の状態になった場合、IP phone への電力の供給を優先させます。
- AP B の最大電力を 9000 ミリ W に割り当てます。

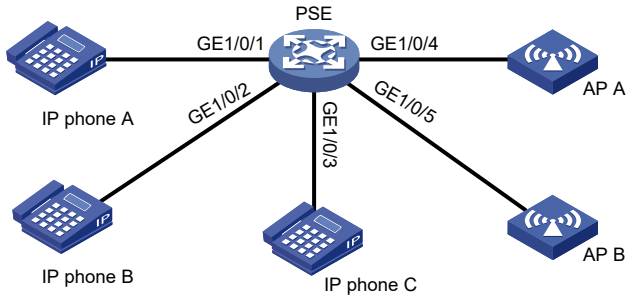


図 10-2 ネットワーク図

II. 設定手順

装置で、電力管理を有効に設定します。GigabitEthernet 1/0/1、GigabitEthernet 1/0/2、GigabitEthernet 1/0/3 で電力供給の優先度を critical に設定します。

```
<PSE> system-view
[PSE] interface gigabitethernet 1/0/1
[PSE-GigabitEthernet1/0/1] poe enable
[PSE-GigabitEthernet1/0/1] poe priority critical
[PSE-GigabitEthernet1/0/1] quit
[PSE] interface gigabitethernet 1/0/2
[PSE-GigabitEthernet1/0/2] poe enable
[PSE-GigabitEthernet1/0/2] poe priority critical
[PSE-GigabitEthernet1/0/2] quit
[PSE] interface gigabitethernet 1/0/3
[PSE-GigabitEthernet1/0/3] poe enable
[PSE-GigabitEthernet1/0/3] poe priority critical
[PSE-GigabitEthernet1/0/3] quit
```

GigabitEthernet 1/0/4、GigabitEthernet 1/0/5 で電力管理を有効に設定します。GigabitEthernet 1/0/5 の最大電力を 9000 ミリ W に設定します。

```
[PSE] interface gigabitethernet 1/0/4
[PSE-GigabitEthernet1/0/4] poe enable
[PSE-GigabitEthernet1/0/4] quit
[PSE] interface gigabitethernet 1/0/5
[PSE-GigabitEthernet1/0/5] poe enable
[PSE-GigabitEthernet1/0/5] poe max-power 9000
```

III. 設定の確認

IP phone と AP で正常に電力が取得できることを確認するため、IP phone と AP を PSE に接続します。（詳細は省略します。）

10.12 PoEのトラブルシューティング

10.12.1 PI の優先度を critical に設定できない

I. 症状

PI の電力供給の優先度の設定が失敗しました。

II. 分析

可能性のある理由を以下に示します。

1) PI の保証余力電力が PI で要求された最大電力よりも小さいです。
2) PI の優先度がすでに設定されています。

III. 解決策

以下を確認してください。

1) 1 番目のケースの場合、PSE の最大電力を増加するか、PSE の残りの電力を変更できない場合、PI の最大電力を削減します。
2) 2 番目のケースの場合、すでに設定されている優先度を削除します。
3) 問題が解決しない場合、NEC に問い合わせてください。

10.12.2 PI に PoE プロファイルを適用できない

I. 症状

PI に PoE プロファイルを適用できません。

II. 分析

可能性のある理由を以下に示します。

1) PoE プロファイルのいくつかの設定がすでに設定されています。
2) PoE プロファイルのいくつかの設定が PI の設定要件を満たしていません。
3) すでに別の PoE プロファイルが PI に適用されています。

III. 解決策

以下を確認してください。

1) 1 番目のケースの場合、もとの設定を削除します。
2) 2 番目のケースの場合、PoE プロファイルの設定を修正します。
3) 3 番目のケースの場合、PI から予定していない PoE プロファイルの適用を削除します。
4) 問題が解決しない場合、NEC に問い合わせてください。

目次

このセクションのページは **9-x-x** です。

11 章 NetMeister 11-1
11.1 概要 11-1
11.1.1 NetMeister の利用 11-1
11.1.2 設定手段について 11-3
11.2 設定作業リスト 11-4
11.2.1 手動設定による NetMeister の利用 11-5
11.2.2 ゼロタッチプロビジョニング機能による NetMeister の利用 11-7
11.3 NetMeister による管理 11-15
11.3.1 タブ一覧 11-15
11.4 NetMeister の設定例 11-16
11.5 NetMeister 利用のトラブルシューティング 11-18
11.5.1 NetMeister に QX が登録できない 11-18
11.5.2 NetMeister でグラフが正しく表示されない。 11-18
11.5.3 NetMeister のリモートログインが使えない 11-19
11.5.4 ファームウェア更新が成功しない 11-19
11.5.5 NetMeisterPrime 機能が使用できない 11-20

11章 NetMeister

> 🕮 **メモ:**
> Version 7.1.16 を含む以降のソフトウェアから親機モードでの NetMeister への接続をサポートしています。

11.1 概要

NetMeister(ネットマイスター)は、NEC プラットフォームズが提供するクラウド型統合管理サービスです。NetMeister 対応のネットワーク機器をクラウド上で一元的に管理することができます。この章では、本装置を NetMeister に登録するための設定について説明します。

NetMeister の操作/詳細に関しては、以下 NetMeister ポータルサイトをご確認ください。

https://www.necplatforms.co.jp/product/netmeister/

11.1.1 NetMeister の利用

NetMeister を利用する場合、あらかじめ NetMeister のサイトで「アカウント登録」と「グループ登録」が必要です。

QX シリーズは、NetMeister における親機モード、および、子機モードをサポートします。

親機モードでは、NetMeister と MQTT によって直接接続状態を確立し、NetMeister によって管理する事ができます。ただし、親機モードには、NetMeister Prime(有償サービス) の利用が必要です。NetMeister Prime については NetMeister が提供する操作ガイドをご確認ください。

子機モードでは、親機モードの装置と連携する事で NetMeister からの応答を受け、NetMeister によって管理する事ができます。図 11-1に示すように、親機モードの機器が設置されている環境が必要です。子機モードだけでは NetMeister を利用できません。

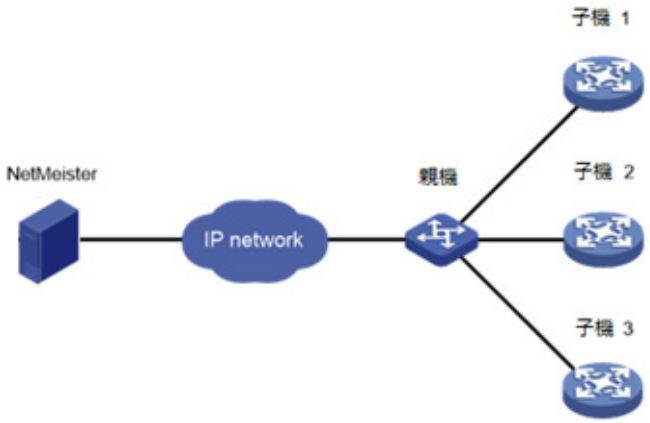


図 11-1 NetMeister との接続イメージ

子機モードを NetMeister によって管理する場合、親機モードの機器と同じのグループに属する必要があります。図 11-2に示すように、子機モードは、親機モードの機器との通信と NetMeister と直接通信の両方を利用して NetMeister 上で管理され、NetMeister に関する通信は https(ssl)でおこなわれます。(デフォルトポート番号: 443) 親機モードの NetMeister に関する通信は mqtt(デフォルトポート番号:8883)と https(ssl)でおこなわれます。 (デフォルトポート番号:443)

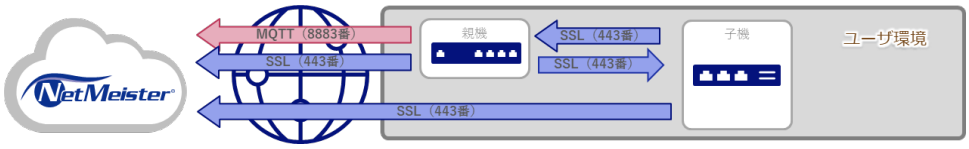


図 11-2 NetMeister への通信イメージ

図 11-3に示すように、プロキシサーバを用いて外部ネットワークに接続をしている環境でも NetMeister を利用可能です。プロキシサーバのアドレスを設定することで、NetMeister 宛の通信をプロキシサーバ経由でおこなうようことが可能です。

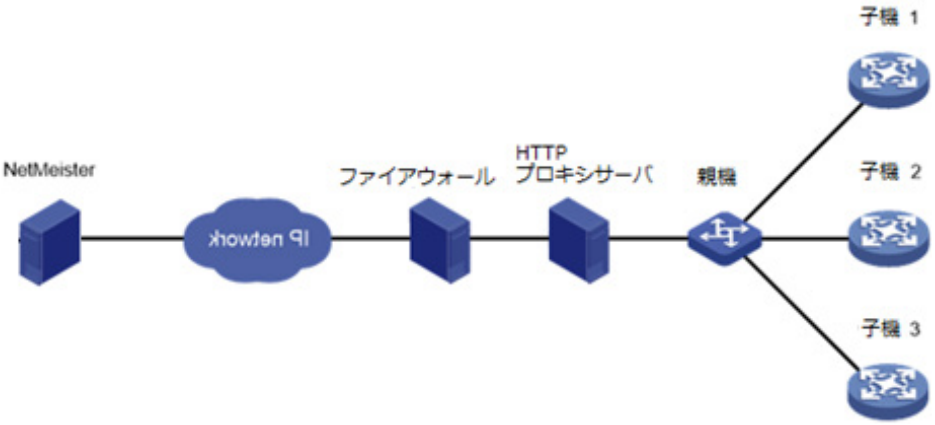


図 11-3 プロキシサーバを用いた NetMeister との接続イメージ

図 11-4に示すように、子機で NetMeister への接続に proxy サーバを利用する場合、NetMeister 宛の通信のみ proxy サーバを経由します。親機と子機の間にプロキシサーバ及びファイアウォールがある様な特殊な環境の場合、親機と子機の間の通信を透過させるために、ファイアウォールで親機の LAN 側 IP 宛の通信を許可する必要があります。同様に、

ファイアウォールを跨ぐ位置にある NTP サーバ/DNS サーバ/SSH クライアント等との通信をする場合は、それらの許可も必要です。

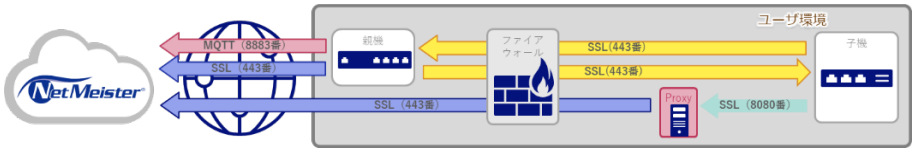


図 11-4 プロキシサーバを用いた NetMeister の通信イメージ

11.1.2 設定手段について

装置を NetMeister で管理をするためには、装置に手動でコンフィグを設定して環境に接続する手段と、ゼロタッチプロビジョニング機能(ZTP 機能)を利用して接続する手段があります。

ゼロタッチプロビジョニング機能は、スタートアップコンフィグレーションファイルを設定されていない状態で装置が起動する場合、NetMeister の親機から受けた DHCP パケットの情報を元に NetMeister から自動でコンフィグレーションファイルを取得し、適用することを可能にします。ゼロタッチプロビジョニング機能は装置に起動コンフィグが設定されていない状態で起動した際に自動で動作します。

図 11-5に示すように、ゼロタッチプロビジョニング機能を利用する場合、管理者が事前に NetMeister 上に装置情報と利用するコンフィグレーションファイルを登録しておくことで、現場で装置設置をする作業者が、装置の操作をすることなく NetMeister に接続することが可能です。

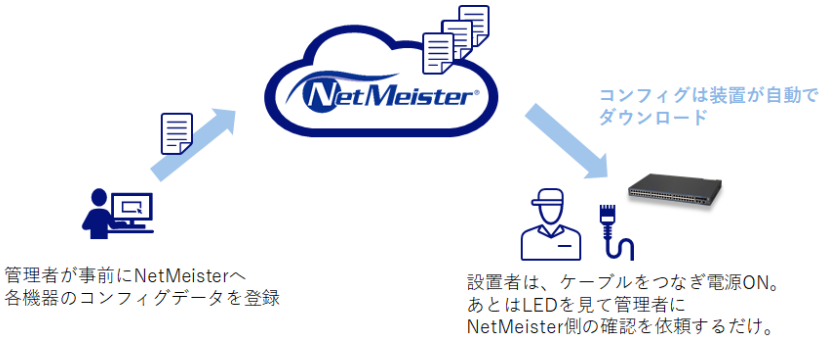


図 11-5 ゼロタッチプロビジョニングのイメージ

ゼロタッチプロビジョニング機能は、Auto Config 機能と交互に実行されます。Auto Config 機能についてはオペレーションマニュアルのセクション 1 はじめに “Auto Config”を参照してください。

11.2 設定作業リスト

設定作業リスト
手動設定による NetMeister の利用
外部ネットワークへの接続準備 ● (必須設定項目) 自装置の IP アドレスの設定 ● (必須設定項目) 使用する DNS サーバの設定 ● (必須設定項目) ルーティングの設定
NetMeister機能に関係する追加設定 ● (推奨設定項目) 時刻、及び、タイムゾーン(+9:00)の設定 ● (オプション設定項目) Web コンソールユーザの設定 ● (オプション設定項目) SSH ユーザの設定 ● (オプション設定項目) LLDP の設定
NetMeisterを利用するための設定 親機モードの場合 ● (オプション設定項目) NetMeister 上に表示するホスト名の設定 ● (必須設定項目) 親機モードの設定 ● (必須設定項目) グループ ID とグループパスワードの設定 ● (オプション設定項目) MQTT ポート番号の設定 ● (必須設定項目) 拠点 ID の指定 ● (オプション設定項目) プロキシサーバのアドレスの設定 ● (必須設定項目) NetMeister 機能の有効化 子機モードの場合 ● (オプション設定項目) NetMeister 上に表示するホスト名の設定 ● (必須設定項目) グループ ID とグループパスワードの設定 ● (必須設定項目) 親機の IP アドレスとポート番号の設定 ● (オプション設定項目) プロキシサーバのアドレスの設定 ● (必須設定項目) NetMeister 機能の有効化
ゼロタッチプロビジョニング機能による NetMeister の利用
事前準備作業 ● (必須設定項目)親機の設定 ● (必須設定項目)コンフィグレーションファイルの準備 ● (必須設定項目)装置情報の確認
NetMeisterへの情報登録 ● (必須設定項目)コンフィグレーションファイルの登録 ● (必須設定項目)装置情報の登録 ● (必須設定項目)プロビジョニングの設定
設置作業 ● (必須設定項目)プロビジョニングの有効化

11.2.1 手動設定による NetMeister の利用

I. 外部ネットワークへの接続準備

NetMeister と通信をするために、装置は親機を通して外部ネットワークに接続できる環境に接続されている必要があります。自装置の IP アドレス、使用する DNS サーバ、ルーティングの設定をしてください。DNS サーバは、親機から通知される NetMeister のアドレスを把握するために必要です。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． VLAN インタフェースを作成し、VLAN interface view に移行する	**interface vlan-interface** *vlan-interface-id*	ー
3． VLAN インタフェースに IP アドレスを割り当てる	・固定アドレスを割り当てる。 **ip address** *ip-address* { *mask* | *mask-length* } [**sub**] ・DHCPでアドレスを取得する **ip address dhcp-alloc**	デフォルト：設定なし
4． VLAN view から戻る	**quit**	ー
5． DNS サーバの IP アドレスを指定する	**dns server** *ip-address*	デフォルト：設定なし DHCPサーバから情報を取得する場合は設定の必要はありません。
6． ルーティングの設定をする	**ip route-static** 0.0.0.0 { 0.0.0.0 | 0 } { *interface-type interface-number* [*next-hop-address* [**nexthop-index** *index-string*]] | *next-hop-address* [**nexthop-index** *index-string*] [**permanent**] } [**preference** *preference*] [**description** *text*]	デフォルト：設定なし DHCPサーバから情報を取得する場合は設定の必要はありません。

II. NetMeister 機能に関係する追加設定

NetMeister で利用する機能によっては従来の装置機能を設定しておく必要があります。

それぞれの機能の設定手順についてはそれぞれの機能の章を参照してください。

NetMeister 機能	必要設定	補足
CPU/メモリ/温度/ポートトラフィック情報表示	時刻 （手動/NTP）、及び、タイムゾーン（+9:00）	設定をしない場合、正しいグラフ情報になりません。
HTTPSでリモートログインする	Webコンソール利用設定	
SSHでリモートログインする	SSH接続利用設定	
デバイスマップを見る（L2モード）	LLDP有効化	親機でも設定が必要です。

III. NetMeister を利用するための設定

1)　親機モードの場合

NetMeister を利用するために、NetMeister のサイトで設定したグループ ID、グループパスワードを設定してください。MQTT のポート番号は 443 に変更が可能です。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. (オプション設定項目) NetMeister 上に表示するホスト名を設定する	**sysname** *sysname*	デフォルト：装置名
3. 親機モードを有効にする	**netmeister mode parent**	デフォルト：無効
4. グループ ID とグループパスワードを設定する	**netmeister account** *account* **password** { **cipher** *cipherPassword* | **simple** *plainPassword* }	デフォルト：設定なし
5. (オプション設定項目) MQTT ポート番号の設定	**netmeister parent-mode mqtt port { 8883 | 443]**	デフォルト：8883
6. 拠点 ID の指定	**netmeister parent-mode sitename** *string*	デフォルト：設定なし
7. (オプション設定項目) プロキシサーバのアドレスを指定する。	**netmeister proxy url** *url* [**username** *username* **password** { **cipher** | **simple** } *string*]	デフォルト：設定なし
8. NetMeister 機能の有効化	**netmeister enable**	デフォルト：無効

2)　子機モードの場合

NetMeister を利用するために、NetMeister のサイトで設定したグループ ID、グループパスワードと、親機の IP アドレス、ポート番号の設定をしてください。プロキシサーバのアドレスを設定すると、NetMeister への https 通信のために任意のプロキシサーバを利用します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. (オプション設定項目) NetMeister 上に表示するホスト名を設定する	**sysname** sysname	デフォルト：装置名
3. グループ ID とグループパスワードを設定する	**netmeister account** *account* **password** { **cipher** *cipherPassword* | **simple** *plainPassword* }	デフォルト：設定なし
4. 親機の IP アドレスとポート番号を指定する	**netmeister parent ip** *ip-address* [**port** *port-number*]	デフォルト：設定なし 最大2つまで設定が可能です。 ポート番号を指定しない場合、デフォルトで443が使用されます。
5. (オプション設定項目) プロキシサーバのアドレスを指定する。	**netmeister proxy url** *url* [**username** *username* **password** { **cipher** | **simple** } *string*]	デフォルト：設定なし
6. NetMeister 機能の有効化	**netmeister enable**	デフォルト：無効

IV. NetMeister の表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
NetMeisterおよび親機との接続状態を表示する	**display netmeister**

11.2.2 ゼロタッチプロビジョニング機能による NetMeister の利用

🕮 **メモ:**
ゼロタッチプロビジョニング機能は Version 7.1.9 を含む以降のソフトウェアからサポートしています。

I. 事前準備作業

🕮 **メモ:**
ゼロタッチプロビジョニング機能の利用可能条件:
- 子機モードで接続する場合、親機モードで接続している装置が必要です。
- Option43 を付与できる DHCP サーバが必要です。
- 事前に装置で利用する正しいコンフィグレーションファイルの準備が必要です。
- 準備するコンフィグレーションファイルは、 1 装置につき 1 つ必要です。
- 事前に利用する装置の MAC アドレス、シリアルナンバー、装置名の情報が必要です。
- コンフィグダウンロード時は、NetMeister 側でダウンロードの有効時間の指定が必要です。

1) DHCP サーバの設定

ゼロタッチプロビジョニング機能を利用する場合、DHCP サーバで Option43 の設定をするか、NetMeister 機能のゼロタッチプロビジョニング子機対応をサポートする親機を DHCP サーバとしてください。設定方法は親機のマニュアル、および NetMeister 操作ガイドを参照してください。

- DHCP サーバ設定 : 子機が外部ネットワークに通信ができるように IP アドレス/DNS サーバアドレス/デフォルトゲートウェイアドレスを設定してください。また、Option43 で以下の内容を通知してください。

  Option43 のフォーマット :

  NEC,zerotouch,<親機 IPv4 アドレス>,<親機待ち受けポート>

  例）NEC,zerotouch,192.0.2.1,443

- NetMeister 機能のゼロタッチプロビジョニング子機対応をサポートする親機を DHCP サーバとして利用する場合、ゼロタッチをおこなう装置にのみ Option43 を付与する設定が可能です。設定方法は使用する親機のマニュアルを参照してください。

メモ:

Option 43 によって通知された親機モードの装置が proxy サーバを利用して NetMeister に接続している場合、子機は NetMeister からのコンフィグレーションファイル取得にその装置と同様の proxy サーバを経由します。親機との通信は proxy サーバを経由しません。Version 7.1.16 を含む以降のソフトウェアからは proxy サーバを経由したゼロタッチプロビジョニングを行う場合以外は Option 43 を必要としません。

2) コンフィグレーションファイルの準備

ゼロタッチプロビジョニング機能で設定を行う対象装置のために、コンフィグファイルをテキストで作成し、zip 圧縮してください。間違ったコンフィグファイルを使用しないよう、あらかじめ実機で確認をしたコンフィグを使用することを推奨します。

下記に用意するコンフィグレーションファイルのサンプル（子機モード）を示します。

```
#
 clock timezone JST add 09:00:00
#
 ssh server enable
#
 ip https enable
#
 lldp global enable
#
interface Vlan-interface1
 ip address dhcp-alloc
#
 ntp-service enable
 ntp-service unicast-server 1.1.1.2
#
line vty 0
 authentication-mode scheme
#
local-user nec class manage
 password simple qx12345678
 service-type ssh https
 authorization-attribute user-role network-admin
#
 netmeister enable
 netmeister account test password simple abcdefg
 netmeister parent ip 1.1.1.1 port 443
#
```

3) 装置情報の確認

ゼロタッチプロビジョニング機能を利用する装置の MAC アドレス、シリアルナンバー、装置名の情報を確認してください。 MAC アドレス、シリアルナンバー、装置名は、梱包箱または装置の本体ラベルに記載されています。

II. NetMeister への情報登録

NetMeister にログインしてください。(NetMeister を利用するためのアカウントおよびグループの作成についての説明は省略します。NetMeister 操作ガイドを確認してください。)

1) NetMeister でのゼロタッチプロビジョニングは、NetMeister 画面左側メニューの「設定」からおこないます。

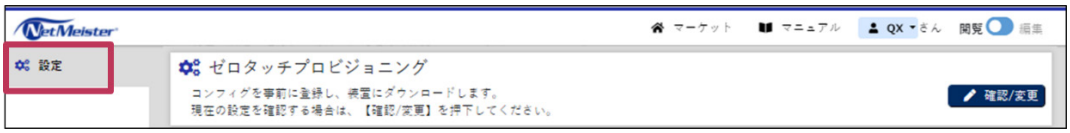


図 11-6 設定メニューの表示

2) ゼロタッチプロビジョニングの設定のために編集モードにします。



図 11-7 編集モードへの変更

3) コンフィグレーションファイルを NetMeister 上に登録します。



図 11-8 コンフィグ登録画面

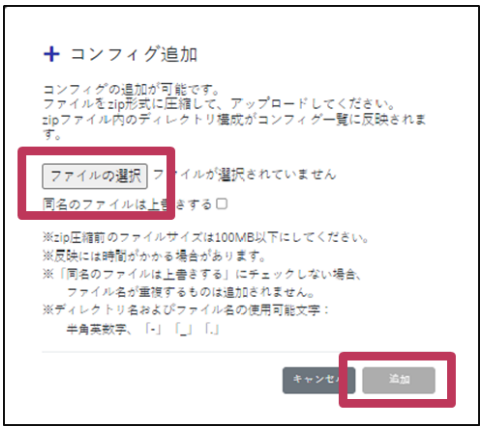


図 11-9 コンフィグの選択

メモ:

NetMeister へのコンフィグレーションファイルの登録は zip 形式でおこないます。複数のコンフィグレーションファイルをフォルダに格納して zip 圧縮しておくことで一度に登録も可能です。

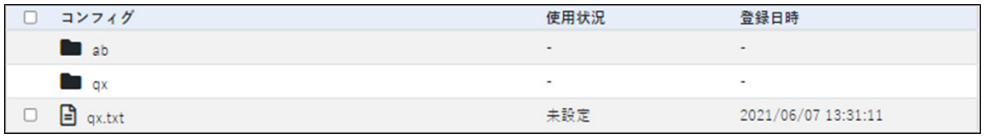


図 11-10 コンフィグ登録後の表示

4)　ゼロタッチプロビジョニングを利用する装置情報を登録します。



図 11-11 登録待ち装置設定画面



図 11-12 装置情報の登録例

メモ:

装置情報の登録では、シリアル番号の入力は大文字小文字を区別します。
MAC アドレスの入力は大文字小文字を区別しません。
「：」「-」などは含めないでください。
シリーズ名、機種名の選択を間違えないよう注意してください。



図 11-13 登録後の表示

5)　登録したコンフィグレーションファイルと装置情報を紐づけます。



図 11-14 プロビジョニングの設定画面

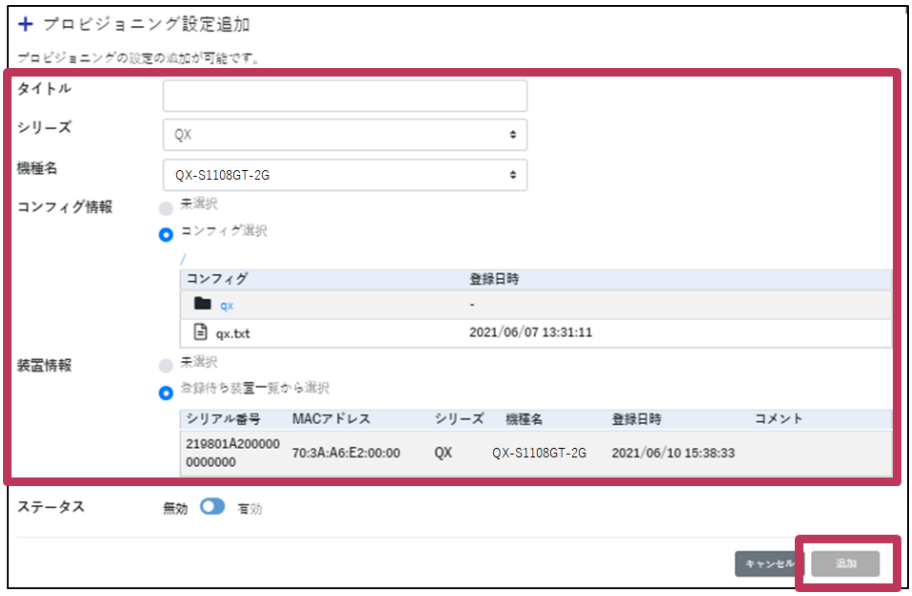


図 11-15 装置とコンフィグの選択

メモ:

タイトルは任意の文字列を入力してください。
シリーズ名と装置名を選択すると、他は選択可能なものだけが表示されますので任意の組み合わせを選択してください。
設置作業者がすぐに作業をしない場合はステータスを[無効]で登録しておきます。

III. 設置作業

1) 設置作業者が作業する時間を考慮し、コンフィグのダウンロード可能時間を設定します。一覧から対象の行を選択すると、現在の設定情報が下に表示されます。



図 11-16 プロビジョニング設定一覧

2) 選択した設定のステータスを[編集]から有効にし、コンフィグダウンロード可能時間を設定します。



図 11-17 ステータスの変更と DL 有効時間の設定

🕮 **メモ:**

有効時にダウンロード後の無効パターンを指定できますが、QX のゼロタッチプロビジョニングは、ダウンロード完了時はコンフィグを次回起動のコンフィグとして保存、再起動しますので、どちらを選んでも 1 度のみの取得動作です。(次回以降の起動時は保存済のコンフィグを使用して起動します。)

---

3) 設置場所で設置作業者が指定の装置を開梱します。
4) 準備後、管理者に装置設置開始の連絡をします。
5) 管理者は NetMeister 上で対象のゼロタッチプロビジョニングの有効化をします。
6) 設置作業者は指定の環境に装置を接続します。
7) 接続した装置は NetMeister から自動的にコンフィグを取得します。

   QX のゼロタッチプロビジョニングでは、取得したコンフィグデータを自動で次回起動のコンフィグとしてセットし、再起動します。

   DHCP サーバの設定ミスやインターネット環境に出られない環境など、何らかの理由で失敗している場合はリトライを繰り返し、再起動はしません。環境を見直してください。ゼロタッチプロビジョニングのプロセスを止めるためには、CLI で<Ctrl+C>または<Ctrl+D>を押下してください。

8) 再起動を LED 変化で確認し、管理者に連絡します。

   起動時の LED 変化は下記の通りです。

表 11-1 QX-S1100G シリーズ

状態	Power LED
Boot 起動	オレンジ点灯
System 起動中	緑点滅→点灯(3 回)→(ポート LED 上下点灯)→緑点灯
ゼロタッチプロビジョニング中	緑点灯(及びポート LinkUP)
ゼロタッチプロビジョニング成功時	(自動再起動)オレンジ点灯
起動中	緑点滅→点灯(3 回)→(ポート LED 上下点灯)→緑点灯
起動完了	緑点灯(及びポート LinkUP)

9)　NetMeister 上で状態を確認します。



図 11-18 動作状態の確認

結果がダウンロード成功の場合、コンフィグ取得を終えています。装置詳細画面に装置が表示されたことをチェックしてください。装置情報の誤入力や、環境の問題で NetMeister にアクセスができていない場合はカウントがされません。



図 11-19 装置一覧の確認

装置が再起動し、起動したにもかかわらず装置一覧に表示されない場合、準備されたコンフィグに NetMeister に接続するための設定の不備がある可能性があります。

装置一覧に装置が表示されれば NetMeister で管理ができています。

IV. 参考

NetMeister であらかじめアカウント管理から通知設定でゼロタッチ通知にチェックをいれておくと、ゼロタッチプロビジョニングによるコンフィグ取得成功時にメールが通知されます。

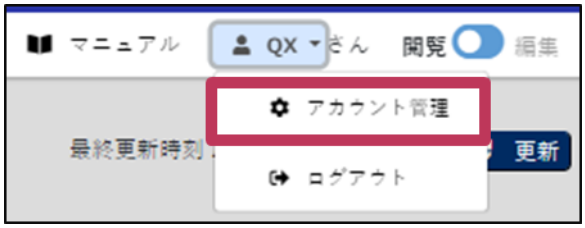


図 11-20 アカウント管理



図 11-21 通知の設定

11.3 NetMeisterによる管理

Netmeister の操作、及び、対応機能に関しては、NetMeister が提供する操作ガイドをご確認ください。

11.3.1 タブ一覧

NetMeister 上の装置詳細の画面に表示されるタブは、機器ごとに表示される内容が異なります。また、表示のレイアウトは NetMeister 側の更新によって変わる可能性があります。

本装置は以下のタブに対応しています。

タブ名	説明
装置概要	装置の詳細画面を表示します。 詳細はNetMeisterが提供する操作ガイドをご確認ください。
アラーム	温度異常/FAN 異常/CPU 異常/メモリ異常/異常再起動時にアラームを送信します。温度センサや FAN を持たない装置はそれらのアラームを送信することはありません。温度/FAN/CPU/メモリのしきい値はシステム管理の各種しきい値設定値に依存します。
コンフィグ	NetMeister 上にコンフィグを保存、装置の次回起動コンフィグとの比較、反映が可能です。

デバイスリスト	MAC テーブルと ARP テーブルを合わせた情報を表示します。
ログ	V7.3.49 を含む以降のソフトウェアで NetMiester prime 利用時に表示されます。 定期ログ送信を有効にし、時刻を指定して保存することで、NetMeister に定期的に装置情報一括取得(diag)データが保存されるようになります。
VLAN	display vlan コマンド、及び、display interface Vlan-interface brief コマンド相当の情報を表示します。
ポート状態	物理インタフェースの情報を表示します。

11.4 NetMeisterの設定例

I. ネットワーク要件

図 11-22に示すように、Device B を親機とし、子機である Device A の設定をします。

- あらかじめ NetMeister のサイトで「アカウント登録」をし、「グループ登録」としてグループ ID(aaa)とグループパスワード(abcd1234)が設定されていることとします。
- あらかじめ親機は外部ネットワークに接続するための設定を行い、グループ ID(aaa)に属していることとします。
- DNS サーバとして 10.0.0.254 が動作していることとします。

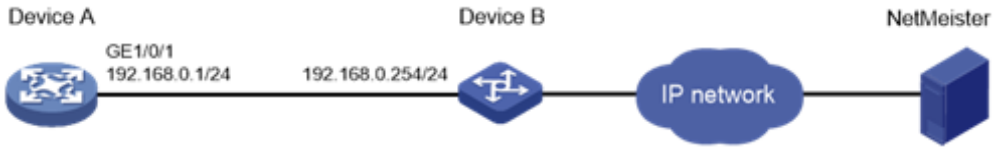


図 11-22 ネットワーク図

II. 設定手順

1. 外部ネットワークへの接続準備をします。

#VLAN インタフェースを作成し、IP アドレスをインタフェースに割り当てます。

```
<DeviceA> system-view
[DeviceA] vlan 1
[DeviceA-vlan1] port gigabitethernet 1/0/1
[DeviceA-vlan1] quit
[DeviceA] interface vlan-interface 1
[DeviceA -Vlan-interface1] ip address 192.168.0.1 24
[DeviceA -Vlan-interface1] quit
```

DNS サーバを指定します。

```
[DeviceA] dns server 10.0.0.254
```

ルーティング設定をします。

```
[DeviceA] ip route-static 0.0.0.0 0 192.168.0.254
```

2. その他の追加機能の設定をします。

時刻とタイムゾーン(+9:00)の設定をします。

```
[DeviceA] clock timezone JST add 09:00:00
[DeviceA] ntp-service enable
[DeviceA] ntp-service unicast-server 192.168.0.254
```

ssh と web コンソールアクセス用の設定をします。

```
[DeviceA]ssh server enable
[DeviceA]ip https enable
[DeviceA]line vty 0
[DeviceA-line-vty0]authentication-mode scheme
[DeviceA-line-vty0]local-user nec class manage
[DeviceA-luser-manage-nec]password simple qx12345678
[DeviceA-luser-manage-nec]service-type ssh https
[DeviceA-luser-manage-nec]authorization-attribute user-role network-admin
[DeviceA-luser-manage-nec]quit
```

lldp の有効化をします。

```
[DeviceA] lldp global enable
```

3. NetMeister を利用するための設定をします。

グループ ID(aaa)とグループパスワード(abcd1234)を設定します。

```
[DeviceA] netmeister account aaa password simple abcd1234
```

親機の IP アドレスとポート番号(デフォルト:443)を指定します。

```
[DeviceA] netmeister parent ip 192.168.0.254 port 443
```

NetMeister 機能の有効化をします。

```
[DeviceA] netmeister enable
```

III. 設定の確認

1. 外部ネットワークと疎通ができることを確認するために、いずれかの外部ネットワークと ping の疎通ができることを確認します。

```
<SwitchA>ping 1.1.1.1
Ping 1.1.1.1 (1.1.1.1): 56 data bytes, press CTRL+C to break
56 bytes from 1.1.1.1: icmp_seq=0 ttl=52 time=68.584 ms
56 bytes from 1.1.1.1: icmp_seq=1 ttl=52 time=49.657 ms
56 bytes from 1.1.1.1: icmp_seq=2 ttl=52 time=48.447 ms
56 bytes from 1.1.1.1: icmp_seq=3 ttl=52 time=58.423 ms
56 bytes from 1.1.1.1: icmp_seq=4 ttl=52 time=59.423 ms

--- Ping statistics for 1.1.1.1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 48.447/56.907/68.584/7.336 ms
```

2. NetMeister および親機との接続状態を確認します。

```
<SwitchA> display netmeister
NetMeister state                    : Enabled
Connection state with NetMeister    : Connected
Account name                        : aaa
Parent 1:
 IP address                    : 192.168.0.254
 Port number                   : 443
 Connection state              : Connected
```

11.5 NetMeister利用のトラブルシューティング

NetMeister 操作ガイドにも装置毎の機能対応一覧、及び、NetMeister 機能に関する注意事項、FAQ が記載されていますので参照して下さい。

11.5.1 NetMeister に QX が登録できない

I. 症状

QX で NetMeister を利用したいが NetMeister に装置が登録できない。

II. 解決策

親機モードで利用する場合

1) 同一グループに既に子機モードで登録されていないか確認し、登録されている場合は装置削除します。
2) NetMeister 上のライセンスの数が十分か確認します。
3) 外部ネットワークに DNS を使用した通信ができることを確認します。
4) 問題が解決しない場合、NetMeister のサイトから問い合わせをしてください。

子機モードで利用する場合

1) 同一グループに既に親機モードで登録されていないか確認し、登録されている場合は装置削除します。
2) 親機となる装置が NetMeister に接続できているか確認します。
3) 子機で設定したグループ ID およびパスワードが親機で設定しているものと同じであるか確認します。
4) 子機から外部ネットワークに DNS を使用した通信ができることを確認します。
5) 問題が解決しない場合、NetMeister のサイトから問い合わせをしてください。

11.5.2 NetMeister でグラフが正しく表示されない。

I. 症状

QX の装置詳細画面でグラフ情報が正しく表示されない。

II. 解決策

1) 装置にタイムゾーン(+9:00)が設定されていることを確認します。
2) 装置の時刻が正しいことを確認します。
3) NetMeister に装置登録した後に時刻設定を変更した場合は、周期的な装置情報更新のために、1 時間待つか NetMeister 機能を一度無効にし、再度有効にします。
4) 問題が解決しない場合、NetMeister のサイトから問い合わせてください。

11.5.3 NetMeister のリモートログインが使えない

I. 症状

QX にリモートログインができない。

II. 解決策

1) 同一拠点 ID にリモートログインの起点装置が存在することを確認します。詳細は NetMeister 操作ガイドを参照して下さい。
2) 装置に ssh または web コンソール接続の設定がされてあることを確認します。
3) リモートログインでのアクセスに利用する PC がプライベートアドレスではないことを確認します。
4) 操作 PC と対象の装置間でファイアウォールやフィルタなど、通信制限がない事を確認します。
5) 環境がプロキシやファイアウォールを利用していないことを確認します。
6) 問題が解決しない場合、NetMeister のサイトから問い合わせてください。

11.5.4 ファームウェア更新が成功しない

I. 症状

NetMeister で管理している装置のファームウェア更新(バージョンアップ)が成功しない。

II. 解決策

1) タスク一覧からタスクの状態を確認します。
2) タスク結果が失敗と表示され、詳細理由にディレクトリサイズが足りない、または、セットに失敗したと表示されている場合、装置のディレクトリサイズが不足していますので不要なファイルを削除します。

🕮 **メモ:**

ファームウェア更新をするためには、NetMeister から取得する ipe 形式のソフトウェアと、それを bin ファイルに解凍する分のディレクトリの空き容量が必要です。
ソフトウェア v7.1.7 を含む以降のバージョンでは、NetMeister 機能[コマンド実行]によって、NetMeister からディレクトリ確認コマンド(**dir**)及び削除コマンド(**delete /unreserved**)等の実行が可能です。v7.1.7 以前のバージョンでは NetMeister 機能[リモートログイン]やコンソールケーブル接続等して、直接装置でコマンドを実行してください。

---

3) 問題が解決しない場合、NEC に問い合わせてください。

11.5.5 NetMeisterPrime 機能が使用できない

I. 症状

NetMeister に prime ライセンスを適用(またはトライアル)したが機能が使用できない。

II. 解決策

1) NetMeister メニューからライセンスの適用状態を確認し、適用されていない場合は適用操作をします。(NetMeister が提供する NetMeister 操作ガイド参照)
2) 子機モードの場合、手動で有償化操作をする必要があります。
3) prime 機能にはライセンス適用をして有償化装置になった時に即座に利用できるものと、周期的な装置情報更新のタイミングで識別され使用可能になる機能がありますので、1 時間待つか NetMeister 機能を一度無効にし、再度有効にします。
4) 問題が解決しない場合、NetMeister のサイトから問い合わせてください。

QX-S1100G シリーズ Ethernet スイッチ

オペレーションマニュアル

10. 謝辞

本マニュアルは以下に示す章で構成されています。

01-謝辞

目次

このセクションのページは **10-x-x** です。

1章 謝辞（Acknowledgments） **1-1**

1章 謝辞（Acknowledgments）

This document provides copyright information regarding the third-party software that are included, either in whole or in part, in this product.

Acknowledgements:
This product includes software developed by the University of California, Berkeley and its contributors.
This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/).
This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).
This product includes software developed by the University of California, Lawrence Berkeley Laboratory and its contributors.

This product contains third parties component softwares and they will be used and distributed under the specific license.
If you want to obtain source code of Open Source Software included in this product, please send a request to our support team: https://www.nec.com/, we will provide the source code included in this product in exchange for a fee no higher than the physical cost of providing the source code.

[boolean.h 1.19]
[COPYRIGHT]
Copyright (C) 2004-2007 Internet Systems Consortium, Inc. ("ISC")
Copyright (C) 1998-2001 Internet Software Consortium.

[LICENSE]
Permission to use, copy, modify, and/or distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ISC DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

[bootstrap 2.3.2]
[COPYRIGHT]
Copyright 2012 Twitter, Inc.

[LICENSE]
Apache License
Version 2.0, January 2004
http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition,

"control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the
   Work or Derivative Works thereof in any medium, with or without
   modifications, and in Source or Object form, provided that You
   meet the following conditions:

   (a) You must give any other recipients of the Work or
       Derivative Works a copy of this License; and

   (b) You must cause any modified files to carry prominent notices
       stating that You changed the files; and

   (c) You must retain, in the Source form of any Derivative Works
       that You distribute, all copyright, patent, trademark, and
       attribution notices from the Source form of the Work,
       excluding those notices that do not pertain to any part of
       the Derivative Works; and

   (d) If the Work includes a "NOTICE" text file as part of its
       distribution, then any Derivative Works that You distribute must
       include a readable copy of the attribution notices contained
       within such NOTICE file, excluding those notices that do not
       pertain to any part of the Derivative Works, in at least one
       of the following places: within a NOTICE text file distributed
       as part of the Derivative Works; within the Source form or
       documentation, if provided along with the Derivative Works; or,
       within a display generated by the Derivative Works, if and
       wherever such third-party notices normally appear. The contents
       of the NOTICE file are for informational purposes only and
       do not modify the License. You may add Your own attribution
       notices within Derivative Works that You distribute, alongside
       or as an addendum to the NOTICE text from the Work, provided
       that such additional attribution notices cannot be construed
       as modifying the License.

   You may add Your own copyright statement to Your modifications and
   may provide additional or different license terms and conditions
   for use, reproduction, or distribution of Your modifications, or
   for any such Derivative Works as a whole, provided Your use,
   reproduction, and distribution of the Work otherwise complies with
   the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise,
   any Contribution intentionally submitted for inclusion in the Work
   by You to the Licensor shall be under the terms and conditions of
   this License, without any additional terms or conditions.
   Notwithstanding the above, nothing herein shall supersede or modify
   the terms of any separate license agreement you may have executed
   with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade
   names, trademarks, service marks, or product names of the Licensor,
   except as required for reasonable and customary use in describing the
   origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or
   agreed to in writing, Licensor provides the Work (and each
   Contributor provides its Contributions) on an "AS IS" BASIS,
   WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or
   implied, including, without limitation, any warranties or conditions
   of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A
   PARTICULAR PURPOSE. You are solely responsible for determining the
   appropriateness of using or redistributing the Work and assume any
   risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory,
   whether in tort (including negligence), contract, or otherwise,
   unless required by applicable law (such as deliberate and grossly
   negligent acts) or agreed to in writing, shall any Contributor be
   liable to You for damages, including any direct, indirect, special,

incidental, or consequential damages of any character arising as a
result of this License or out of the use or inability to use the
Work (including but not limited to damages for loss of goodwill,
work stoppage, computer failure or malfunction, or any and all
other commercial damages or losses), even if such Contributor
has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing
the Work or Derivative Works thereof, You may choose to offer,
and charge a fee for, acceptance of support, warranty, indemnity,
or other liability obligations and/or rights consistent with this
License. However, in accepting such obligations, You may act only
on Your own behalf and on Your sole responsibility, not on behalf
of any other Contributor, and only if You agree to indemnify,
defend, and hold each Contributor harmless for any liability
incurred by, or claims asserted against, such Contributor by reason
of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

[bootstrap-datetimepicker 1.2]
[COPYRIGHT]
Copyright 2012 Stefan Petre

[LICENSE]

Apache License
Version 2.0, January 2004
http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction,
and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by
the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all
other entities that control, are controlled by, or are under common
control with that entity. For the purposes of this definition,
"control" means (i) the power, direct or indirect, to cause the
direction or management of such entity, whether by contract or
otherwise, or (ii) ownership of fifty percent (50%) or more of the
outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity
exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications,
including but not limited to software source code, documentation
source, and configuration files.

"Object" form shall mean any form resulting from mechanical
transformation or translation of a Source form, including but
not limited to compiled object code, generated documentation,
and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or
Object form, made available under the License, as indicated by a
copyright notice that is included in or attached to the work
(an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object
form, that is based on (or derived from) the Work and for which the
editorial revisions, annotations, elaborations, or other modifications
represent, as a whole, an original work of authorship. For the purposes
of this License, Derivative Works shall not include works that remain

separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

   (a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

   (b) You must cause any modified files to carry prominent notices stating that You changed the files; and

   (c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

   (d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and

wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

APPENDIX: How to apply the Apache License to your work.

To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets "[]" replaced with your own identifying information. (Don't include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a

```
      file or class name and description of purpose be included on the
      same "printed page" as the copyright notice for easier
      identification within third-party archives.

   Copyright 2012 Sebastien MALOT

   Licensed under the Apache License, Version 2.0 (the "License");
   you may not use this file except in compliance with the License.
   You may obtain a copy of the License at

       http://www.apache.org/licenses/LICENSE-2.0

   Unless required by applicable law or agreed to in writing, software
   distributed under the License is distributed on an "AS IS" BASIS,
   WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
   See the License for the specific language governing permissions and
   limitations under the License.
--------------------------------------------------------------------------
---
[bootstrap-dropdown 2.3.2]
[COPYRIGHT]
  Copyright 2013 Twitter, Inc.

[LICENSE]
                                 Apache License
                           Version 2.0, January 2004
                        http://www.apache.org/licenses/

   TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

   1. Definitions.

      "License" shall mean the terms and conditions for use, reproduction,
      and distribution as defined by Sections 1 through 9 of this document.

      "Licensor" shall mean the copyright owner or entity authorized by
      the copyright owner that is granting the License.

      "Legal Entity" shall mean the union of the acting entity and all
      other entities that control, are controlled by, or are under common
      control with that entity. For the purposes of this definition,
      "control" means (i) the power, direct or indirect, to cause the
      direction or management of such entity, whether by contract or
      otherwise, or (ii) ownership of fifty percent (50%) or more of the
      outstanding shares, or (iii) beneficial ownership of such entity.

      "You" (or "Your") shall mean an individual or Legal Entity
      exercising permissions granted by this License.

      "Source" form shall mean the preferred form for making modifications,
      including but not limited to software source code, documentation
      source, and configuration files.

      "Object" form shall mean any form resulting from mechanical
      transformation or translation of a Source form, including but
      not limited to compiled object code, generated documentation,
      and conversions to other media types.

      "Work" shall mean the work of authorship, whether in Source or
      Object form, made available under the License, as indicated by a
      copyright notice that is included in or attached to the work
      (an example is provided in the Appendix below).

      "Derivative Works" shall mean any work, whether in Source or Object
      form, that is based on (or derived from) the Work and for which the
      editorial revisions, annotations, elaborations, or other modifications
      represent, as a whole, an original work of authorship. For the purposes
      of this License, Derivative Works shall not include works that remain
      separable from, or merely link (or bind by name) to the interfaces of,
      the Work and Derivative Works thereof.
```

"Contribution" shall mean any work of authorship, including
the original version of the Work and any modifications or additions
to that Work or Derivative Works thereof, that is intentionally
submitted to Licensor for inclusion in the Work by the copyright owner
or by an individual or Legal Entity authorized to submit on behalf of
the copyright owner. For the purposes of this definition, "submitted"
means any form of electronic, verbal, or written communication sent
to the Licensor or its representatives, including but not limited to
communication on electronic mailing lists, source code control systems,
and issue tracking systems that are managed by, or on behalf of, the
Licensor for the purpose of discussing and improving the Work, but
excluding communication that is conspicuously marked or otherwise
designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity
on behalf of whom a Contribution has been received by Licensor and
subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of
this License, each Contributor hereby grants to You a perpetual,
worldwide, non-exclusive, no-charge, royalty-free, irrevocable
copyright license to reproduce, prepare Derivative Works of,
publicly display, publicly perform, sublicense, and distribute the
Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of
this License, each Contributor hereby grants to You a perpetual,
worldwide, non-exclusive, no-charge, royalty-free, irrevocable
(except as stated in this section) patent license to make, have made,
use, offer to sell, sell, import, and otherwise transfer the Work,
where such license applies only to those patent claims licensable
by such Contributor that are necessarily infringed by their
Contribution(s) alone or by combination of their Contribution(s)
with the Work to which such Contribution(s) was submitted. If You
institute patent litigation against any entity (including a
cross-claim or counterclaim in a lawsuit) alleging that the Work
or a Contribution incorporated within the Work constitutes direct
or contributory patent infringement, then any patent licenses
granted to You under this License for that Work shall terminate
as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the
Work or Derivative Works thereof in any medium, with or without
modifications, and in Source or Object form, provided that You
meet the following conditions:

   (a) You must give any other recipients of the Work or
       Derivative Works a copy of this License; and

   (b) You must cause any modified files to carry prominent notices
       stating that You changed the files; and

   (c) You must retain, in the Source form of any Derivative Works
       that You distribute, all copyright, patent, trademark, and
       attribution notices from the Source form of the Work,
       excluding those notices that do not pertain to any part of
       the Derivative Works; and

   (d) If the Work includes a "NOTICE" text file as part of its
       distribution, then any Derivative Works that You distribute must
       include a readable copy of the attribution notices contained
       within such NOTICE file, excluding those notices that do not
       pertain to any part of the Derivative Works, in at least one
       of the following places: within a NOTICE text file distributed
       as part of the Derivative Works; within the Source form or
       documentation, if provided along with the Derivative Works; or,
       within a display generated by the Derivative Works, if and
       wherever such third-party notices normally appear. The contents
       of the NOTICE file are for informational purposes only and

do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

APPENDIX: How to apply the Apache License to your work.

To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets "[]" replaced with your own identifying information. (Don't include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same "printed page" as the copyright notice for easier

identification within third-party archives.

Copyright 2012 Sebastien MALOT

Licensed under the Apache License, Version 2.0 (the "License");
you may not use this file except in compliance with the License.
You may obtain a copy of the License at

http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software
distributed under the License is distributed on an "AS IS" BASIS,
WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
See the License for the specific language governing permissions and
limitations under the License.

[bootstrap-modal 2.1]
[COPYRIGHT]
Copyright 2012 Jordan Schroter

[LICENSE]

Apache License
Version 2.0, January 2004
http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction,
and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by
the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all
other entities that control, are controlled by, or are under common
control with that entity. For the purposes of this definition,
"control" means (i) the power, direct or indirect, to cause the
direction or management of such entity, whether by contract or
otherwise, or (ii) ownership of fifty percent (50%) or more of the
outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity
exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications,
including but not limited to software source code, documentation
source, and configuration files.

"Object" form shall mean any form resulting from mechanical
transformation or translation of a Source form, including but
not limited to compiled object code, generated documentation,
and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or
Object form, made available under the License, as indicated by a
copyright notice that is included in or attached to the work
(an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object
form, that is based on (or derived from) the Work and for which the
editorial revisions, annotations, elaborations, or other modifications
represent, as a whole, an original work of authorship. For the purposes
of this License, Derivative Works shall not include works that remain
separable from, or merely link (or bind by name) to the interfaces of,
the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including

the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

   (a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

   (b) You must cause any modified files to carry prominent notices stating that You changed the files; and

   (c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

   (d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside

or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

APPENDIX: How to apply the Apache License to your work.

To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets "[]" replaced with your own identifying information. (Don't include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same "printed page" as the copyright notice for easier identification within third-party archives.

Copyright 2012 Sebastien MALOT

Licensed under the Apache License, Version 2.0 (the "License");
you may not use this file except in compliance with the License.
You may obtain a copy of the License at

http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software
distributed under the License is distributed on an "AS IS" BASIS,
WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
See the License for the specific language governing permissions and
limitations under the License.

[bootstrap-tab 2.3.2]
[COPYRIGHT]
Copyright 2013 Twitter, Inc.

[LICENSE]

Apache License
Version 2.0, January 2004
http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction,
and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by
the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all
other entities that control, are controlled by, or are under common
control with that entity. For the purposes of this definition,
"control" means (i) the power, direct or indirect, to cause the
direction or management of such entity, whether by contract or
otherwise, or (ii) ownership of fifty percent (50%) or more of the
outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity
exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications,
including but not limited to software source code, documentation
source, and configuration files.

"Object" form shall mean any form resulting from mechanical
transformation or translation of a Source form, including but
not limited to compiled object code, generated documentation,
and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or
Object form, made available under the License, as indicated by a
copyright notice that is included in or attached to the work
(an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object
form, that is based on (or derived from) the Work and for which the
editorial revisions, annotations, elaborations, or other modifications
represent, as a whole, an original work of authorship. For the purposes
of this License, Derivative Works shall not include works that remain
separable from, or merely link (or bind by name) to the interfaces of,
the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including
the original version of the Work and any modifications or additions
to that Work or Derivative Works thereof, that is intentionally

submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

   (a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

   (b) You must cause any modified files to carry prominent notices stating that You changed the files; and

   (c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

   (d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed

as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

APPENDIX: How to apply the Apache License to your work.

To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets "[]" replaced with your own identifying information. (Don't include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same "printed page" as the copyright notice for easier identification within third-party archives.

Copyright 2012 Sebastien MALOT

```
   Licensed under the Apache License, Version 2.0 (the "License");
   you may not use this file except in compliance with the License.
   You may obtain a copy of the License at

       http://www.apache.org/licenses/LICENSE-2.0

   Unless required by applicable law or agreed to in writing, software
   distributed under the License is distributed on an "AS IS" BASIS,
   WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
   See the License for the specific language governing permissions and
   limitations under the License.
-------------------------------------------------------------------------------
---
[bootstrapSwitch 1.3.0]
[COPYRIGHT]
  bootstrapSwitch v1.3 by Larentis Mattia @spiritualGuru

[LICENSE]
                                 Apache License
                           Version 2.0, January 2004
                        http://www.apache.org/licenses/

   TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

   1. Definitions.

      "License" shall mean the terms and conditions for use, reproduction,
      and distribution as defined by Sections 1 through 9 of this document.

      "Licensor" shall mean the copyright owner or entity authorized by
      the copyright owner that is granting the License.

      "Legal Entity" shall mean the union of the acting entity and all
      other entities that control, are controlled by, or are under common
      control with that entity. For the purposes of this definition,
      "control" means (i) the power, direct or indirect, to cause the
      direction or management of such entity, whether by contract or
      otherwise, or (ii) ownership of fifty percent (50%) or more of the
      outstanding shares, or (iii) beneficial ownership of such entity.

      "You" (or "Your") shall mean an individual or Legal Entity
      exercising permissions granted by this License.

      "Source" form shall mean the preferred form for making modifications,
      including but not limited to software source code, documentation
      source, and configuration files.

      "Object" form shall mean any form resulting from mechanical
      transformation or translation of a Source form, including but
      not limited to compiled object code, generated documentation,
      and conversions to other media types.

      "Work" shall mean the work of authorship, whether in Source or
      Object form, made available under the License, as indicated by a
      copyright notice that is included in or attached to the work
      (an example is provided in the Appendix below).

      "Derivative Works" shall mean any work, whether in Source or Object
      form, that is based on (or derived from) the Work and for which the
      editorial revisions, annotations, elaborations, or other modifications
      represent, as a whole, an original work of authorship. For the purposes
      of this License, Derivative Works shall not include works that remain
      separable from, or merely link (or bind by name) to the interfaces of,
      the Work and Derivative Works thereof.

      "Contribution" shall mean any work of authorship, including
      the original version of the Work and any modifications or additions
      to that Work or Derivative Works thereof, that is intentionally
      submitted to Licensor for inclusion in the Work by the copyright owner
      or by an individual or Legal Entity authorized to submit on behalf of
```

the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

   (a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

   (b) You must cause any modified files to carry prominent notices stating that You changed the files; and

   (c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

   (d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and
may provide additional or different license terms and conditions
for use, reproduction, or distribution of Your modifications, or
for any such Derivative Works as a whole, provided Your use,
reproduction, and distribution of the Work otherwise complies with
the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise,
   any Contribution intentionally submitted for inclusion in the Work
   by You to the Licensor shall be under the terms and conditions of
   this License, without any additional terms or conditions.
   Notwithstanding the above, nothing herein shall supersede or modify
   the terms of any separate license agreement you may have executed
   with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade
   names, trademarks, service marks, or product names of the Licensor,
   except as required for reasonable and customary use in describing the
   origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or
   agreed to in writing, Licensor provides the Work (and each
   Contributor provides its Contributions) on an "AS IS" BASIS,
   WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or
   implied, including, without limitation, any warranties or conditions
   of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A
   PARTICULAR PURPOSE. You are solely responsible for determining the
   appropriateness of using or redistributing the Work and assume any
   risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory,
   whether in tort (including negligence), contract, or otherwise,
   unless required by applicable law (such as deliberate and grossly
   negligent acts) or agreed to in writing, shall any Contributor be
   liable to You for damages, including any direct, indirect, special,
   incidental, or consequential damages of any character arising as a
   result of this License or out of the use or inability to use the
   Work (including but not limited to damages for loss of goodwill,
   work stoppage, computer failure or malfunction, or any and all
   other commercial damages or losses), even if such Contributor
   has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing
   the Work or Derivative Works thereof, You may choose to offer,
   and charge a fee for, acceptance of support, warranty, indemnity,
   or other liability obligations and/or rights consistent with this
   License. However, in accepting such obligations, You may act only
   on Your own behalf and on Your sole responsibility, not on behalf
   of any other Contributor, and only if You agree to indemnify,
   defend, and hold each Contributor harmless for any liability
   incurred by, or claims asserted against, such Contributor by reason
   of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

APPENDIX: How to apply the Apache License to your work.

To apply the Apache License to your work, attach the following
boilerplate notice, with the fields enclosed by brackets "[]"
replaced with your own identifying information. (Don't include
the brackets!) The text should be enclosed in the appropriate
comment syntax for the file format. We also recommend that a
file or class name and description of purpose be included on the
same "printed page" as the copyright notice for easier
identification within third-party archives.

Copyright 2012 Sebastien MALOT

Licensed under the Apache License, Version 2.0 (the "License");
you may not use this file except in compliance with the License.

You may obtain a copy of the License at

http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

[busybox 1.20.1]
[LICENSE]

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.
51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to

exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to

this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED

OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author
Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
This is free software, and you are welcome to redistribute it
under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than `show w' and `show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program `Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon>, 1 April 1989
Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Library General Public License instead of this License.

[cpio 2.11]
[COPYRIGHT]
Copyright (C) 1990, 1991, 1992, 2001, 2006, 2007, 2009, 2010 Free Software Foundation, Inc.

[LICENSE]

GNU GENERAL PUBLIC LICENSE
Version 3, 29 June 2007

Copyright (C) 2007 Free Software Foundation, Inc. <http://fsf.org/>
Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The GNU General Public License is a free, copyleft license for software and other kinds of works.

The licenses for most software and other practical works are designed to take away your freedom to share and change the works. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change all versions of a program--to make sure it remains free software for all its users. We, the Free Software Foundation, use the GNU General Public License for most of our software; it applies also to any other work released this way by its authors. You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for them if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you these rights or asking you to surrender the rights. Therefore, you have certain responsibilities if you distribute copies of the software, or if you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must pass on to the recipients the same freedoms that you received. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

Developers that use the GNU GPL protect your rights with two steps: (1) assert copyright on the software, and (2) offer you this License giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains that there is no warranty for this free software. For both users' and authors' sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.

Some devices are designed to deny users access to install or run modified versions of the software inside them, although the manufacturer can do so. This is fundamentally incompatible with the aim of protecting users' freedom to change the software. The systematic pattern of such abuse occurs in the area of products for individuals to

use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains, we stand ready to extend this provision to those domains in future versions of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents. States should not allow patents to restrict development and use of software on general-purpose computers, but in those that do, we wish to avoid the special danger that patents applied to a free program could make it effectively proprietary. To prevent this, the GPL assures that patents cannot be used to render the program non-free.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS

0. Definitions.

"This License" refers to version 3 of the GNU General Public License.

"Copyright" also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

"The Program" refers to any copyrightable work licensed under this License. Each licensee is addressed as "you". "Licensees" and "recipients" may be individuals or organizations.

To "modify" a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a "modified version" of the earlier work or a work "based on" the earlier work.

A "covered work" means either the unmodified Program or a work based on the Program.

To "propagate" a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well.

To "convey" a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays "Appropriate Legal Notices" to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

1. Source Code.

The "source code" for a work means the preferred form of the work for making modifications to it. "Object code" means any non-source form of a work.

A "Standard Interface" means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The "System Libraries" of an executable work include anything, other than the work as a whole, that (a) is included in the normal form of

packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A "Major Component", in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The "Corresponding Source" for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work's System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

2. Basic Permissions.

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered by this License only if the output, given its content, constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed; section 10 makes it unnecessary.

3. Protecting Users' Legal Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of technological measures.

4. Conveying Verbatim Copies.

You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice; keep intact all notices stating that this License and any non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

5. Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

a) The work must carry prominent notices stating that you modified it, and giving a relevant date.

b) The work must carry prominent notices stating that it is released under this License and any conditions added under section 7. This requirement modifies the requirement in section 4 to "keep intact all notices".

c) You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it.

d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.

A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution medium, is called an "aggregate" if the compilation and its resulting copyright are not used to limit the access or legal rights of the compilation's users beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate.

6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, in one of these ways:

a) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange.

b) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as long as you offer spare parts or customer support for that product model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical medium customarily used for software interchange, for a price no

more than your reasonable cost of physically performing this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge.

c) Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source. This alternative is allowed only occasionally and noncommercially, and only if you received the object code with such an offer, in accord with subsection 6b.

d) Convey the object code by offering access from a designated place (gratis or for a charge), and offer equivalent access to the Corresponding Source in the same way through the same place at no further charge. You need not require recipients to copy the Corresponding Source along with the object code. If the place to copy the object code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.

e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.

A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object code work.

A "User Product" is either (1) a "consumer product", which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, "normally used" refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

"Installation Information" for a User Product means any methods, procedures, authorization keys, or other information required to install and execute modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in ROM).

The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and

protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

7. Additional Terms.

"Additional permissions" are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

a) Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or

b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or

c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or

d) Limiting the use for publicity purposes of names of licensors or authors of the material; or

e) Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or

f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on those licensors and authors.

All other non-permissive additional terms are considered "further restrictions" within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions;

the above requirements apply either way.

8. Termination.

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

10. Automatic Licensing of Downstream Recipients.

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An "entity transaction" is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

11. Patents.

A "contributor" is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The

work thus licensed is called the contributor's "contributor version".

A contributor's "essential patent claims" are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For purposes of this definition, "control" includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a "patent license" is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To "grant" such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. "Knowingly relying" means you have actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient's use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is "discriminatory" if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement, or that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.

12. No Surrender of Others' Freedom.

If conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot convey a

covered work so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

13. Use with the GNU Affero General Public License.

Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed under version 3 of the GNU Affero General Public License into a single combined work, and to convey the resulting work. The terms of this License will continue to apply to the part which is the covered work, but the special requirements of the GNU Affero General Public License, section 13, concerning interaction through a network will apply to the combination as such.

14. Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of the GNU General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU General Public License, you may choose any version ever published by the Free Software Foundation.

If the Program specifies that a proxy can decide which future versions of the GNU General Public License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Program.

Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.

15. Disclaimer of Warranty.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

17. Interpretation of Sections 15 and 16.

If the disclaimer of warranty and limitation of liability provided

```
above cannot be given local legal effect according to their terms,
reviewing courts shall apply local law that most closely approximates
an absolute waiver of all civil liability in connection with the
Program, unless a warranty or assumption of liability accompanies a
copy of the Program in return for a fee.

                     END OF TERMS AND CONDITIONS

            How to Apply These Terms to Your New Programs

  If you develop a new program, and you want it to be of the greatest
possible use to the public, the best way to achieve this is to make it
free software which everyone can redistribute and change under these terms.

  To do so, attach the following notices to the program.  It is safest
to attach them to the start of each source file to most effectively
state the exclusion of warranty; and each file should have at least
the "copyright" line and a pointer to where the full notice is found.

    <one line to give the program's name and a brief idea of what it does.>
    Copyright (C) <year>  <name of author>

    This program is free software: you can redistribute it and/or modify
    it under the terms of the GNU General Public License as published by
    the Free Software Foundation, either version 3 of the License, or
    (at your option) any later version.

    This program is distributed in the hope that it will be useful,
    but WITHOUT ANY WARRANTY; without even the implied warranty of
    MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
    GNU General Public License for more details.

    You should have received a copy of the GNU General Public License
    along with this program.  If not, see <http://www.gnu.org/licenses/>.

Also add information on how to contact you by electronic and paper mail.

  If the program does terminal interaction, make it output a short
notice like this when it starts in an interactive mode:

    <program>  Copyright (C) <year>  <name of author>
    This program comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
    This is free software, and you are welcome to redistribute it
    under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate
parts of the General Public License.  Of course, your program's commands
might be different; for a GUI interface, you would use an "about box".

  You should also get your employer (if you work as a programmer) or school,
if any, to sign a "copyright disclaimer" for the program, if necessary.
For more information on this, and how to apply and follow the GNU GPL, see
<http://www.gnu.org/licenses/>.

  The GNU General Public License does not permit incorporating your program
into proprietary programs.  If your program is a subroutine library, you
may consider it more useful to permit linking proprietary applications with
the library.  If this is what you want to do, use the GNU Lesser General
Public License instead of this License.  But first, please read
<http://www.gnu.org/philosophy/why-not-lgpl.html>.

--------------------------------------------------------------------------
---
[curl 7.21.2]
[COPYRIGHT]
  Copyright (c) 1996 - 2010, Daniel Stenberg, <daniel@haxx.se>.
  All rights reserved.

[LICENSE]
 Permission to use, copy, modify, and distribute this software for any purpose
```

with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder.

[domain stack framework 8.0.0 (part of FreeBSD 8.0.0)]
[COPYRIGHT]
Copyright (c) 1992-2009 The FreeBSD Project. All rights reserved.

[LICENSE]
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The 4.4BSD and 4.4BSD-Lite software is distributed under the following terms:

All of the documentation and software included in the 4.4BSD and 4.4BSD-Lite Releases is copyrighted by The Regents of the University of California.

Copyright 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:
This product includes software developed by the University of California, Berkeley and its contributors.
4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND

ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The Institute of Electrical and Electronics Engineers and the American National Standards Committee X3, on Information Processing Systems have given us permission to reprint portions of their documentation.

In the following statement, the phrase ``this text'' refers to portions of the system documentation.

Portions of this text are reprinted and reproduced in electronic form in the second BSD Networking Software Release, from IEEE Std 1003.1-1988, IEEE Standard Portable Operating System Interface for Computer Environments (POSIX), copyright C 1988 by the Institute of Electrical and Electronics Engineers, Inc. In the event of any discrepancy between these versions and the original IEEE Standard, the original IEEE Standard is the referee document.

In the following statement, the phrase ``This material'' refers to portions of the system documentation.

This material is reproduced with permission from American National Standards Committee X3, on Information Processing Systems. Computer and Business Equipment Manufacturers Association (CBEMA), 311 First St., NW, Suite 500, Washington, DC 20001-2178. The developmental work of Programming Language C was completed by the X3J11 Technical Committee.

The views and conclusions contained in the software and documentation are those of the authors and should not be interpreted as representing official policies, either expressed or implied, of the Regents of the University of California.

NOTE: The copyright of UC Berkeley's Berkeley Software Distribution ("BSD") source has been updated. The copyright addendum may be found at ftp://ftp.cs.berkeley.edu/pub/4bsd/README.Impt.License.Change and is included below.

July 22, 1999

To All Licensees, Distributors of Any Version of BSD:

As you know, certain of the Berkeley Software Distribution ("BSD") source code files require that further distributions of products containing all or portions of the software, acknowledge within their advertising materials that such products contain software developed by UC Berkeley and its contributors.

Specifically, the provision reads:

```
"     * 3. All advertising materials mentioning features or use of this software
       *    must display the following acknowledgement:
       *    This product includes software developed by the University of
       *    California, Berkeley and its contributors."
```

Effective immediately, licensees and distributors are no longer required to include the acknowledgement within advertising materials. Accordingly, the foregoing paragraph of those BSD Unix files containing it is hereby deleted in its entirety.

William Hoskins
Director, Office of Technology Licensing

University of California, Berkeley

[dosfstools 3.0.12]
[COPYRIGHT]
Copyright (C) 1998-2005 Roman Hodek <Roman.Hodek@informatik.uni-erlangen.de>

[LICENSE]
GNU GENERAL PUBLIC LICENSE
Version 3, 29 June 2007

Copyright (C) 2007 Free Software Foundation, Inc. <http://fsf.org/>
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The GNU General Public License is a free, copyleft license for software and other kinds of works.

The licenses for most software and other practical works are designed to take away your freedom to share and change the works. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change all versions of a program--to make sure it remains free software for all its users. We, the Free Software Foundation, use the GNU General Public License for most of our software; it applies also to any other work released this way by its authors. You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for them if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you these rights or asking you to surrender the rights. Therefore, you have certain responsibilities if you distribute copies of the software, or if you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must pass on to the recipients the same freedoms that you received. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

Developers that use the GNU GPL protect your rights with two steps: (1) assert copyright on the software, and (2) offer you this License giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains that there is no warranty for this free software. For both users' and authors' sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.

Some devices are designed to deny users access to install or run modified versions of the software inside them, although the manufacturer can do so. This is fundamentally incompatible with the aim of protecting users' freedom to change the software. The systematic pattern of such abuse occurs in the area of products for individuals to use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains, we stand ready to extend this provision to those domains in future versions of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents. States should not allow patents to restrict development and use of

software on general-purpose computers, but in those that do, we wish to avoid the special danger that patents applied to a free program could make it effectively proprietary. To prevent this, the GPL assures that patents cannot be used to render the program non-free.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS

0. Definitions.

"This License" refers to version 3 of the GNU General Public License.

"Copyright" also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

"The Program" refers to any copyrightable work licensed under this License. Each licensee is addressed as "you". "Licensees" and "recipients" may be individuals or organizations.

To "modify" a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a "modified version" of the earlier work or a work "based on" the earlier work.

A "covered work" means either the unmodified Program or a work based on the Program.

To "propagate" a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well.

To "convey" a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays "Appropriate Legal Notices" to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

1. Source Code.

The "source code" for a work means the preferred form of the work for making modifications to it. "Object code" means any non-source form of a work.

A "Standard Interface" means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The "System Libraries" of an executable work include anything, other than the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A "Major Component", in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The "Corresponding Source" for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work's System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

2. Basic Permissions.

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered by this License only if the output, given its content, constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed; section 10 makes it unnecessary.

3. Protecting Users' Legal Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of technological measures.

4. Conveying Verbatim Copies.

You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice; keep intact all notices stating that this License and any non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all

recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

5. Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

a) The work must carry prominent notices stating that you modified it, and giving a relevant date.

b) The work must carry prominent notices stating that it is released under this License and any conditions added under section 7. This requirement modifies the requirement in section 4 to "keep intact all notices".

c) You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it.

d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.

A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution medium, is called an "aggregate" if the compilation and its resulting copyright are not used to limit the access or legal rights of the compilation's users beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate.

6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, in one of these ways:

a) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange.

b) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as long as you offer spare parts or customer support for that product model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical medium customarily used for software interchange, for a price no more than your reasonable cost of physically performing this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge.

c) Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source. This alternative is allowed only occasionally and noncommercially, and only if you received the object code with such an offer, in accord

with subsection 6b.

d) Convey the object code by offering access from a designated place (gratis or for a charge), and offer equivalent access to the Corresponding Source in the same way through the same place at no further charge. You need not require recipients to copy the Corresponding Source along with the object code. If the place to copy the object code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.

e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.

A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object code work.

A "User Product" is either (1) a "consumer product", which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, "normally used" refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

"Installation Information" for a User Product means any methods, procedures, authorization keys, or other information required to install and execute modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in ROM).

The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

7. Additional Terms.

"Additional permissions" are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

a) Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or

b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or

c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or

d) Limiting the use for publicity purposes of names of licensors or authors of the material; or

e) Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or

f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on those licensors and authors.

All other non-permissive additional terms are considered "further restrictions" within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions; the above requirements apply either way.

8. Termination.

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third

paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

10. Automatic Licensing of Downstream Recipients.

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An "entity transaction" is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

11. Patents.

A "contributor" is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's "contributor version".

A contributor's "essential patent claims" are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For

purposes of this definition, "control" includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a "patent license" is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To "grant" such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. "Knowingly relying" means you have actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient's use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is "discriminatory" if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement, or that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.

12. No Surrender of Others' Freedom.

If conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot convey a covered work so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

13. Use with the GNU Affero General Public License.

Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed under version 3 of the GNU Affero General Public License into a single combined work, and to convey the resulting work. The terms of this License will continue to apply to the part which is the covered work, but the special requirements of the GNU Affero General Public License, section 13, concerning interaction through a network will apply to the combination as such.

14. Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of the GNU General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU General Public License, you may choose any version ever published by the Free Software Foundation.

If the Program specifies that a proxy can decide which future versions of the GNU General Public License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Program.

Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.

15. Disclaimer of Warranty.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

17. Interpretation of Sections 15 and 16.

If the disclaimer of warranty and limitation of liability provided above cannot be given local legal effect according to their terms, reviewing courts shall apply local law that most closely approximates an absolute waiver of all civil liability in connection with the Program, unless a warranty or assumption of liability accompanies a copy of the Program in return for a fee.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively state the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

```
    <one line to give the program's name and a brief idea of what it does.>
    Copyright (C) <year>  <name of author>

    This program is free software: you can redistribute it and/or modify
    it under the terms of the GNU General Public License as published by
    the Free Software Foundation, either version 3 of the License, or
    (at your option) any later version.

    This program is distributed in the hope that it will be useful,
    but WITHOUT ANY WARRANTY; without even the implied warranty of
    MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
    GNU General Public License for more details.

    You should have received a copy of the GNU General Public License
    along with this program.  If not, see <http://www.gnu.org/licenses/>.
```

Also add information on how to contact you by electronic and paper mail.

If the program does terminal interaction, make it output a short notice like this when it starts in an interactive mode:

```
    <program>  Copyright (C) <year>  <name of author>
    This program comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
    This is free software, and you are welcome to redistribute it
    under certain conditions; type `show c' for details.
```

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, your program's commands might be different; for a GUI interface, you would use an "about box".

You should also get your employer (if you work as a programmer) or school, if any, to sign a "copyright disclaimer" for the program, if necessary. For more information on this, and how to apply and follow the GNU GPL, see <http://www.gnu.org/licenses/>.

The GNU General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Lesser General Public License instead of this License. But first, please read <http://www.gnu.org/philosophy/why-not-lgpl.html>.

[dynamic linking loader 0.9.32 (part of uclibc 0.9.32)]
[LICENSE]

GNU LESSER GENERAL PUBLIC LICENSE
Version 2.1, February 1999

```
 Copyright (C) 1991, 1999 Free Software Foundation, Inc.
     51 Franklin St, Fifth Floor, Boston, MA  02110-1301  USA
 Everyone is permitted to copy and distribute verbatim copies
 of this license document, but changing it is not allowed.
```

[This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less

of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an

appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for

that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked

with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or

distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free

programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the library's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA

Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the library, if necessary. Here is a sample; alter the names:

```
  Yoyodyne, Inc., hereby disclaims all copyright interest in the
  library `Frob' (a library for tweaking knobs) written by James Random Hacker.

  <signature of Ty Coon>, 1 April 1990
  Ty Coon, President of Vice

That's all there is to it!


------------------------------------------------------------------------------
---
[freeradius-server3.0.10]
[COPYRIGHT]
  Copyright (C) 1999-2015 The FreeRADIUS Server Project

  Copyright (C) 1999, 2000, 2001, 2002, 2003, 2004, 2005, 2006, 2007, 2008, 2009
Alan DeKok
  <aland@deployingradius.com>

  Copyright (C) 1996, 1997, 1999, 2000, 2002, 2003, 2004, 2005 Free
  Software Foundation, Inc.

  Copyright (C) 2011-2015 Arran Cudbard-Bell <a.cudbardb@freeradius.org>

  Copyright (C) 2003, 2004, 2005 Kostas Kalevras <kkalev@noc.ntua.gr>

  Copyright (C) 2004  Cladju Consulting, Inc.

  Copyright (C) 2001, 2002, 2003, 2004, 2005 Google, Inc.

  Copyright (C) 2003, 2004  Michael Richardson <mcr@sandelman.ottawa.on.ca>

  Copyright (C) 2002, 2003, 2004 Novell, Inc.

  Copyright (C) 2002  Miguel A.L. Paraz <mparaz@mparaz.com>

  Copyright (C) 2002 Simon Ekstrand <simon@routemeister.net>

  Copyright (C) 2001  Chad Miller <cmiller@surfsouth.com>

  Copyright (C) 2001 hereUare Communications, Inc.

  Copyright (C) 2000 Jochen Friedrich <jochen@scram.de>

  Copyright (C) 2000, 2002 Miquel van Smoorenburg

  Copyright (C) 2000  Jeff Carneal <jeff@apex.net>

  Copyright (C) 2000  Alan Curry <pacman@world.std.com>

  Copyright (C) 2000  David Kerry <davidk@snti.com>

  Copyright (C) 2000  Dmitri Ageev <d_ageev@ortcc.ru>

  Copyright (C) 2000  Nathan Neulinger <nneul@umr.edu>

  Copyright (C) 2000  Mike Machado <mike@innercite.com>

  Copyright (C) 2000, 2001  Chad Miller <cmiller@surfsouth.com>

  Copyright (C) 1997, 1998, 1999 Cistron Internet Services B.V.

  Copyright (C) 1999 Kunihiro Ishiguro <kunihiro@zebra.org>

[LICENSE]
                    GNU GENERAL PUBLIC LICENSE
                       Version 2, June 1991

 Copyright (C) 1989, 1991 Free Software Foundation, Inc.
                       51 Franklin St, Fifth Floor, Boston, MA  02110-1301  USA
```

Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program

is covered only if its contents constitute a work based on the
Program (independent of having been made by running the Program).
Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's
source code as you receive it, in any medium, provided that you
conspicuously and appropriately publish on each copy an appropriate
copyright notice and disclaimer of warranty; keep intact all the
notices that refer to this License and to the absence of any warranty;
and give any other recipients of the Program a copy of this License
along with the Program.

You may charge a fee for the physical act of transferring a copy, and
you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion
of it, thus forming a work based on the Program, and copy and
distribute such modifications or work under the terms of Section 1
above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices
stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in
whole or in part contains or is derived from the Program or any
part thereof, to be licensed as a whole at no charge to all third
parties under the terms of this License.

c) If the modified program normally reads commands interactively
when run, you must cause it, when started running for such
interactive use in the most ordinary way, to print or display an
announcement including an appropriate copyright notice and a
notice that there is no warranty (or else, saying that you provide
a warranty) and that users may redistribute the program under
these conditions, and telling the user how to view a copy of this
License. (Exception: if the Program itself is interactive but
does not normally print such an announcement, your work based on
the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If
identifiable sections of that work are not derived from the Program,
and can be reasonably considered independent and separate works in
themselves, then this License, and its terms, do not apply to those
sections when you distribute them as separate works. But when you
distribute the same sections as part of a whole which is a work based
on the Program, the distribution of the whole must be on the terms of
this License, whose permissions for other licensees extend to the
entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest
your rights to work written entirely by you; rather, the intent is to
exercise the right to control the distribution of derivative or
collective works based on the Program.

In addition, mere aggregation of another work not based on the Program
with the Program (or with a work based on the Program) on a volume of
a storage or distribution medium does not bring the other work under
the scope of this License.

3. You may copy and distribute the Program (or a work based on it,
under Section 2) in object code or executable form under the terms of
Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable
source code, which must be distributed under the terms of Sections
1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three
years, to give any third party, for a charge no more than your

cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other

circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

```
    <one line to give the program's name and a brief idea of what it does.>
    Copyright (C) <year>  <name of author>

    This program is free software; you can redistribute it and/or modify
    it under the terms of the GNU General Public License as published by
    the Free Software Foundation; either version 2 of the License, or
    (at your option) any later version.

    This program is distributed in the hope that it will be useful,
    but WITHOUT ANY WARRANTY; without even the implied warranty of
    MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
    GNU General Public License for more details.

    You should have received a copy of the GNU General Public License
    along with this program; if not, write to the Free Software
    Foundation, Inc., 51 Franklin St, Fifth Floor, Boston, MA  02110-1301  USA
```

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

```
    Gnomovision version 69, Copyright (C) year name of author
    Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
    This is free software, and you are welcome to redistribute it
    under certain conditions; type `show c' for details.
```

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than `show w' and `show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

```
  Yoyodyne, Inc., hereby disclaims all copyright interest in the program
  `Gnomovision' (which makes passes at compilers) written by James Hacker.

  <signature of Ty Coon>, 1 April 1989
  Ty Coon, President of Vice
```

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Library General Public License instead of this License.

[freescale-openflow-controller 1.0]

[COPYRIGHT]

Copyright (c) 2012, 2013 Freescale.

[LICENSE]

Apache License
Version 2.0, January 2004
http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

   "License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

   "Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

   "Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

   "You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

   "Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

   "Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

   "Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

   "Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

   "Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

   "Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of

this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

   (a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

   (b) You must cause any modified files to carry prominent notices stating that You changed the files; and

   (c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

   (d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

   You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or

```
      agreed to in writing, Licensor provides the Work (and each
      Contributor provides its Contributions) on an "AS IS" BASIS,
      WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or
      implied, including, without limitation, any warranties or conditions
      of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A
      PARTICULAR PURPOSE. You are solely responsible for determining the
      appropriateness of using or redistributing the Work and assume any
      risks associated with Your exercise of permissions under this License.

   8. Limitation of Liability. In no event and under no legal theory,
      whether in tort (including negligence), contract, or otherwise,
      unless required by applicable law (such as deliberate and grossly
      negligent acts) or agreed to in writing, shall any Contributor be
      liable to You for damages, including any direct, indirect, special,
      incidental, or consequential damages of any character arising as a
      result of this License or out of the use or inability to use the
      Work (including but not limited to damages for loss of goodwill,
      work stoppage, computer failure or malfunction, or any and all
      other commercial damages or losses), even if such Contributor
      has been advised of the possibility of such damages.

   9. Accepting Warranty or Additional Liability. While redistributing
      the Work or Derivative Works thereof, You may choose to offer,
      and charge a fee for, acceptance of support, warranty, indemnity,
      or other liability obligations and/or rights consistent with this
      License. However, in accepting such obligations, You may act only
      on Your own behalf and on Your sole responsibility, not on behalf
      of any other Contributor, and only if You agree to indemnify,
      defend, and hold each Contributor harmless for any liability
      incurred by, or claims asserted against, such Contributor by reason
      of your accepting any such warranty or additional liability.

   END OF TERMS AND CONDITIONS

   APPENDIX: How to apply the Apache License to your work.

      To apply the Apache License to your work, attach the following
      boilerplate notice, with the fields enclosed by brackets "[]"
      replaced with your own identifying information. (Don't include
      the brackets!)  The text should be enclosed in the appropriate
      comment syntax for the file format. We also recommend that a
      file or class name and description of purpose be included on the
      same "printed page" as the copyright notice for easier
      identification within third-party archives.

   Copyright 2012 Sebastien MALOT

   Licensed under the Apache License, Version 2.0 (the "License");
   you may not use this file except in compliance with the License.
   You may obtain a copy of the License at

       http://www.apache.org/licenses/LICENSE-2.0

   Unless required by applicable law or agreed to in writing, software
   distributed under the License is distributed on an "AS IS" BASIS,
   WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
   See the License for the specific language governing permissions and
   limitations under the License.
-------------------------------------------------------------------------------
---
[ftp client 8.0.0 (part of FreeBSD 8.0.0)]
[COPYRIGHT]
  Copyright (c) 1992-2009 The FreeBSD Project. All rights reserved.

[LICENSE]
Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:
1. Redistributions of source code must retain the above copyright
   notice, this list of conditions and the following disclaimer.
```

2. Redistributions in binary form must reproduce the above copyright
   notice, this list of conditions and the following disclaimer in the
   documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS ``AS IS'' AND
ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
SUCH DAMAGE.

The 4.4BSD and 4.4BSD-Lite software is distributed under the following
terms:

All of the documentation and software included in the 4.4BSD and 4.4BSD-Lite
Releases is copyrighted by The Regents of the University of California.

Copyright 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
         The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:
1. Redistributions of source code must retain the above copyright
   notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright
   notice, this list of conditions and the following disclaimer in the
   documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software
   must display the following acknowledgement:
This product includes software developed by the University of
California, Berkeley and its contributors.
4. Neither the name of the University nor the names of its contributors
   may be used to endorse or promote products derived from this software
   without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND
ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE
FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
SUCH DAMAGE.

The Institute of Electrical and Electronics Engineers and the American
National Standards Committee X3, on Information Processing Systems have
given us permission to reprint portions of their documentation.

In the following statement, the phrase ``this text'' refers to portions
of the system documentation.

Portions of this text are reprinted and reproduced in electronic form in
the second BSD Networking Software Release, from IEEE Std 1003.1-1988, IEEE
Standard Portable Operating System Interface for Computer Environments
(POSIX), copyright C 1988 by the Institute of Electrical and Electronics
Engineers, Inc. In the event of any discrepancy between these versions
and the original IEEE Standard, the original IEEE Standard is the referee
document.

In the following statement, the phrase ``This material'' refers to portions
of the system documentation.

This material is reproduced with permission from American National Standards Committee X3, on Information Processing Systems. Computer and Business Equipment Manufacturers Association (CBEMA), 311 First St., NW, Suite 500, Washington, DC 20001-2178. The developmental work of Programming Language C was completed by the X3J11 Technical Committee.

The views and conclusions contained in the software and documentation are those of the authors and should not be interpreted as representing official policies, either expressed or implied, of the Regents of the University of California.

NOTE: The copyright of UC Berkeley's Berkeley Software Distribution ("BSD") source has been updated. The copyright addendum may be found at ftp://ftp.cs.berkeley.edu/pub/4bsd/README.Impt.License.Change and is included below.

July 22, 1999

To All Licensees, Distributors of Any Version of BSD:

As you know, certain of the Berkeley Software Distribution ("BSD") source code files require that further distributions of products containing all or portions of the software, acknowledge within their advertising materials that such products contain software developed by UC Berkeley and its contributors.

Specifically, the provision reads:

" * 3. All advertising materials mentioning features or use of this software
 * must display the following acknowledgement:
 * This product includes software developed by the University of
 * California, Berkeley and its contributors."

Effective immediately, licensees and distributors are no longer required to include the acknowledgement within advertising materials. Accordingly, the foregoing paragraph of those BSD Unix files containing it is hereby deleted in its entirety.

William Hoskins
Director, Office of Technology Licensing
University of California, Berkeley

[grpc 1.4.2]
[COPYRIGHT]
Copyright 2015, Google Inc.
All rights reserved.

[LICENSE]
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
* Neither the name of Google Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,

```
SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT
LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE,
DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY
THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT
(INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE
OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
--------------------------------------------------------------------------
---
[inet stack 8.0.0 (part of FreeBSD 8.0.0)]
[COPYRIGHT]
  Copyright (c) 1992-2009 The FreeBSD Project. All rights reserved.

[LICENSE]
Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:
1. Redistributions of source code must retain the above copyright
   notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright
   notice, this list of conditions and the following disclaimer in the
   documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS ``AS IS'' AND
ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
ARE DISCLAIMED.  IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
SUCH DAMAGE.

The 4.4BSD and 4.4BSD-Lite software is distributed under the following
terms:

All of the documentation and software included in the 4.4BSD and 4.4BSD-Lite
Releases is copyrighted by The Regents of the University of California.

Copyright 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
         The Regents of the University of California.  All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:
1. Redistributions of source code must retain the above copyright
   notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright
   notice, this list of conditions and the following disclaimer in the
   documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software
   must display the following acknowledgement:
This product includes software developed by the University of
California, Berkeley and its contributors.
4. Neither the name of the University nor the names of its contributors
   may be used to endorse or promote products derived from this software
   without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND
ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
ARE DISCLAIMED.  IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE
FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
SUCH DAMAGE.
```

The Institute of Electrical and Electronics Engineers and the American National Standards Committee X3, on Information Processing Systems have given us permission to reprint portions of their documentation.

In the following statement, the phrase ``this text'' refers to portions of the system documentation.

Portions of this text are reprinted and reproduced in electronic form in the second BSD Networking Software Release, from IEEE Std 1003.1-1988, IEEE Standard Portable Operating System Interface for Computer Environments (POSIX), copyright C 1988 by the Institute of Electrical and Electronics Engineers, Inc. In the event of any discrepancy between these versions and the original IEEE Standard, the original IEEE Standard is the referee document.

In the following statement, the phrase ``This material'' refers to portions of the system documentation.

This material is reproduced with permission from American National Standards Committee X3, on Information Processing Systems. Computer and Business Equipment Manufacturers Association (CBEMA), 311 First St., NW, Suite 500, Washington, DC 20001-2178. The developmental work of Programming Language C was completed by the X3J11 Technical Committee.

The views and conclusions contained in the software and documentation are those of the authors and should not be interpreted as representing official policies, either expressed or implied, of the Regents of the University of California.

NOTE: The copyright of UC Berkeley's Berkeley Software Distribution ("BSD") source has been updated. The copyright addendum may be found at ftp://ftp.cs.berkeley.edu/pub/4bsd/README.Impt.License.Change and is included below.

July 22, 1999

To All Licensees, Distributors of Any Version of BSD:

As you know, certain of the Berkeley Software Distribution ("BSD") source code files require that further distributions of products containing all or portions of the software, acknowledge within their advertising materials that such products contain software developed by UC Berkeley and its contributors.

Specifically, the provision reads:

```
"     * 3. All advertising materials mentioning features or use of this software
       *    must display the following acknowledgement:
       *    This product includes software developed by the University of
       *    California, Berkeley and its contributors."
```

Effective immediately, licensees and distributors are no longer required to include the acknowledgement within advertising materials. Accordingly, the foregoing paragraph of those BSD Unix files containing it is hereby deleted in its entirety.

William Hoskins
Director, Office of Technology Licensing
University of California, Berkeley

[jquery-ui 1.9.2]
[COPYRIGHT]
Copyright 2012 jQuery Foundation and other contributors,
http://jqueryui.com/

[LICENSE]
This software consists of voluntary contributions made by many

```
individuals (AUTHORS.txt, http://jqueryui.com/about) For exact
contribution history, see the revision history and logs, available
at http://jquery-ui.googlecode.com/svn/

Permission is hereby granted, free of charge, to any person obtaining
a copy of this software and associated documentation files (the
"Software"), to deal in the Software without restriction, including
without limitation the rights to use, copy, modify, merge, publish,
distribute, sublicense, and/or sell copies of the Software, and to
permit persons to whom the Software is furnished to do so, subject to
the following conditions:

The above copyright notice and this permission notice shall be
included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND,
EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF
MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND
NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE
LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION
OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION
WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

--------------------------------------------------------------------------
---
[jquery.event.drag 2.2]
[COPYRIGHT]
  Copyright (c) 2008-2021 ThreeDubMedia

[LICENSE]
Permission is hereby granted, free of charge, to any person
obtaining a copy of this software and associated documentation
files (the "Software"), to deal in the Software without
restriction, including without limitation the rights to use,
copy, modify, merge, publish, distribute, sublicense, and/or sell
copies of the Software, and to permit persons to whom the
Software is furnished to do so, subject to the following
conditions:

The above copyright notice and this permission notice shall be
included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND,
EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES
OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND
NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT
HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY,
WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING
FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR
OTHER DEALINGS IN THE SOFTWARE.
--------------------------------------------------------------------------
---
[json c 0.12]
[COPYRIGHT]
  Copyright (c) 2009-2012 Eric Haszlakiewicz

[LICENSE]
Permission is hereby granted, free of charge, to any person obtaining a
copy of this software and associated documentation files (the "Software"),
to deal in the Software without restriction, including without limitation
the rights to use, copy, modify, merge, publish, distribute, sublicense,
and/or sell copies of the Software, and to permit persons to whom the
Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included
in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,
FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE
```

AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER
LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,
OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE
SOFTWARE.

[COPYRIGHT]
Copyright (c) 2004, 2005 Metaparadigm Pte Ltd

[LICENSE]
Permission is hereby granted, free of charge, to any person obtaining a
copy of this software and associated documentation files (the "Software"),
to deal in the Software without restriction, including without limitation
the rights to use, copy, modify, merge, publish, distribute, sublicense,
and/or sell copies of the Software, and to permit persons to whom the
Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included
in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,
FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE
AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER
LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,
OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE
SOFTWARE.

[jstree 3.0.0]
[COPYRIGHT]
  Copyright (c) 2013 Ivan Bozhanov

[LICENSE]
Permission is hereby granted, free of charge, to any person
obtaining a copy of this software and associated documentation
files (the "Software"), to deal in the Software without
restriction, including without limitation the rights to use,
copy, modify, merge, publish, distribute, sublicense, and/or sell
copies of the Software, and to permit persons to whom the
Software is furnished to do so, subject to the following
conditions:

The above copyright notice and this permission notice shall be
included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND,
EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES
OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND
NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT
HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY,
WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING
FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR
OTHER DEALINGS IN THE SOFTWARE.

[libiconv 1.13.1]
[LICENSE]
                  GNU LIBRARY GENERAL PUBLIC LICENSE
                       Version 2, June 1991

 Copyright (C) 1991 Free Software Foundation, Inc.
 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA
 Everyone is permitted to copy and distribute verbatim copies
 of this license document, but changing it is not allowed.

[This is the first released version of the library GPL. It is
 numbered 2 because it goes with version 2 of the ordinary GPL.]

                            Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Library General Public License, applies to some specially designated Free Software Foundation software, and to any other libraries whose authors decide to use it. You can use it for your libraries, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library, or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link a program with the library, you must provide complete object files to the recipients so that they can relink them with the library, after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

Our method of protecting your rights has two steps: (1) copyright the library, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the library.

Also, for each distributor's protection, we want to make certain that everyone understands that there is no warranty for this free library. If the library is modified by someone else and passed on, we want its recipients to know that what they have is not the original version, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that companies distributing free software will individually obtain patent licenses, thus in effect transforming the program into proprietary software. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License, which was designed for utility programs. This license, the GNU Library General Public License, applies to certain designated libraries. This license is quite different from the ordinary one; be sure to read it in full, and don't assume that anything in it is the same as in the ordinary license.

The reason we have a separate public license for some libraries is that they blur the distinction we usually make between modifying or adding to a program and simply using it. Linking a program with a library, without changing the library, is in some sense simply using the library, and is analogous to running a utility program or application program. However, in a textual and legal sense, the linked executable is a combined work, a derivative of the original library, and the ordinary General Public License treats it as such.

Because of this blurred distinction, using the ordinary General Public License for libraries did not effectively promote software sharing, because most developers did not use the libraries. We concluded that weaker conditions might promote sharing better.

However, unrestricted linking of non-free programs would deprive the users of those programs of all benefit from the free status of the libraries themselves. This Library General Public License is intended to permit developers of non-free programs to use free libraries, while preserving your freedom as a user of such programs to change the free libraries that are incorporated in them. (We have not seen how to achieve this as regards changes in header files, but we have achieved it as regards changes in the actual functions of the Library.) The hope is that this will lead to faster development of free libraries.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, while the latter only works together with the library.

Note that it is possible for a library to be covered by the ordinary General Public License rather than by this special one.

GNU LIBRARY GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Library General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion

of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a

medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also compile or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more

than the cost of performing this distribution.

c) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

d) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or

otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Library General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

Appendix: How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the library's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Library General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Library General Public License for more details.

You should have received a copy of the GNU Library General Public License along with this library; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA

Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the library, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the library `Frob' (a library for tweaking knobs) written by James Random Hacker.

<signature of Ty Coon>, 1 April 1990
Ty Coon, President of Vice

That's all there is to it!

[libpcap 1.2.0]
[LICENSE]
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright

```
     notice, this list of conditions and the following disclaimer in
     the documentation and/or other materials provided with the
     distribution.
  3. The names of the authors may not be used to endorse or promote
     products derived from this software without specific prior
     written permission.

THIS SOFTWARE IS PROVIDED ``AS IS'' AND WITHOUT ANY EXPRESS OR
IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED
WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.
--------------------------------------------------------------------------------
---
[libssh2 1.4.3]
[COPYRIGHT]
  Copyright (c) 2004-2007 Sara Golemon <sarag@libssh2.org>
  Copyright (c) 2005,2006 Mikhail Gusarov <dottedmag@dottedmag.net>
  Copyright (c) 2006-2007 The Written Word, Inc.
  Copyright (c) 2007 Eli Fant <elifantu@mail.ru>
  Copyright (c) 2009 Daniel Stenberg
  Copyright (C) 2008, 2009 Simon Josefsson
  All rights reserved.

[LICENSE]
  Redistribution and use in source and binary forms,
  with or without modification, are permitted provided
  that the following conditions are met:

    Redistributions of source code must retain the above
    copyright notice, this list of conditions and the
    following disclaimer.

    Redistributions in binary form must reproduce the above
    copyright notice, this list of conditions and the following
    disclaimer in the documentation and/or other materials
    provided with the distribution.

    Neither the name of the copyright holder nor the names
    of any other contributors may be used to endorse or
    promote products derived from this software without
    specific prior written permission.

  THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND
  CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES,
  INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES
  OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
  ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR
  CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
  SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING,
  BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR
  SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS
  INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY,
  WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING
  NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE
  USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY
  OF SUCH DAMAGE.


--------------------------------------------------------------------------------
---
[liburcu 0.6.8]
[COPYRIGHT]
  Copyright (c) 2009 Mathieu Desnoyers <mathieu.desnoyers@efficios.com>
  Copyright (c) 2009 Paul E. McKenney, IBM Corporation.

[LICENSE]
  This library is free software; you can redistribute it and/or
  modify it under the terms of the GNU Lesser General Public
  License as published by the Free Software Foundation; either
  version 2.1 of the License, or (at your option) any later version.
```

```
  This library is distributed in the hope that it will be useful,
  but WITHOUT ANY WARRANTY; without even the implied warranty of
  MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the GNU
  Lesser General Public License for more details.

  You should have received a copy of the GNU Lesser General Public
  License along with this library; if not, write to the Free Software
  Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

  IBM's contributions to this file may be relicensed under LGPLv2 or later.

--------------------------------------------------------------------------------
---
[multiselect 0.9.5]
[COPYRIGHT]
  Copyright (c) 2012 Louis Cuny

[LICENSE]
            DO WHAT THE FUCK YOU WANT TO PUBLIC LICENSE
                    Version 2, December 2004

 Copyright (C) 2004 Sam Hocevar <sam@hocevar.net>

 Everyone is permitted to copy and distribute verbatim or modified
 copies of this license document, and changing it is allowed as long
 as the name is changed.

            DO WHAT THE FUCK YOU WANT TO PUBLIC LICENSE
   TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

  0. You just DO WHAT THE FUCK YOU WANT TO.
--------------------------------------------------------------------------------
---
[ncurses 5.7]
[COPYRIGHT]
  Copyright (c) 1998-2004,2006 Free Software Foundation, Inc.

[LICENSE]
--                                                                          --
-- Permission is hereby granted, free of charge, to any person obtaining a  --
-- copy of this software and associated documentation files (the            --
-- "Software"), to deal in the Software without restriction, including      --
-- without limitation the rights to use, copy, modify, merge, publish,      --
-- distribute, distribute with modifications, sublicense, and/or sell copies --
-- of the Software, and to permit persons to whom the Software is furnished --
-- to do so, subject to the following conditions:                           --
--                                                                          --
-- The above copyright notice and this permission notice shall be included  --
-- in all copies or substantial portions of the Software.                   --
--                                                                          --
-- THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS  --
-- OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF               --
-- MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN --
-- NO EVENT SHALL THE ABOVE COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM,      --
-- DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR    --
-- OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE --
-- USE OR OTHER DEALINGS IN THE SOFTWARE.                                   --
--                                                                          --
-- Except as contained in this notice, the name(s) of the above copyright   --
-- holders shall not be used in advertising or otherwise to promote the     --
-- sale, use or other dealings in this Software without prior written       --
-- authorization.                                                           --
--------------------------------------------------------------------------------
---
[net-snmp 5.4.3]
Various copyrights apply to this package, listed in various separate
parts below.  Please make sure that you read all the parts.

---- Part 1: CMU/UCD copyright notice: (BSD like) -----
```

Copyright 1989, 1991, 1992 by Carnegie Mellon University

Derivative Work - 1996, 1998-2000
Copyright 1996, 1998-2000 The Regents of the University of California

All Rights Reserved

Permission to use, copy, modify and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appears in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of CMU and The Regents of the University of California not be used in advertising or publicity pertaining to distribution of the software without specific written permission.

CMU AND THE REGENTS OF THE UNIVERSITY OF CALIFORNIA DISCLAIM ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL CMU OR THE REGENTS OF THE UNIVERSITY OF CALIFORNIA BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM THE LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

---- Part 2: Networks Associates Technology, Inc copyright notice (BSD) -----

Copyright (c) 2001-2003, Networks Associates Technology, Inc
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of the Networks Associates Technology, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 3: Cambridge Broadband Ltd. copyright notice (BSD) -----

Portions of this code are copyright (c) 2001-2003, Cambridge Broadband Ltd.
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright
  notice, this list of conditions and the following disclaimer in the
  documentation and/or other materials provided with the distribution.

* The name of Cambridge Broadband Ltd. may not be used to endorse or
  promote products derived from this software without specific prior
  written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER ``AS IS'' AND ANY
EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE
LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF
SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR
BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY,
WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE
OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN
IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 4: Sun Microsystems, Inc. copyright notice (BSD) -----

Copyright ?2003 Su Microsystems, Inc., 4150 Network Circle, Santa Clara,
California 95054, U.S.A. All rights reserved.

Use is subject to license terms below.

This distribution may include materials developed by third parties.

Sun, Sun Microsystems, the Sun logo and Solaris are trademarks or registered
trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice,
  this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright
  notice, this list of conditions and the following disclaimer in the
  documentation and/or other materials provided with the distribution.

* Neither the name of the Sun Microsystems, Inc. nor the
  names of its contributors may be used to endorse or promote
  products derived from this software without specific prior written
  permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS
IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO,
THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR
CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL,
EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,
PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS;
OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY,
WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR
OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF
ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 5: Sparta, Inc copyright notice (BSD) -----

Copyright (c) 2003-2010, Sparta, Inc
All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice,
  this list of conditions and the following disclaimer.

```
* Redistributions in binary form must reproduce the above copyright
  notice, this list of conditions and the following disclaimer in the
  documentation and/or other materials provided with the distribution.

* Neither the name of Sparta, Inc nor the names of its contributors may
  be used to endorse or promote products derived from this software
  without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS
IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO,
THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR
CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL,
EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,
PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS;
OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY,
WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR
OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF
ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 6: Cisco/BUPTNIC copyright notice (BSD) -----

Copyright (c) 2004, Cisco, Inc and Information Network
Center of Beijing University of Posts and Telecommunications.
All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice,
  this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright
  notice, this list of conditions and the following disclaimer in the
  documentation and/or other materials provided with the distribution.

* Neither the name of Cisco, Inc, Beijing University of Posts and
  Telecommunications, nor the names of their contributors may
  be used to endorse or promote products derived from this software
  without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS
IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO,
THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR
CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL,
EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,
PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS;
OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY,
WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR
OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF
ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 7: Fabasoft R&D Software GmbH & Co KG copyright notice (BSD) -----

Copyright (c) Fabasoft R&D Software GmbH & Co KG, 2003
oss@fabasoft.com
Author: Bernhard Penz <bernhard.penz@fabasoft.com>

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice,
  this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright
  notice, this list of conditions and the following disclaimer in the
  documentation and/or other materials provided with the distribution.
```

```
*  The name of Fabasoft R&D Software GmbH & Co KG or any of its subsidiaries,
   brand or product names may not be used to endorse or promote products
   derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER ``AS IS'' AND ANY
EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE COPYRIGHT HOLDER BE
LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF
SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR
BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY,
WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE
OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN
IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

--------------------------------------------------------------------------
---
[ntp 4.2 6p2-RC4]
This file is automatically generated from html/copyright.html

  Copyright Notice

   jpg "Clone me," says Dolly sheepishly.

   Last update: 11-May-2010 04:41 UTC

     ____________________________________________________________________

   The following copyright notice applies to all files collectively
   called the Network Time Protocol Version 4 Distribution. Unless
   specifically declared otherwise in an individual file, this notice
   applies as if the text was explicitly included in the file.
*************************************************************************
*                                                                       *
* Copyright (c) University of Delaware 1992-2010                        *
*                                                                       *
* Permission to use, copy, modify, and distribute this software and     *
* its documentation for any purpose with or without fee is hereby       *
* granted, provided that the above copyright notice appears in all      *
* copies and that both the copyright notice and this permission         *
* notice appear in supporting documentation, and that the name          *
* University of Delaware not be used in advertising or publicity        *
* pertaining to distribution of the software without specific,          *
* written prior permission. The University of Delaware makes no         *
* representations about the suitability this software for any           *
* purpose. It is provided "as is" without express or implied            *
* warranty.                                                             *
*                                                                       *
*************************************************************************

   The following individuals contributed in part to the Network Time
   Protocol Distribution Version 4 and are acknowledged as authors of
   this work.
    1. [1]Mark Andrews <mark_andrews@isc.org> Leitch atomic clock
       controller
    2. [2]Bernd Altmeier <altmeier@atlsoft.de> hopf Elektronik serial
       line and PCI-bus devices
    3. [3]Viraj Bais <vbais@mailman1.intel.com> and [4]Clayton Kirkwood
       <kirkwood@striderfm.intel.com> port to WindowsNT 3.5
    4. [5]Michael Barone <michael,barone@lmco.com> GPSVME fixes
    5. [6]Karl Berry <karl@owl.HQ.ileaf.com> syslog to file option
    6. [7]Greg Brackley <greg.brackley@bigfoot.com> Major rework of WINNT
       port. Clean up recvbuf and iosignal code into separate modules.
    7. [8]Marc Brett <Marc.Brett@westgeo.com> Magnavox GPS clock driver
    8. [9]Piete Brooks <Piete.Brooks@cl.cam.ac.uk> MSF clock driver,
       Trimble PARSE support
    9. [10]Nelson B Bolyard <nelson@bolyard.me> update and complete
       broadcast and crypto features in sntp
   10. [11]Jean-Francois Boudreault
       <Jean-Francois.Boudreault@viagenie.qc.ca> IPv6 support
```

11. [12]Reg Clemens <reg@dwf.com> Oncore driver (Current maintainer)
12. [13]Steve Clift <clift@ml.csiro.au> OMEGA clock driver
13. [14]Casey Crellin <casey@csc.co.za> vxWorks (Tornado) port and help with target configuration
14. [15]Sven Dietrich <sven_dietrich@trimble.com> Palisade reference clock driver, NT adj. residuals, integrated Greg's Winnt port.
15. [16]John A. Dundas III <dundas@salt.jpl.nasa.gov> Apple A/UX port
16. [17]Torsten Duwe <duwe@immd4.informatik.uni-erlangen.de> Linux port
17. [18]Dennis Ferguson <dennis@mrbill.canet.ca> foundation code for NTP Version 2 as specified in RFC-1119
18. [19]John Hay <jhay@icomtek.csir.co.za> IPv6 support and testing
19. [20]Dave Hart <davehart@davehart.com> General maintenance, Windows port interpolation rewrite
20. [21]Claas Hilbrecht <neoclock4x@linum.com> NeoClock4X clock driver
21. [22]Glenn Hollinger <glenn@herald.usask.ca> GOES clock driver
22. [23]Mike Iglesias <iglesias@uci.edu> DEC Alpha port
23. [24]Jim Jagielski <jim@jagubox.gsfc.nasa.gov> A/UX port
24. [25]Jeff Johnson <jbj@chatham.usdesign.com> massive prototyping overhaul
25. [26]Hans Lambermont <Hans.Lambermont@nl.origin-it.com> or [27]<H.Lambermont@chello.nl> ntpsweep
26. [28]Poul-Henning Kamp <phk@FreeBSD.ORG> Oncore driver (Original author)
27. [29]Frank Kardel [30]<kardel (at) ntp (dot) org> PARSE <GENERIC> driver (>14 reference clocks), STREAMS modules for PARSE, support scripts, syslog cleanup, dynamic interface handling
28. [31]William L. Jones <jones@hermes.chpc.utexas.edu> RS/6000 AIX modifications, HPUX modifications
29. [32]Dave Katz <dkatz@cisco.com> RS/6000 AIX port
30. [33]Craig Leres <leres@ee.lbl.gov> 4.4BSD port, ppsclock, Magnavox GPS clock driver
31. [34]George Lindholm <lindholm@ucs.ubc.ca> SunOS 5.1 port
32. [35]Louis A. Mamakos <louie@ni.umd.edu> MD5-based authentication
33. [36]Lars H. Mathiesen <thorinn@diku.dk> adaptation of foundation code for Version 3 as specified in RFC-1305
34. [37]Danny Mayer <mayer@ntp.org>Network I/O, Windows Port, Code Maintenance
35. [38]David L. Mills <mills@udel.edu> Version 4 foundation: clock discipline, authentication, precision kernel; clock drivers: Spectracom, Austron, Arbiter, Heath, ATOM, ACTS, KSI/Odetics; audio clock drivers: CHU, WWV/H, IRIG
36. [39]Wolfgang Moeller <moeller@gwdgv1.dnet.gwdg.de> VMS port
37. [40]Jeffrey Mogul <mogul@pa.dec.com> ntptrace utility
38. [41]Tom Moore <tmoore@fievel.daytonoh.ncr.com> i386 svr4 port
39. [42]Kamal A Mostafa <kamal@whence.com> SCO OpenServer port
40. [43]Derek Mulcahy <derek@toybox.demon.co.uk> and [44]Damon Hart-Davis <d@hd.org> ARCRON MSF clock driver
41. [45]Rob Neal <neal@ntp.org> Bancomm refclock and config/parse code maintenance
42. [46]Rainer Pruy <Rainer.Pruy@informatik.uni-erlangen.de> monitoring/trap scripts, statistics file handling
43. [47]Dirce Richards <dirce@zk3.dec.com> Digital UNIX V4.0 port
44. [48]Wilfredo S 疣 chez <wanchez@apple.com> added support for NetInfo
45. [49]Nick Sayer <mrapple@quack.kfu.com> SunOS streams modules
46. [50]Jack Sasportas <jack@innovativeinternet.com> Saved a Lot of space on the stuff in the html/pic/ subdirectory
47. [51]Ray Schnitzler <schnitz@unipress.com> Unixware1 port
48. [52]Michael Shields <shields@tembel.org> USNO clock driver
49. [53]Jeff Steinman <jss@pebbles.jpl.nasa.gov> Datum PTS clock driver
50. [54]Harlan Stenn <harlan@pfcs.com> GNU automake/autoconfigure makeover, various other bits (see the ChangeLog)
51. [55]Kenneth Stone <ken@sdd.hp.com> HP-UX port
52. [56]Ajit Thyagarajan <ajit@ee.udel.edu>IP multicast/anycast support
53. [57]Tomoaki TSURUOKA <tsuruoka@nc.fukuoka-u.ac.jp>TRAK clock driver
54. [58]Paul A Vixie <vixie@vix.com> TrueTime GPS driver, generic

```
      TrueTime clock driver
   55. [59]Ulrich Windl <Ulrich.Windl@rz.uni-regensburg.de> corrected and
       validated HTML documents according to the HTML DTD

   ____________________________________________________________________

References

   1. mailto:%20mark_andrews@isc.org
   2. mailto:%20altmeier@atlsoft.de
   3. mailto:%20vbais@mailman1.intel.co
   4. mailto:%20kirkwood@striderfm.intel.com
   5. mailto:%20michael.barone@lmco.com
   6. mailto:%20karl@owl.HQ.ileaf.com
   7. mailto:%20greg.brackley@bigfoot.com
   8. mailto:%20Marc.Brett@westgeo.com
   9. mailto:%20Piete.Brooks@cl.cam.ac.uk
  10. mailto:%20nelson@bolyard.me
  11. mailto:%20Jean-Francois.Boudreault@viagenie.qc.ca
  12. mailto:%20reg@dwf.com
  13. mailto:%20clift@ml.csiro.au
  14. mailto:casey@csc.co.za
  15. mailto:%20Sven_Dietrich@trimble.COM
  16. mailto:%20dundas@salt.jpl.nasa.gov
  17. mailto:%20duwe@immd4.informatik.uni-erlangen.de
  18. mailto:%20dennis@mrbill.canet.ca
  19. mailto:%20jhay@icomtek.csir.co.za
  20. mailto:%20davehart@davehart.com
  21. mailto:%20neoclock4x@linum.com
  22. mailto:%20glenn@herald.usask.ca
  23. mailto:%20iglesias@uci.edu
  24. mailto:%20jagubox.gsfc.nasa.gov
  25. mailto:%20jbj@chatham.usdesign.com
  26. mailto:Hans.Lambermont@nl.origin-it.com
  27. mailto:H.Lambermont@chello.nl
  28. mailto:%20phk@FreeBSD.ORG
  29. http://www4.informatik.uni-erlangen.de/%7ekardel
  30. mailto:%20kardel(at)ntp(dot)org
  31. mailto:%20jones@hermes.chpc.utexas.edu
  32. mailto:%20dkatz@cisco.com
  33. mailto:%20leres@ee.lbl.gov
  34. mailto:%20lindholm@ucs.ubc.ca
  35. mailto:%20louie@ni.umd.edu
  36. mailto:%20thorinn@diku.dk
  37. mailto:%20mayer@ntp.org
  38. mailto:%20mills@udel.edu
  39. mailto:%20moeller@gwdgv1.dnet.gwdg.de
  40. mailto:%20mogul@pa.dec.com
  41. mailto:%20tmoore@fievel.daytonoh.ncr.com
  42. mailto:%20kamal@whence.com
  43. mailto:%20derek@toybox.demon.co.uk
  44. mailto:%20d@hd.org
  45. mailto:%20neal@ntp.org
  46. mailto:%20Rainer.Pruy@informatik.uni-erlangen.de
  47. mailto:%20dirce@zk3.dec.com
  48. mailto:%20wsanchez@apple.com
  49. mailto:%20mrapple@quack.kfu.com
  50. mailto:%20jack@innovativeinternet.com
  51. mailto:%20schnitz@unipress.com
  52. mailto:%20shields@tembel.org
  53. mailto:%20pebbles.jpl.nasa.gov
  54. mailto:%20harlan@pfcs.com
  55. mailto:%20ken@sdd.hp.com
  56. mailto:%20ajit@ee.udel.edu
  57. mailto:%20tsuruoka@nc.fukuoka-u.ac.jp
  58. mailto:%20vixie@vix.com
  59. mailto:%20Ulrich.Windl@rz.uni-regensburg.de
--------------------------------------------------------------------------
---
[openldap 2.4.45]
[COPYRIGHT]
```

```
  Copyright 1998-2017 The OpenLDAP Foundation
  All rights reserved.

[NOTE]
Redistribution and use in source and binary forms, with or without
modification, are permitted only as authorized by the OpenLDAP
Public License.

A copy of this license is available in the file LICENSE in the
top-level directory of the distribution or, alternatively, at
<http://www.OpenLDAP.org/license.html>.

OpenLDAP is a registered trademark of the OpenLDAP Foundation.

Individual files and/or contributed packages may be copyright by
other parties and/or subject to additional restrictions.

This work is derived from the University of Michigan LDAP v3.3
distribution.  Information concerning this software is available
at <http://www.umich.edu/~dirsvcs/ldap/ldap.html>.

This work also contains materials derived from public sources.

Additional information about OpenLDAP can be obtained at
<http://www.openldap.org/>.

---

Portions Copyright 1998-2012 Kurt D. Zeilenga.
Portions Copyright 1998-2006 Net Boolean Incorporated.
Portions Copyright 2001-2006 IBM Corporation.
All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted only as authorized by the OpenLDAP
Public License.

---

Portions Copyright 1999-2008 Howard Y.H. Chu.
Portions Copyright 1999-2008 Symas Corporation.
Portions Copyright 1998-2003 Hallvard B. Furuseth.
Portions Copyright 2007-2011 Gavin Henry.
Portions Copyright 2007-2011 Suretec Systems Ltd.
All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that this notice is preserved.
The names of the copyright holders may not be used to endorse or
promote products derived from this software without their specific
prior written permission.  This software is provided ``as is''
without express or implied warranty.

---

Portions Copyright (c) 1992-1996 Regents of the University of Michigan.
All rights reserved.

Redistribution and use in source and binary forms are permitted
provided that this notice is preserved and that due credit is given
to the University of Michigan at Ann Arbor.  The name of the
University may not be used to endorse or promote products derived
from this software without specific prior written permission.  This
software is provided ``as is'' without express or implied warranty.

[LICENSE]
The OpenLDAP Public License
  Version 2.8, 17 August 2003

Redistribution and use of this software and associated documentation
```

("Software"), with or without modification, are permitted provided
that the following conditions are met:

1. Redistributions in source form must retain copyright statements
   and notices,

2. Redistributions in binary form must reproduce applicable copyright
   statements and notices, this list of conditions, and the following
   disclaimer in the documentation and/or other materials provided
   with the distribution, and

3. Redistributions must contain a verbatim copy of this document.

The OpenLDAP Foundation may revise this license from time to time.
Each revision is distinguished by a version number. You may use
this Software under terms of this license revision or under the
terms of any subsequent revision of the license.

THIS SOFTWARE IS PROVIDED BY THE OPENLDAP FOUNDATION AND ITS
CONTRIBUTORS ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES,
INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT
SHALL THE OPENLDAP FOUNDATION, ITS CONTRIBUTORS, OR THE AUTHOR(S)
OR OWNER(S) OF THE SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT,
INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING,
BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER
CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN
ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE
POSSIBILITY OF SUCH DAMAGE.

The names of the authors and copyright holders must not be used in
advertising or otherwise to promote the sale, use or other dealing
in this Software without specific, written prior permission. Title
to copyright in this Software shall at all times remain with copyright
holders.

OpenLDAP is a registered trademark of the OpenLDAP Foundation.

Copyright 1999-2003 The OpenLDAP Foundation, Redwood City,
California, USA. All Rights Reserved. Permission to copy and
distribute verbatim copies of this document is granted.

[openpam 20071221]
[COPYRIGHT]
  Copyright (c) 2002-2003 Networks Associates Technology, Inc.
  Copyright (c) 2004-2007 Dag-Erling Sm テク rgrav
  All rights reserved.

[LICENSE]
This software was developed for the FreeBSD Project by ThinkSec AS and
Network Associates Laboratories, the Security Research Division of
Network Associates, Inc. under DARPA/SPAWAR contract N66001-01-C-8035
("CBOSS"), as part of the DARPA CHATS research program.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:
1. Redistributions of source code must retain the above copyright
   notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright
   notice, this list of conditions and the following disclaimer in the
   documentation and/or other materials provided with the distribution.
3. The name of the author may not be used to endorse or promote
   products derived from this software without specific prior written
   permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS ``AS IS'' AND

```
ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
ARE DISCLAIMED.  IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
SUCH DAMAGE.

--------------------------------------------------------------------------
---
[openssh 5.3p1]
The licences which components of this software fall under are as
follows.  First, we will summarize and say that all components
are under a BSD licence, or a licence more free than that.

OpenSSH contains no GPL code.

1)
     * Copyright (c) 1995 Tatu Ylonen <ylo@cs.hut.fi>, Espoo, Finland
     *                    All rights reserved
     *
     * As far as I am concerned, the code I have written for this software
     * can be used freely for any purpose.  Any derived versions of this
     * software must be clearly marked as such, and if the derived work is
     * incompatible with the protocol description in the RFC file, it must be
     * called by a name other than "ssh" or "Secure Shell".

    [Tatu continues]
     *  However, I am not implying to give any licenses to any patents or
     * copyrights held by third parties, and the software includes parts that
     * are not under my direct control.  As far as I know, all included
     * source code is used in accordance with the relevant license agreements
     * and can be used freely for any purpose (the GNU license being the most
     * restrictive); see below for details.

    [However, none of that term is relevant at this point in time.  All of
    these restrictively licenced software components which he talks about
    have been removed from OpenSSH, i.e.,

     - RSA is no longer included, found in the OpenSSL library
     - IDEA is no longer included, its use is deprecated
     - DES is now external, in the OpenSSL library
     - GMP is no longer used, and instead we call BN code from OpenSSL
     - Zlib is now external, in a library
     - The make-ssh-known-hosts script is no longer included
     - TSS has been removed
     - MD5 is now external, in the OpenSSL library
     - RC4 support has been replaced with ARC4 support from OpenSSL
     - Blowfish is now external, in the OpenSSL library

    [The licence continues]

    Note that any information and cryptographic algorithms used in this
    software are publicly available on the Internet and at any major
    bookstore, scientific library, and patent office worldwide.  More
    information can be found e.g. at "http://www.cs.hut.fi/crypto".

    The legal status of this program is some combination of all these
    permissions and restrictions.  Use only at your own responsibility.
    You will be responsible for any legal consequences yourself; I am not
    making any claims whether possessing or using this is legal or not in
    your country, and I am not taking any responsibility on your behalf.


                                NO WARRANTY

    BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY
```

```
FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW.  EXCEPT WHEN
OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES
PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED
OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF
MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.  THE ENTIRE RISK AS
TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU.  SHOULD THE
PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING,
REPAIR OR CORRECTION.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING
WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR
REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES,
INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING
OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED
TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY
YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER
PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE
POSSIBILITY OF SUCH DAMAGES.

2)
    The 32-bit CRC compensation attack detector in deattack.c was
    contributed by CORE SDI S.A. under a BSD-style license.

     * Cryptographic attack detector for ssh - source code
     *
     * Copyright (c) 1998 CORE SDI S.A., Buenos Aires, Argentina.
     *
     * All rights reserved. Redistribution and use in source and binary
     * forms, with or without modification, are permitted provided that
     * this copyright notice is retained.
     *
     * THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESS OR IMPLIED
     * WARRANTIES ARE DISCLAIMED. IN NO EVENT SHALL CORE SDI S.A. BE
     * LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY OR
     * CONSEQUENTIAL DAMAGES RESULTING FROM THE USE OR MISUSE OF THIS
     * SOFTWARE.
     *
     * Ariel Futoransky <futo@core-sdi.com>
     * <http://www.core-sdi.com>

3)
    ssh-keyscan was contributed by David Mazieres under a BSD-style
    license.

     * Copyright 1995, 1996 by David Mazieres <dm@lcs.mit.edu>.
     *
     * Modification and redistribution in source and binary forms is
     * permitted provided that due credit is given to the author and the
     * OpenBSD project by leaving this copyright notice intact.

4)
    The Rijndael implementation by Vincent Rijmen, Antoon Bosselaers
    and Paulo Barreto is in the public domain and distributed
    with the following license:

     * @version 3.0 (December 2000)
     *
     * Optimised ANSI C code for the Rijndael cipher (now AES)
     *
     * @author Vincent Rijmen <vincent.rijmen@esat.kuleuven.ac.be>
     * @author Antoon Bosselaers <antoon.bosselaers@esat.kuleuven.ac.be>
     * @author Paulo Barreto <paulo.barreto@terra.com.br>
     *
     * This code is hereby placed in the public domain.
     *
     * THIS SOFTWARE IS PROVIDED BY THE AUTHORS ''AS IS'' AND ANY EXPRESS
     * OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED
     * WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
     * ARE DISCLAIMED.  IN NO EVENT SHALL THE AUTHORS OR CONTRIBUTORS BE
     * LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
```

```
 * CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF
 * SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR
 * BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY,
 * WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE
 * OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE,
 * EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
```

5)

One component of the ssh source code is under a 3-clause BSD license, held by the University of California, since we pulled these parts from original Berkeley code.

```
 * Copyright (c) 1983, 1990, 1992, 1993, 1995
 *      The Regents of the University of California.  All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 * 1. Redistributions of source code must retain the above copyright
 *    notice, this list of conditions and the following disclaimer.
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in the
 *    documentation and/or other materials provided with the distribution.
 * 3. Neither the name of the University nor the names of its contributors
 *    may be used to endorse or promote products derived from this software
 *    without specific prior written permission.
 *
 * THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND
 * ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
 * ARE DISCLAIMED.  IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE
 * FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
 * DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
 * OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
 * LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
 * OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
 * SUCH DAMAGE.
```

6)

Remaining components of the software are provided under a standard 2-term BSD licence with the following names as copyright holders:

```
     Markus Friedl
     Theo de Raadt
     Niels Provos
     Dug Song
     Aaron Campbell
     Damien Miller
     Kevin Steves
     Daniel Kouril
     Wesley Griffin
     Per Allansson
     Nils Nordman
     Simon Wilkinson
```

Portable OpenSSH additionally includes code from the following copyright holders, also under the 2-term BSD license:

```
     Ben Lindstrom
     Tim Rice
     Andre Lucas
     Chris Adams
     Corinna Vinschen
     Cray Inc.
     Denis Parker
     Gert Doering
     Jakob Schlyter
     Jason Downs
     Juha Yrj □?      Michael Stone
```

```
        NetworksAssociates Technology, Inc.
        Solar Designer
        Todd C. Miller
        Wayne Schroeder
        William Jones
        Darren Tucker
        Sun Microsystems
        The SCO Group
        Daniel Walsh

     * Redistribution and use in source and binary forms, with or without
     * modification, are permitted provided that the following conditions
     * are met:
     * 1. Redistributions of source code must retain the above copyright
     *    notice, this list of conditions and the following disclaimer.
     * 2. Redistributions in binary form must reproduce the above copyright
     *    notice, this list of conditions and the following disclaimer in the
     *    documentation and/or other materials provided with the distribution.
     *
     * THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS'' AND ANY EXPRESS OR
     * IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES
     * OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED.
     * IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT,
     * INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
     * NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE,
     * DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY
     * THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT
     * (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF
     * THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

8) Portable OpenSSH contains the following additional licenses:

    a) md5crypt.c, md5crypt.h

         * "THE BEER-WARE LICENSE" (Revision 42):
         * <phk@login.dknet.dk> wrote this file.  As long as you retain this
         * notice you can do whatever you want with this stuff. If we meet
         * some day, and you think this stuff is worth it, you can buy me a
         * beer in return.   Poul-Henning Kamp

    b) snprintf replacement

        * Copyright Patrick Powell 1995
        * This code is based on code written by Patrick Powell
        * (papowell@astart.com) It may be used for any purpose as long as this
        * notice remains intact on all source code distributions

    c) Compatibility code (openbsd-compat)

       Apart from the previously mentioned licenses, various pieces of code
       in the openbsd-compat/ subdirectory are licensed as follows:

       Some code is licensed under a 3-term BSD license, to the following
       copyright holders:

         Todd C. Miller
         Theo de Raadt
         Damien Miller
         Eric P. Allman
         The Regents of the University of California
         Constantin S. Svintsoff

         * Redistribution and use in source and binary forms, with or without
         * modification, are permitted provided that the following conditions
         * are met:
         * 1. Redistributions of source code must retain the above copyright
         *    notice, this list of conditions and the following disclaimer.
         * 2. Redistributions in binary form must reproduce the above copyright
         *   notice, this list of conditions and the following disclaimer in the
         *   documentation and/or other materials provided with the distribution.
```

```
          * 3. Neither the name of the University nor the names of its contributors
          *    may be used to endorse or promote products derived from this software
          *     without specific prior written permission.
          *
          * THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS''
AND
          * ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
          * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE
          * ARE DISCLAIMED.  IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE
          *  FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
CONSEQUENTIAL
          * DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
          * OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
          * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
STRICT
          * LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY
WAY
          * OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY
OF
          * SUCH DAMAGE.

       Some code is licensed under an ISC-style license, to the following
       copyright holders:

         Internet Software Consortium.
         Todd C. Miller
         Reyk Floeter
         Chad Mynhier

         * Permission to use, copy, modify, and distribute this software for any
         * purpose with or without fee is hereby granted, provided that the above
         * copyright notice and this permission notice appear in all copies.
         *
         * THE SOFTWARE IS PROVIDED "AS IS" AND TODD C. MILLER DISCLAIMS ALL
         *  WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED
WARRANTIES
         * OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL TODD C. MILLER BE
LIABLE
         * FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY
DAMAGES
         * WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN
ACTION
         * OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR
IN
         * CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

       Some code is licensed under a MIT-style license to the following
       copyright holders:

         Free Software Foundation, Inc.

         * Permission is hereby granted, free of charge, to any person obtaining
a  *
         * copy of this software and associated documentation files (the        *
         * "Software"), to deal in the Software without restriction, including
*
         * without limitation the rights to use, copy, modify, merge, publish,
*
         * distribute, distribute with modifications, sublicense, and/or sell
*
         * copies of the Software, and to permit persons to whom the Software is
*
         * furnished to do so, subject to the following conditions:            *
         *                                                                     *
         * The above copyright notice and this permission notice shall be included
*
         * in all copies or substantial portions of the Software.              *
         *                                                                     *
```

```
         * THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS
*
         * OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF           *
         * MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT.
*
         * IN NO EVENT SHALL THE ABOVE COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM,
*
         * DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR
*
         * OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR
*
         * THE USE OR OTHER DEALINGS IN THE SOFTWARE.                           *
         *                                                                      *
         * Except as contained in this notice, the name(s) of the above copyright
*
         * holders shall not be used in advertising or otherwise to promote the
*
         * sale, use or other dealings in this Software without prior written    *
         * authorization.                                                       *

************************************************************************/

------------------------------------------------------------------------------
---
[openssl 1.0.2n]
  LICENSE ISSUES
  ==============

  The OpenSSL toolkit stays under a double license, i.e. both the conditions of
  the OpenSSL License and the original SSLeay license apply to the toolkit.
  See below for the actual license texts. Actually both licenses are BSD-style
  Open Source licenses. In case of any license issues related to OpenSSL
  please contact openssl-core@openssl.org.

  OpenSSL License
  ---------------

/* ====================================================================
 * Copyright (c) 1998-2017 The OpenSSL Project.  All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 *
 * 1. Redistributions of source code must retain the above copyright
 *    notice, this list of conditions and the following disclaimer.
 *
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in
 *    the documentation and/or other materials provided with the
 *    distribution.
 *
 * 3. All advertising materials mentioning features or use of this
 *    software must display the following acknowledgment:
 *    "This product includes software developed by the OpenSSL Project
 *    for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
 *
 * 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
 *    endorse or promote products derived from this software without
 *    prior written permission. For written permission, please contact
 *    openssl-core@openssl.org.
 *
 * 5. Products derived from this software may not be called "OpenSSL"
 *    nor may "OpenSSL" appear in their names without prior written
 *    permission of the OpenSSL Project.
 *
 * 6. Redistributions of any form whatsoever must retain the following
 *    acknowledgment:
 *    "This product includes software developed by the OpenSSL Project
 *    for use in the OpenSSL Toolkit (http://www.openssl.org/)"
```

```
 *
 * THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
 * EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
 * PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE OpenSSL PROJECT OR
 * ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
 * SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
 * NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
 * LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
 * STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
 * ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
 * OF THE POSSIBILITY OF SUCH DAMAGE.
 * ====================================================================
 *
 * This product includes cryptographic software written by Eric Young
 * (eay@cryptsoft.com).  This product includes software written by Tim
 * Hudson (tjh@cryptsoft.com).
 *
 */

 Original SSLeay License
 -----------------------

/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
 * All rights reserved.
 *
 * This package is an SSL implementation written
 * by Eric Young (eay@cryptsoft.com).
 * The implementation was written so as to conform with Netscapes SSL.
 *
 * This library is free for commercial and non-commercial use as long as
 * the following conditions are aheared to.  The following conditions
 * apply to all code found in this distribution, be it the RC4, RSA,
 * lhash, DES, etc., code; not just the SSL code.  The SSL documentation
 * included with this distribution is covered by the same copyright terms
 * except that the holder is Tim Hudson (tjh@cryptsoft.com).
 *
 * Copyright remains Eric Young's, and as such any Copyright notices in
 * the code are not to be removed.
 * If this package is used in a product, Eric Young should be given attribution
 * as the author of the parts of the library used.
 * This can be in the form of a textual message at program startup or
 * in documentation (online or textual) provided with the package.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 * 1. Redistributions of source code must retain the copyright
 *    notice, this list of conditions and the following disclaimer.
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in the
 *    documentation and/or other materials provided with the distribution.
 * 3. All advertising materials mentioning features or use of this software
 *    must display the following acknowledgement:
 *    "This product includes cryptographic software written by
 *     Eric Young (eay@cryptsoft.com)"
 *    The word 'cryptographic' can be left out if the rouines from the library
 *    being used are not cryptographic related :-).
 * 4. If you include any Windows specific code (or a derivative thereof) from
 *   the apps directory (application code) you must include an acknowledgement:
 *   "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"
 *
 * THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND
 * ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
 * ARE DISCLAIMED.  IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
 * FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
 * DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
 * OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
```

```
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
 * LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
 * OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
 * SUCH DAMAGE.
 *
 * The licence and distribution terms for any publically available version or
 * derivative of this code cannot be changed.  i.e. this code cannot simply be
 * copied and put under another distribution licence
 * [including the GNU Public Licence.]
 */

------------------------------------------------------------------------------
---
[ovsdb 2.1.0 (part of openvswitch 2.1.0)]
[COPYRIGHT]
  Copyright (c) 2009, 2010, 2011, 2012, 2013 Nicira, Inc.

[LICENSE]
                                 Apache License
                           Version 2.0, January 2004
                        http://www.apache.org/licenses/

   TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

   1. Definitions.

      "License" shall mean the terms and conditions for use, reproduction,
      and distribution as defined by Sections 1 through 9 of this document.

      "Licensor" shall mean the copyright owner or entity authorized by
      the copyright owner that is granting the License.

      "Legal Entity" shall mean the union of the acting entity and all
      other entities that control, are controlled by, or are under common
      control with that entity. For the purposes of this definition,
      "control" means (i) the power, direct or indirect, to cause the
      direction or management of such entity, whether by contract or
      otherwise, or (ii) ownership of fifty percent (50%) or more of the
      outstanding shares, or (iii) beneficial ownership of such entity.

      "You" (or "Your") shall mean an individual or Legal Entity
      exercising permissions granted by this License.

      "Source" form shall mean the preferred form for making modifications,
      including but not limited to software source code, documentation
      source, and configuration files.

      "Object" form shall mean any form resulting from mechanical
      transformation or translation of a Source form, including but
      not limited to compiled object code, generated documentation,
      and conversions to other media types.

      "Work" shall mean the work of authorship, whether in Source or
      Object form, made available under the License, as indicated by a
      copyright notice that is included in or attached to the work
      (an example is provided in the Appendix below).

      "Derivative Works" shall mean any work, whether in Source or Object
      form, that is based on (or derived from) the Work and for which the
      editorial revisions, annotations, elaborations, or other modifications
      represent, as a whole, an original work of authorship. For the purposes
      of this License, Derivative Works shall not include works that remain
      separable from, or merely link (or bind by name) to the interfaces of,
      the Work and Derivative Works thereof.

      "Contribution" shall mean any work of authorship, including
      the original version of the Work and any modifications or additions
      to that Work or Derivative Works thereof, that is intentionally
      submitted to Licensor for inclusion in the Work by the copyright owner
      or by an individual or Legal Entity authorized to submit on behalf of
```

the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

   (a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

   (b) You must cause any modified files to carry prominent notices stating that You changed the files; and

   (c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

   (d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and
may provide additional or different license terms and conditions
for use, reproduction, or distribution of Your modifications, or
for any such Derivative Works as a whole, provided Your use,
reproduction, and distribution of the Work otherwise complies with
the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise,
any Contribution intentionally submitted for inclusion in the Work
by You to the Licensor shall be under the terms and conditions of
this License, without any additional terms or conditions.
Notwithstanding the above, nothing herein shall supersede or modify
the terms of any separate license agreement you may have executed
with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade
names, trademarks, service marks, or product names of the Licensor,
except as required for reasonable and customary use in describing the
origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or
agreed to in writing, Licensor provides the Work (and each
Contributor provides its Contributions) on an "AS IS" BASIS,
WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or
implied, including, without limitation, any warranties or conditions
of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A
PARTICULAR PURPOSE. You are solely responsible for determining the
appropriateness of using or redistributing the Work and assume any
risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory,
whether in tort (including negligence), contract, or otherwise,
unless required by applicable law (such as deliberate and grossly
negligent acts) or agreed to in writing, shall any Contributor be
liable to You for damages, including any direct, indirect, special,
incidental, or consequential damages of any character arising as a
result of this License or out of the use or inability to use the
Work (including but not limited to damages for loss of goodwill,
work stoppage, computer failure or malfunction, or any and all
other commercial damages or losses), even if such Contributor
has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing
the Work or Derivative Works thereof, You may choose to offer,
and charge a fee for, acceptance of support, warranty, indemnity,
or other liability obligations and/or rights consistent with this
License. However, in accepting such obligations, You may act only
on Your own behalf and on Your sole responsibility, not on behalf
of any other Contributor, and only if You agree to indemnify,
defend, and hold each Contributor harmless for any liability
incurred by, or claims asserted against, such Contributor by reason
of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

[ping 8.0.0 (part of FreeBSD 8.0.0)]
[COPYRIGHT]
Copyright (c) 1992-2009 The FreeBSD Project. All rights reserved.

[LICENSE]
Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:
1. Redistributions of source code must retain the above copyright
notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright
notice, this list of conditions and the following disclaimer in the
documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS ``AS IS'' AND
ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
SUCH DAMAGE.

The 4.4BSD and 4.4BSD-Lite software is distributed under the following
terms:

All of the documentation and software included in the 4.4BSD and 4.4BSD-Lite
Releases is copyrighted by The Regents of the University of California.

Copyright 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:
1. Redistributions of source code must retain the above copyright
   notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright
   notice, this list of conditions and the following disclaimer in the
   documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software
   must display the following acknowledgement:
This product includes software developed by the University of
California, Berkeley and its contributors.
4. Neither the name of the University nor the names of its contributors
   may be used to endorse or promote products derived from this software
   without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND
ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE
FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
SUCH DAMAGE.

The Institute of Electrical and Electronics Engineers and the American
National Standards Committee X3, on Information Processing Systems have
given us permission to reprint portions of their documentation.

In the following statement, the phrase ``this text'' refers to portions
of the system documentation.

Portions of this text are reprinted and reproduced in electronic form in
the second BSD Networking Software Release, from IEEE Std 1003.1-1988, IEEE
Standard Portable Operating System Interface for Computer Environments
(POSIX), copyright C 1988 by the Institute of Electrical and Electronics
Engineers, Inc. In the event of any discrepancy between these versions
and the original IEEE Standard, the original IEEE Standard is the referee
document.

In the following statement, the phrase ``This material'' refers to portions
of the system documentation.

This material is reproduced with permission from American National
Standards Committee X3, on Information Processing Systems. Computer and
Business Equipment Manufacturers Association (CBEMA), 311 First St., NW,

Suite 500, Washington, DC 20001-2178. The developmental work of
Programming Language C was completed by the X3J11 Technical Committee.

The views and conclusions contained in the software and documentation are
those of the authors and should not be interpreted as representing official
policies, either expressed or implied, of the Regents of the University
of California.

NOTE: The copyright of UC Berkeley's Berkeley Software Distribution ("BSD")
source has been updated. The copyright addendum may be found at
ftp://ftp.cs.berkeley.edu/pub/4bsd/README.Impt.License.Change and is
included below.

July 22, 1999

To All Licensees, Distributors of Any Version of BSD:

As you know, certain of the Berkeley Software Distribution ("BSD") source
code files require that further distributions of products containing all or
portions of the software, acknowledge within their advertising materials
that such products contain software developed by UC Berkeley and its
contributors.

Specifically, the provision reads:

" * 3. All advertising materials mentioning features or use of this software
 * must display the following acknowledgement:
 * This product includes software developed by the University of
 * California, Berkeley and its contributors."

Effective immediately, licensees and distributors are no longer required to
include the acknowledgement within advertising materials. Accordingly, the
foregoing paragraph of those BSD Unix files containing it is hereby deleted
in its entirety.

William Hoskins
Director, Office of Technology Licensing
University of California, Berkeley

[ping6 8.0.0 (part of FreeBSD 8.0.0)]
[COPYRIGHT]
Copyright (c) 1992-2009 The FreeBSD Project. All rights reserved.

[LICENSE]
Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:
1. Redistributions of source code must retain the above copyright
notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright
notice, this list of conditions and the following disclaimer in the
documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS ``AS IS'' AND
ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
SUCH DAMAGE.

The 4.4BSD and 4.4BSD-Lite software is distributed under the following
terms:

All of the documentation and software included in the 4.4BSD and 4.4BSD-Lite Releases is copyrighted by The Regents of the University of California.

Copyright 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:
This product includes software developed by the University of California, Berkeley and its contributors.
4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The Institute of Electrical and Electronics Engineers and the American National Standards Committee X3, on Information Processing Systems have given us permission to reprint portions of their documentation.

In the following statement, the phrase ``this text'' refers to portions of the system documentation.

Portions of this text are reprinted and reproduced in electronic form in the second BSD Networking Software Release, from IEEE Std 1003.1-1988, IEEE Standard Portable Operating System Interface for Computer Environments (POSIX), copyright C 1988 by the Institute of Electrical and Electronics Engineers, Inc. In the event of any discrepancy between these versions and the original IEEE Standard, the original IEEE Standard is the referee document.

In the following statement, the phrase ``This material'' refers to portions of the system documentation.

This material is reproduced with permission from American National Standards Committee X3, on Information Processing Systems. Computer and Business Equipment Manufacturers Association (CBEMA), 311 First St., NW, Suite 500, Washington, DC 20001-2178. The developmental work of Programming Language C was completed by the X3J11 Technical Committee.

The views and conclusions contained in the software and documentation are those of the authors and should not be interpreted as representing official policies, either expressed or implied, of the Regents of the University of California.

NOTE: The copyright of UC Berkeley's Berkeley Software Distribution ("BSD") source has been updated. The copyright addendum may be found at ftp://ftp.cs.berkeley.edu/pub/4bsd/README.Impt.License.Change and is included below.

July 22, 1999

To All Licensees, Distributors of Any Version of BSD:

As you know, certain of the Berkeley Software Distribution ("BSD") source code files require that further distributions of products containing all or portions of the software, acknowledge within their advertising materials that such products contain software developed by UC Berkeley and its contributors.

Specifically, the provision reads:

```
"    * 3. All advertising materials mentioning features or use of this software
      *    must display the following acknowledgement:
      *    This product includes software developed by the University of
      *    California, Berkeley and its contributors."
```

Effective immediately, licensees and distributors are no longer required to include the acknowledgement within advertising materials. Accordingly, the foregoing paragraph of those BSD Unix files containing it is hereby deleted in its entirety.

William Hoskins
Director, Office of Technology Licensing
University of California, Berkeley

[pthread 0.9.32 (part of uclibc 0.9.32)]
[LICENSE]

GNU LESSER GENERAL PUBLIC LICENSE
Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.
51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts
as the successor of the GNU Library Public License, version 2, hence
the version number 2.1.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source

code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The

former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or

table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the

library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF

SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the library's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA

Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the library, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the library `Frob' (a library for tweaking knobs) written by James Random Hacker.

<signature of Ty Coon>, 1 April 1990
Ty Coon, President of Vice

That's all there is to it!

[pure-ftpd 1.0.29]
[COPYRIGHT]
Copyright (c) 2001 - 2010
Frank Denis <j at pureftpd dot org> with help of contributors.

[LICENSE]
Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND THE AUTHOR DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

```
--------------------------------------------------------------------------
---
[python 2.7.18]
[COPYRIGHT]
  Copyright (c) 2001, 2002, 2003, 2004, 2005, 2006, 2007, 2008, 2009, 2010, 2011,
  2012, 2013, 2014, 2015, 2016, 2017, 2018, 2019, 2020 Python Software Foundation.
All
  rights reserved.

  Copyright (c) 2000 BeOpen.com.
  All rights reserved.

  Copyright (c) 1995-2001 Corporation for National Research Initiatives.
  All rights reserved.

  Copyright (c) 1991-1995 Stichting Mathematisch Centrum.
  All rights reserved.

[LICENSE]
PYTHON SOFTWARE FOUNDATION LICENSE VERSION 2
--------------------------------------------

1. This LICENSE AGREEMENT is between the Python Software Foundation
("PSF"), and the Individual or Organization ("Licensee") accessing and
otherwise using this software ("Python") in source or binary form and
its associated documentation.

2. Subject to the terms and conditions of this License Agreement, PSF hereby
grants Licensee a nonexclusive, royalty-free, world-wide license to reproduce,
analyze, test, perform and/or display publicly, prepare derivative works,
distribute, and otherwise use Python alone or in any derivative version,
provided, however, that PSF's License Agreement and PSF's notice of copyright,
i.e., "Copyright (c) 2001, 2002, 2003, 2004, 2005, 2006, 2007, 2008, 2009, 2010,
2011, 2012, 2013, 2014, 2015, 2016, 2017, 2018, 2019, 2020 Python Software
Foundation;
All Rights Reserved" are retained in Python alone or in any derivative version
prepared by Licensee.

3. In the event Licensee prepares a derivative work that is based on
or incorporates Python or any part thereof, and wants to make
the derivative work available to others as provided herein, then
Licensee hereby agrees to include in any such work a brief summary of
the changes made to Python.

4. PSF is making Python available to Licensee on an "AS IS"
basis.  PSF MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR
IMPLIED.  BY WAY OF EXAMPLE, BUT NOT LIMITATION, PSF MAKES NO AND
DISCLAIMS ANY REPRESENTATION OR WARRANTY OF MERCHANTABILITY OR FITNESS
FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF PYTHON WILL NOT
INFRINGE ANY THIRD PARTY RIGHTS.

5. PSF SHALL NOT BE LIABLE TO LICENSEE OR ANY OTHER USERS OF PYTHON
FOR ANY INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES OR LOSS AS
A RESULT OF MODIFYING, DISTRIBUTING, OR OTHERWISE USING PYTHON,
OR ANY DERIVATIVE THEREOF, EVEN IF ADVISED OF THE POSSIBILITY THEREOF.

6. This License Agreement will automatically terminate upon a material
breach of its terms and conditions.

7. Nothing in this License Agreement shall be deemed to create any
relationship of agency, partnership, or joint venture between PSF and
Licensee.  This License Agreement does not grant permission to use PSF
trademarks or trade name in a trademark sense to endorse or promote
products or services of Licensee, or any third party.

8. By copying, installing or otherwise using Python, Licensee
agrees to be bound by the terms and conditions of this License
Agreement.
```

BEOPEN.COM LICENSE AGREEMENT FOR PYTHON 2.0

BEOPEN PYTHON OPEN SOURCE LICENSE AGREEMENT VERSION 1

1. This LICENSE AGREEMENT is between BeOpen.com ("BeOpen"), having an office at 160 Saratoga Avenue, Santa Clara, CA 95051, and the Individual or Organization ("Licensee") accessing and otherwise using this software in source or binary form and its associated documentation ("the Software").

2. Subject to the terms and conditions of this BeOpen Python License Agreement, BeOpen hereby grants Licensee a non-exclusive, royalty-free, world-wide license to reproduce, analyze, test, perform and/or display publicly, prepare derivative works, distribute, and otherwise use the Software alone or in any derivative version, provided, however, that the BeOpen Python License is retained in the Software, alone or in any derivative version prepared by Licensee.

3. BeOpen is making the Software available to Licensee on an "AS IS" basis. BEOPEN MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED. BY WAY OF EXAMPLE, BUT NOT LIMITATION, BEOPEN MAKES NO AND DISCLAIMS ANY REPRESENTATION OR WARRANTY OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF THE SOFTWARE WILL NOT INFRINGE ANY THIRD PARTY RIGHTS.

4. BEOPEN SHALL NOT BE LIABLE TO LICENSEE OR ANY OTHER USERS OF THE SOFTWARE FOR ANY INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES OR LOSS AS A RESULT OF USING, MODIFYING OR DISTRIBUTING THE SOFTWARE, OR ANY DERIVATIVE THEREOF, EVEN IF ADVISED OF THE POSSIBILITY THEREOF.

5. This License Agreement will automatically terminate upon a material breach of its terms and conditions.

6. This License Agreement shall be governed by and interpreted in all respects by the law of the State of California, excluding conflict of law provisions. Nothing in this License Agreement shall be deemed to create any relationship of agency, partnership, or joint venture between BeOpen and Licensee. This License Agreement does not grant permission to use BeOpen trademarks or trade names in a trademark sense to endorse or promote products or services of Licensee, or any third party. As an exception, the "BeOpen Python" logos available at http://www.pythonlabs.com/logos.html may be used according to the permissions granted on that web page.

7. By copying, installing or otherwise using the software, Licensee agrees to be bound by the terms and conditions of this License Agreement.

CNRI LICENSE AGREEMENT FOR PYTHON 1.6.1
---

1. This LICENSE AGREEMENT is between the Corporation for National Research Initiatives, having an office at 1895 Preston White Drive, Reston, VA 20191 ("CNRI"), and the Individual or Organization ("Licensee") accessing and otherwise using Python 1.6.1 software in source or binary form and its associated documentation.

2. Subject to the terms and conditions of this License Agreement, CNRI hereby grants Licensee a nonexclusive, royalty-free, world-wide license to reproduce, analyze, test, perform and/or display publicly, prepare derivative works, distribute, and otherwise use Python 1.6.1 alone or in any derivative version, provided, however, that CNRI's License Agreement and CNRI's notice of copyright, i.e., "Copyright (c) 1995-2001 Corporation for National Research Initiatives; All Rights Reserved" are retained in Python 1.6.1 alone or in any derivative version prepared by Licensee. Alternately, in lieu of CNRI's License Agreement, Licensee may substitute the following text (omitting the

quotes): "Python 1.6.1 is made available subject to the terms and conditions in CNRI's License Agreement. This Agreement together with Python 1.6.1 may be located on the Internet using the following unique, persistent identifier (known as a handle): 1895.22/1013. This Agreement may also be obtained from a proxy server on the Internet using the following URL: http://hdl.handle.net/1895.22/1013".

3. In the event Licensee prepares a derivative work that is based on or incorporates Python 1.6.1 or any part thereof, and wants to make the derivative work available to others as provided herein, then Licensee hereby agrees to include in any such work a brief summary of the changes made to Python 1.6.1.

4. CNRI is making Python 1.6.1 available to Licensee on an "AS IS" basis. CNRI MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED. BY WAY OF EXAMPLE, BUT NOT LIMITATION, CNRI MAKES NO AND DISCLAIMS ANY REPRESENTATION OR WARRANTY OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF PYTHON 1.6.1 WILL NOT INFRINGE ANY THIRD PARTY RIGHTS.

5. CNRI SHALL NOT BE LIABLE TO LICENSEE OR ANY OTHER USERS OF PYTHON 1.6.1 FOR ANY INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES OR LOSS AS A RESULT OF MODIFYING, DISTRIBUTING, OR OTHERWISE USING PYTHON 1.6.1, OR ANY DERIVATIVE THEREOF, EVEN IF ADVISED OF THE POSSIBILITY THEREOF.

6. This License Agreement will automatically terminate upon a material breach of its terms and conditions.

7. This License Agreement shall be governed by the federal intellectual property law of the United States, including without limitation the federal copyright law, and, to the extent such U.S. federal law does not apply, by the law of the Commonwealth of Virginia, excluding Virginia's conflict of law provisions. Notwithstanding the foregoing, with regard to derivative works based on Python 1.6.1 that incorporate non-separable material that was previously distributed under the GNU General Public License (GPL), the law of the Commonwealth of Virginia shall govern this License Agreement only as to issues arising under or with respect to Paragraphs 4, 5, and 7 of this License Agreement. Nothing in this License Agreement shall be deemed to create any relationship of agency, partnership, or joint venture between CNRI and Licensee. This License Agreement does not grant permission to use CNRI trademarks or trade name in a trademark sense to endorse or promote products or services of Licensee, or any third party.

8. By clicking on the "ACCEPT" button where indicated, or by copying, installing or otherwise using Python 1.6.1, Licensee agrees to be bound by the terms and conditions of this License Agreement.

ACCEPT

CWI LICENSE AGREEMENT FOR PYTHON 0.9.0 THROUGH 1.2

Copyright (c) 1991 - 1995, Stichting Mathematisch Centrum Amsterdam, The Netherlands. All rights reserved.

Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of Stichting Mathematisch Centrum or CWI not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission.

STICHTING MATHEMATISCH CENTRUM DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL STICHTING MATHEMATISCH CENTRUM BE LIABLE

FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES
WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN
ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT
OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

[respond 1.3.1]
[COPYRIGHT]
copyright (c) 2012: Scott Jehl, Paul Irish, Nicholas Zakas.

[LICENSE]
Dual MIT/BSD license

[result.h 1.73]
[COPYRIGHT]
Copyright (C) 2004-2009, 2012, 2014 Internet Systems Consortium, Inc. ("ISC")
Copyright (C) 1998-2001, 2003 Internet Software Consortium.

[LICENSE]
Permission to use, copy, modify, and/or distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ISC DISCLAIMS ALL WARRANTIES WITH
REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS. IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT,
INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
PERFORMANCE OF THIS SOFTWARE.

[rpcapd 4.1.2 (part of winpcap 4.1.2)]
[COPYRIGHT]
Copyright (c) 1999 - 2005 NetGroup, Politecnico di Torino (Italy).
Copyright (c) 2005 - 2010 CACE Technologies, Davis (California).
All rights reserved.

[LICENSE]
Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:

1. Redistributions of source code must retain the above copyright
   notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright
   notice, this list of conditions and the following disclaimer in the
   documentation and/or other materials provided with the distribution.
3. Neither the name of the Politecnico di Torino, CACE Technologies nor
   the names of its contributors may be used to endorse or promote products
   derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS"
AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE
FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
SUCH DAMAGE.

This product includes software developed by the University of California,
Lawrence Berkeley Laboratory and its contributors.

[COPYRIGHT]
Portions Copyright (c) 1990, 1991, 1992, 1993, 1994, 1995, 1996, 1997
The Regents of the University of California. All rights reserved.

[LICENSE]
Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:
1. Redistributions of source code must retain the above copyright
   notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright
   notice, this list of conditions and the following disclaimer in the
   documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software
   must display the following acknowledgement: "This product includes software
   developed by the University of California, Berkeley and its contributors."
4. Neither the name of the University nor the names of its contributors
   may be used to endorse or promote products derived from this software without
   specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE INSTITUTE AND CONTRIBUTORS ``AS IS'' AND
ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE
FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
SUCH DAMAGE.

[COPYRIGHT]
Portions Copyright (c) 1983 Regents of the University of California.
All rights reserved.

[LICENSE]
Redistribution and use in source and binary forms are permitted provided that
the above copyright notice and this paragraph are duplicated in all such forms
and that any documentation, advertising materials, and other materials related
to such distribution and use acknowledge that the software was developed by the
University of California, Berkeley. The name of the University may not be used
to endorse or promote products derived from this software without specific prior
written permission.

THIS SOFTWARE IS PROVIDED ``AS IS'' AND WITHOUT ANY EXPRESS OR IMPLIED
WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF
MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE.

[ruby 2.0.0]
[COPYRIGHT]
  Copyright (C) 1993-2013 Yukihiro Matsumoto. All rights reserved.

[LICENSE]
Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:
1. Redistributions of source code must retain the above copyright
notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright
notice, this list of conditions and the following disclaimer in the
documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS ``AS IS'' AND
ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE

```
FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
SUCH DAMAGE.
--------------------------------------------------------------------------
---
[slickgrid 2.1]
[COPYRIGHT]
  Copyright (c) 2010 Michael Leibman, http://github.com/mleibman/slickgrid

[LICENSE]
Permission is hereby granted, free of charge, to any person obtaining
a copy of this software and associated documentation files (the
"Software"), to deal in the Software without restriction, including
without limitation the rights to use, copy, modify, merge, publish,
distribute, sublicense, and/or sell copies of the Software, and to
permit persons to whom the Software is furnished to do so, subject to
the following conditions:

The above copyright notice and this permission notice shall be
included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND,
EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF
MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND
NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE
LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION
OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION
WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.
--------------------------------------------------------------------------
---
[sqlite3 3.35.5]
** 2006 June 7
**
** The author disclaims copyright to this source code.  In place of
** a legal notice, here is a blessing:
**
**    May you do good and not evil.
**    May you find forgiveness for yourself and forgive others.
**    May you share freely, never taking more than you give.
**
*************************************************************************
-------------------------------------------------------------------------------
---
[tcl-snmptools 1.0]
[COPYRIGHT]
  Copyright (C) 2008  Alexandros Stergiakis

[LICENSE]
                    GNU GENERAL PUBLIC LICENSE
                       Version 3, 29 June 2007

 Copyright (C) 2007 Free Software Foundation, Inc. <http://fsf.org/>
 Everyone is permitted to copy and distribute verbatim copies
 of this license document, but changing it is not allowed.

                            Preamble

  The GNU General Public License is a free, copyleft license for
software and other kinds of works.

  The licenses for most software and other practical works are designed
to take away your freedom to share and change the works.  By contrast,
the GNU General Public License is intended to guarantee your freedom to
share and change all versions of a program--to make sure it remains free
software for all its users.  We, the Free Software Foundation, use the
GNU General Public License for most of our software; it applies also to
```

any other work released this way by its authors. You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for them if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you these rights or asking you to surrender the rights. Therefore, you have certain responsibilities if you distribute copies of the software, or if you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must pass on to the recipients the same freedoms that you received. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

Developers that use the GNU GPL protect your rights with two steps: (1) assert copyright on the software, and (2) offer you this License giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains that there is no warranty for this free software. For both users' and authors' sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.

Some devices are designed to deny users access to install or run modified versions of the software inside them, although the manufacturer can do so. This is fundamentally incompatible with the aim of protecting users' freedom to change the software. The systematic pattern of such abuse occurs in the area of products for individuals to use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains, we stand ready to extend this provision to those domains in future versions of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents. States should not allow patents to restrict development and use of software on general-purpose computers, but in those that do, we wish to avoid the special danger that patents applied to a free program could make it effectively proprietary. To prevent this, the GPL assures that patents cannot be used to render the program non-free.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS

0. Definitions.

"This License" refers to version 3 of the GNU General Public License.

"Copyright" also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

"The Program" refers to any copyrightable work licensed under this License. Each licensee is addressed as "you". "Licensees" and "recipients" may be individuals or organizations.

To "modify" a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a "modified version" of the earlier work or a work "based on" the earlier work.

A "covered work" means either the unmodified Program or a work based on the Program.

To "propagate" a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well.

To "convey" a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays "Appropriate Legal Notices" to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

1. Source Code.

The "source code" for a work means the preferred form of the work for making modifications to it. "Object code" means any non-source form of a work.

A "Standard Interface" means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The "System Libraries" of an executable work include anything, other than the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A "Major Component", in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The "Corresponding Source" for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work's System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

2. Basic Permissions.

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited

permission to run the unmodified Program. The output from running a covered work is covered by this License only if the output, given its content, constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed; section 10 makes it unnecessary.

3. Protecting Users' Legal Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of technological measures.

4. Conveying Verbatim Copies.

You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice; keep intact all notices stating that this License and any non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

5. Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

a) The work must carry prominent notices stating that you modified it, and giving a relevant date.

b) The work must carry prominent notices stating that it is released under this License and any conditions added under section 7. This requirement modifies the requirement in section 4 to "keep intact all notices".

c) You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it.

d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.

A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution medium, is called an "aggregate" if the compilation and its resulting copyright are not used to limit the access or legal rights of the compilation's users beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate.

6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, in one of these ways:

a) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange.

b) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as long as you offer spare parts or customer support for that product model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical medium customarily used for software interchange, for a price no more than your reasonable cost of physically performing this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge.

c) Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source. This alternative is allowed only occasionally and noncommercially, and only if you received the object code with such an offer, in accord with subsection 6b.

d) Convey the object code by offering access from a designated place (gratis or for a charge), and offer equivalent access to the Corresponding Source in the same way through the same place at no further charge. You need not require recipients to copy the Corresponding Source along with the object code. If the place to copy the object code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.

e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.

A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object code work.

A "User Product" is either (1) a "consumer product", which means any tangible personal property which is normally used for personal, family,

or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, "normally used" refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

"Installation Information" for a User Product means any methods, procedures, authorization keys, or other information required to install and execute modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in ROM).

The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

7. Additional Terms.

"Additional permissions" are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

a) Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or

b) Requiring preservation of specified reasonable legal notices or

author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or

c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or

d) Limiting the use for publicity purposes of names of licensors or authors of the material; or

e) Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or

f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on those licensors and authors.

All other non-permissive additional terms are considered "further restrictions" within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions; the above requirements apply either way.

8. Termination.

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work

occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

10. Automatic Licensing of Downstream Recipients.

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An "entity transaction" is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

11. Patents.

A "contributor" is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's "contributor version".

A contributor's "essential patent claims" are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For purposes of this definition, "control" includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a "patent license" is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To "grant" such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. "Knowingly relying" means you have actual knowledge that, but for the patent license, your conveying the

covered work in a country, or your recipient's use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is "discriminatory" if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement, or that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.

12. No Surrender of Others' Freedom.

If conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot convey a covered work so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

13. Use with the GNU Affero General Public License.

Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed under version 3 of the GNU Affero General Public License into a single combined work, and to convey the resulting work. The terms of this License will continue to apply to the part which is the covered work, but the special requirements of the GNU Affero General Public License, section 13, concerning interaction through a network will apply to the combination as such.

14. Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of the GNU General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU General Public License, you may choose any version ever published by the Free Software Foundation.

If the Program specifies that a proxy can decide which future versions of the GNU General Public License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Program.

Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.

15. Disclaimer of Warranty.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

17. Interpretation of Sections 15 and 16.

If the disclaimer of warranty and limitation of liability provided above cannot be given local legal effect according to their terms, reviewing courts shall apply local law that most closely approximates an absolute waiver of all civil liability in connection with the Program, unless a warranty or assumption of liability accompanies a copy of the Program in return for a fee.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively state the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This program is free software: you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation, either version 3 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program. If not, see <http://www.gnu.org/licenses/>.

```
Also add information on how to contact you by electronic and paper mail.

  If the program does terminal interaction, make it output a short
notice like this when it starts in an interactive mode:

    <program>  Copyright (C) <year>  <name of author>
    This program comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
    This is free software, and you are welcome to redistribute it
    under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate
parts of the General Public License.  Of course, your program's commands
might be different; for a GUI interface, you would use an "about box".

  You should also get your employer (if you work as a programmer) or school,
if any, to sign a "copyright disclaimer" for the program, if necessary.
For more information on this, and how to apply and follow the GNU GPL, see
<http://www.gnu.org/licenses/>.

  The GNU General Public License does not permit incorporating your program
into proprietary programs.  If your program is a subroutine library, you
may consider it more useful to permit linking proprietary applications with
the library.  If this is what you want to do, use the GNU Lesser General
Public License instead of this License.  But first, please read
<http://www.gnu.org/philosophy/why-not-lgpl.html>.

--------------------------------------------------------------------------------
---
[tcltk 8.5.8]
[COPYRIGHT]
  Copyright (c) 1987-1994 The Regents of the University of California.
  Copyright (c) 1993-1996 Lucent Technologies.
  Copyright (c) 1994-1998 Sun Microsystems, Inc.
  Copyright (c) 1998-2000 by Scriptics Corporation.
  Copyright (c) 2002 by Kevin B. Kenny.  All rights reserved.

[LICENSE]
This software is copyrighted by the Regents of the University of
California, Sun Microsystems, Inc., Scriptics Corporation, ActiveState
Corporation and other parties.  The following terms apply to all files
associated with the software unless explicitly disclaimed in
individual files.

The authors hereby grant permission to use, copy, modify, distribute,
and license this software and its documentation for any purpose, provided
that existing copyright notices are retained in all copies and that this
notice is included verbatim in any distributions. No written agreement,
license, or royalty fee is required for any of the authorized uses.
Modifications to this software may be copyrighted by their authors
and need not follow the licensing terms described here, provided that
the new terms are clearly indicated on the first page of each file where
they apply.

IN NO EVENT SHALL THE AUTHORS OR DISTRIBUTORS BE LIABLE TO ANY PARTY
FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES
ARISING OUT OF THE USE OF THIS SOFTWARE, ITS DOCUMENTATION, OR ANY
DERIVATIVES THEREOF, EVEN IF THE AUTHORS HAVE BEEN ADVISED OF THE
POSSIBILITY OF SUCH DAMAGE.

THE AUTHORS AND DISTRIBUTORS SPECIFICALLY DISCLAIM ANY WARRANTIES,
INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY,
FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT.  THIS SOFTWARE
IS PROVIDED ON AN "AS IS" BASIS, AND THE AUTHORS AND DISTRIBUTORS HAVE
NO OBLIGATION TO PROVIDE MAINTENANCE, SUPPORT, UPDATES, ENHANCEMENTS, OR
MODIFICATIONS.

GOVERNMENT USE: If you are acquiring this software on behalf of the
U.S. government, the Government shall have only "Restricted Rights"
in the software and related documentation as defined in the Federal
```

Acquisition Regulations (FARs) in Clause 52.227.19 (c) (2). If you
are acquiring the software on behalf of the Department of Defense, the
software shall be classified as "Commercial Computer Software" and the
Government shall have only "Restricted Rights" as defined in Clause
252.227-7013 (c) (1) of DFARs. Notwithstanding the foregoing, the
authors grant the U.S. Government and others acting in its behalf
permission to use and distribute the software in accordance with the
terms specified in this license.

[telnet 7.2.0 (part of FreeBSD 7.2.0)]
[COPYRIGHT]
Copyright (c) 1992-2009 The FreeBSD Project. All rights reserved.

[LICENSE]
Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:
1. Redistributions of source code must retain the above copyright
notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright
notice, this list of conditions and the following disclaimer in the
documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY AUTHOR AND CONTRIBUTORS ``AS IS'' AND
ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
ARE DISCLAIMED. IN NO EVENT SHALL AUTHOR OR CONTRIBUTORS BE LIABLE
FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
SUCH DAMAGE.

The 4.4BSD and 4.4BSD-Lite software is distributed under the following
terms:

All of the documentation and software included in the 4.4BSD and 4.4BSD-Lite
Releases is copyrighted by The Regents of the University of California.

Copyright 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:
1. Redistributions of source code must retain the above copyright
notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright
notice, this list of conditions and the following disclaimer in the
documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software
must display the following acknowledgement:
This product includes software developed by the University of
California, Berkeley and its contributors.
4. Neither the name of the University nor the names of its contributors
may be used to endorse or promote products derived from this software
without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND
ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE
FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY

OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
SUCH DAMAGE.

The Institute of Electrical and Electronics Engineers and the American
National Standards Committee X3, on Information Processing Systems have
given us permission to reprint portions of their documentation.

In the following statement, the phrase ``this text'' refers to portions
of the system documentation.

Portions of this text are reprinted and reproduced in electronic form in
the second BSD Networking Software Release, from IEEE Std 1003.1-1988, IEEE
Standard Portable Operating System Interface for Computer Environments
(POSIX), copyright C 1988 by the Institute of Electrical and Electronics
Engineers, Inc. In the event of any discrepancy between these versions
and the original IEEE Standard, the original IEEE Standard is the referee
document.

In the following statement, the phrase ``This material'' refers to portions
of the system documentation.

This material is reproduced with permission from American National
Standards Committee X3, on Information Processing Systems. Computer and
Business Equipment Manufacturers Association (CBEMA), 311 First St., NW,
Suite 500, Washington, DC 20001-2178. The developmental work of
Programming Language C was completed by the X3J11 Technical Committee.

The views and conclusions contained in the software and documentation are
those of the authors and should not be interpreted as representing official
policies, either expressed or implied, of the Regents of the University
of California.

NOTE: The copyright of UC Berkeley's Berkeley Software Distribution ("BSD")
source has been updated. The copyright addendum may be found at
ftp://ftp.cs.berkeley.edu/pub/4bsd/README.Impt.License.Change and is
included below.

July 22, 1999

To All Licensees, Distributors of Any Version of BSD:

As you know, certain of the Berkeley Software Distribution ("BSD") source
code files require that further distributions of products containing all or
portions of the software, acknowledge within their advertising materials
that such products contain software developed by UC Berkeley and its
contributors.

Specifically, the provision reads:

```
"     * 3. All advertising materials mentioning features or use of this software
       *    must display the following acknowledgement:
       *    This product includes software developed by the University of
       *    California, Berkeley and its contributors."
```

Effective immediately, licensees and distributors are no longer required to
include the acknowledgement within advertising materials. Accordingly, the
foregoing paragraph of those BSD Unix files containing it is hereby deleted
in its entirety.

William Hoskins
Director, Office of Technology Licensing
University of California, Berkeley

[tftp-hpa 5.2]
[COPYRIGHT]
  Copyright (c) 1983 Regents of the University of California.
  Copyright (c) 1999-2009 H. Peter Anvin
  Copyright (c) 2011 Intel Corporation; author: H. Peter Anvin

```
  All rights reserved.

[LICENSE]
  Redistribution and use in source and binary forms, with or without
  modification, are permitted provided that the following conditions
  are met:
  1. Redistributions of source code must retain the above copyright
     notice, this list of conditions and the following disclaimer.
  2. Redistributions in binary form must reproduce the above copyright
     notice, this list of conditions and the following disclaimer in the
     documentation and/or other materials provided with the distribution.
  3. All advertising materials mentioning features or use of this software
     must display the following acknowledgement:
         This product includes software developed by the University of
         California, Berkeley and its contributors.
  4. Neither the name of the University nor the names of its contributors
     may be used to endorse or promote products derived from this software
     without specific prior written permission.

  THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND
  ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
  IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
  ARE DISCLAIMED.  IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE
  FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
  DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
  OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
  HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
  LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
  OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
  SUCH DAMAGE.


--------------------------------------------------------------------------
---
[timer 0.9.32 (part of uclibc 0.9.32)]
[LICENSE]
                    GNU LESSER GENERAL PUBLIC LICENSE
                         Version 2.1, February 1999

 Copyright (C) 1991, 1999 Free Software Foundation, Inc.
     51 Franklin St, Fifth Floor, Boston, MA  02110-1301  USA
 Everyone is permitted to copy and distribute verbatim copies
 of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL.  It also counts
 as the successor of the GNU Library Public License, version 2, hence
 the version number 2.1.]

                             Preamble

  The licenses for most software are designed to take away your
freedom to share and change it.  By contrast, the GNU General Public
Licenses are intended to guarantee your freedom to share and change
free software--to make sure the software is free for all its users.

  This license, the Lesser General Public License, applies to some
specially designated software packages--typically libraries--of the
Free Software Foundation and other authors who decide to use it.  You
can use it too, but we suggest you first think carefully about whether
this license or the ordinary General Public License is the better
strategy to use in any particular case, based on the explanations below.

  When we speak of free software, we are referring to freedom of use,
not price.  Our General Public Licenses are designed to make sure that
you have the freedom to distribute copies of free software (and charge
for this service if you wish); that you receive source code or can get
it if you want it; that you can change the software and use pieces of
it in new free programs; and that you are informed that you can do
these things.
```

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the

Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not

excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the library's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA

Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the library, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the library `Frob' (a library for tweaking knobs) written by James Random Hacker.

<signature of Ty Coon>, 1 April 1990
Ty Coon, President of Vice

That's all there is to it!

[traceroute 8.0.0 (part of FreeBSD 8.0.0)]
[COPYRIGHT]
Copyright (c) 1992-2009 The FreeBSD Project. All rights reserved.

[LICENSE]
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright

notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright
notice, this list of conditions and the following disclaimer in the
documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS ``AS IS'' AND
ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
SUCH DAMAGE.

The 4.4BSD and 4.4BSD-Lite software is distributed under the following
terms:

All of the documentation and software included in the 4.4BSD and 4.4BSD-Lite
Releases is copyrighted by The Regents of the University of California.

Copyright 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:
1. Redistributions of source code must retain the above copyright
notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright
notice, this list of conditions and the following disclaimer in the
documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software
must display the following acknowledgement:
This product includes software developed by the University of
California, Berkeley and its contributors.
4. Neither the name of the University nor the names of its contributors
may be used to endorse or promote products derived from this software
without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND
ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE
FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
SUCH DAMAGE.

The Institute of Electrical and Electronics Engineers and the American
National Standards Committee X3, on Information Processing Systems have
given us permission to reprint portions of their documentation.

In the following statement, the phrase ``this text'' refers to portions
of the system documentation.

Portions of this text are reprinted and reproduced in electronic form in
the second BSD Networking Software Release, from IEEE Std 1003.1-1988, IEEE
Standard Portable Operating System Interface for Computer Environments
(POSIX), copyright C 1988 by the Institute of Electrical and Electronics
Engineers, Inc. In the event of any discrepancy between these versions
and the original IEEE Standard, the original IEEE Standard is the referee
document.

In the following statement, the phrase ``This material'' refers to portions

of the system documentation.

This material is reproduced with permission from American National Standards Committee X3, on Information Processing Systems. Computer and Business Equipment Manufacturers Association (CBEMA), 311 First St., NW, Suite 500, Washington, DC 20001-2178. The developmental work of Programming Language C was completed by the X3J11 Technical Committee.

The views and conclusions contained in the software and documentation are those of the authors and should not be interpreted as representing official policies, either expressed or implied, of the Regents of the University of California.

NOTE: The copyright of UC Berkeley's Berkeley Software Distribution ("BSD") source has been updated. The copyright addendum may be found at ftp://ftp.cs.berkeley.edu/pub/4bsd/README.Impt.License.Change and is included below.

July 22, 1999

To All Licensees, Distributors of Any Version of BSD:

As you know, certain of the Berkeley Software Distribution ("BSD") source code files require that further distributions of products containing all or portions of the software, acknowledge within their advertising materials that such products contain software developed by UC Berkeley and its contributors.

Specifically, the provision reads:

" * 3. All advertising materials mentioning features or use of this software
 * must display the following acknowledgement:
 * This product includes software developed by the University of
 * California, Berkeley and its contributors."

Effective immediately, licensees and distributors are no longer required to include the acknowledgement within advertising materials. Accordingly, the foregoing paragraph of those BSD Unix files containing it is hereby deleted in its entirety.

William Hoskins
Director, Office of Technology Licensing
University of California, Berkeley

[traceroute6 8.0.0 (part of FreeBSD 8.0.0)]
[COPYRIGHT]
Copyright (c) 1992-2009 The FreeBSD Project. All rights reserved.

[LICENSE]
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF

SUCH DAMAGE.

The 4.4BSD and 4.4BSD-Lite software is distributed under the following terms:

All of the documentation and software included in the 4.4BSD and 4.4BSD-Lite Releases is copyrighted by The Regents of the University of California.

Copyright 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:
This product includes software developed by the University of California, Berkeley and its contributors.
4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The Institute of Electrical and Electronics Engineers and the American National Standards Committee X3, on Information Processing Systems have given us permission to reprint portions of their documentation.

In the following statement, the phrase ``this text'' refers to portions of the system documentation.

Portions of this text are reprinted and reproduced in electronic form in the second BSD Networking Software Release, from IEEE Std 1003.1-1988, IEEE Standard Portable Operating System Interface for Computer Environments (POSIX), copyright C 1988 by the Institute of Electrical and Electronics Engineers, Inc. In the event of any discrepancy between these versions and the original IEEE Standard, the original IEEE Standard is the referee document.

In the following statement, the phrase ``This material'' refers to portions of the system documentation.

This material is reproduced with permission from American National Standards Committee X3, on Information Processing Systems. Computer and Business Equipment Manufacturers Association (CBEMA), 311 First St., NW, Suite 500, Washington, DC 20001-2178. The developmental work of Programming Language C was completed by the X3J11 Technical Committee.

The views and conclusions contained in the software and documentation are those of the authors and should not be interpreted as representing official policies, either expressed or implied, of the Regents of the University of California.

NOTE: The copyright of UC Berkeley's Berkeley Software Distribution ("BSD")

source has been updated. The copyright addendum may be found at ftp://ftp.cs.berkeley.edu/pub/4bsd/README.Impt.License.Change and is included below.

July 22, 1999

To All Licensees, Distributors of Any Version of BSD:

As you know, certain of the Berkeley Software Distribution ("BSD") source code files require that further distributions of products containing all or portions of the software, acknowledge within their advertising materials that such products contain software developed by UC Berkeley and its contributors.

Specifically, the provision reads:

```
"    * 3. All advertising materials mentioning features or use of this software
      *    must display the following acknowledgement:
      *    This product includes software developed by the University of
      *    California, Berkeley and its contributors."
```

Effective immediately, licensees and distributors are no longer required to include the acknowledgement within advertising materials. Accordingly, the foregoing paragraph of those BSD Unix files containing it is hereby deleted in its entirety.

William Hoskins
Director, Office of Technology Licensing
University of California, Berkeley

[u-boot 1.1.4]
[COPYRIGHT]
(C) Copyright 2000 - 2005
Wolfgang Denk, DENX Software Engineering, wd@denx.de.

[NOTE]
NOTE! This copyright does *not* cover the so-called "standalone" applications that use U-Boot services by means of the jump table provided by U-Boot exactly for this purpose - this is merely considered normal use of U-Boot, and does *not* fall under the heading of "derived work".

The header files "include/image.h" and "include/asm-*/u-boot.h" define interfaces to U-Boot. Including these (unmodified) header files in another file is considered normal use of U-Boot, and does *not* fall under the heading of "derived work".

Also note that the GPL below is copyrighted by the Free Software Foundation, but the instance of code that it refers to (the U-Boot source code) is copyrighted by me and others who actually wrote it.
-- Wolfgang Denk

[LICENSE]

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.
59 Temple Place, Suite 330, Boston, MA 02111-1307 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to

using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot

impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

[uclibc 0.9.32 (part of uclibc 0.9.32)]
[LICENSE]

GNU LESSER GENERAL PUBLIC LICENSE
Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.
51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General

Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for

writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the

ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one

of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your

rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by

the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the library's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA

```
Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or your
school, if any, to sign a "copyright disclaimer" for the library, if
necessary.  Here is a sample; alter the names:

  Yoyodyne, Inc., hereby disclaims all copyright interest in the
  library `Frob' (a library for tweaking knobs) written by James Random Hacker.

  <signature of Ty Coon>, 1 April 1990
  Ty Coon, President of Vice

That's all there is to it!


------------------------------------------------------------------------------
---
[unix stack 8.0.0 (part of FreeBSD 8.0.0)]
[COPYRIGHT]
  Copyright (c) 1992-2009 The FreeBSD Project. All rights reserved.

[LICENSE]
Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:
1. Redistributions of source code must retain the above copyright
   notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright
   notice, this list of conditions and the following disclaimer in the
   documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS ``AS IS'' AND
ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
ARE DISCLAIMED.  IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
SUCH DAMAGE.

The 4.4BSD and 4.4BSD-Lite software is distributed under the following
terms:

All of the documentation and software included in the 4.4BSD and 4.4BSD-Lite
Releases is copyrighted by The Regents of the University of California.

Copyright 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
         The Regents of the University of California.  All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:
1. Redistributions of source code must retain the above copyright
   notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright
   notice, this list of conditions and the following disclaimer in the
   documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software
   must display the following acknowledgement:
This product includes software developed by the University of
California, Berkeley and its contributors.
4. Neither the name of the University nor the names of its contributors
   may be used to endorse or promote products derived from this software
   without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND
ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
```

IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The Institute of Electrical and Electronics Engineers and the American National Standards Committee X3, on Information Processing Systems have given us permission to reprint portions of their documentation.

In the following statement, the phrase ``this text'' refers to portions of the system documentation.

Portions of this text are reprinted and reproduced in electronic form in the second BSD Networking Software Release, from IEEE Std 1003.1-1988, IEEE Standard Portable Operating System Interface for Computer Environments (POSIX), copyright C 1988 by the Institute of Electrical and Electronics Engineers, Inc. In the event of any discrepancy between these versions and the original IEEE Standard, the original IEEE Standard is the referee document.

In the following statement, the phrase ``This material'' refers to portions of the system documentation.

This material is reproduced with permission from American National Standards Committee X3, on Information Processing Systems. Computer and Business Equipment Manufacturers Association (CBEMA), 311 First St., NW, Suite 500, Washington, DC 20001-2178. The developmental work of Programming Language C was completed by the X3J11 Technical Committee.

The views and conclusions contained in the software and documentation are those of the authors and should not be interpreted as representing official policies, either expressed or implied, of the Regents of the University of California.

NOTE: The copyright of UC Berkeley's Berkeley Software Distribution ("BSD") source has been updated. The copyright addendum may be found at ftp://ftp.cs.berkeley.edu/pub/4bsd/README.Impt.License.Change and is included below.

July 22, 1999

To All Licensees, Distributors of Any Version of BSD:

As you know, certain of the Berkeley Software Distribution ("BSD") source code files require that further distributions of products containing all or portions of the software, acknowledge within their advertising materials that such products contain software developed by UC Berkeley and its contributors.

Specifically, the provision reads:

```
"     * 3. All advertising materials mentioning features or use of this software
       *    must display the following acknowledgement:
       *    This product includes software developed by the University of
       *    California, Berkeley and its contributors."
```

Effective immediately, licensees and distributors are no longer required to include the acknowledgement within advertising materials. Accordingly, the foregoing paragraph of those BSD Unix files containing it is hereby deleted in its entirety.

William Hoskins
Director, Office of Technology Licensing
University of California, Berkeley

```
------------------------------------------------------------------------------
---
[wireshark 2.4.6]
This text consists of three parts:

Part I: Some remarks regarding the license given in
Part II: The actual license that covers Wireshark.
Part III: Other applicable licenses.

When in doubt: Part II/III is the legally binding part, Part I is just
there to make it easier for people that are not familiar with the GPLv2.


------------------------------------------------------------------------
Part I:

Wireshark is distributed under the GNU GPLv2. There are no restrictions
on its use. There are restrictions on its distribution in source or
binary form.

Most parts of Wireshark are covered by a "GPL version 2 or later" license.
Some files are covered by different licenses that are compatible with
the GPLv2.

As a notable exception, some utilities distributed with the Wireshark source are
covered by other licenses that are not themselves directly compatible with the
GPLv2. This is OK, as only the tools themselves are licensed this way, the
output of the tools is not considered a derived work, and so can be safely
licensed for Wireshark's use. An incomplete selection of these tools includes:
 - the pidl utility (tools/pidl) is licensed under the GPLv3+.

Parts of Wireshark can be built and distributed as libraries. These
parts are still covered by the GPL, and NOT by the Lesser General Public
License or any other license.

If you integrate all or part of Wireshark into your own application, then
that application must be released under a license compatible with the GPL.

The full text of the GNU GPL and some of the other applicable licenses follows.

------------------------------------------------------------------------
Part II:

                    GNU GENERAL PUBLIC LICENSE
                       Version 2, June 1991

 Copyright (C) 1989, 1991 Free Software Foundation, Inc.,
 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA
 Everyone is permitted to copy and distribute verbatim copies
 of this license document, but changing it is not allowed.

                            Preamble

  The licenses for most software are designed to take away your
freedom to share and change it.  By contrast, the GNU General Public
License is intended to guarantee your freedom to share and change free
software--to make sure the software is free for all its users.  This
General Public License applies to most of the Free Software
Foundation's software and to any other program whose authors commit to
using it.  (Some other Free Software Foundation software is covered by
the GNU Lesser General Public License instead.)  You can apply it to
your programs, too.

  When we speak of free software, we are referring to freedom, not
price.  Our General Public Licenses are designed to make sure that you
have the freedom to distribute copies of free software (and charge for
this service if you wish), that you receive source code or can get it
if you want it, that you can change the software or use pieces of it
in new free programs; and that you know you can do these things.
```

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent

access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions

of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc.,

```
    51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this
when it starts in an interactive mode:

    Gnomovision version 69, Copyright (C) year name of author
    Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
    This is free software, and you are welcome to redistribute it
    under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate
parts of the General Public License.  Of course, the commands you use may
be called something other than `show w' and `show c'; they could even be
mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your
school, if any, to sign a "copyright disclaimer" for the program, if
necessary.  Here is a sample; alter the names:

  Yoyodyne, Inc., hereby disclaims all copyright interest in the program
  `Gnomovision' (which makes passes at compilers) written by James Hacker.

  <signature of Ty Coon>, 1 April 1989
  Ty Coon, President of Vice

This General Public License does not permit incorporating your program into
proprietary programs.  If your program is a subroutine library, you may
consider it more useful to permit linking proprietary applications with the
library.  If this is what you want to do, use the GNU Lesser General
Public License instead of this License.

------------------------------------------------------------------------
Part III:

Parts of this software are licensed as follows

   Copyright (c) 1988, 1992, 1993
        The Regents of the University of California.  All rights reserved.

   Redistribution and use in source and binary forms, with or without
   modification, are permitted provided that the following conditions
   are met:
   1. Redistributions of source code must retain the above copyright
      notice, this list of conditions and the following disclaimer.
   2. Redistributions in binary form must reproduce the above copyright
      notice, this list of conditions and the following disclaimer in the
      documentation and/or other materials provided with the distribution.
   3. Neither the name of the University nor the names of its contributors
      may be used to endorse or promote products derived from this software
      without specific prior written permission.

   THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND
   ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
   IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
   ARE DISCLAIMED.  IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE
   FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
   DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
   OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
   HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
   LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
   OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
   SUCH DAMAGE.


   Copyright (c) 2003 Markus Friedl.  All rights reserved.

   Redistribution and use in source and binary forms, with or without
   modification, are permitted provided that the following conditions
```

are met:
1. Redistributions of source code must retain the above copyright
notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright
notice, this list of conditions and the following disclaimer in the
documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS'' AND ANY EXPRESS OR
IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES
OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED.
IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT,
INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE,
DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY
THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT
(INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF
THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright (c) 2003 Endace Technology Ltd, Hamilton, New Zealand.
All rights reserved.

This software and documentation has been developed by Endace Technology Ltd.
along with the DAG PCI network capture cards. For further information please
visit http://www.endace.com/.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice,
this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright
notice, this list of conditions and the following disclaimer in the
documentation and/or other materials provided with the distribution.

3. The name of Endace Technology Ltd may not be used to endorse or promote
products derived from this software without specific prior written
permission.

THIS SOFTWARE IS PROVIDED BY ENDACE TECHNOLOGY LTD ``AS IS'' AND ANY EXPRESS
OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES
OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO
EVENT SHALL ENDACE TECHNOLOGY LTD BE LIABLE FOR ANY DIRECT, INDIRECT,
INCIDENTAL,
SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,
PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS;
OR
BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER
IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE
POSSIBILITY OF SUCH DAMAGE.

Copyright (C) 1995, 1996, 1997, and 1998 WIDE Project.
All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:
1. Redistributions of source code must retain the above copyright
notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright
notice, this list of conditions and the following disclaimer in the
documentation and/or other materials provided with the distribution.
3. Neither the name of the project nor the names of its contributors
may be used to endorse or promote products derived from this software
without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE PROJECT AND CONTRIBUTORS ``AS IS'' AND

```
   ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
   IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
   ARE DISCLAIMED.  IN NO EVENT SHALL THE PROJECT OR CONTRIBUTORS BE LIABLE
   FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
   DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
   OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
   HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
   LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
   OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
   SUCH DAMAGE.


   Copyright (c) 1997, 1999 Hellmuth Michaelis. All rights reserved.

   Redistribution and use in source and binary forms, with or without
   modification, are permitted provided that the following conditions
   are met:
   1. Redistributions of source code must retain the above copyright
      notice, this list of conditions and the following disclaimer.
   2. Redistributions in binary form must reproduce the above copyright
      notice, this list of conditions and the following disclaimer in the
      documentation and/or other materials provided with the distribution.

   THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS ``AS IS'' AND
   ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
   IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
   ARE DISCLAIMED.  IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
   FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
   DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
   OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
   HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
   LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
   OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
   SUCH DAMAGE.
--------------------------------------------------------------------------------
---
[wpa_supplicant 2.6]
[COPYRIGHT]
  Copyright (c) 2002-2016, Jouni Malinen <j@w1.fi> and contributors
  All Rights Reserved.

[LICENSE]
This software may be distributed, used, and modified under the terms of
BSD license:

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions are
met:

1. Redistributions of source code must retain the above copyright
   notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright
   notice, this list of conditions and the following disclaimer in the
   documentation and/or other materials provided with the distribution.

3. Neither the name(s) of the above-listed copyright holder(s) nor the
   names of its contributors may be used to endorse or promote products
   derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS
"AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT
LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR
A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT
OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT
LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE,
DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY
THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT
(INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE
```

```
OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
------------------------------------------------------------------------------
---
[xzdec 5.2.2(part of xz 5.2.2)]
////////////////////////////////////////////////////////////////////////////
//
//
/// \file       xzdec.c
/// \brief      Simple single-threaded tool to uncompress .xz or .lzma files
//
//  Author:     Lasse Collin
//
//  This file has been put into the public domain.
//  You can do whatever you want with this file.
//
////////////////////////////////////////////////////////////////////////////
//
------------------------------------------------------------------------------
---
[zlib 1.2.3]
[COPYRIGHT]
  Copyright (C) 1995-2005 Jean-loup Gailly and Mark Adler

[LICENSE]
  This software is provided 'as-is', without any express or implied
  warranty.  In no event will the authors be held liable for any damages
  arising from the use of this software.

  Permission is granted to anyone to use this software for any purpose,
  including commercial applications, and to alter it and redistribute it
  freely, subject to the following restrictions:

  1. The origin of this software must not be misrepresented; you must not
     claim that you wrote the original software. If you use this software
     in a product, an acknowledgment in the product documentation would be
     appreciated but is not required.
  2. Altered source versions must be plainly marked as such, and must not be
     misrepresented as being the original software.
  3. This notice may not be removed or altered from any source distribution.

  Jean-loup Gailly        Mark Adler
  jloup@gzip.org          madler@alumni.caltech.edu


------------------------------------------------------------------------------
---
```