NEC

GVT-073439-001-00 1.20

QX-S5300G 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	2018/10	初版発行
1.1	2019/01	「08-セキュリティ」の「1 章 AAA」に再認証を行う際の RADIUS サーバ選択モードの設定を追加しました。
1.2	2019/10	・「01-はじめに」の「14 章 装置管理」にパリティエラーモニター機能を追加しました。 ・「01-はじめに」の「14 章 装置管理」にリソース監視機能を追加しました。 ・「03-アクセス」の「1 章 Ethernet インタフェース」の **link-deray** コマンドの設定範囲が変わりました。 ・「03-アクセス」の「1 章 Ethernet インタフェース」の combo enable に **auto** オプションが追加され、デフォルトを **auto** に変更しました。 ・「03-アクセス」の「6 章 リンクアグリゲーション」の port link-aggregation group コマンドに force オプションを追加しました。 ・「10-システム管理」に「NetMeister 機能」を追加しました。 ・誤記訂正
1.3	2020/02/24	誤記訂正
1.4	2020/03	・「07-ACL and QoS」の「1 章 ACL」に VLAN インタフェースのパケットフィルタリング適用範囲の設定を追加しました。 ・誤記訂正
1.5	2020/06	・「07-ACL and QoS」の「5 章 トラフィックポリシング、GTS、ラインレート」の「5.3. トラフィックポリシングの設定」に重要情報を追記しました。
1.6	2020/09	・「10-システム管理」の「1章 システムの保守とデバッグ」に「1.4. レートリミットロギング機能」を追加しました。
1.7	2020/12	・「03-アクセス」の「16 章 L2PT」16.3.3. aggregate interface view のプロトコルでの L2PT の有効化にオプションを追加しました。 ・誤記訂正
1.8	2021/09	・「08-セキュリティ」の「11 章 SSH」に ssh2 algorithm コマンドの記載を追加しました。
1.9	2021/12	・「11-謝辞」更新
1.10	2022/01	・「07-ACL and QoS」の「13 章 データバッファ機能」に「13.5 データバッファの手動設定」と「13.6. データバッファの表示と維持」を追加しました。 ・「07-ACL and QoS」の「13 章 データバッファ機能」の図 13-1 の差し替え。説明内容の変更を行いました。
1.11	2022/10	・10-システム管理の12章 NetMeisterにIRF対応に関する記載を追加しました。 ・誤記訂正

版数	日付	改版内容
1.12	2023/01	・「01-はじめに」の「14章 装置管理」に「14.17. CPU使用率のモニタリングの設定」を追加しました。 ・「03-アクセス」の「8章 STP」に「8.33. 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」にメモを追加しました。 ・「03-アクセス」の「9章 ループ検出」の「9.1.4. ポート状態自動回復」の誤記訂正をしました。 ・「03-アクセス」の「10章 VLAN」の「10.1.5. IPサブネットベースVLAN」の誤記訂正をしました。 ・「03-アクセス」の「10章 VLAN」の「10.2.1. 制限とガイドライン」の誤記訂正をしました。 ・「09-高可用性」の「8章 Track」の「8.5.1. TrackとNQAの関連づけ」からdelayに関するパラメータを削除しました(誤記訂正)。
1.13	2023/05	・「04-IPサービス」の「2章 Gratuitous ARP」に「2.7. デバイスのMACアドレス変更に対するgratuitous ARPパケット再送信の設定」を追加しました。 ・「11-システム管理」の「3章NTP」のdisplay ntp-service traceコマンドの説明を修正しました。
1.14	2023/07	・「01-はじめに」の「3章 ログイン」に、Webインタフェースからのアクセス方法を追加しました。 ・「01-はじめに」の「7章 ログインユーザの制御」に「7.3. Webログインの制御」を追加しました。 ・「01-はじめに」の「14章 装置管理」の「表 14-3 温度アラームの推奨温度のしきい値とデフォルトのしきい値」を修正しました。 ・「01-はじめに」に「18章 Webコンソールによるログイン」を追加しました。 ・「02-IRFスタック」の「1章 IRFスタック」の「1.2.3. IRFスタック物理インタフェースの選択」の説明内容を修正しました。 ・「02-IRFスタック」の「1章 IRFスタック」の「1.6.3. BFD MADの設定」の説明内容を修正しました。 ・「03-アクセス」の「8章 STP」の「8.30.7. 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。 ・「08-セキュリティ」の「8章 パスワード管理」の表8-1 特殊文字について誤記修正しました。
1.15	2023/09	・10-システム管理の12章 NetMeisterに親機モード運用時の設定を追加しました。
1.16	2024/05	・「01-はじめに」の「17章 Auto Config」に「17.3 USBベース Auto Configの使用」を追加しました。 ・「03-アクセス」の「10章 VLAN」の「10.9.3 IP サブネットベース VLAN 設定例」について誤記修正しました。 ・「10-システム管理」の「13章NetMeister」にVer7.4.37リリースに伴う変更、修正、その他誤記修正を実施しました。
1.17	2024/11	・「01-はじめに」の「14章 装置管理」に「14.11. 装置の温度アラームのしきい値の設定」に10GBASE-T-SFP+接続時の推奨温度アラームしきい値を追加しました。 ・「02-IRFスタック」の「1章 IRFスタック」の「1.5. IRFスタックユニットの設定」に重要事項を追加しました。 ・「02-IRFスタック」の「1章 IRFスタック」のport group interfaceの誤記訂正をしました。

版数	日付	改版内容
1.18	2025/07	・「01-はじめに」 の「 18章 Webコンソールによるログイン 」の「18.2.1 制限とガイドライン」を修正しました。 ・「03-アクセス」 の「 13章 QinQ 」の「13.2. 制限とガイドライン」を修正しました。 ・「09-高可用性」 の「 4章 RRPP 」の「4.3. RRPPの設定作業リスト」に注意を追加しました。 ・「10-システム管理」 の「13章 NetMeister 」の重複している章を削除しました。 ・「10-システム管理」 の「13章 NetMeister 」の「13.5. NetMeisterの設定例」について誤記修正しました。
1.19	2026/1	・「08-セキュリティ」 の「 4章 MACアドレス認証 」の「4.14.MACアドレス認証ユーザのロギングの有効化」にinterface viewの説明を追加しました。 ・「08-セキュリティ」 の「 7章 ポートセキュリティ」の「7.7.セキュアMACアドレスの設定」にinterface viewの説明を追加しました。
1.20	2026/10	・「01-はじめに」の「1章 CLI」に「1.8. コマンド履歴バッファの管理と使用」を追加しました。 ・「03-アクセス」 の「 9章 ループ検出 」の「9.3.1. 制限とガイドライン」に説明を追加しました。 ・「03-アクセス」 の「 14章 VLANマッピング 」の「14.2. 制限とガイドライン」を修正しました。 ・「04-IPサービス」 の「 10章 DHCPスヌーピング 」の「14.2. 制限とガイドライン」を説明を追加しました。 ・「07- ACL and QoS」 の「 4章 プライオリティマッピング 」の「4.1. 概要」の誤記訂正をしました。 ・「07- ACL and QoS」 の「 4章 プライオリティマッピング 」の「4.1.1. プライオリティ」の誤記訂正をしました。 ・「07- ACL and QoS」 の「 4章 プライオリティマッピング 」の「4.1.4 プライオリティのマッピング手順」の誤記訂正をしました。 ・「07- ACL and QoS」 の「 4章 プライオリティマッピング 」の「4.1. 概要」の誤記訂正と画像差し替えをしました。 ・「07- ACL and QoS」 の「 4章 プライオリティマッピング 」の「4.3. プライオリティマッピングの設定」の誤記訂正をしました。 ・「07- ACL and QoS」 の「 4章 プライオリティマッピング 」の「4.6. プライオリティマッピングの表示と維持」の誤記訂正をしました。 ・「07- ACL and QoS」 の「 12章 付録 」の「12.2.1. プライオリティマッピング」の誤記訂正をしました。 ・「09- 高可用性」 の「 4章 RRPP 」の「4.1.6. プロトコルと標準」を削除しました。 ・「09- 高可用性」 の「 9章 Smart Link 」の「5.4.2. Smart Linkグループのプロテクトvlanの設定」のメモを修正しました。 ・「10-システム管理」 の「9章 ポートミラーリング 」の「9.5.3 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」の誤記訂正をしました。 ・「10-システム管理」 の「13章 NetMeister 」にVer7.4.48リリースに伴う変更、修正を実施しました。

Copyright © NEC Corporation 2018-2026

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-S5300G Series Ethernet Switches Command References* 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-S5300G Series Ethernet Switches Command References* 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

バージョン

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

関連マニュアル

次のマニュアルには、QX-S5300G 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-S5300G 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-S5300G 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-S5300G シリーズ Series Ethernet Switches Command References	機能に関するコマンドについて説明しています。
QX-S5300G 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

このコマンド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。

- **IRF スタック**

  IRF スタック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、SSH 等の設定について説明します。

- **高可用性**

  Ethernet OAM、CFD、DLDP、RRPP、BFD 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 つまたは複数を選択します。
{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**	表示を無視したり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**	表示を無視したり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セクションで構成されています。

01 - はじめに

02 - IRF スタック

03 - アクセス

04 - IP サービス

05 - ルーティングプロトコル

06 - マルチキャスト

07 - ACL and QoS

08 - セキュリティ

09 - 高可用性

10 - システム管理

11 - 謝辞

QX-S5300G 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-RBAC

03-ログイン

04-コンソールポートによる最初のログイン

05-CLI によるログイン

06-SNMP によるログイン

07-ログインユーザの制御

08-FTP

09-TFTP

10-ファイルシステム管理

11-コンフィグレーションファイル管理

12-ソフトウェアのアップグレード

13-ISSU

14-装置管理

15-Python

16-Comware 7 python 拡張 API

17-Auto Config

18-Web コンソールによるログイン

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. 概要 1-1
1.2. CLI view の記述 1-1
1.2.1. user view から system view への移行 1-2
1.2.2. 各 view から上位 view への戻り 1-2
1.2.3. user view への戻り 1-2
1.3. コマンドラインを使ったオンラインヘルプ 1-2
1.4. コマンドの undo 1-3
1.5. コマンドの実行 1-4
1.5.1. コマンドラインの編集 1-4
1.5.2. 引数の文字列あるいはテキストタイプ値の入力 1-5
1.5.3. インタフェースタイプの入力 1-5
1.5.4. コマンドの補完 1-6
1.5.5. コマンドエイリアスの設定と使用方法 1-6
1.5.6. ホットキーを使用した設定と使用方法 1-7
1.5.7. 情報の同期出力 1-9
1.6. コマンドラインのエラーメッセージ 1-10
1.7. 履歴コマンドの保存 1-10
1.7.1. 履歴コマンドのルール 1-11
1.8. コマンド履歴バッファの管理と使用 1-11
1.8.1. コマンド履歴バッファ内のコマンドの表示 1-11
1.9. CLI 表示の管理 1-12
1.9.1. 出力のスクリーンの休止 1-12
1.9.2. 表示コマンドの各出力ラインの番号表示 1-13
1.9.3. 出力のフィルタリング 1-13
1.9.4. display コマンドのファイルへの保存 1-16
1.9.5. display コマンドからの出力の有効的な表示、管理 1-17
1.10. 稼働中の設定の保存 1-17

1章 CLI

1.1. 概要

Command-Line Interface（CLI）は、装置とユーザ間の相互運用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。

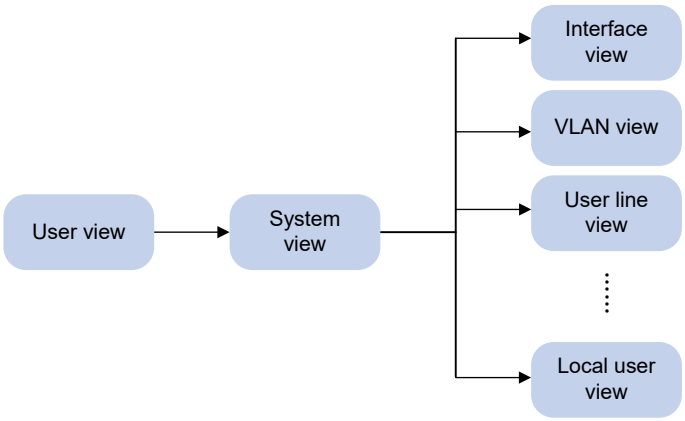
CLI には、さまざまな方法でログインすることができます。たとえばコンソールポートを使用する、あるいは Telnet、SSH を使用することでログインすることができます。ログイン方法については、セクション 1 *はじめに オペレーションマニュアルの”ログイン”*を参照してください。

1.2. CLI viewの記述

コマンドは機能によって異なる view にグループ分けされています。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 1-1 に示すような階層構造となっています。各 view は、どこで何を行うのかを一意に示すプロンプトとなります。たとえば[Switch-vlan100]という view は、VLAN100 view で、その VLAN の属性を設定することができます。

図 1-1 CLI view



CLI でログインした後、最初に user view に入ります。user view のプロンプトは<*Device-name*>で、*Device-name* は装置名を示します。デフォルトは装置名で、**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 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 からさらに、異なる 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 にポートを追加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。

view プロンプトでクエスチョン“?”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を表示します。

1.2.1. user view から system view への移行

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

1.2.2. 各 view から上位 view への戻り

操作	コマンド
各viewから上位viewに戻る	**quit**

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

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

1.2.3. user view への戻り

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

以下の手順で、他の view から user view へ戻ります。

操作	コマンド
user viewに戻る	**return**

1.3. コマンドラインを使ったオンラインヘルプ

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。すべてのプロンプトで“?”を入力し、その view で利用できるコマンドを表示するか、コマンドのいずれかの位置で、すべての有効なオプションを表示することができます。

CLI オンラインヘルプにアクセスするには以下の方法を行います。

- 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キーワードを表示します。

```
<Switch> ?
  User view commands:
    archive           Archive configuration
    backup            Backup the startup configuration file to a TFTP server
    boot-loader       Software image file management
    …
```

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

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

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

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

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

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

```
<Switch> q?
  quit
<Switch> display ftp?
  ftp
  ftp-server
  ftp-user
```

1.4. コマンドのundo

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

ほとんどの設定コマンドに、undo を付加できます。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。

たとえば Information Center を有効にするために、**info-center enable** コマンドを使用した場合、**undo info-center enable** コマンドで Information Center を無効にします。(Information Center は、デフォルトで有効です。)

1.5. コマンドの実行

コマンドを入力することで以下のことができます。

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

1.5.1. コマンドラインの編集

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。終了するには **Enter** を押してコマンドを実行します。

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	編集バッファが一杯でなければ、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。コマンドの最大の長さは、511文字です。コマンドの最大の長さに達した場合、システムは次の行に自動的に移ります。次の行に移るには、**Enter** を押します。
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。
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 （↑）	前に入力した履歴バッファを表示します。
下矢印キー （↓）	次に入力した履歴バッファを表示します。
Tab	キーワードの一部でTABキーを押した場合、システムは自動的にキーワードを補完します。 1. ただ 1 つマッチングしたら、システムは不完全なキーワードを完全なキーワードに置き換えて、それを次の行に表示します。 2. マッチするものが複数ある場合、キーワードを選択するため TAB キーを複数回押してください。 3. マッチするものが全くない場合は、システムは不完全なキーワードを補完せず、再度それを次の行に表示します。

1.5.2. 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” ” ”（マニュアルでは” “ ”と表記されることがあります）
- バックスラッシュ”\”
- スペース

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

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。

1.5.3. インタフェースタイプの入力

インタフェースタイプは、次のいずれかの形式で入力できます。

- インタフェースタイプのフルスペル。
- インタフェースタイプを固有に識別する略語。
- インタフェース型の頭字語。

コマンドラインでは、すべてのインタフェースタイプで大文字と小文字が区別されません。 表 1-2 は、インタフェースタイプの完全なつづりと頭字語を示しています。

たとえばインタフェースのコマンドを使用してインタフェースの view に入るには GigabitEthernet 1/0/1 は、次の形式でコマンドラインを入力できます。

- **interface gigabitethernet 1/0/1**
- **interface g 1/0/1**
- **interface ge 1/0/1**

インタフェースタイプとインタフェースの間のスペースは必要ありません。

表 1-2 インタフェース型の完全な綴りと頭字語

フルスペル	頭字語
Bridge-Aggregation	BAGG
FortyGigE	FGE
GigabitEthernet	GE
InLoopBack	InLoop
LoopBack	Loop
M-GigabitEthernet	MGE
NULL	NULL
Ten-GigabitEthernet	XGE
Vlan-interface	Vlan-int

1.5.4. コマンドの補完

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

Tab キーを押すことで、完全なコマンドを表示、入力することができます

1.5.5. コマンドエイリアスの設定と使用方法

コマンドのエイリアスを設定した後、コマンドを実行するため、エイリアスを入力することができます。たとえば、**display ip routing-table** コマンドを行うために **alias siprt** コマンドを設定することができます。そしてコマンドを実行する場合、**alias siprt** を入力することで **display ip routing-table** コマンドを実行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したコマンドを実行したのち、装置はエイリアスの代わりにキーワードを保存します。カレントコンフィグレーションはオリジナルコマンドが表示されます。

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 | include Static** を行う場合、**shinc routing-table Static** を入力することで実行することができます。**display ip interface | include GigabitEthernet1/0/1** コマンドを実行する場合、**shinc interface GigabitEthernet1/0/1** を入力することで実行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。パラメータの指定を設定するのに失敗した場合、コマンドは不完全で、エイリアスで表示されるコマンドの文字列を表示します。

表 1-3 にシステム定義のコマンドエイリアスを示します。

表 1-3 システム定義の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

エイリアス	コマンド
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**	―
2. コマンドエイリアスを設定する	**alias** *alias command*	デフォルト：設定なし
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。

1.5.6. ホットキーを使用した設定と使用方法

システムは CLI を補助するため、ホットキーをサポートします。

表 1-4 にデフォルト定義のホットキーを示します。

ホットキーを押すことでコマンドを入力することと同じことを行うことができます。これらのホットキーは装置が定義しています。

ホットキーは 1 つのコマンドあるいは機能のみ対応します。同一のホットキーに複数のコマンドあるいは機能を割り当てた場合、最後に設定したコマンドあるいは機能が適用されます。

コマンドあるいは機能に複数のホットキーを割り当てることができます。コマンドあるいは機能を実行するため、割り当てられたホットキーを使用してください。

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

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**	―
2. コマンドをホットキーに割り当てる	**hotkey** *hotkey* { *command* | **function** *function* | **none** }	デフォルト： デフォルトのホットキーを表 1-4に示します。
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。

表 1-4 デフォルト定義のホットキー

ホットキー	機能あるいはコマンド
Ctrl+A	**move_the_cursor_to_the_beginning_of_the_line** 行の先頭にカーソルを移動します。
Ctrl+B	**move_the_cursor_one_character_to_the_left** カーソルを1文字、左に移動します。
Ctrl+C	**stop_the_current_command** 現在のコマンドを停止します。
Ctrl+D	**erase_the_character_at_the_cursor** カーソル上の文字を削除します。
Ctrl+E	**move_the_cursor_to_the_end_of_the_line** 行の行末にカーソルを移動します。
Ctrl+F	**move_the_cursor_one_character_to_the_right** カーソルを1文字、右に移動します。
Ctrl+G	**display current-configuration** カレントコンフィグレーションを表示します。
Ctrl+H	**erase_the_character_to_the_left_of_the_cursor** カーソルの1つ左の文字を削除します。
Ctrl+K	**abort_the_connection_request** 現在の接続要求を中断します。
Ctrl+L	**display ip routing-table** IPv4ルーティングテーブル情報を表示します。
Ctrl+N	**display_the_next_command_in_the_history_buffer** 履歴バッファの次のコマンドを表示します。
Ctrl+O	**undo debugging all** すべてのデバッグ機能を無効にします。
Ctrl+P	**display_the_previous_command_in_the_history_buffer** 履歴バッファの前のコマンドを表示します。
Ctrl+R	**redisplay_the_current_line** 現在の行を再表示します。
Ctrl+T	ー
Ctrl+U	ー
Ctrl+V	**paste_text_from_the_clipboard** クリップボードからテキストデータをペーストします。
Ctrl+W	**delete_the_word_to_the_left_of_the_cursor** カーソルの左の単語を削除します。
Ctrl+X	**delete_all_characters_from_the_beginning_of_the_line_to_the_cursor** カーソルの左にあるすべての文字を削除します。

ホットキー	機能あるいはコマンド
Ctrl+Y	**delete_all_characters_from_the_cursor_to_the_end_of_the_line** カーソルから行末までのすべての文字を削除します。
Ctrl+Z	**return_to_the_User_View** user viewに戻ります。
Ctrl+]	**kill_incoming_connection_or_redirect_connection** 現在の接続を終了します。
Esc+B	**move_the_cursor_back_one_word** カーソルを1単語前に移動します。
Esc+D	**delete_all_characters_from_the_cursor_to_the_end_of_the_word** カーソルから単語の最後までのすべての文字列を削除します。
Esc+F	**move_the_cursor_forward_one_word** カーソルを1単語後に移動します。
Esc+N	**move_the_cursor_down_a_line** カーソルを下の行に移動します。Enterキーを押下する前にホットキーを使用することができます。
Esc+P	**move_the_cursor_up_a_line** カーソルを上の行に移動します。Enterキーを押下する前にホットキーを使用することができます。
Esc+<	**move_the_cursor_to_the_beginning_of_the_clipboard** クリップボードの最初にカーソルを移動します。
Esc+>	**move_the_cursor_to_the_end_of_the_clipboard** クリップボードの最後にカーソルを移動します。

1.5.7. 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Chapter 11 *Network Management and Monitoring Command References*の”*Information Center*”を参照してください。

1.6. コマンドラインのエラーメッセージ

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

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

表 1-5 コマンドラインのエラーメッセージ

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.	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。

1.7. 履歴コマンドの保存

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

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

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
履歴を実行するために呼び出す方法	Windows 200xあるいはXPのハイパーターミナルあるいはTelnetで、再度実行するコマンドが表示されるまで上下矢印キー（↑ あるいは ↓）を押します。 Windows 9xのハイパーターミナルで、再度実行するコマンドが表示されるまで**Ctrl+P** と**Ctrl+N**を押します。	履歴を呼び出すことはできません。
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。

1.7.1. 履歴コマンドのルール

履歴コマンドを使用したときのルールを示します。

- 正しいフォーマットで入力されたコマンドを履歴に保存します。たとえば、不完全なコマンドが入力された場合、バッファされたコマンドも不完全となります。
- 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 回のみ履歴に保存します。異なるフォーマットのコマンドを連続して複数入力された場合、各コマンドが履歴に保存されます。たとえば **display cu** コマンドと **display current-configuration** コマンドの 2 つのエントリが連続して入力された場合、**display cu** コマンドと **display current-configuration** コマンドが履歴に保存されますが、**display cu** コマンドが繰り返し入力された場合、**display cu** コマンドが 1 回のみ履歴に保存されます。
- バッファが一杯の状態では、新しいコマンドを保存するため、最も古いコマンドの履歴が削除されます。

1.8. コマンド履歴バッファの管理と使用

1.8.1. コマンド履歴バッファ内のコマンドの表示

コマンド履歴バッファにコマンドを表示するには、任意のビューで次のコマンドを実行します。

操作	コマンド
ユーザ行のコマンド履歴バッファにコマンドを表示します。	**display history-command**
すべてのユーザ行のコマンド履歴バッファにコマンドを表示します。	**display history-command all**

1.8.2. コマンド履歴バッファ内のコマンドの呼び出し

重要：
パスワード設定コマンドは呼び出せません。

上下矢印キーを使用してコマンドに移動し、Enter キーを押します。

1.8.3. コマンド履歴バッファでコマンドの繰り返し

現在のコマンド履歴バッファにあるコマンドを複数回呼び出して実行できます。

I. ガイドライン

repeat コマンドはどのビューでも使用できます。ただし、コマンドを繰り返すには、まずコマンドのビューを入力する必要があります。複数のコマンドを繰り返すには、最初のコマンドのビューを最初に入力する必要があります。

repeat コマンドは実行された順にコマンドを実行します。

システムは対話型コマンドを繰り返すとき、ユーザの操作を待機します。

システムはすべてのパスワード設定コマンドをスキップします。

操作	コマンド
現在のユーザ行のコマンド履歴バッファでコマンドを繰り返します。	**repeat** [*number*] [**count** *times*] [**delay** *seconds*]

1.9. CLI表示の管理

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

1.9.1. 出力のスクリーンの休止

表示する情報が 1 つのスクリーンを上回る場合、以下の表で示される方法のうちの 1 つを用いて情報出力を休止することができます。詳細な情報を表示させるために出力管理キーに記載されているキーを使用したり、表示を停止することができます。

通常、24 行が 1 つのスクリーンに表示されます。スクリーン画面に表示される行数を変更するため、**screen-length** *screen-length* コマンドを使用できます。詳細は、Chapter 1 *Fundamentals Command References* の”*Login management commands*”を参照してください。

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

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. 複数のスクリーン出力機能の無効化

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

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：user line viewの **screen-length** *screen-length*コマンドの設定によってデフォルトは変わります。 このコマンドは現在の画面のみ適用されます。

1.9.2. 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（－）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：

システム時間の情報を各出力ラインに番号を表示して出力します。

```
<Switch> display clock | by-linenum
    1:  06:14:21 UTC Sat 01/01/2011
```

1.9.3. 出力のフィルタリング

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

- **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 1-6 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 1-6 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。

文字	意味	例
{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”、“foooood“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い。	”\<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。
\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 を含む最後の行の後の情報を表示します。

<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 scheme
 user-role network-operator
#
 ssh server enable
#
return
```

display ip routing-table コマンドで**| exclude Direct** を使用し、ダイレクトルート以外のルートを表示します。

<Switch> display ip routing-table | exclude Direct

```
         Destinations : 12       Routes : 12

Destination/Mask    Proto   Pre  Cost         NextHop         Interface
2.2.2.0/24          OSPF    10   2            1.1.2.2         Vlan 2
```

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
```

1.9.4. 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、動作によって変化します。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：

システム時間の情報をファイル名 clock.txt のファイルに分離して保存します。

<Switch> display clock > clock.txt

clock.txt のファイルに保存されているかどうかシステム時間を確認します。

<Switch> more clock.txt

```
06:03:58 UTC Sat 01/01/2014
```

システム時間の情報を clock.txt の最後に追記します。

<Switch> display clock >> clock.txt

clock.txt のファイルに追記されているかどうかシステム時間を確認します。

<Switch> more clock.txt

```
06:03:58 UTC Sat 01/01/2014
06:04:58 UTC Sat 01/01/2014
```

1.9.5. 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に番号をつけます。
- **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*] [**>** *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
```

1.10. 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 Chapter 1 *Fundamentals Command References* の”*Configuration file management commands*”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 RBAC 2-1
2.1. 概要 2-1
2.1.1. 許可の割り当て 2-1
2.1.2. ユーザロールの割り当て 2-3
2.2. 設定作業リスト 2-4
2.3. ユーザロールの作成 2-4
2.4. ユーザロールのルールの設定 2-5
2.4.1. 設定の制限とガイドライン 2-5
2.4.2. 設定手順 2-5
2.5. 機能グループの設定 2-6
2.6. リソースアクセスポリシーの設定 2-7
2.6.1. ユーザロールのインタフェースポリシーの設定 2-7
2.6.2. ユーザロールの VLAN ポリシーの変更 2-7
2.7. ユーザロールの割り当て 2-8
2.7.1. デフォルトユーザロール機能の有効化 2-8
2.7.2. リモート AAA 認証ユーザへのユーザロールの割り当て 2-9
2.7.3. ローカル AAA 認証ユーザへのユーザロールの割り当て 2-9
2.7.4. 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 2-10
2.8. 一時的なユーザロールの許可設定 2-11
2.8.1. 設定ガイドライン 2-11
2.8.2. ユーザロールの認証の設定 2-12
2.8.3. 一時的なユーザロールの許可の取得 2-13
2.9. RBAC 設定の表示と維持 2-13
2.10. RBAC の設定例 2-14
2.10.1. ローカル AAA 認証ユーザの RBAC の設定例 2-14
2.10.2. RADIUS 認証ユーザの RBAC の設定例 2-16
2.10.3. RBAC の一時的なユーザロールの許可の設定例 2-20
2.11. RBAC のトラブルシューティング 2-23
2.11.1. 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 2-23
2.11.2. RADIUS ユーザによるログインがいつも失敗する 2-23

2章 RBAC

2.1. 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。RBAC では、ユーザのアクセス制限のために、ユーザロール(role)を使用します。

RBAC は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、許可管理を容易にすることができます。

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、新たにユーザロールを作成、割り当てをすることだけで管理することが可能になります。たとえば、ユーザのジョブの責任を変更する場合、ユーザロールの許可を変更するか、新しいユーザロールを割り当てることができます。

2.1.1. 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。(セクション 1 *はじめに オペレーションマニュアルの”RBAC”の”ユーザロールのルール”*を参照してください。)
- アクセスを許可するインタフェース、VLAN を指定するアクセスポリシーを定義します。(セクション 1 *はじめに オペレーションマニュアルの”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、VLAN のリソースに関連したコマンドを使用するには、ユーザロールで、必要なコマンドとリソースにアクセスできるように設定します。

たとえば、ユーザロールは、**qos apply policy** コマンドと GigabitEthernet 1/0/1 インタフェースにアクセスできるように設定した場合、このユーザロールでは、interface view に移行し、**qos apply policy** コマンドを使用することができますが、ほかの interface view に入ることはできません。またほかのコマンドを使用することもできません。もしユーザロールでインタフェースへのアクセスを設定し、**qos apply policy** コマンドへのアクセス許可していない場合、**qos apply policy** コマンドを使用することはできません。

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もとづいて管理されます。

- **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セクション 1 *はじめに オペレーションマニュアル*の”*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 2-1 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** コマンド、**authentication-mode** コマンド、**protocol inbound** コマンド、**set authentication password** コマンド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 2-1 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。

ユーザロール名	許可
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**、**quit**、**ssh2**、**super**、**system-view**、**telnet**、**tracert** 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。もしユーザロールが **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。

2.1.2. 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依存し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、セクション 8 *セキュリティ オペレーションマニュアル*の”*AAA*”、”*SSH*”を参照してください。ユーザラインの詳細は、セクション 1 *はじめに オペレーションマニュアル*の”*ログイン*”、”*CLI によるログイン*”を参照してください。

2.2. 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
(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

2.3. 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、最大 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

2.4. 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。

2.4.1. 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とき、以下の制限とガイドラインに従ってください。

- 1 つのユーザロールには最大 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。

2.4.2. 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とき、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。

2.5. 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**	―
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 ⚠ **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。

2.6. リソースアクセスポリシーの設定

各ユーザロールは 1 つのインタフェースポリシー、VLAN ポリシーがあります。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 のユーザロールを設定することができます。設定されたポリシーは、設定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。

2.6.1. 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. user role 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。 このコマンドは**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 : user role interface policy viewでアクセス可能なインタフェースは設定されていません。 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。

2.6.2. ユーザロールの VLAN ポリシーの変更

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. user role 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。 このコマンドは**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 user role VLAN policy viewでアクセス可能なVLANは設定されていません。 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。

2.7. 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（セクション 1 *はじめに オペレーションマニュアル*の”*RBAC*”の”*ユーザロールの割り当て*”を参照してください）で割り当てる手順が異なります。AAA 認証の詳細は、セクション 8 *セキュリティ オペレーションマニュアル*の”*AAA*”を参照してください。

2.7.1. デフォルトユーザロール機能の有効化

AAA サーバがユーザロールをユーザに許可しない場合、デフォルトユーザロール機能は 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。

デフォルトユーザロールとしてシステムに存在するすべてのユーザロールを指定することができます。

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。

2.7.2. 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。

2.7.3. 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。もし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** }	―
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。

操作	コマンド	補足
4. （オプション設定項目）不要なユーザロールを削除する	**undo authorization-attribute user-role** *role-name*	ユーザは割り当てられたユーザロールに対してアクセス可能なシステムのアイテムとリソースを使用することができます。 ユーザロールが不要である場合（たとえばデフォルトユーザロール）、ユーザロールを削除するため、このコマンドを使用します。

2.7.4. 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セクション 1 *はじめに オペレーションマニュアル*の”*ログイン*”、”*CLI によるログイン*”を参照してください。SSH の詳細はセクション 8 *セキュリティ オペレーションマニュアル*の”*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**	―
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、セクション 1 *はじめに オペレーションマニュアル*の”*CLIによるログイン*”を参照してください。

操作	コマンド	補足
3. ユーザラインのユーザロールを指定する	**user-role** *role-name*	デフォルト：AUXユーザラインのユーザロールはnetwork-adminが指定されます。ほかのユーザラインのユーザロールは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。

2.8. 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。

2.8.1. 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 2-2 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しません。装置は**$enab***n*$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とき、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 のユーザロールの許可を取得する場合、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 2-2 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。
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。詳細はセクション 8 *セキュリティ オペレーションマニュアルの”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。もし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。

2.8.2. 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**	―

操作	コマンド	補足
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** *rolename*	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** *rolename*] [{ **hash** | **simple** } *password*]	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。 もし**role** *rolename*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。

2.8.3. 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
1. ユーザロールを使用した一時的な許可を取得する	**super** [*rolename*]	*rolename*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。

2.9. 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*]

操作	コマンド
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**]

2.10. RBACの設定例

2.10.1. ローカル AAA 認証ユーザの RBAC の設定例

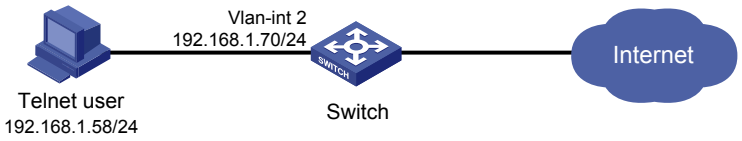
I. ネットワーク要件

図 2-1 に示すように、装置は 192.168.1.58 の 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 のみ設定できるようにします。

図 2-1 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 10～VLAN 20 のみ設定するユーザロールを許可するために VLAN ポリシーを変更します。

[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

```
New local user added.
```

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

ユーザからデフォルトユーザロール network-operator を削除します。この設定はユーザがユーザロール **role1** のみ許可されるようにするために行います。

[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 Tues 01/01/2013
```

[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.
```

2.10.2. RADIUS 認証ユーザの RBAC の設定例

I. ネットワーク要件

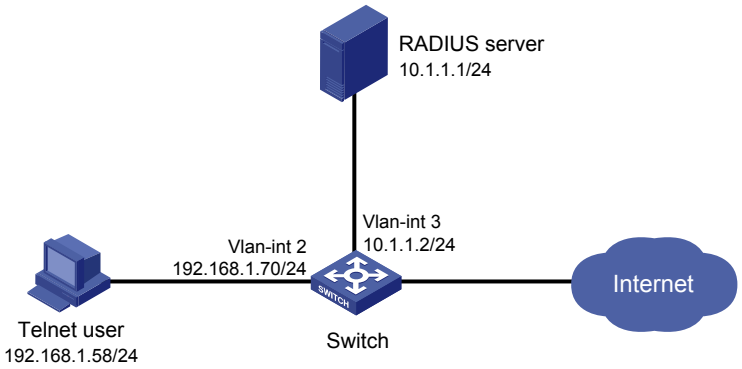
図 2-2 に示すように、装置は 10.1.1.1/24 の Free RADIUS サーバを使用し、192.168.1.58 の Telnet ユーザを含むログインユーザに AAA サービスを提供します。Telnet ユーザはユーザ名 **hello@bbb** を持ち、ユーザロール **role2** が割り当てられます。

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 1/0/20 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 2-2 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] 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 1/0/20 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 1/0/20

[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
…

(display 表示結果は省略します。)

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 1/0/20 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 1/0/2 と GigabitEthernet 1/0/22 を使用します。

[Switch] vlan 10

[Switch-vlan10] port gigabitethernet 1/0/2

[Switch-vlan10] port gigabitethernet 1/0/22

```
Permission denied.
```

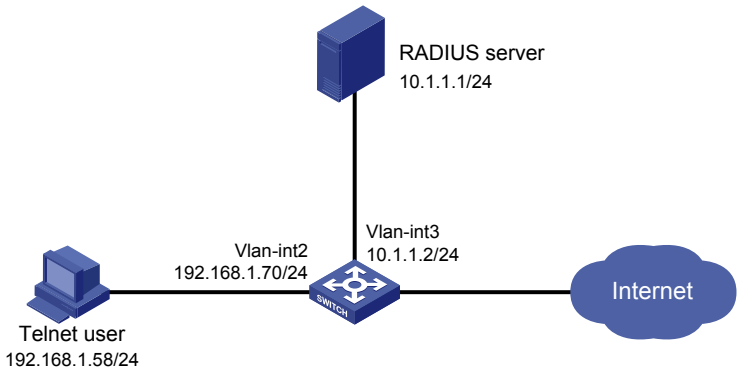
2.10.3. RBAC の一時的なユーザロールの許可の設定例

I. ネットワーク要件

図 2-3 に示すように、装置は 192.168.1.58 の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** が割りあてられます。

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 2-3 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。

[Router-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

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

[Switch-isp-bbb] authentication login local

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

[Switch-isp-bbb] authorization login local

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

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

[Switch] local-user test class manage

```
New local user added.
```

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

ユーザのパスワードを **aabbcc** に設定します。

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

level-0 をユーザに割り当てます。

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

デフォルトユーザロール network-operator を削除します。

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

[Switch-luser-manage-test] 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 192.168.1.59 ...

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とき、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。

2.11. 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。

2.11.1. 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。

2.11.2. 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。もし 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とき、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。

3 章 ログイン 3-1

3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やコンソール、Telnet、SSH、Web、SNMP を含む他のアクセス方法を変更することができます。

表 3-1 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	デフォルトでは、コンソールポートでのログインは有効、ユーザ名やパスワードの認証なし、ユーザロールは network-admin です。 ログイン後、装置のセキュリティの対応を行うため、パスワードあるいは認証スキームモードを設定します。
	Telnet 接続によるログイン	デフォルトでは Telnet 接続によるログインは無効です。 Telnet 接続によるログインを行うため、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	デフォルトでは SSH 接続によるログインは無効です。SSH 接続によるログインを行うため、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アクセス		デフォルトでWebインタフェースからのログインは無効です。Webインタフェースによるログインを行うため、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。
SNMP からのアクセス	デフォルトでは SNMP によるログインは無効です。 SNMP によるログインを行うため、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。

4 章 コンソールポートによる最初のログイン 4-1

4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)と端末エミュレーションプログラム(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。端末エミュレーションプログラムの使用方法についてはプログラムのユーザガイドあるいはオンラインヘルプを参照してください。

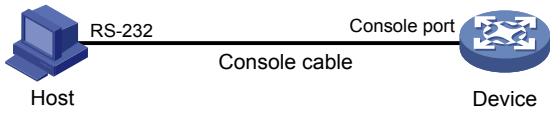
コンソールポートでログインする場合は以下の手順に従ってください。

1. PC のシリアルポートに Dsub9 ピンメスコネクタを接続します。
2. 装置のコンソールポートを確認し、装置のコンソールポートにコンソールケーブルの RJ-45 コネクタを接続します。

注意 ：

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 4-1 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 で端末エミュレーションソフトウェア(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

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

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。

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

目次

このセクションのページは **1-x-x** です。

5 章 CLI によるログイン 5-1
5.1. CLI によるログインについて 5-1
5.1.1. CLI 概要 5-1
5.1.2. ログイン認証モード 5-2
5.1.3. ユーザロール 5-2
5.2. 制限とガイドライン 5-3
5.3. コンソールポートあるいは USB からのローカルログイン 5-3
5.3.1. コンソールポートあるいは USB からのローカルログインについて 5-3
5.3.2. 制限とガイドライン 5-4
5.3.3. 設定作業リスト 5-4
5.3.4. コンソールポートあるいは USB ログインポートからのローカルログイン設定 5-4
5.3.5. AUX ユーザラインの共通設定 5-6
5.4. Telnet からのログイン 5-7
5.4.1. Telnet からのログインについて 5-7
5.4.2. 制限とガイドライン 5-7
5.4.3. 装置の Telnet ログインの設定 5-8
5.4.4. 装置から Telnet サーバへの Telnet 接続 5-13
5.5. SSH からのログイン 5-13
5.5.1. SSH について 5-13
5.5.2. 装置の SSH ログインの設定 5-14
5.5.3. 装置から SSH サーバへの SSH 接続 5-15
5.6. CLI ログインの表示と維持 5-16

5章 CLI によるログイン

5.1. CLIによるログインについて

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 を含む他のアクセス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、セクション 1 *はじめに オペレーションマニュアル* の”*ログインユーザの制御*”を参照してください。

5.1.1. CLI 概要

I. 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 5-1 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5-1 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
USBライン	USBポート
VTY(Virtual type terminal)ユーザライン	TelnetあるいはSSH

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、AUX、VTY、USB ラインの順番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)が設定されている場合、VTY インタフェースの VTY0 と VTY3 は空いています。ユーザが装置に Telnet を行うとき、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。

III. 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。

5.1.2. 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 5-2 のようにユーザラインで異なる設定が必要です。

表5-2 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、セクション 8 *セキュリティ オペレーションマニュアル*の”*AAA*”を参照してください。

5.1.3. ユーザロール

ユーザはログインするとき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、セクション 1 *はじめに オペレーションマニュアル*の”*RBAC*”を参照してください。

装置はログイン認証モード、ユーザタイプ、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。

- もし none あるいは password 認証モードが使用される場合、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。
- もし scheme 認証モードが使用される場合、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。

5.2. 制限とガイドライン

user line view と user line class view の両方で有効なコマンドで以下のルールを適用します。

- 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さま適用されます。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。

5.3. コンソールポートあるいはUSBからのローカルログイン

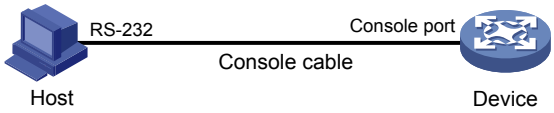
5.3.1. コンソールポートあるいは USB からのローカルログインについて

図 5-1 のように装置にログインし、管理するため、コンソールポートあるいは USB で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セクション 1 *はじめに オペレーションマニュアル*の”*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。

USB ポートを使用してログインする場合、以下の方法でログインすることができます。

1. 装置の USB ポートに bluetooth モデムを接続します。
2. bluetooth モデムに接続を確立するためモバイル端末を使用します。

図 5-1 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有効で、認証を必要としません。装置のセキュリティの対応を行うため、パスワードあるいは認証スキームモードを設定します。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。

デフォルトで USB ポートは有効で、認証を必要としません。装置のセキュリティの対応を行うため、パスワードあるいは認証スキームモードを設定します。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。

5.3.2. 制限とガイドライン

コンソールログインあるいは USB ログインの設定は、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。

5.3.3. 設定作業リスト

コンソールログインあるいは USB 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あるいはUSBログイン用のログイン認証の設定: 1. none 認証の設定 2. password 認証の設定 3. 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	―

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されません。次にログインするユーザのみ適用されます。

IRF スタックユニットを使用して複数の装置を構成する前に、各装置の AUX line class view に移行し、以下の設定を行ってください。

- 認証の無効化
- ユーザロール network-admin の割り当て

5.3.4. コンソールポートあるいは USB ログインポートからのローカルログイン設定

I. 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/USB line view に移行する **line** { **aux** | **usb** } *first-number* [*last-number*] • AUX line class view に移行する **line class** { **aux** | **usb** }	どちらか一方を使用します。
3. none 認証モードを有効にする	**authentication-mode none**	デフォルト：**none**
4. ユーザロールを割り当てる	**user-role** *role-name*	デフォルト：**network-admin**

コンソールポートあるいは USB ログインポートを使用して、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。

II. 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. AUX line view あるいは class view に移行する	• AUX line view に移行する **line** { **aux** | **usb** } *first-number* [*last-number*] • AUX line class view に移行する **line class** { **aux** | **usb** }	どちらか一方を使用します。
3. password 認証モードを有効にする	**authentication-mode password**	デフォルト：**none**
4. password を設定する	**set authentication password** { **hash** | **simple** } *password*	デフォルト：設定なし
5. ユーザロールを割り当てる	**user-role** *role-name*	デフォルト：**network-admin**

コンソールポートあるいは USB ログインポートを使用して、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。

III. 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. AUX line view あるいは class view に移行する	• AUX line view に移行する **line** { **aux** | **usb** } *first-number* [*last-number*] • AUX line class view に移行する **line class** { **aux** | **usb** }	どちらか一方を使用します。
3. scheme 認証を有効にする	**authentication-mode scheme**	デフォルト：**none**

scheme 認証を使用するため、以下の設定が完了している必要があります。

- ISP domain view でコンソールログイン方法を設定します。
- リモート認証を使用し、スキームを設定します。
- 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います。

詳細はセクション 8 *セキュリティ オペレーションマニュアル*の”*AAA*”を参照してください。

コンソールポートあるいは USB ログインポートを使用して、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。

5.3.5. AUX ユーザラインの共通設定

I. 制限とガイドライン

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。

II. 設定手順

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**	―
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** | **usb** } *first-number* [*last-number*] • AUX line class view に移行する **line class** { **aux** | **usb** }	どちらか一方を使用します。
3. 通信速度を設定する	**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** { **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に設定されると拡張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。

操作	コマンド	備考
7. 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ったり、異常な端末表示となる場合があります。
8. 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。
9. 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
10. 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に設定します。
11. 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 ユーザがuser lineを通してログインしたとき、指定されたコマンドを自動で実行し、コマンドを実行したのちユーザ接続を切断します。 AUX line viewあるいはAUX line class viewでは設定できません。

5.4. Telnetからのログイン

5.4.1. Telnet からのログインについて

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ができます。

5.4.2. 制限とガイドライン

Telnet ログインの設定は、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。

5.4.3. 装置の Telnet ログインの設定

I. 設定作業リスト

操作	備考
(必須設定項目) Telnetからのログイン認証の設定 1. none 認証の設定 2. password 認証の設定 3. 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	―
(オプション設定項目) VTYユーザラインの共通設定	―

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**	―
2. Telnet サーバを有効化する	**telnet server enable**	デフォルト：無効
3. 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。
4. 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。
5. (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**

図 5-2 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。もしログインユーザ数が最大である場合、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。

図 5-2 none 認証の Telnet 接続

```
<Switch>
```

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**	ー
2. Telnet サーバを有効にする	**telnet server enable**	デフォルト：無効
3. 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。
4. 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。
5. password の設定	**set authentication password** { **hash** | **simple** } *password*	デフォルト：設定なし
6. (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**

図 5-3 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。もしログインユーザ数が最大である場合、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。

図 5-3 password 認証による Telnet 接続

```
Password:
<Switch>
```

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**	ー
2. Telnet サーバを有効にする	**telnet server enable**	デフォルト：無効

操作	コマンド	備考
3. 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。
4. 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。

詳細はセクション 8 *セキュリティ オペレーションマニュアル*の”*AAA*”を参照してください。

図 5-4 のように次回 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。もしログインユーザ数が最大である場合、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。

図 5-4 Scheme 認証による Telnet 接続

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

V. 現在の Telnet ユーザの共通設定

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. 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Chapter 8 *Security Command References*の”*AAA commands*”を参照してください。
3. system view に移行する	**system-view**	―
4. 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

VI. VTY ユーザラインの共通設定

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。
3. 端末サービスを有効にする	**shell**	デフォルト：有効
4. 端末タイプを設定する	**terminal type** { **ansi** | **vt100** }	デフォルト：ANSI
5. 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。
6. 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。

操作	コマンド	備考
7. 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。
8. 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** プロトコルの変更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。 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。
9. 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 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。

5.4.4. 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。もし Telnet サーバが異なるサブネットにある場合、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 5-5 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**	―
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*]	―

5.5. SSHからのログイン

5.5.1. SSH について

SSH は、より強固なセキュリティを持ったログイン方法のアプローチです。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。詳細はセクション 8 *セキュリティ オペレーションマニュアル*の”*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 からのログインは無効です。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 ログインの設定を行う必要があります。

5.5.2. 装置の SSH ログインの設定

I. 装置の SSH ログインの設定手順について

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については、セクション 8 *セキュリティ オペレーションマニュアル*の"*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
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**	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さま適用されます。 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。

操作	コマンド	備考
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。
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** 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. (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Chapter 8 *Security Command References*の”*AAA commands*”を参照してください。
9. system view から戻る	**quit**	―
10. (オプション設定項目)VTY ユーザラインの共通設定	セクション1 *はじめに オペレーションマニュアル*の”*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。	―

5.5.3. 装置から SSH サーバへの SSH 接続

装置は SSH クライアントとして SSH サーバにログインすることができます。もし SSH サーバが異なるサブネットにある場合、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 5-6 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*
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については、セクション 8 *セキュリティ オペレーションマニュアル*の”*SSH*”を参照してください。

5.6. 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** | **usb** | **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** | **usb** | **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、ある接続を開放します。このコマンドで自分が使用している接続を開放することはできません。
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** | **usb** | **vty** } *num2* }	user viewで使用可能です。

目次

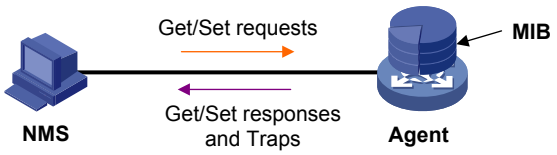
このセクションのページは **1-x-x** です。

6 章 SNMP によるログイン 6-1

6章 SNMP によるログイン

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 に関する詳細はセクション 10 *システム管理 オペレーションマニュアル*の”*SNMP* ”を参照してください。

デフォルトで SNMP は無効です。SNMP を使用して装置にアクセスするため、SNMP アクセス以外の他のログイン方法を用いて、SNMP アクセス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. ログインユーザの制御について 7-1
7.2. Telnet/SSH ログインの制御 7-1
7.2.1. Telnet ログインの制御 7-1
7.2.2. SSH ログインの制御 7-1
7.2.3. Telnet ログイン制御の設定例 7-1
7.3. Web ログインの制御 7-2
7.3.1. 送信元 IP アドレスベースの Web ログインの制御 7-2
7.3.2. 設定例 7-3
7.4. SNMP ログインの制御 7-4
7.4.1. 概要 7-4
7.4.2. SNMP ログインの制御の設定例 7-4

7章　ログインユーザの制御

7.1. ログインユーザの制御について

不正なアクセスを防ぐため ACL を使用し、ユーザのふるまいを監視/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 の詳細はセクション 7 *ACL and QoS オペレーションマニュアル*の”*ACL* ”を参照してください。

7.2. Telnet/SSHログインの制御

7.2.1. Telnet ログインの制御

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** *acl-number* • **telnet server ipv6 acl** [**ipv6**] *acl-number*	デフォルト：ACLはなし

7.2.2. SSH ログインの制御

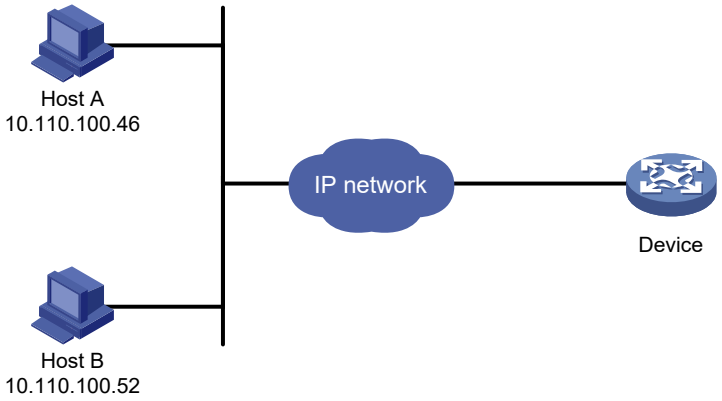
操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. SSH ログインをフィルタする ACL を適用する	• **ssh server acl** { *advanced-acl-number* | *basic-acl-number* | **mac** *mac-acl-number* } • **ssh server ipv6 acl** [**ipv6**] { *advanced-acl-number* | *basic-acl-number* | **mac** *mac-acl-number* }	デフォルト：ACLはなし 詳細はChapter 8 *Security Command References*の”*SSH commands*”を参照してください。

7.2.3. Telnet ログイン制御の設定例

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 number 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 ACL を適用します。

[Switch] telnet server acl 2000

7.3. 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。

7.3.1. 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。

以下に Web ログインを制御する設定を示します。

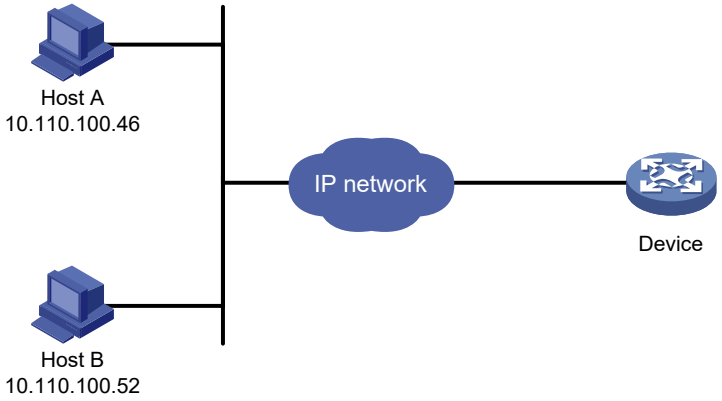
操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Web ログインをフィルタする ACL を適用する	• **ip http acl** *acl-number* • **ip https acl** *acl-number*	デフォルト：設定なし

7.3.2. 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
```

7.4. SNMPログインの制御

7.4.1. 概要

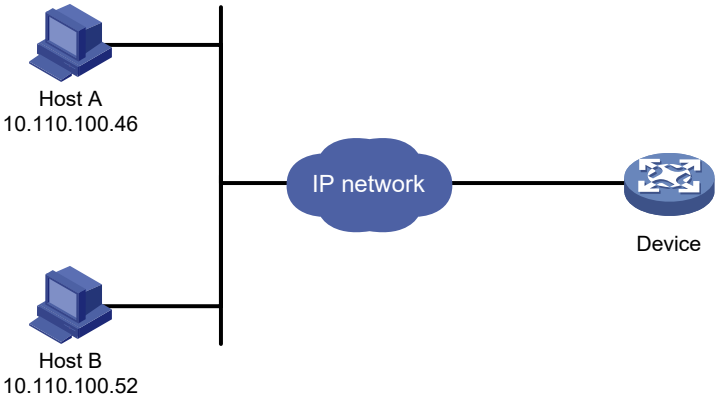
SNMP ログインの詳細はセクション 10 *システム管理 オペレーションマニュアル*の“*SNMP*”を参照してください。

7.4.2. SNMP ログインの制御の設定例

I. ネットワーク要件

図 7-3 のように装置が 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 number 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 FTP 8-1
8.1. FTP について 8-1
8.1.1. FTP のファイル転送モード 8-1
8.1.2. FTP 動作モード 8-1
8.2. FTP サーバの使用 8-1
8.2.1. FTP サーバ設定作業リスト 8-1
8.2.2. FTP の有効化 8-2
8.2.3. 認証および許可の設定 8-2
8.2.4. FTP サーバのアクセス制御 8-2
8.2.5. 接続パラメータの設定 8-3
8.2.6. 送信 FTP パケットの DSCP 値の設定 8-3
8.2.7. FTP 接続の手動解放 8-4
8.2.8. FTP サーバの表示と維持 8-4
8.2.9. FTP サーバ設定例 8-4
8.3. FTP クライアントの使用 8-6
8.3.1. FTP クライアント設定作業リスト 8-6
8.3.2. FTP 接続の確立 8-6
8.3.3. コマンドとヘルプ情報の表示 8-9
8.3.4. FTP サーバのファイルとディレクトリの表示 8-9
8.3.5. FTP サーバのディレクトリの管理 8-9
8.3.6. FTP クライアントのディレクトリの管理 8-10
8.3.7. FTP サーバのファイルの操作 8-10
8.3.8. 別のユーザアカウントへの変更 8-10
8.3.9. FTP 接続のメンテナンスとトラブルシューティング 8-11
8.3.10. FTP 接続の終了 8-11
8.3.11. FTP クライアントの表示と維持 8-11
8.3.12. FTP クライアント設定例 8-11

8章 FTP

8.1. FTPについて

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 は、TCP ポート 20 および 21 を使ってファイルを転送します。ポート 20 はデータの伝送に、ポート 21 は制御コマンドの伝送に使われます。FTP の詳細については、”RFC 959”を参照してください。

8.1.1. FTP のファイル転送モード

FTP は、2 つのモードでファイルを送信します。

- **Binary バイナリモード**–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”**.app**”、”**.bin**”、 ”**.btm**”のファイルです。
- **ASCII モード**–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。

デフォルトで FTP サーバは binary モードを使用します。

8.1.2. FTP 動作モード

FTP 動作モードは、以下のモードがあります。

- **Active モード(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 モード(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。

8.2. 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。

8.2.1. FTP サーバ設定作業リスト

FTP サーバを設定するには次の作業を行ってください。

作業リスト
(必須設定項目) FTPの有効化
(必須設定項目) 認証および許可の設定
(オプション設定項目) FTPサーバのアクセス制御
(オプション設定項目) 接続パラメータの設定
(オプション設定項目) 送信FTPパケットのDSCP値の設定
(オプション設定項目) FTP接続の手動解放

8.2.2. FTP の有効化

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

8.2.3. 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、も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、Chapter 8 *Security Command References* の”*AAA commands*”を参照してください。

8.2.4. FTP サーバのアクセス制御

I. FTP サーバのアクセス制御について

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

II. 制限とガイドライン

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

III. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. (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** { *advanced-acl-number* | *basic-acl-number* | **ipv6** { *advanced-acl-number* | *basic-acl-number* } }	デフォルト：設定なし

8.2.5. 接続パラメータの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. (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、これらの接続は終了します。
3. (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、Chapter 8 *Security Command Referencesの”AAA commands”*を参照してください。

8.2.6. 送信 FTP パケットの DSCP 値の設定

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) 送信 FTP パケットの DSCP 値を設定する	1. IPv4 で動作する FTP サーバ: **ftp server dscp** *dscp-value* 2. IPv6 で動作する FTP サーバ: **ftp server ipv6 dscp** *dscp-value*	デフォルト：0

8.2.7. 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	1. 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* 2. 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*]

8.2.8. 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。

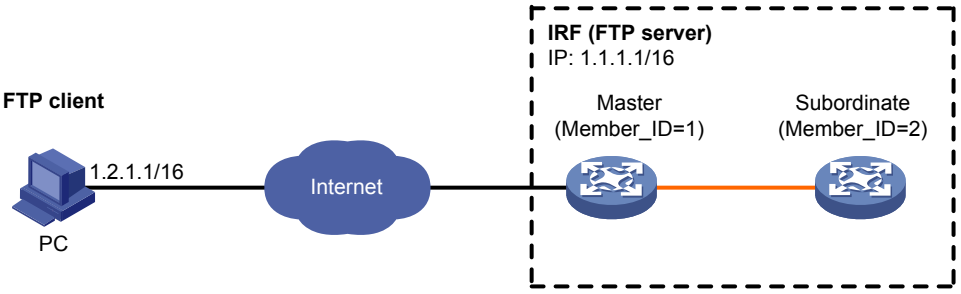
操作	コマンド
FTPサーバの設定とステータス情報を表示する	**display ftp-server**
オンラインFTPユーザの詳細情報を表示する	**display ftp-user**

8.2.9. FTP サーバ設定例

I. ネットワーク要件

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

図 8-1 ネットワーク図



Note: The orange line represents an IRF connection.

II. 設定手順

1. 図 8-1 に示すように IP アドレスを設定し、IRF スタックユニットと PC で互いに通信できることを確認します。(詳細は省略します。)
2. FTP サーバを設定します。

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

ローカルユーザアカウント **abc** を作成し、パスワードを **123456**、ユーザロールを **network-admin**、フラッシュのルートディレクトリを作業ディレクトリ、サービスタイプを FTP に設定します。(IRF スタックメンバ装置のフラッシュのルートディレクトリに作業ディレクトリを設定する場合、**authorization-attribute** コマンドの flash:/を slot2#flash:/.に置き換えます)

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

<Switch> system-view

[Switch] local-user abc class manage

[Switch-luser-abc] password simple 123456

ユーザにユーザロール network-admin を割り当てます。フラッシュメモリのルートディレクトリに作業ディレクトリを設定します。

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

サービスタイプ FTP をユーザに割り当てます。

[Switch-luser-abc] service-type ftp

[Switch-luser-abc] quit

FTP ユーザを有効にします。

[Switch] ftp server enable

[Switch] quit

3. FTP クライアントから FTP を実行します。

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

c:\> ftp 1.1.1.1

```
Connected to 1.1.1.1.
220 FTP service ready.
```

```
User(1.1.1.1:(none)):abc
331 Password required for abc.
Password:
230 User logged in.
```

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

ftp> ascii

```
200 TYPE is now ASCII
```

ftp> get config.cfg back-config.cfg

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

ftp> binary

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

ftp> put temp.bin

FTP からログアウトします。

ftp> bye

8.3. FTPクライアントの使用

8.3.1. FTP クライアント設定作業リスト

FTP サーバを設定するには次の作業を行ってください。

作業リスト
(必須設定項目) FTP接続の確立
(オプション設定項目) コマンドとヘルプ情報の表示
(オプション設定項目) FTPサーバのファイルとディレクトリを表示
(オプション設定項目) FTPサーバのディレクトリの管理
(オプション設定項目) FTPクライアントのディレクトリの管理
(オプション設定項目) FTPサーバのファイルの操作
(オプション設定項目) 別のユーザアカウントへの変更
(オプション設定項目) FTP接続のメンテナンスとトラブルシューティング
(オプション設定項目) FTP接続の終了

8.3.2. FTP 接続の確立

I. FTP 接続確率の設定作業リスト

FTP 接続を確立するには次の作業を行ってください。

作業リスト
(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
(必須設定項目) FTP接続の確立
(オプション設定項目) FTP転送モードと動作モードを設定する

II. 制限とガイドライン

ftp コマンドで設定された送信元 IP アドレスは **ftp client source** コマンドで設定されたコマンドより優先されます。

ftp ipv6 コマンドで設定された送信元 IP アドレスは **ftp client ipv6 source** コマンドで設定されたコマンドより優先されます。

III. 送信 FTP パケットの送信元 IP アドレスを設定する

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	• IPv4 **ftp client source** { **interface** *interface-type interface-number* | **ip** *source-ip-address* } • IPv6 **ftp client ipv6 source** { **interface** *interface-type interface-number* | **ipv6** *source-ipv6-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。 RFC3484で定義された送信元IPv6アドレスが自動で選択されます。

IV. FTP 接続の確立

操作	コマンド	補足
FTPサーバにログインする	• IPv4 1. (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-name* | *interface-type interface-number* } | **ip** *source-ip-address* }] * 2. (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*] • IPv6 1. (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** { **interface** *interface-type interface-number* | **ipv6** *source-ipv6-address* }] * [**-i** *interface-type interface-number*] 2. (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**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。 **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。

V. FTP 転送モードと動作モードを設定する

操作	コマンド	補足
FTP転送モードを設定する	1. ASCII に設定する **ascii** 2. 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

8.3.3. コマンドとヘルプ情報の表示

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	1. **help** [*command-name*] 2. **?** [*command-name*]

8.3.4. FTP サーバのファイルとディレクトリの表示

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	1. 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*]] 2. 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*]]

8.3.5. FTP サーバのディレクトリの管理

I. 前提条件

FTP サーバのディレクトリ、ファイルを表示する場合、**dir** コマンド、**ls** コマンドを使用します。

II. 操作方法

操作	コマンド
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*

8.3.6. FTP クライアントのディレクトリの管理

操作	コマンド	補足
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* **|** **/**]	―

8.3.7. FTP サーバのファイルの操作

I. 前提条件

FTP サーバのディレクトリ、ファイルを表示する場合、**dir** コマンド、**ls** コマンドを使用します。

II. 操作方法

操作	コマンド	補足
FTPサーバの指定したファイルを完全に削除する	**delete** *remotefile*	―
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*]	―
FTPサーバのファイルにFTPクライアントのファイルの内容を追記する	**append** *localfile* [*remotefile*]	―
ローカルファイルをアップロードする	**newer** *remotefile*	―

8.3.8. 別のユーザアカウントへの変更

I. 別のユーザアカウントへの変更について

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。

新しいアカウントに変更することで、FTP 接続を再確立することなく、異なるユーザ権限を取得することができます。

II. 制限とガイドライン

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。

III. 設定手順

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*]

8.3.9. FTP 接続のメンテナンスとトラブルシューティング

I. FTP 接続のメンテナンスとトラブルシューティングについて

FTP サーバに FTP 接続を確立したのち、このコマンドを使用して FTP 接続に関する問題を検出し、トラブルシューティングを行うことができます。

II. 設定手順

操作	コマンド	補足
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

8.3.10. 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	1. **disconnect** 2. **close**
F TPサーバとの接続を切断し、user viewに戻る	1. **bye** 2. **quit**

8.3.11. 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**

8.3.12. FTP クライアント設定例

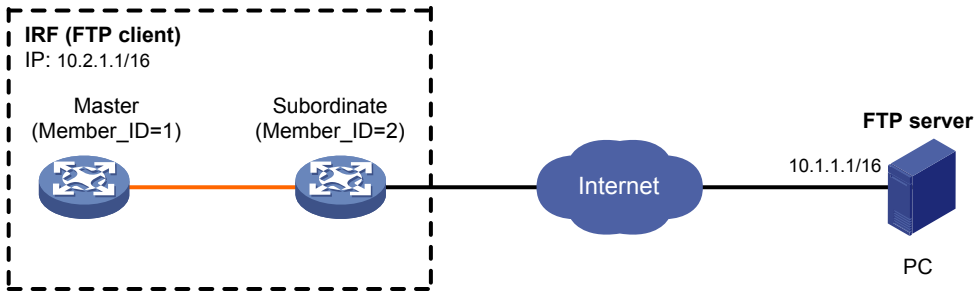
I. ネットワーク要件

図 8-2 に示すように PC は FTP サーバとして動作します。ユーザ名 **abc**、パスワード **123456** のユーザアカウントは PC 上で作成されています。

- FTP クライアントとして IRF スタックユニットが FTP サーバにログインします。
- FTP サーバから FTP クライアントに **temp.bin** ファイルをダウンロードします。

- バックアップ用として FTP クライアントから FTP サーバに設定ファイル **config.cfg** をアップロードします。

図 8-2 ネットワーク図



Note: The orange line represents an IRF connection.

II. 設定手順

図 8-2 に示すように IP アドレスを設定し、IRF スタックユニットと PC で互いに通信できることを確認します。(詳細は省略します。)

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

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

<Switch> ftp 10.1.1.1

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

ftp>

FTP 転送モードをバイナリに設定します。

ftp> binary

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

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

ftp> get temp.bin

```
227 Entering Passive Mode (192,168,0,20,207,117)
150 "C:\Users\wKF5122\Desktop\FTP\temp.bin" file ready to send (13507003 byt
es) in IMAGE / Binary mode
226 Transfer finished successfully.
```

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

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

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

ftp> ascii

```
227 Entering Passive Mode (192,168,0,20,207,237)
150 "C:\Users\wKF5122\Desktop\FTP\config.cfg" file ready to receive in ASCII
 mode
226 Transfer finished successfully.
5205 bytes sent in 0.000 seconds (11.28 Mbytes/s)
```

<Switch>

目次

このセクションのページは **1-x-x** です。

9 章 TFTP 9-1
9.1. TFTP について 9-1
9.2. 制限とガイドライン 9-1
9.3. IPv4 TFTP クライアントの設定 9-1
9.4. IPv6 TFTP クライアントの設定 9-2

9章 TFTP

9.1. TFTPについて

TFTP (Trivial File Transfer Protocol)は、セキュアな信頼されたネットワークにてファイルの転送を行うために、FTP を簡略化したプロトコルです。TFTP は UDP ポート 69 を使用してデータを送信します。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にて使用する場合に適しています。

9.2. 制限とガイドライン

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。もし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。もし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。

9.3. 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。

9.4. 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**	―
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** *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-ip-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**	―
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。

10 章 ファイルシステム管理……10-1
10.1. ファイルシステム管理について……10-1
10.1.1. 記憶媒体とファイルシステム……10-1
10.1.2. ディレクトリ……10-2
10.1.3. ファイル……10-2
10.1.4. ディレクトリ名とファイル名の仕様……10-3
10.2. 制限とガイドライン……10-4
10.3. ファイルシステムと記憶媒体の管理……10-5
10.3.1. マウントとアンマウント……10-5
10.3.2. 記憶媒体のフォーマット……10-5
10.3.3. 記憶媒体の回復……10-6
10.4. ファイルとディレクトリの管理……10-6
10.4.1. ファイルシステムのプロンプトモード設定……10-6
10.4.2. ディレクトリ情報の表示……10-6
10.4.3. テキストファイルの内容表示……10-7
10.4.4. カレント作業ディレクトリの表示……10-7
10.4.5. カレント作業ディレクトリの変更……10-7
10.4.6. ディレクトリの作成……10-7
10.4.7. ファイル名やディレクトリ名の変更……10-7
10.4.8. ファイルのコピー……10-7
10.4.9. ファイルの移動……10-8
10.4.10. ファイルの削除/回復……10-8
10.4.11. ディレクトリの削除……10-9
10.4.12. ファイルとディレクトリのアーカイブ(圧縮)……10-9
10.4.13. ファイルとディレクトリの解凍……10-9
10.4.14. ファイルの圧縮……10-10
10.4.15. ファイルの解凍……10-10

10章 ファイルシステム管理

この章では、記録媒体、ディレクトリ、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。

注意 ：
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。

10.1. ファイルシステム管理について

10.1.1. 記憶媒体とファイルシステム

装置はフラッシュメモリ、USB メモリの記憶媒体をサポートします。

I. 記憶媒体の命名ルール

フラッシュメモリのファイルシステムはフラッシュメモリと同一の名前です。名前は以下の部分があります。

- 記憶媒体のタイプ **flash**
- コロン（:）

USB ディスクと USB ディスクのファイルシステムは以下の部分があります。

- 記憶媒体のタイプ **usb**
- シーケンス番号、a、b、c のような小文字の英字
- パーティション番号、0 で固定です。

たとえば USB ディスクのファイルシステム名は **usba0:**です。

重要 ：
小文字で記憶媒体名を入力してください。

II. ファイルシステムの場所

Master 装置のファイルシステムを識別するため、ファイルシステムの位置を指定する必要がありません。

メンバ装置のファイルシステムを識別するため、**slot***n*#で指定する必要があります。*n* はメンバ装置の IRF スタックメンバ ID を示します。たとえば **slot2#**は IRF スタックメンバ装置 2 にあるファイルシステムを示します。

重要　：

スロットの文字列(IRF スタック時)は、小文字で入力してください。

III. デフォルトファイルシステム

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上で動作します。デフォルトファイルシステム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、稼働中のコンフィグレーションの設定をデフォルトファイルシステムの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、BootWare あるいは Boot ROM 画面で設定する必要があります。詳細は QX-S5300G シリーズインスタレーションマニュアルを参照してください。

10.1.2. ディレクトリ

ディレクトリはツリー型で構成されます。

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も呼ばれます。

III. ディレクトリの命名ルール

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。

10.1.3. 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。

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

10.1.4. ディレクトリ名とファイル名の仕様

I. ディレクトリ名の仕様

ディレクトリ名には、絶対パスと相対パスがあります。例えば作業ディレクトリは **flash:/**です。図 10-1 の test2 の設定には、以下の方法が使用できます。

- **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 10-1 ディレクトリ階層の例



II. ファイル名の仕様

ファイルを指定するとき、表 10-1 に示すフォーマットの 1 つでファイル名を入力する必要があります。ディレクトリを指定するとき、*drive* と *path* の引数のルールに従ってください。

表 10-1 ファイル名のフォーマット

フォーマット	説明	例
file-name	カレント作業ディレクトリのファイルを指定します。	**a.cfg**：**a.cfg**という名前のファイルがカレント作業ディレクトリの下にあることを示します。

フォーマット	説明	例
[path/]file-name	カレント作業ディレクトリの指定されたフォルダのファイルを指定します。 path引数は、フォルダ名を意味します。もしファイルが1層のフォルダにある場合、引数でフォルダ名を指定してください。 ファイルが多階層フォルダの下のファイルにある場合、スラッシュ（/）で各フォルダ名を分けてください。	**test/a.cfg**：**a.cfg**というファイルがカレント作業ディレクトリのtestフォルダの下にあることを示します。 **test/subtest/a.cfg**：**a.cfg**というファイルがカレント作業ディレクトリの**test**フォルダの下の**subtest**サブフォルダにあることを示します。
drive:/[path]/file-name	装置の記憶媒体の中のファイルを指定します。 drive引数は、記憶媒体名を意味します。 マスタ上の記憶媒体は、通常flash:あるいはcfa0:です。 複数の記憶媒体がある場合、drive引数は必要です。	**flash:/test/a.cfg**： **a.cfg**というファイルがフラッシュメモリのルートディレクトリの**test**フォルダの下にあることを示します。

10.2. 制限とガイドライン

- ファイル操作中に記憶媒体の抜き差し、あるいは IRF スタックの Master/Member 装置の切り替えは行わないでください。ファイルシステムが破損する恐れがあります。

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

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

USB メモリ上のファイル名の変更、ファイルの圧縮、解凍、削除、回復、移動、あるいは USB メモリにファイルのコピーを行う前に、USB メモリのプロテクトが解除されていることを確認してください。

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。

10.3. ファイルシステムと記憶媒体の管理

10.3.1. マウントとアンマウント

I. 制限とガイドライン

一般的に、ホットスワップ可能な記憶媒体は、装置に搭載されたとき自動的にマウントされます。もしシステムが自動で記憶媒体をマウントしなかった場合、記憶媒体にアクセスする前に手動でマウントさせる必要があります。

装置から記憶媒体を取り外すとき、装置から切断させるためにアンマウントする必要があります。アンマウントしなかった場合、記憶媒体のファイルや記憶媒体が破損する可能性があります。

USB メモリをアンマウントする場合、USB メモリが認識されており、USB メモリ LED が点滅していないことを確認する必要があります。そうでない場合、USB インタフェースあるいは USB メモリは破損する可能性があります。

記憶媒体をアンマウントする前に、他のユーザが記憶媒体にアクセスしていないことを確認してください。そうでない場合、アンマウントの処理は失敗します。

II. マウント設定手順

user view で以下の操作を実行します。

操作	コマンド	補足
記憶媒体をマウントする	**mount** *medium-name*	デフォルト : 装置に接続したとき記憶媒体は自動でマウントされます。

III. アンマウント設定手順

user view で以下の操作を実行します。

操作	コマンド	補足
記憶媒体をアンマウントする	**umount** *medium-name*	デフォルト : 装置に接続したとき記憶媒体は自動でマウントされます。

10.3.2. 記憶媒体のフォーマット

I. 制限とガイドライン

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。

II. 設定手順

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*

10.3.3. 記憶媒体の回復

I. 制限とガイドライン

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。そうでないと回復作業は失敗します。

II. 設定手順

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** *medium-name*

10.4. ファイルとディレクトリの管理

10.4.1. ファイルシステムのプロンプトモード設定

I. ファイルシステムのプロンプトモード設定について

ファイルシステムには、次の 2 つのプロンプトモードがあります。

- **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**:どのような操作に対しても、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。

II. 設定手順

以下にプロンプトモードの設定を示します。

操作	コマンド	補足
1. system view へ移行する	**system-view**	―
2. ファイルシステム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**

10.4.2. 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
ディレクトリあるいはファイルの情報を表示する	**dir** [**/all**] [*file-url* | **/all-filesystems**]

10.4.3. 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*

10.4.4. 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**

10.4.5. 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* | **..** | **/** }

10.4.6. 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*

10.4.7. ファイル名や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
ファイル名を変更する	**rename** *{ source-file | source-directory } { dest-file | dest-directory }*

10.4.8. 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* | *dest-directory* }

10.4.9. 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** *fileurl-source fileurl-dest*

10.4.10. ファイルの削除/回復

I. ファイルの削除/回復について

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。

記憶媒体は.trash というごみ箱を使用します。

II. 制限とガイドライン

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。

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。

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

III. ファイルの削除

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-url*
ファイルを完全に削除する	**delete /unreserved** *file-url*
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**]

IV. ファイルの回復

user view で以下の操作を実行します。

操作	コマンド
ファイルをごみ箱から元に戻す	**undelete** *file-url*

10.4.11. ディレクトリの削除

I. 制限とガイドライン

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。

II. 設定手順

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*

10.4.12. ファイルとディレクトリのアーカイブ(圧縮)

I. ファイルとディレクトリのアーカイブ(圧縮)について

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。

II. 設定手順

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** *fileurl-dest* [**verbose**] **source** { *fileurl-source-list* |*source-directory-list* } &<1-5>

10.4.13. ファイルとディレクトリの解凍

I. ファイルとディレクトリの解凍について

圧縮ファイルからファイルとディレクトリを解凍することができます。

II. 設定手順

user view で実行可能です。

操作	コマンド
ファイルを解凍する	**tar extract archive-file** *fileurl-dest* [**verbose**] [**screen** | **to** *directory-name*]
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** *fileurl-dest*

10.4.14. ファイルの圧縮

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** *filename*

10.4.15. ファイルの解凍

user view で以下の操作を実行します。

操作	コマンド
ファイルを解凍する	**gunzip** *filename*

目次

このセクションのページは **1-x-x** です。

11 章 コンフィグレーションファイル管理 11-1
11.1. 概要 11-1
11.1.1. コンフィグレーションタイプ 11-1
11.1.2. カレントコンフィグレーション読み込みプロセス 11-2
11.1.3. スタートアップコンフィグレーションファイルの冗長化 11-2
11.1.4. コンフィグレーションファイルの内容とフォーマット 11-3
11.2. カレントコンフィグレーションの保存 11-3
11.3. 2 つのコンフィグレーションファイルの設定の差分表示 11-5
11.4. 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設定 11-6
11.5. 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と復元 11-7
11.5.1. 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と復元 11-7
11.5.2. 前提条件 11-7
11.5.3. 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 11-8
11.5.4. 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 11-8
11.6. 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 11-9
11.7. コンフィグレーションファイルの表示と維持 11-9

11章 コンフィグレーションファイル管理

11.1. 概要

コンフィグレーションファイルは、装置のソフトウェア機能の設定のコマンドのセットを保存します。現在のコンフィグレーションファイルを再起動後にも適用させるため、保存します。将来使用するために、ホストにコンフィグレーションファイルのバックアップを行うことができます。

コンフィグレーションファイルを管理するため、CLI あるいは Boot メニューを使用することができます。この章では CLI のコンフィグレーションファイルの管理を記載します。

11.1.1. コンフィグレーションタイプ

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。スタートアップコンフィグレーションで起動されたのち、カレント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。(詳細はセクション 1 *はじめに オペレーションマニュアル*の”*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。)

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以下の方法があります。

- 装置を起動後に何も設定を変更しない状態で **display current-configuration** を実行します。
- 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。
- **display startup** コマンドでコンフィグレーションファイルのファイル名を表示し、スタートアップコンフィグレーションに設定されているファイルを **more** コマンドで表示します。

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はスタートアップコンフィグレーションと新しく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、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。

11.1.2. カレントコンフィグレーション読み込みプロセス

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“.cfg”ファイルというテキストファイル、拡張子が“.mdb”というバイナリデータを保存します。

- “.cfg”ファイルは人が読めるテキストファイルです。表示するには more コマンドを使用します。設定を保存する際の拡張子は“.cfg”を使用する必要があります。
- “.mdb”ファイルは装置が読み込むためのファイルです。装置は”.mdb“の方が”.cfg“よりも速く読み込みます。

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。ファイル選択のルールについては“スタートアップコンフィグレーションファイルの冗長化”を参照してください。
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。

もし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。

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

11.1.3. スタートアップコンフィグレーションファイルの冗長化

冗長化のために、通常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の他に、バックアップのスタートアップコンフィグレーションを設定しておくことができます。

システムは以下の順番で次回に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検索します。

1. 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検索します。
2. 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が無効あるいは不正である場合、次回の起動に使用する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検索します。

もし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。

11.1.4. 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。起動時、コンフィグレーションファイルの読み込み失敗を防ぐため、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。
- 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/LfDIf8ROLtV
ErJ/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
#
```

11.2. カレントコンフィグレーションの保存

I. カレントコンフィグレーションの保存方法について

カレントコンフィグレーションをコンフィグレーションファイルに保存するとき、次回に起動する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。(セクション 1 *はじめに オペレーション*マ

ニュアルの”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。

II. 制限とガイドライン

スタートアップコンフィグレーションの喪失を防ぐ為に、保存の最中に再起動や電源断が発生しないように注意してください。

IRF スタックの分裂によりメンバ装置が離れた後、メンバ装置の設定はカレントコンフィグレーション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はまだ保持されています。しかし IRF スタックユニットが回復する前にカレントコンフィグレーションの保存を行うと、メンバ装置の設定が次回の起動に使用するコンフィグレーションファイルから削除されます。

IRF スタックが分裂したのち、保存したカレントコンフィグレーションを次回の起動に使用するコンフィグレーションファイルに保存した場合、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回復するため以下の方法を使用します。

1. IRF スタックの分裂を直します。
2. 装置が IRF スタックユニットに再加入した後、メンバ装置を再起動します。
3. メンバ装置の設定が IRF スタックユニットのカレントコンフィグレーションに保持されていることを確認するため、**display current-configuration** コマンドを実行します。
4. カレントコンフィグレーションを次回の起動に使用するコンフィグレーションファイルに保存します。

⚠ 重要　：

コンフィグレーションの回復を正常に行う為、メンバ装置が離れている時に IRF スタックのほかの装置を再起動させないでください。

拡張インタフェースカードがシステムから取り外された時、設定はメモリに残されていますが、システムのカレントコンフィグレーションから削除されます。交換する拡張インタフェースカードを実装するまえにカレントコンフィグレーションを保存した場合、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から拡張インタフェースカードの設定が削除されます。

拡張インタフェースカードを取り外したのち、カレントコンフィグレーションを保存した場合、拡張インタフェースカードの設定を次回に起動するスタートアップコンフィグレーションに回復させる手順を以下に示します。

1. 交換する拡張インタフェースカードを実装します。
2. 交換する拡張インタフェースカードがオンラインになったのち、拡張インタフェースカードの設定が自動でメモリからカレントコンフィグレーションに回復したことを確認するため、**display current-configuration** コマンドを実行します。
3. カレントコンフィグレーションの設定を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に保存します。

⚠ 重要　：

コンフィグレーションの回復を正常に行う為、拡張インタフェースカードが取り外されたのちに装置を再起動させないでください。

III. 設定手順

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する （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ない）	**save** *file-url* [**all** | **slot** *slot-number*]	―
記憶媒体のルートディレクトリに現在の設定を保存し、次回のシステム起動で使用され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	**save** [**safely**] [**backup** | **main**] [**force**]	このコマンドはフラッシュメモリ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。 もし**safety**パラメータを使用した場合、コマンドはメインスタートアップコンフィグレーションファイルに設定を保存します。もし**force**パラメータを指定した場合、設定は既存の次回のシステム起動で使用されるコンフィグレーションファイルに保存します。**force**パラメータを指定しない場合、新規の次回のシステム起動で使用されるコンフィグレーションファイルに保存します。

11.3. 2つのコンフィグレーションファイルの設定の差分表示

I. コンフィグレーションファイルの設定の比較について

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ことができます。

比較を行うため、次回に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場合、システムは以下の順番で次回に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検索します。

1. 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検索します。
2. 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が無効あるいは不正である場合、次回の起動に使用する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検索します。

メインとバックアップ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が無効あるいは不正である場合、システムは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が存在しないと画面に表示します。

II. 設定手順

すべての view で 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ことができます。

操作	コマンド
指定された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*
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設定の差分を表示する	1. 方法 1 **display diff configfile** *file-name-s* **current-configuration** 2. 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に使用する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	1. 方法 1 **display diff configfile** *file-name-s* **startup-configuration** 2. 方法 2 **display diff startup-configuration configfile** *file-name-d*
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カレント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	1. 方法 1 **display diff current-configuration startup-configuration** 2. 方法 2 **display current-configuration diff** 3. 方法 3 **display diff startup-configuration current-configuration**

11.4. 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設定

I. 制限とガイドライン

注意　：

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

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。

II. 前提条件

IRF スタックユニットでは、指定されたコンフィグレーションファイルが有効であり、各メンバ装置上の記憶媒体のルートディレクトリに保存されていることを確認します。また、すべての IRF スタックメンバ装置間で記憶媒体が同じタイプであることを確認します。

III. 設定手順

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**]	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。 デフォルト：装置の種類によって異なります。 **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。

11.5. 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と復元

11.5.1. 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と復元

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ことができます。

11.5.2. 前提条件

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。

- サーバに読み書き許可があることを確認してください。
- 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が指定されていない場合、バックアップは失敗します。

11.5.3. 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

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
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* | **ipv6** *ipv6-server* } [*dest-filename*]	―

11.5.4. 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。

- 各メンバ装置のフラッシュメモリ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
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* | **ipv6** *ipv6-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**

11.6. 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

I. 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について

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することができます。

メイン、バックアップあるいは、メイン／バックアップの両方のコンフィグレーションファイルが削除されている場合、次回の起動は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。

II. 制限とガイドライン

⚠ 注意　：
この作業を行うと、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ファイルを、装置から完全に削除します。削除を行う前に必要に応じてバックアップを行ってください。

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。

III. 設定手順

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**]	

11.7. 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*]]]

操作	コマンド
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**

目次

このセクションのページは **1-x-x** です。

12 章 ソフトウェアのアップグレード 12-1
12.1. ソフトウェアのアップグレードについて 12-1
12.1.1. ソフトウェアタイプ 12-1
12.1.2. ソフトウェアリリース形式 12-1
12.1.3. アップグレード方法 12-2
12.1.4. ソフトウェアの読み込み 12-2
12.2. 制限とガイドライン 12-3
12.3. CLI アップグレード手順 12-3
12.3.1. アップグレード設定作業リスト 12-3
12.3.2. 前提条件 12-3
12.3.3. Boot ROM への Boot ROM イメージのアップグレード 12-4
12.3.4. スタートアップソフトウェアファイルの指定とアップグレードの完了 12-4
12.4. ソフトウェア設定の表示と維持 12-5
12.5. CLI によるソフトウェアアップグレード例 12-6
12.5.1. 再起動によるソフトウェアアップグレード例 12-6

12章 ソフトウェアのアップグレード

12.1. ソフトウェアのアップグレードについて

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。

この章では CLI からソフトウェアをアップグレードする方法について記載します。すべてのソフトウェアアップグレードを比較する場合、セクション 1 *はじめに オペレーションマニュアル*の”*ソフトウェアのアップグレード*”の”*アップグレード方法*”を参照してください。

12.1.1. 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。

Boot ROM イメージ―”.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**–Boot Rom イメージと 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 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。

12.1.2. ソフトウェアリリース形式

ソフトウェアは以下の形式でリリースされます。

- Boot イメージ、System ソフトウェアイメージは拡張子“.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。

メモ ：

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。

12.1.3. 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 • 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 • Comware イメージ	装置が正常に起動しないときに使用します。 この方法では、まずコンソールケーブルを接続してください。次に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。起動中の指示に従ってCtrl+Bを押すことでBootメニューにアクセスすることができます。 ⚠ **重要：** 他の手段がない場合にのみ、本方法を使用してください。

この章では CLI からのアップグレードのみ記載します。

12.1.4. ソフトウェアの読み込み

I. 起動用ソフトウェアイメージ

Comware イメージは、メイン（プライマリ）とバックアップの 2 セットを指定することができます。Comware イメージの Boot イメージとシステムイメージは同じ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。もし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。

II. 起動時のソフトウェア読み込みプロセス

装置は BootROM イメージの読み込みと初期化を実施した後に以下の手順で起動を行ないます。

1. メインイメージを読み込みます。
2. メインイメージが存在しないか使用できない時、バックアップイメージを読み込みます。
3. バックアップイメージが存在しないか使用できない時、装置は起動を中断します。

12.2. 制限とガイドライン

正しく起動させる為に、起動用ソフトウェアは装置のフラッシュメモリに保存してください。USB メモリに置く場合、USB メモリを起動中は抜かないようにしてください。

12.3. CLIアップグレード手順

12.3.1. アップグレード設定作業リスト

作業リスト
(オプション設定項目) Boot ROMにBoot ROMイメージを読み込ませます。 Boot ROMイメージが必要な場合、続くアップグレード時間を短縮させるために行います。予期しない電気的な故障によって引き起こされるアップグレードの問題を避けることができます。 この処理を省略した場合、装置は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ときに自動でBoot ROMをアップグレードします。
(必須設定項目) スタートアップソフトウェアファイルとして指定します。
(オプション設定項目) マスタ装置からメンバ装置への同期 メンバ装置の持っているスタートアップソフトウェアがマスタ装置と異なる場合に使用できます。

12.3.2. 前提条件

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 コマンドで完全に削除します。詳細は、セクション 1 *はじめに オペレーションマニュアルの”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 の設定や操作方法についての詳細は、セクション 1 *はじめに オペレーションマニュアルの”FTP”、”TFTP”*を参照してください。

12.3.3. Boot ROM への Boot ROM イメージのアップグレード

user view で以下の操作を実行します。

操作	コマンド	補足
記憶媒体のルートディレクトリからBoot ROMの通常のエリアへBoot ROMイメージをアップグレードする	**bootrom update file** *file-url* **slot** *slot-number-list*	*file-url*はダウンロードしたソフトウェアファイルを指定します。新しいBoot ROMイメージは再起動後に適用されます。

12.3.4. スタートアップソフトウェアファイルの指定とアップグレードの完了

全装置のスタートアップソフトウェアファイルを一括指定する場合、user view で以下の操作を実行します。

操作	コマンド	補足
1. すべての装置の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	1. アプローチ 1: **boot-loader file** *ipe-filename* **all** { **backup** | **main** } 2. アプローチ 2: **boot-loader file boot** *filename* **system** *filename* [feature filename&<*1-30*>] **all** { **backup** | **main** }	―
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. 装置を再起動する	**reboot**	起動後、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。

各装置個別にスタートアップソフトウェアファイルを指定する場合、user view で以下の操作を実行します。

操作	コマンド	補足
1. IRF スタックのマスタ装置の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	1. アプローチ 1: **boot-loader file** *ipe-filename* **slot** *slot-number* { **backup** | **main** } 2. アプローチ 2: **boot-loader file boot** *filename* **system** *filename* [feature filename&<*1-30*>]**slot** *slot-number* { **backup** | **main** }	―
2. IRF スタックのメンバ装置のメイン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	1. アプローチ 1: **boot-loader file** *ipe-filename* **slot** *slot-number* { **backup** | **main** } 2. アプローチ 2: **boot-loader file boot** *filename* **system** *filename* [feature filename&<*1-30*>]**slot** *slot-number* { **backup** | **main** }	1つの装置のみアップグレードする場合、省略してください。
3. 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。
4. 装置の再起動	**reboot**	起動後、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。
5. (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。

12.4. ソフトウェア設定の表示と維持

すべての view で **display** コマンドを実行できます。

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*]

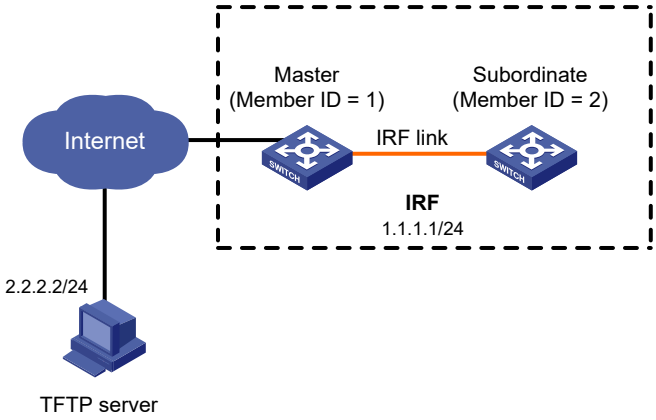
12.5. CLIによるソフトウェアアップグレード例

12.5.1. 再起動によるソフトウェアアップグレード例

I. ネットワーク要件

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

図 12-1 ネットワーク図



II. 設定手順

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

装置と TFTP サーバの両方で TFTP の設定を行います。(詳細は省略します。)

カレントソフトウェアの情報を表示します。

<Switch> display version

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

<Switch> tftp 2.2.2.2 get startup-a2105.ipe

ソフトウェアファイル **startup-a2105-backup.ipe** をバックアップします。もし記憶媒体に十分な空きスペースがない場合、この作業はスキップします。

<Switch> copy startup-a2105.ipe startup-a2105_backup.ipe

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

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

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

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

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

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

スタートアップソフトウェアの設定を確認します。

<Switch> display boot-loader

装置の再起動を行い、アップグレードを完了させます。

<Switch> reboot

III. 設定の確認

装置が正しいソフトウェアで動作しているか確認します。

<Switch> display version

目次

このセクションのページは **1-x-x** です。

13 章 ISSU 13-1
13.1. 概要 13-1
13.1.1. ISSU の利点 13-1
13.1.2. ISSU の方法 13-1
13.2. 制限とガイドライン 13-2
13.3. ISSU の必要条件 13-3
13.3.1. コンソールポートを通した装置へのログイン 13-3
13.3.2. 装置の動作状態の確認 13-3
13.3.3. アップグレードイメージの準備 13-3
13.3.4. ISSU 方法の識別 13-3
13.3.5. 機能の状態の確認 13-3
13.3.6. アップグレード手順の決定 13-4
13.3.7. 稼働中の設定の適用と保存 13-4
13.4. issu コマンドによる ISSU の実行 13-5
13.4.1. 複数の IRF スタックメンバでの ISSU の実行 13-5
13.4.2. 複数の IRF スタックメンバでの ISSU の互換性のないバージョンの ISSU の実行 13-7
13.4.3. 1 つの IRF スタックメンバでの互換性のあるバージョンの ISSU の実行 13-8
13.4.4. 1 つの IRF スタックメンバでの互換性のないバージョンの ISSU の実行 13-9
13.5. ISSU の表示と維持 13-10
13.6. ISSU の設定例 13-10
13.6.1. 現在のネットワークの状態と要件の解析 13-10
13.6.2. 実行手順 13-11

13章 ISSU

13.1. 概要

ISSU(In-Service Software Upgrade)は、パケット転送の中断を最小限にし、ソフトウェアのアップグレードを行うことができる機能です。

特に指定しない限り、この章で使用する“アップグレード”はソフトウェアのアップグレードとダウングレードの両方を示します。

13.1.1. ISSU の利点

装置のソフトウェアには、ブートソフトウェア、システムソフトウェアが含まれます。ISSU はソフトウェアのアップグレードを分けてアップグレードすることができます。

13.1.2. ISSU の方法

ISSU はソフトウェアのバージョン間の互換性に依存したソフトウェアリリースによって決定します。

ISSU の前に、**display version comp-matrix file** コマンドを使用して、旧/新のソフトウェアの互換性を表示し、推奨するアップグレード(アップグレード方法の列)の ISSU 方法について示します。ISSU 方法が異なると、異なるアップグレード手順が必要であり、現在のサービスに異なる影響をもたらします。

ISSU は以下のアップグレードタイプがあります。

- **互換性のあるバージョンの ISSU アップグレード**－新しいソフトウェアバージョンが稼働中のソフトウェアバージョンと互換性があります。アップグレードタイプを表 13-1 に示します。
- **互換性のないバージョンの ISSU アップグレード**－新しいソフトウェアバージョンが稼働中のソフトウェアバージョンと互換性がありません。2 つのバージョンは同時に動作させることができません。

  このアップグレードタイプは 1 つのアップグレード方法(互換性のないアップグレードと呼ばれます)しかサポートしません。コントロールプレーンとデータプレーンの両方をアップグレードするために、この方法はコールドリブートが必要です。ハードウェアの冗長性が有効でないならば、互換性がないアップグレードはサービスの中断が発生します。

ISSU 方法の識別については、セクション 1 *はじめに オペレーションマニュアル*の“*ISSU*”の“*ISSU 方法の識別*”を参照してください。

表 13-1 互換性のあるバージョンの ISSU アップグレード

ISSU 方法	説明
インクリメントアップグレード • サービスアップ	インクリメントアップグレードは、新しいソフトウェアと古いソフトウェア間の違いを解析し、異なる部分のみアップグレードします。 サービスを継続するには、バックアッププロセスが必要であり、メ

ISSU 方法	説明
グレード • ファイルアップグレード	インプロセスとバックアッププロセスの切り替えが必要です。 • **サービスアップグレード**–この方法はアップグレードされたサービスモジュールのみ関係します。ほかのサービスモジュールはアップグレード中に通常のサービスを提供します。 • **ファイルアップグレード**–この方法は、隠しシステムプログラムファイルのみ関係します。アップグレード中、システムは動作し、通常のサービスを提供します。
リブート	⚠ **注意:** ハードウェアの冗長性がない場合、リブート方法は、サービスの中断が避けられません。アップグレードによるサービス中断に対する影響を最小化するように、計画的に停止時間をスケジュールしてください。 アップグレードを完了させるため、メンバ装置をアップグレードします。1つのメンバ装置が再起動している間、他のメンバ装置はサービスを提供することができます。

13.2. 制限とガイドライン

ISSU を行う間、以下の制限とガイドラインに従ってください。

- 以下の処理は実行することができません。
  - メンバ装置の再起動
  - ISSU に関係しないコマンドの実行
  - ソフトウェアイメージファイルの変更、削除、名前の変更
- サービス継続性を向上させるには、ISSU を 1 ステップで実行しない限り、推奨される ISSU 手順に従ってください。次のステップに進む前に、ステップが完了していることを確認してください。
- 以下のコマンドを実行する前に、システムの動作状態を確認する前に **display device** コマンドを使用してください。
  - **issu load** コマンド
  - **issu run switchover** コマンド
  - **issu commit** コマンド

  もしシステムに何らかの問題がある場合、ISSU を行う前にシステムのトラブルシュートを行ってください。
- ソフトウェアイメージのすべて、あるいは一部のソフトウェアイメージをアップグレードするため、issu コマンドを使用してください。ソフトウェアイメージの一部のみアップグレードする場合、新しいイメージが、アップグレードしないイメージと互換性があることを確認してください。競合している場合、アップグレードは失敗します。

ISSU を行った後、装置の設定を行う場合、装置に再ログインしてください。

13.3. ISSUの必要条件

ISSU を正しく実行するために、すべての必要条件が行われていることを確認してください。

13.3.1. コンソールポートを通した装置へのログイン

コンソールポートを通して装置にログインしてください。Telnet あるいは SSH を使用している場合、ISSU が完了する前に装置から切断する必要があります。

複数のユーザがいる場合、装置へのログインは 1 管理者のみとし、ほかの管理者はアップグレード中にログインしないでください。

13.3.2. 装置の動作状態の確認

display device コマンドを使用して、システムの動作状態を確認し、システムが正常に動作していることを確認してください。

13.3.3. アップグレードイメージの準備

1. **dir** コマンドを使用して IRF スタックメンバの記憶媒体に IPE ファイルとソフトウェア用の十分な空き容量があることを確認してください。記憶媒体に十分な空き容量が無い場合、**delete /unreserved** *file-url* コマンドを使用して不要なファイルを削除してください。パラメータを使用した場合、**/unreserved** 削除したファイルは復旧できません。詳細はセクション 1 *はじめに オペレーションマニュアルの“ファイルシステムの管理”*を参照してください。
2. FTP あるいは TFTP を使用して、ソフトウェアファイルあるいは IPE ファイルをマスタの記憶媒体のルートディレクトリにダウンロードあるいはアップロードしてください。

13.3.4. ISSU 方法の識別

display version comp-matrix file コマンドを使用して、旧/新のソフトウェアの互換性を表示し、推奨するアップグレード(アップグレード方法の列)の ISSU 方法について示します。

- 互換性のあるアップグレードが必要な場合、推奨される ISSU 方式を識別するため **Upgrade Way** フィールドを確認してください。
- 互換性のないアップグレードが必要な場合、**Incompatible upgrade** 文字列のコマンド出力を確認してください。

ISSU のアップグレードタイプについては表 13-1 を参照してください。

13.3.5. 機能の状態の確認

ISSU を行っている間にサービスを継続するため、以下の機能の設定を行ってください。

機能	設定要件
GR、NSR	LDP、RSVP、OSPF、BGP、FSPFを含んだGRあるいはNSRを有効にしてください。

機能	設定要件
BFD	LDP、RSVP、OSPF、RIP、BGP、VRRP、NQAを含んだBFDを無効にしてください。ISSUを実行中にサービスが中断される可能性があります。
リンクアグリゲーション	ダイナミックアグリゲーショングループのすべてのメンバーポートでLACPタイムアウト間隔（**lacp period short**コマンドは設定されません。）を長くしてください。もし短いとトラフィックの転送がアップグレード中に中断される可能性があります。
IRFスタック	IRFスタックユニットで互換性のアップグレードを実行する前にIRF MADが無効であることを確認してください。 IRF MADを使用する場合、アップグレードが完了した後、IRF MADを有効にしてください。 IRFスタックbridge MACアドレスの保持の設定を以下のようにしてください。 • 互換性のあるバージョンにアップグレードするため、**irf mac-address persistent timer** コマンドあるいは **irf mac-address persistent always** コマンドを使用して、IRF スタック bridge MAC アドレスの保持を設定してください。 • IRF スタックを互換性のないバージョンにアップグレードするため、IRF スタックのブリッジの MAC アドレスが、**issu load** コマンドが要求するメンバ装置の MAC アドレスである場合、**irf mac-address persistent always** コマンドを使用してください。

13.3.6. アップグレード手順の決定

1. ハードウェアの冗長性の条件を識別してください。

   以下の条件の場合、ISSU はサービスを維持することができます。

   - IRF スタックユニットに複数のメンバが存在し、リングトポロジを使用しています。

重要:

ハードウェアの冗長性がない場合、アップグレードを行う間、サービスの中断が避けられません。アップグレードによるサービス中断に対する影響を十分に考慮してください。

2. セクション 1 *はじめに オペレーションマニュアル*の“*ISSU*”の“*ISSU コマンドによる ISSU の実行*”に示す手順を実行してください。

13.3.7. 稼働中の設定の適用と保存

1. 新しいソフトウェアバージョンでサポートしていないコマンドを削除してください。
2. 稼働中の設定を保存するため、**save** コマンドを使用してください。

13.4. issuコマンドによるISSUの実行

メモ ：

- **issu load** コマンドを実行すると、指定した Standby 装置が自動的に再起動します。再起動中に **issu rollback** コマンドを実行すると、正常に動作しないことがありますので、再起動中に **issu rollback** コマンドを実行しないでください。
- **issu rollback-timer** コマンドを変更する場合は、装置の再起動時間より大きい値にしてください。再起動中にロールバックタイマがタイムアウトすると、正常に動作しないことがあります。
- ソフトウェア bin ファイルを指定してアップデートする場合、**issu load file boot** *filename* **system** *filename* **feature** *filename* **slot** *slot-number* コマンドを使用して Freeradius の feature イメージを一緒にアップデートする必要があります。QX-S5300G シリーズは Radius サーバ機能をサポートしていません。

13.4.1. 複数の IRF スタックメンバでの ISSU の実行

I. 制限とガイドライン

最初にメンバ装置をアップグレードしてください。そして元のマスタ装置を含む残りのメンバ装置をアップグレードしてください。

II. 設定手順

操作	コマンド	補足
1. (オプション設定項目)ロールバックタイマを設定する	1. system view へ移行する **system-view** 2. ロールバックタイマを設定する **issu rollback-timer** *minutes* 3. user view へ戻る **quit**	デフォルト：45分 **issu run switchover**コマンドを実行したとき、タイマは開始します。
2. システムの動作状態を確認する	**display device**	次のステップに移行する前にシステムが動作していることを確認してください。
3. IRF スタックメンバのメインで起動するソフトウェアアップグレードを指定し、メンバのソフトウェアをアップグレードする	• アプローチ 1 **issu load file** { **boot** *filename* | **system** *filename* | **feature** *filename* }*** slot** *slot-number*&<1-9> • アプローチ 2 **issu load file ipe** *ipe-filename* **slot** *slot-number*&<1-9>	アップグレードされるIRFスタックメンバのメンバIDを**slot** *slot-number*&<1-9>オプションで指定します。

操作	コマンド	補足
4. システムの動作状態を確認する	**display device**	次のステップに移行する前にシステムが動作していることを確認してください。前のステップでエラーがあった場合、**issu rollback**コマンドでアップグレードをロールバックしてください。
5. マスタ/メンバの切り替えを実行する	**issu run switchover**	タイマが満了する前に**issu accept**コマンドあるいは**issu commit**コマンドを実行しない場合、システムは自動的に元のソフトウェアバージョンにロールバックします。
6. (オプション設定項目)アップグレードを許可し、自動ロールバックタイマを削除する	**issu accept**	―
7. システムの動作状態を確認する	**display device**	次のステップに移行する前にシステムが動作していることを確認してください。前のステップでエラーがあった場合、**issu rollback**コマンドでアップグレードをロールバックしてください。
8. ISSU プロセスを完了するため、(元のマスタを含む)アップグレードされた IRF スタックメンバをアップグレードする	**issu commit slot** *slot-number*	1つのIRFスタックメンバをアップグレードさせるため、**issu commit**コマンドを使用した後、別のメンバのアップグレードを行う前に、メンバが再起動し、IRFスタックに加入するのを待つ必要があります。すべてのメンバがアップグレードされた後、ISSUプロセスは終了し、ISSUの状態は初期状態に移行します。
9. ISSU が完了していることを確認する	**display issu state**	**ISSU state**フィールドが**Init**である場合、ISSUが完了しています。

13.4.2. 複数の IRF スタックメンバでの ISSU の互換性のないバージョンの ISSU の実行

I. 制限とガイドライン

最初にメンバ装置をアップグレードしてください。そして元のマスタ装置を含む残りのメンバ装置をアップグレードしてください。

II. 設定手順

操作	コマンド	補足
1. システムの動作状態を確認する	**display device**	次のステップに移行する前にシステムが動作していることを確認してください。
2. IRF スタックメンバをアップグレードし、IRF スタックメンバ用にメインで起動するソフトウェアのアップグレードソフトウェアを設定する	• アプローチ 1 **issu load file** { **boot** *filename* | **system** *filename* | **feature** *filename* } * **slot** *slot-number*&<1-9> • アプローチ 2 **issu load file ipe** *ipe-filename* **slot** *slot-number*&<1-9>	IRFスタックのメンバのメンバIDを**slot** *slot-number*&<1-9>オプションで指定します。IRFスタックのメンバ装置がリング構成で接続されている場合、NECはサービス中断を削減するため、このコマンドで半分のメンバを指定することを推奨します。IRFスタックのメンバは物理的に接続されていることを確認してください。
3. システムの動作状態を確認する	**display device**	次のステップに移行する前にシステムが動作していることを確認してください。前のステップでエラーがあった場合、**issu rollback**コマンドでアップグレードをロールバックしてください。
4. ISSU プロセスを完了するため、すべてのアップグレードされていないメンバをアップグレードさせ、IRF スタックのマスタ/メンバの切り替えを行う	**issu run switchover**	すべてのメンバがアップグレードされた後、ISSUプロセスは終了し、ISSUの状態は初期状態に移行します。

操作	コマンド	補足
5. ISSU が完了していることを確認する	**display issu state**	**ISSU state**フィールドが**Init**である場合、ISSUが完了しています。

13.4.3. 1 つの IRF スタックメンバでの互換性のあるバージョンの ISSU の実行

互換性のあるバージョンにインクリメントアップグレードを実行するため、user view で以下のコマンドを実行します。

操作	コマンド	補足
1. システムの動作状態を確認する	**display device**	次のステップに移行する前にシステムが動作していることを確認してください。
2. IRF スタックメンバをアップグレードし、IRF スタックメンバ用にメインで起動するソフトウェアのアップグレードソフトウェアを設定する	• アプローチ 1 **issu load file** { **boot** *filename* | **system** *filename* | **feature** *filename* } * **slot** *slot-number* • アプローチ 2 **issu load file ipe** *ipe-filename* **slot** *slot-number*	IRFスタックメンバのメンバIDを**slot** *slot-number*オプションで指定します。
3. システムの動作状態を確認する	**display device**	次のステップに移行する前にシステムが動作していることを確認してください。前のステップでエラーがあった場合、**issu rollback**コマンドでアップグレードをロールバックしてください。

操作	コマンド	補足
4. ISSU プロセスを完了させる	**issu commit slot** *slot-number*	ー
5. ISSU が完了していることを確認する	**display issu state**	**ISSU state**フィールドが**Init**である場合、ISSUが完了しています。

13.4.4. 1 つの IRF スタックメンバでの互換性のないバージョンの ISSU の実行

操作	コマンド	補足
1. システムの動作状態を確認する	**display device**	次のステップに移行する前にシステムが動作していることを確認してください。
2. IRF スタックメンバをアップグレードし、IRF スタックメンバ用にメインで起動するソフトウェアのアップグレードソフトウェアを設定する	• アプローチ 1 **issu load file** { **boot** *filename* | **system** *filename* | **feature** *filename* } * **slot** *slot-number* • アプローチ 2 **issu load file ipe** *ipe-filename* **slot** *slot-number*	IRFスタックメンバのメンバIDを**slot** *slot-number*オプションで指定します。

操作	コマンド	補足
3. ISSU が完了していることを確認する	**display issu state**	**ISSU state**フィールドが**Init**である場合、ISSUが完了しています。

13.5. ISSUの表示と維持

特に明記されていない限り、**issu** コマンドが使用されているかどうかに関係なく、ISSU で **display** コマンドと **reset** コマンドを使用できます。

display コマンドはすべての view で実行し、**reset** は user view で実行します。

操作	コマンド	補足
ロールバックタイマの情報を表示する	**display issu rollback-timer**	—
ISSU状態を表示する	**display issu state**	—
ソフトウェアの互換性を表示する	**display version comp-matrix file** { **boot** *filename* | **system** *filename* } * **display version comp-matrix file ipe** *ipe-filename*	—

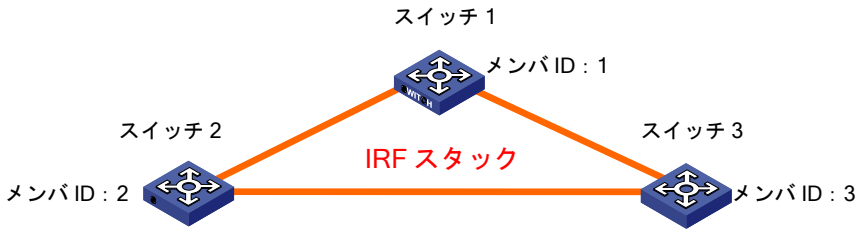
13.6. ISSUの設定例

13.6.1. 現在のネットワークの状態と要件の解析

I. アップグレード要件

図 13-1 にスイッチ 1、2、3 の 3 台で IRF スタックを構成しています。Master スイッチのメンバ ID は 1 で、優先度は 10 です。スイッチ 2 のメンバ ID は 2 で、優先度は 9 です。スイッチ 3 のメンバ ID は 3 で、優先度は 1 です。ISSU プロセスの間、指定された Standby スイッチとして、スイッチ 2 を選択します。

図 13-1 IRF スタック構成図



13.6.2. 実行手順

メモ:

- ISSU によってソフトウェアをアップグレードする場合は、system イメージと boot イメージの指定だけではアップグレードできません。**issu load file boot** *filename* **system** *filename* **feature** *filename* **slot** *slot-number* コマンドで feature イメージを一緒に指定してください。
- 実行手順は boot イメージと system イメージによる手順を示しています。QX-S5300G シリーズ bin ファイルを使用して ISSU でアップグレードするときは、feature イメージを一緒に指定してください。
- QX-S5300G シリーズは Radius サーバ機能をサポートしていません。アップグレード時に feature イメージの指定が必要ですが、機能はサポートしていません。

I. 必要条件

TFTP サーバの準備

新しいソフトウェアファイルを取得します。TFTP クライアントがファイルにアクセスできるように、TFTP サーバの作業ディレクトリにファイルを保存します。

II. ISSU の準備

1. ソフトウェアファイル soft-version2.ipe のダウンロード

各 IRF スタックメンバ装置のフラッシュのルートディレクトリにソフトウェアファイル soft-version2.ipe をダウンロードし、各 IRF スタックユニットにソフトウェアをコピーします。

<IRF>tftp 192.168.1.95 get soft-version2.ipe

```
Press CTRL+C to abort.
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 75.8M  100 75.8M    0     0   120k      0  0:10:45  0:10:45 --:--:--  110k
```

<IRF> copy soft-boot-version2.bin slot2#flash:/

<IRF> copy soft-system-version2.bin slot2#flash:/

<IRF> copy soft-boot-version2.bin slot3#flash:/

<IRF> copy soft-system-version2.bin slot3#flash:/

2. IRF スタックメンバ装置の状態の確認

すべての IRF スタックメンバ装置が正しく動作していることを確認します。

<IRF>display device

```
Slot Type                State    Subslot  Soft Ver            Patch Ver
1    QX-S5324GT-4X1C     Master   0        1.1.1               None
2    QX-S5324GT-4X1C     Standby  0        1.1.1               None
3    QX-S5324GT-4X1C     Standby  0        1.1.1               None
```

3. 現在のソフトウェアファイルの確認

IRF スタックメンバ装置の現在のソフトウェアファイルが同じであるかどうかを確認します。もし異なる場合、ISSU を行うことができません。

<IRF> display boot-loader

```
Software images on slot 1:
Current software images:
  flash:/soft-boot-version1.bin
  flash:/soft-system-version1.bin
Main startup software images:
  flash:/soft-boot-version1.bin
  flash:/soft-system-version1.bin
Backup startup software images:
  None
Software images on slot 2:
Current software images:
  flash:/soft-boot-version1.bin
  flash:/soft-system-version1.bin
Main startup software images:
  flash:/soft-boot-version1.bin
  flash:/soft-system-version1.bin
Backup startup software images:
  None
Software images on slot 3:
Current software images:
  flash:/soft-boot-version1.bin
  flash:/soft-system-version1.bin
Main startup software images:
  flash:/soft-boot-version1.bin
  flash:/soft-system-version1.bin
Backup startup software images:
  None
```

<IRF>

4. 新しいソフトウェアファイルの確認

新しいソフトウェアファイルが各 IRF スタックメンバ装置のフラッシュに保存されていることを確認します。もし保存されていない場合、ISSU を行うことができません。

Master スイッチのフラッシュに新しいソフトウェアファイル、ブートファイルが保存されていることを確認します。

<IRF> dir

```
Directory of flash:
   0 drw-           - Feb 26 2016 06:47:02   diagfile
   1 -rw-         735 Feb 25 2016 06:38:35   hostkey
   2 -rw-        3116 Jan 02 2011 23:22:10   ifindex.dat
   3 -rw-           0 Jan 01 2011 00:25:00   lauth.dat
   4 drw-           - Jan 01 2011 00:00:23   license
   5 drw-           - Jan 17 2011 20:02:46   logfile
   6 -rw-    11402240 Feb 24 2016 04:59:23   soft-boot-version1.bin
   7 -rw-    11816960 Jan 01 2011 00:28:48   soft-boot-version2.bin
   8 -rw-    68128768 Feb 24 2016 05:05:16   soft-system-version1.bin
   9 -rw-    70636544 Jan 01 2011 00:31:11   soft-system-version2.bin
  10 drw-           - Jan 01 2011 04:05:07   pkey
  11 drw-           - Jan 01 2011 04:04:21   pki
  12 drw-           - Jan 17 2011 20:06:56   seclog
  13 -rw-         591 Feb 25 2016 06:38:38   serverkey
  14 -rw-        8567 Jan 02 2011 23:22:12   startup.cfg
  15 -rw-      197812 Jan 02 2011 23:22:13   startup.mdb
  20 drw-           - Jan 01 2011 03:30:44   versionInfo


401390 KB total (297818 KB free)
```

<IRF>

新しいソフトウェアファイル soft-system-version2.bin、ブートファイル soft-boot-version2.bin が Master スイッチのフラッシュに保存されています。

Standby スイッチ 2 のフラッシュに新しいソフトウェアファイル、ブートファイルが保存されていることを確認します。

<IRF> dir slot2#flash:/

```
Directory of slot2#flash:
   0 drw-           - Feb 26 2016 06:47:08   diagfile
   1 -rw-         735 Jan 01 2011 00:44:28   hostkey
   2 -rw-        3116 Jan 02 2011 23:22:10   ifindex.dat
   3 -rw-           0 Jun 25 2013 06:13:35   lauth.dat
   4 drw-           - Jan 01 2011 00:00:26   license
   5 drw-           - Jan 01 2011 00:10:13   logfile
   6 -rw-    11402240 Feb 24 2016 04:59:23   soft-boot-version1.bin
   7 -rw-    11816960 Jan 01 2011 00:28:48   soft-boot-version2.bin
   8 -rw-    68128768 Feb 24 2016 05:05:16   soft-system-version1.bin
   9 -rw-    70636544 Jan 01 2011 00:31:11   soft-system-version2.bin
  10 drw-           - Jan 01 2011 00:52:47   pkey
  11 drw-           - Jan 01 2011 00:52:47   pki
  12 drw-           - Jan 01 2011 00:00:25   seclog
```

```
  13 -rw-         591 Jan 01 2011 00:44:30   serverkey
  14 -rw-        8567 Jan 02 2011 23:22:12   startup.cfg
  15 -rw-      197812 Jan 02 2011 23:22:18   startup.mdb
  20 drw-           - Jan 02 2011 04:07:05   versionInfo

380674 KB total (356610 KB free)
```

新しいソフトウェアファイル soft-system-version2.bin、ブートファイル soft-boot-version2.bin が Standby スイッチ 2 のフラッシュに保存されています。

Standby スイッチ 3 のフラッシュに新しいソフトウェアファイル、ブートファイルが保存されていることを確認します。

<IRF> dir slot3#flash:/

```
Directory of slot3#flash:
   0 drw-           - Jan 01 2011 00:01:28   diagfile
   1 -rw-         735 Jan 02 2011 23:40:43   hostkey
   2 -rw-        1782 Jan 01 2011 00:15:30   ifindex.dat
   3 -rw-           0 Jan 03 2011 02:34:17   lauth.dat
   4 drw-           - Jan 01 2011 00:00:28   license
   5 drw-           - Jan 01 2011 00:28:06   logfile
   6 -rw-    11402240 Jun 18 2015 17:38:05   soft-boot-version1.bin
   7 -rw-    11816960 Jan 07 2011 04:37:18   soft-boot-version2.bin
   8 -rw-    68128768 Jun 18 2015 17:38:05   soft-system-version1.bin
   9 -rw-    70636544 Jan 07 2011 04:39:47   soft-system-version2.bin
  10 drw-           - Jan 03 2011 23:05:00   pkey
  11 drw-           - Jan 03 2011 23:04:59   pki
  12 drw-           - Jan 01 2011 00:00:28   seclog
  13 -rw-         591 Jan 02 2011 23:40:45   serverkey
  20 -rw-        5269 Jan 01 2011 00:15:32   startup.cfg
  21 -rw-      177319 Jan 03 2011 03:33:52   startup.mdb
  22 drw-           - Jan 01 2011 00:43:58   versionInfo

380674KB total (356610 KB free)
```

出力では、新しいソフトウェアファイル soft-system-version2.bin、ブートファイル soft-boot-version2.bin が Standby スイッチ 3 のフラッシュに保存されています。

5. 設定の保存

<IRF> save

```
The current configuration will be written to the device. Are you sure? [Y/N]:y
Please input the file name(*.cfg)[flash:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
flash:/startup.cfg exists, overwrite? [Y/N]:y
Validating file. Please wait...
Saved the current configuration to mainboard device successfully.
Slot 2:
Save next configuration file successfully.
Slot 3:
Save next configuration file successfully.
```

<IRF>

設定が各 IRF スタックメンバ装置の設定ファイルに保存されます。

6. ソフトウェアファイルの互換性の確認

現在のソフトウェアファイルと新しいソフトウェアファイルの互換性を確認します。

<IRF> display version comp-matrix file boot flash:/soft-boot-version2.bin system flash:/soft-system-version2.bin

出力は、装置によって異なります。

a. 互換性がある場合

```
Slot                    Upgrade Way
1                       ISSU Reboot
2                       ISSU Reboot
```

新しいソフトウェアと現在のソフトウェアの互換性があることを示しています。互換性 ISSU 方式で ISSU を実行できます。

b. 互換性がない場合

```
Upgrade Way: Incompatible upgrade.
```

新しいソフトウェアと現在のソフトウェアの互換性がないことを示しています。非互換性 ISSU 方式で ISSU を実行できます。

III. 互換性 ISSU 方式でのアップグレードの実行

指定された Standby スイッチのアップグレードを行います。アップグレード後、新しい Master スイッチになります。この例では Standby スイッチのメンバ ID は 2 です。

<IRF> system-view

<IRF>issu load file boot flash:/soft-boot-version2.bin system flash:/soft-system-version2.bin slot 2

```
This operation will delete the rollback point information for the previous upgrade and
maybe get unsaved configuration lost. Continue? [Y/N]:y
Verifying the file flash:/soft-boot-version2.bin on slot 1...Done.
Verifying the file flash:/soft-system-version2.bin on slot 1........Done.
File flash:/soft-boot-version2.bin already exists on slot 2.
File flash:/soft-system-version2.bin already exists on slot 2.
Overwrite the existing files? [Y/N]:n
Verifying the file flash:/soft-boot-version2.bin on slot 2............Done.
Verifying the file flash:/soft-system-version2.bin on slot
2.............................................................Done.
Upgrade summary according to following table:

flash:/soft-boot-version2.bin
  Running Version             New Version
  1.1.1                       1.1.2

flash:/soft-system-version2.bin
  Running Version             New Version
  1.1.1                       1.1.2
```

```
  Slot                          Upgrade Way
  2                             Reboot
Upgrading software images to compatible versions. Continue? [Y/N]:y
This operation maybe take several minutes, please wait...
```

Standby スイッチの再起動後、Standby スイッチのソフトウェアファイル名が version2 であることを確認します。

[IRF] display boot-loader

```
Software images on slot 1:
Current software images:
  flash:/soft-boot-version1.bin
  flash:/soft-system-version1.bin
Main startup software images:
  flash:/soft-boot-version1.bin
  flash:/soft-system-version1.bin
Backup startup software images:
  None
Software images on slot 2:
Current software images:
  flash:/soft-boot-version2.bin
  flash:/soft-system-version2.bin
Main startup software images:
  flash:/soft-boot-version2.bin
  flash:/soft-system-version2.bin
Backup startup software images:
  None
Software images on slot 3:
Current software images:
  flash:/soft-boot-version1.bin
  flash:/soft-system-version1.bin
Main startup software images:
  flash:/soft-boot-version1.bin
  flash:/soft-system-version1.bin
Backup startup software images:
  None
```

<IRF>

Standby スイッチのソフトウェアのファイル名は soft-system-version2.bin、ブートソフトウェアのファイル名は soft-boot-version2.bin です。

Master スイッチを手動で再起動します。

<IRF> issu run switchover

```
Upgrade summary according to following table:

flash:/soft-boot-version2.bin
  Running Version             New Version
```

```
  1.1.1                         1.1.2

flash:/soft-system-version2.bin
  Running Version               New Version
  1.1.1                         1.1.2
  Slot                          Switchover Way
  1                             Master subordinate switchover
Upgrading software images to compatible versions. Continue? [Y/N]:y
This operation maybe take several minutes, please wait...
```

Masterスイッチのメンバ ID は 1 です。再起動後、IRF スタックユニットの Master スイッチは Standby スイッチになります。Standby スイッチ 2 の優先度が Standby スイッチ 3 の優先度よりも高いため、Standby スイッチ 2 が新しい Master スイッチになります。

ISSU を許可し、ロールバックタイマを削除します。

<IRF> issu accept

IRF スタックユニット 1 をアップグレードします。

<IRF> issu commit slot 1

```
Upgrade summary according to following table:

flash:/soft-boot-version2.bin
  Running Version               New Version
  1.1.1                         1.1.2

flash:/soft-system-version2.bin
  Running Version               New Version
  1.1.1                         1.1.2

  Slot                          Upgrade Way
  1                             Reboot
Upgrading software images to compatible versions. Continue? [Y/N]:y
This operation maybe take several minutes, please wait...
```

IRF スタックユニット 3 をアップグレードします。

<IRF> issu commit slot 3

```
File flash:/soft-boot-version2.bin already exists on slot 3.
File flash:/soft-system-version2.bin already exists on slot 3.
Overwrite the existing files? [Y/N]:n
Verifying the file flash:/soft-boot-version2.bin  on slot 3............Done.
Verifying the file flash:/soft-system-version2.bin on slot
3.............................................................Done.
Upgrade summary according to following table:

flash:/soft-boot-version2.bin
  Running Version               New Version
```

```
  1.1.1                        1.1.2

flash:/soft-system-version2.bin
  Running Version              New Version
  1.1.1                        1.1.2

  Slot                         Upgrade Way
  3                            Reboot
Upgrading software images to compatible versions. Continue? [Y/N]:y
This operation maybe take several minutes, please wait...
```

ISSU プロセスが完了し、すべての IRF スタックメンバ装置のソフトウェアファイル、ブートソフトウェアファイルは新しいバージョンにアップグレードされます。

IRF スタックメンバ装置の現在のソフトウェアファイルが soft-system-version2.bin、ブートソフトウェアファイルが soft-boot-version2.bin であることを確認します。

<IRF> display boot-loader

```
Software images on slot 1:
Current software images:
  flash:/soft-boot-version2.bin
  flash:/soft-system-version2.bin
Main startup software images:
  flash:/soft-boot-version2.bin
  flash:/soft-system-version2.bin
Backup startup software images:
  None
Software images on slot 2:
Current software images:
  flash:/soft-boot-version2.bin
  flash:/soft-system-version2.bin
Main startup software images:
  flash:/soft-boot-version2.bin
  flash:/soft-system-version2.bin
Backup startup software images:
  None
Software images on slot 3:
Current software images:
  flash:/soft-boot-version2.bin
  flash:/soft-system-version2.bin
Main startup software images:
  flash:/soft-boot-version2.bin
  flash:/soft-system-version2.bin
Backup startup software images:
  None
```

<IRF>

IV. 非互換性 ISSU 方式でのアップグレードの実行

指定された Standby スイッチのアップグレードを行います。アップグレード後、新しい Master スイッチになります。この例では Standby スイッチのメンバ ID は 2 です。

<IRF> system-view

<IRF>issu load file boot flash:/soft-boot-version2.bin system flash:/soft-system-version2.bin slot 2

```
This operation will delete the rollback point information for the previous upgrade and
maybe get unsaved configuration lost. Continue? [Y/N]:y
flash:/soft-boot-version2.bin already exists on slot 2.
flash:/soft-system-version2.bin already exists on slot 2.
Overwrite it?[Y/N]:n

flash:/soft-boot-version2.bin
  Running Version             New Version
  1.1.1                       1.1.2

flash:/soft-system-version2.bin
  Running Version             New Version
  1.1.1                       1.1.2

  Slot                        Upgrade Way
  2                           Reboot
Upgrading software images to incompatible versions. Continue? [Y/N]:y
```

Standby スイッチの再起動後、アップグレードされていないすべての IRF スタックメンバ装置の再起動とアップグレードを行います。

<IRF> issu run switchover

```
flash:/soft-boot-version2.bin
  Running Version             New Version
  1.1.1                       1.1.2

flash:/soft-system-version2.bin
  Running Version             New Version
  1.1.1                       1.1.2

  Slot                        Upgrade Way
  1                           Reboot
Upgrading software images to incompatible versions. Continue? [Y/N]:y
```

ISSU プロセスが完了し、すべての IRF スタックメンバ装置のソフトウェアファイル、ブートソフトウェアファイルは新しいバージョンにアップグレードされます。

IRF スタックメンバ装置の現在のソフトウェアファイルが soft-system-version2.bin、ブートソフトウェアファイルが soft-boot-version2.bin であることを確認します。

<IRF>display boot-loader

```
Software images on slot 1:
Current software images:
  flash:/soft-boot-version2.bin
  flash:/soft-system-version2.bin
Main startup software images:
  flash:/soft-boot-version2.bin
  flash:/soft-system-version2.bin
Backup startup software images:
  None
Software images on slot 2:
Current software images:
  flash:/soft-boot-version2.bin
  flash:/soft-system-version2.bin
Main startup software images:
  flash:/soft-boot-version2.bin
  flash:/soft-system-version2.bin
Backup startup software images:
  None
Software images on slot 3:
Current software images:
  flash:/soft-boot-version2.bin
  flash:/soft-system-version2.bin
Main startup software images:
  flash:/soft-boot-version2.bin
  flash:/soft-system-version2.bin
Backup startup software images:
  None
```

<IRF>

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. 装置管理作業リスト 14-1
14.2. 装置名の設定 14-1
14.3. システムクロックの設定 14-2
14.3.1. システムクロックの設定 14-2
14.3.2. 制限とガイドライン 14-2
14.3.3. 設定作業リスト 14-2
14.3.4. CLI でのシステムクロックの設定 14-2
14.3.5. NTP を使用したシステムクロックの設定 14-3
14.3.6. タイムゾーンの設定 14-3
14.3.7. サマータイムを設定する 14-3
14.4. 著作権情報表示の有効化 14-3
14.5. バナーの設定 14-4
14.6. パスワードリカバリ機能の無効化 14-5
14.7. USB インタフェースの無効化 14-6
14.8. シャットダウンインターバルの設定 14-6
14.9. メモリ使用しきい値の設定 14-6
14.10. リソース監視の設定 14-8
14.11. 装置の温度アラームのしきい値の設定 14-9
14.12. メモリのパリティエラーアラームの設定 14-11
14.13. エアフローの方向の設定 14-11
14.14. 実装しているトランシーバの確認 14-12
14.14.1. 実装しているトランシーバの確認 14-12
14.15. スケジュール自動実行の設定 14-12
14.15.1. スケジュール自動実行について 14-12
14.15.2. 制限とガイドライン 14-12
14.15.3. 設定手順 14-13
14.15.4. スケジュール自動実行設定例 14-14
14.16. 装置の再起動 14-18
14.16.1. 装置の再起動について 14-18
14.16.2. 制限とガイドライン 14-18
14.16.3. CLI による装置の即時再起動 14-18
14.16.4. 装置のスケジュール再起動 14-19
14.17. CPU 使用率のモニタリングの設定 14-19
14.18. 電源オフアラームの設定 14-20
14.19. 装置管理の情報表示と維持 14-21

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. 装置管理作業リスト

作業リスト
(必須設定項目) 装置名の設定
(必須設定項目) システムクロックの設定
(オプション設定項目) 著作権情報表示の有効化
(オプション設定項目) バナーの設定
(オプション設定項目) パスワードリカバリ機能の無効化
(オプション設定項目) USBインタフェースの無効化
(オプション設定項目) 検出間隔の設定
(必須設定項目) メモリ使用しきい値の設定
(必須設定項目) 装置の温度アラームのしきい値の設定
(必須設定項目) メモリのパリティエラーアラームの設定
(必須設定項目) エアフローの方向の設定
(必須設定項目) 実装したトランシーバの確認
(オプション設定項目) スケジュール自動実行の設定
(オプション設定項目) 装置の再起動

14.2. 装置名の設定

I. 装置名の設定について

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。

II. 設定手順

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
system view に移行する	**system-view**	―
装置名を設定する	**sysname** *sysname*	デフォルト：装置名

14.3. システムクロックの設定

14.3.1. システムクロックの設定

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必須です。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以下の方法で設定できます。

- **None**－ローカルシステムクロック。CLI を用いて手動でシステムクロックを設定します。
- **NTP**－NTP クロックソース。装置が NTP のシステムクロックを使用したとき、手動でシステムクロックを変更できません。NTP についての詳細は、セクション 10 *システム管理 オペレーションマニュアル*の”*NTP*”を参照してください。

装置は UTC を使用してシステムクロックを計算します。

14.3.2. 制限とガイドライン

clock protocol none コマンドを設定した後、タイムゾーンあるいはサマータイムが設定されているかどうかにかかわらず **clock datetime** コマンドでシステムクロックを決定します。

装置がシステムクロックを設定した後、タイムゾーンあるいはサマータイムを設定あるいは変更する場合、装置はシステムクロックを再計算します。システムクロックを表示する場合、**display clock** コマンドを使用します。

14.3.3. 設定作業リスト

作業リスト
(必須設定項目) 以下の2つから、システムクロックの設定方法を選択します。 • CLI でのシステムクロックの設定 • NTP を使用したシステムクロックの設定
(オプション設定項目) タイムゾーンの設定
(オプション設定項目) サマータイムの設定

14.3.4. CLI でのシステムクロックの設定

操作	コマンド	補足
system view に移行する	**system-view**	―
システムクロックのソースにローカルシステムクロックを指定する	**clock protocol none**	デフォルト：**NTPクロックソース**
user view に移行する	**quit**	―
UTC 時間を設定する	**clock datetime** *time date*	デフォルト：UTC 00:00:00 on 01/01/2013

14.3.5. NTP を使用したシステムクロックの設定

操作	コマンド	補足
system view に移行する	**system-view**	―
システムクロックのソースに NTP クロックソースを指定する	**clock protocol ntp**	デフォルト：**NTPクロックソース**

NTP についての詳細は、セクション 10 *システム管理 オペレーションマニュアル*の”*NTP*”を参照してください。

14.3.6. タイムゾーンの設定

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

14.3.7. サマータイムを設定する

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

14.4. 著作権情報表示の有効化

I. 著作権情報表示について

著作権情報の表示を有効にすると、以下のときに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装置にログインした後に user view を終了します。この場合、装置は自動でコンソールセッションを再起動しようとします。

著作権情報の表示を無効にしてある場合、一切表示されることはありません。

II. 設定手順

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

14.5. バナーの設定

I. バナーについて

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

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。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。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。
- **Shell** バナー – ユーザが user view にアクセスした後に表示します。

システムは、Legal バナー、MOTD バナー、Login バナー、Shell バナーの順でバナーを表示します。

II. 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。このとき、コマンドキーワードを含む入力テキストは 510 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。この場合は、2000 文字まで入力できます。

  - **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

    <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。

    <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。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
```

III. 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
system view に移行する	**system-view**	ー
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
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
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
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：設定なし

14.6. パスワードリカバリ機能の無効化

I. パスワードリカバリ機能について

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。

II. 設定手順

操作	コマンド	補足
system view に移行する	**system-view**	ー
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. USBインタフェースの無効化

I. USB インタフェースの無効化について

USB インタフェースを使用してファイルのダウンロードやアップロードを行うことができます。デフォルトで USB インタフェースは有効です。必要に応じて USB インタフェースを無効にすることができます。

II. 前提条件

このコマンドを実行する前に **umount** コマンドですべての USB パーティションをアンマウントしてください。このコマンドの詳細はセクション 1 *Fundamentals Command References* の”*File system management commands*”を参照してください。

III. 設定手順

操作	コマンド	補足
system view に移行する	**system-view**	―
USB インタフェースを無効にする	**usb disable**	デフォルト：有効

14.8. シャットダウンインターバルの設定

I. シャットダウンインターバルについて

いくつかのプロトコルでは特定の条件になるとポートを自動的にシャットダウンします。ポートがシャットダウンした後、装置はポートの検出間隔のタイマを開始します。装置はポートの物理状態を反映させるため、ポートを up 状態に復旧させます。

II. 設定手順

操作	コマンド	補足
system view に移行する	**system-view**	―
シャットダウンインターバルを設定する	**shutdown-interval** *time*	デフォルト：30秒

14.9. メモリ使用しきい値の設定

I. メモリ使用しきい値について

適切な動作とメモリ効率を改善するため、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とき、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。

early warning 機能は、sufficient-memory 状態が維持できなくなった場合に alarm 通知します。

- Sufficient-memory しきい値
- Early-warning しきい値

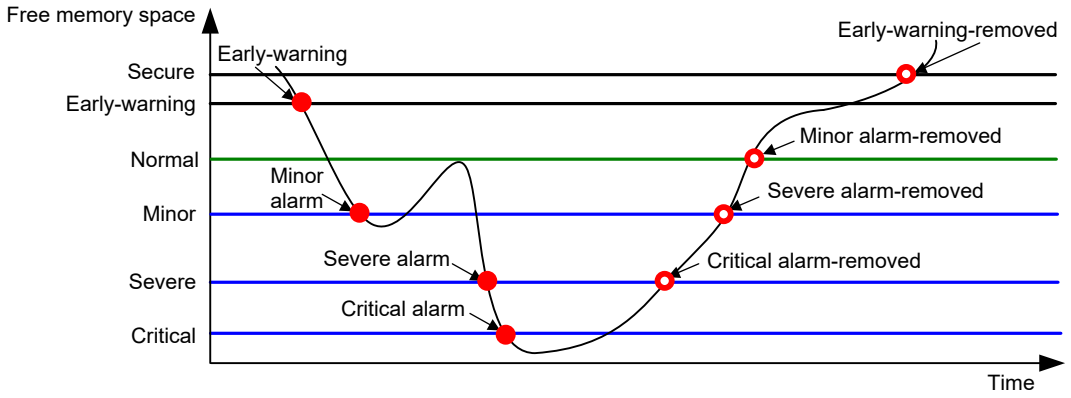
- Normal state しきい値
- Minor alarm しきい値
- Severe alarm しきい値
- Critical alarm しきい値

表 14-1 と図 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 通知	空きメモリ容量が最初にearly-warningしきい値以下に達した	early-warining通知を作成／送信した後、装置は最初にearly-warningがキャンセルされるまで追加でearly-warning通知を作成／送信しません。
Minor alarm通知	空きメモリ容量が最初にminor alarmしきい値以下に達した	minor alarm通知を作成／送信した後、装置は最初に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	空きメモリ容量が最初にsevere alarmしきい値以下に達した	severe alarm通知を作成／送信した後、装置は最初に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	空きメモリ容量が最初にcritical alarmしきい値以下に達した	critical alarm通知を作成／送信した後、装置は最初に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	空きメモリ容量が最初にsevere alarmしきい値以上に達した	ー
Severe alarm-removed 通知	空きメモリ容量が最初に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

図 14-1 メモリ alarm 通知と alarm-removed 通知



II. 設定手順

操作	コマンド	補足
system view に移行する	**system-view**	ー
メモリ使用率しきい値を設定する	**memory-threshold** [**slot** *slot-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. リソース監視の設定

I. リソース監視について

リソース監視機能により、デバイスは利用可能なリソースタイプの量 (ARP エントリのスペースなど) を監視できます。装置は、利用可能な量を周期的にサンプリングし、サンプルを資源枯渇しきい値と比較して、資源枯渇状態を識別する。

デバイスは、サポートされているリソースタイプごとに、マイナーリソース枯渇しきい値と重大リソース枯渇しきい値をサポートします。

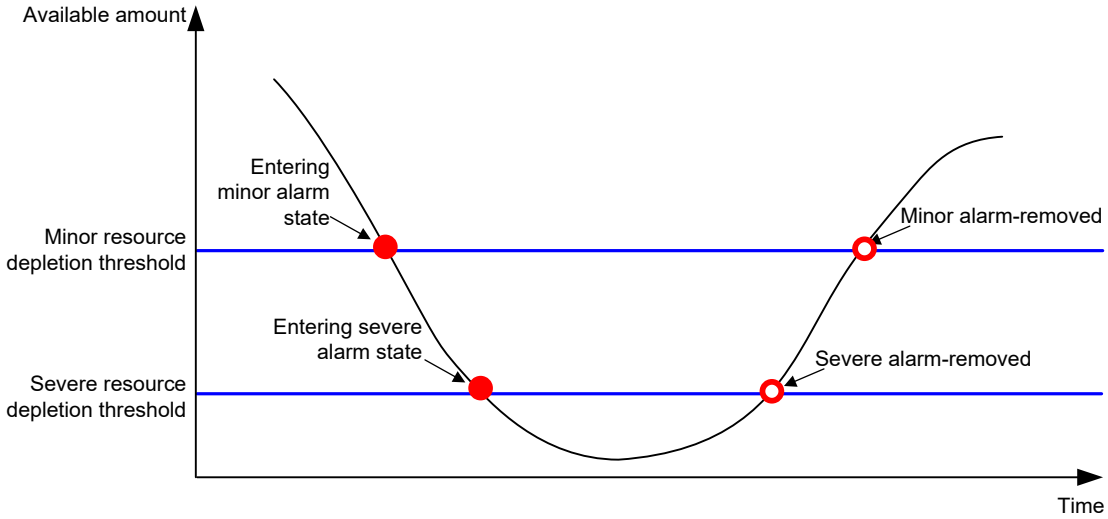
- 使用可能な量がマイナー資源枯渇しきい値以下で、重大資源枯渇しきい値より大きい場合、資源タイプはマイナーアラーム状態になります。
- 使用可能な量が重大な資源枯渇のしきい値以下の場合、資源タイプは重大なアラーム状態になります。
- 使用可能な量がマイナー資源枯渇しきい値を超えると、資源タイプは回復状態になります。

リソースタイプが重大アラーム状態になると、デバイスは重大アラームを発行します。リソースタイプが重大アラーム状態のままである場合、デバイスは重大アラームを定期的に再送信します。

リソースタイプがマイナーアラーム状態になると、デバイスはマイナーアラームを発行します。リソースタイプがマイナーアラーム状態のままであるか、重大アラーム状態からマイナーアラーム状態に変化する場合、デバイスはマイナーリソース枯渇アラームの再送信が有効かどうかを識別しま

す。この機能が無効になっている場合、デバイスは追加のマイナーアラームを発行しません。この機能が有効な場合、デバイスはマイナーアラームを定期的に再送信します。

表 14-2 資源枯渇アラームとアラーム除去通知



II. 設定手順

操作	コマンド	補足
system view に移行する	**system-view**	ー
リソースアラームしきい値を設定する	**resource-monitor resource** *resource-name* **slot** *slot-number* **cpu** *cpu-number* **by-percent minor-threshold** *minor-threshold* **severe-threshold** *severe-threshold*	デフォルト：リソースタイプによって異なります。各リソースの閾値は、**display resource-monitor**コマンドで確認可能です。
リソース枯渇アラームの送信先を指定する	**resource-monitor output** { **netconf-event** | **snmp-notification** | **syslog** } *	デフォルト：**netconf-event** ,**snmp-notification**,**syslog**
マイナーリソースアラームの再送信を有効にする	**resource-monitor minor resend enable**	デフォルト：有効

14.11. 装置の温度アラームのしきい値の設定

I. 装置の温度アラームのしきい値について

装置は以下のしきい値を温度センサによってモニタします。

- 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、あるいは高温ワーニング温度しきい値または高温アラーム温度しきい値に到達したとき、以下の動作を行います。

- イベントを記録します。

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

II. 設定手順

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
system view に移行する	**system-view**	ー
温度アラームしきい値を設定する	**temperature-limit slot** *slot-number* **hotspot** *sensor-number lowerlimit warninglimit* [*alarmlimit*]	デフォルト値は設定によって変わります。デフォルト値を確認する合、**undo temperature-limit**コマンドを使用し、**display environment**コマンドを実行してください。 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 14-3 温度アラームの推奨温度のしきい値とデフォルトのしきい値

装置	sensor	推奨温度の warning limit	デフォルトの warning limit	推奨温度の alarm limit	デフォルトの alarm limit
QX-S5324GT-4X1C	hotspot 1	52	66	57	71
QX-S5348GT-4X1C	hotspot 1	57	61	63	66

📖 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。

10GBASE-T-SFP+接続時は動作温度の上限が 40℃となります。

10GBASE-T-SFP+接続時は以下の推奨値に変更することを推奨します。

表 14-4 温度アラームの推奨温度のしきい値とデフォルトのしきい値(10GBASE-T-SFP+接続時)

装置	sensor	推奨温度の warning limit	デフォルトの warning limit	推奨温度の alarm limit	デフォルトの alarm limit
QX-S5324GT-4X1C	hotspot 1	40	66	45	71

装置	sensor	推奨温度の warning limit	デフォルトの warning limit	推奨温度の alarm limit	デフォルトの alarm limit
QX-S5348GT-4X1C	hotspot 1	44	61	49	66

14.12. メモリのパリティエラーアラームの設定

I. メモリのパリティエラーアラーム

装置は、メモリのパリティエラーを検出します。パリティエラーアラーム機能は、以下の動作を行います。

- 一定の間隔でパリティエラーの統計情報を収集します。エラー数がアラームしきい値を超過した場合、アラームを作成します。
- 検出したパリティエラーのログを生成します。

II. 設定手順

操作	コマンド	補足
system view に移行する	**system-view**	―
メモリのパリティエラーの統計情報を収集する間隔を設定する	**parity-error monitor period** *value*	デフォルト：60秒
メモリのパリティエラーのしきい値を設定する	**parity-error monitor threshold** *value*	デフォルト：5000
メモリのパリティエラーのログの生成を有効にする	**parity-error monitor log enable**	デフォルト：有効

14.13. エアフローの方向の設定

I. エアフローの方向について

QX-S5348GT-4X1C/QX-S5348GT-4X1C では、エアフローの異なる 2 種類のファンユニットが利用できます。エアフローには、ポート側が吸気で電源側が排気のエアフローと電源側が吸気でポート側が排気のエアフローがあります。

ファンユニットは、装置を設置する部屋の換気装置の方向とあわせたエアフローを選択した場合にのみ効果的に廃熱することができます。装置を設置する部屋の換気装置の方向にあわせて使用するファンを選択してください。

選択したファンのエアフローを CLI で設定する必要があります。ファンが正しく動作していない、あるいは実装されたファンのエアフローが設定されたエアフローと異なる方向である場合、装置はトラップを送信してログを記録します。異なるエアフローを示すログが表示された場合は、正しいエアフローを設定してください。

II. 設定手順

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

操作	コマンド	補足
エアフローの方向を設定する	**fan prefer-direction slot** *slot-number* { **power-to-port** | **port-to-power** }	デフォルト：**port-to-power**

14.14. 実装しているトランシーバの確認

14.14.1. 実装しているトランシーバの確認

I. 実装しているトランシーバの確認について

実装しているトランシーバの情報を確認するために以下の内容を表示することができます。

- 実装しているトランシーバタイプ、コネクタタイプ、送信するレーザーの中心波長、転送距離、ベンダ名などの主要パラメータ

装置はトランシーバのベンダ名等を確認します。実装したトランシーバがサポートしているものではない場合、装置はトラップとログメッセージを送出し続けます。ログ生成の詳細については、セクション 10 *システム管理 オペレーションマニュアル*の”*Information Center*”を参照してください。

II. 設定手順

操作	コマンド	補足
実装しているトランシーバの主要なパラメータを表示する	**display transceiver** { **interface** [*interface-type interface-number*] }	―

14.15. スケジュール自動実行の設定

14.15.1. スケジュール自動実行について

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

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

14.15.2. 制限とガイドライン

- システムクロックは再起動により常に一旦初期値に戻ります。スケジュール自動実行を期待通りに動作させる為に、再起動後に必ずシステムクロックの再設定を行うか、NTP によりシステムクロックが設定されるように設定を行ってください。NTP についての詳細については、セクション 10 *システム管理 オペレーションマニュアル*の”*NTP*”を参照してください。
- スケジュール自動実行を行う場合、実行する view と command 引数をチェックしません。command 引数を正確に設定してください。（コマンドの syntax が設定されているか、および正しい view に設定されているかどうかを含みます）

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

14.15.3. 設定手順

以下に 1 回のみのスケジュール自動実行を行う設定を示します。

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

以下に定期的なスケジュール自動実行を行う設定を示します。

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

操作	コマンド	補足
job を作成する	**scheduler job** *job-name*	デフォルト：設定なし
job にコマンドを割り当てる	**command** *id command*	デフォルト：設定なし 複数のコマンドをjobに割り当てることができ、最も小さいIDから実行されます。
system view に戻る	**quit**	ー
スケジュールを作成する	**scheduler schedule** *schedule-name*	デフォルト：設定なし
スケジュールにユーザロールを割り当てる	**user-role** *role-name*	デフォルト：スケジュールを作成したユーザのユーザロールを持ちます。 スケジュールの1つ以上のユーザロールが許可される場合、スケジュールのコマンドは実行できます。
スケジュールに job を割り当てる	**job** *job-name*	デフォルト：設定なし 複数のjobをスケジュールに割り当てることができ、同時に実行できます。
定期的なスケジュールを指定する	1. 指定された時間で定期的にスケジュールを実行する: **time repeating at** *time* [**month-date** [*month-day* | **last**] | **week-day** week-day&<1-7>] 指定された月日で定期的にスケジュールを実行する: **time repeating** [**at** *time* [*date*]] **interval** *interval-time*	デフォルト：設定なし いずれか1つのコマンドで設定します。 実行時間が指定された後、**clock datetime**コマンド、**clock summer-time**コマンド、**clock timezone**コマンドは既に設定された実行時間テーブルを変更しません。

14.15.4. スケジュール自動実行設定例

I. ネットワーク要件

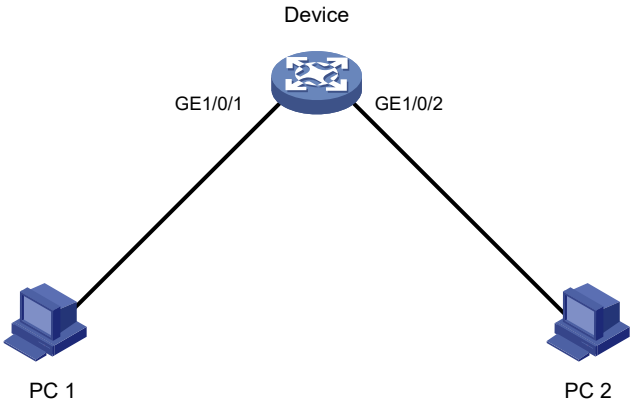
図 14-2 に示すように Device の 2 つのインタフェースがユーザに接続されています。

省電力化を行うため、以下の

エネルギーを節約するため、以下のスケジュールを自動で実行します。

- 月曜日から金曜日の AM8:00 にインタフェースを有効にします。
- 月曜日から金曜日の 18:00 にインタフェースを無効にします。

図 14-2 ネットワーク図



II. 設定手順

system view に移行します。

<Switch> system-view

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

[Switch] scheduler job shutdown-GigabitEthernet1/0/1

[Switch-job-shutdown-GigabitEthernet1/0/1] command 1 system-view

[Switch-job-shutdown-GigabitEthernet1/0/1] command 2 interface gigabitethernet 1/0/1

[Switch-job-shutdown-GigabitEthernet1/0/1] command 3 shutdown

[Switch-job-shutdown-GigabitEthernet1/0/1] quit

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

[Switch] scheduler job start-GigabitEthernet1/0/1

[Switch-job-start-GigabitEthernet1/0/1] command 1 system-view

[Switch-job-start-GigabitEthernet1/0/1] command 2 interface gigabitethernet 1/0/1

[Switch-job-start-GigabitEthernet1/0/1] command 3 undo shutdown

[Switch-job-start-GigabitEthernet1/0/1] quit

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

[Switch] scheduler job shutdown-GigabitEthernet1/0/2

[Switch-job-shutdown-GigabitEthernet1/0/2] command 1 system-view

[Switch-job-shutdown-GigabitEthernet1/0/2] command 2 interface gigabitethernet 1/0/2

[Switch-job-shutdown-GigabitEthernet1/0/2] command 3 shutdown

[Switch-job-shutdown-GigabitEthernet1/0/2] quit

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

[Switch] scheduler job start-GigabitEthernet1/0/2

[Switch-job-start-GigabitEthernet1/0/2] command 1 system-view

[Switch-job-start-GigabitEthernet1/0/2] command 2 interface gigabitethernet 1/0/2

[Switch-job-start-GigabitEthernet1/0/2] command 3 undo shutdown

[Switch-job-start-GigabitEthernet1/0/2] quit

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

[Switch] scheduler schedule START-pc1/pc2

[Switch-schedule-START-pc1/pc2] job start-GigabitEthernet1/0/1

[Switch-schedule-START-pc1/pc2] job start-GigabitEthernet1/0/2

[Switch-schedule-START-pc1/pc2] time repeating at 8:00 week-day mon tue wed thu fri

[Switch-schedule-START-pc1/pc2] quit

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

[Switch] scheduler schedule STOP-pc1/pc2

[Switch-schedule-STOP-pc1/pc2] job shutdown-GigabitEthernet1/0/1

[Switch-schedule-STOP-pc1/pc2] job shutdown-GigabitEthernet1/0/2

[Switch-schedule-STOP-pc1/pc2] time repeating at 18:00 week-day mon tue wed thu fri

[Switch-schedule-STOP-pc1/pc2] quit

III. 設定の確認

すべての job の設定を表示します。

[Switch] display scheduler job

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

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

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

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

スケジュール情報を表示します。

[Switch] display scheduler schedule

```
Schedule name         : START-pc1/pc2
Schedule type         : Run on every Mon Tue Wed Thu Fri at 08:00:00
Start time            : Wed Sep 28 08:00:00 2011
Last execution time   : Wed Sep 28 08:00:00 2011
Last completion time  : Wed Sep 28 08:00:03 2011
Execution counts      : 1
```

```
------------------------------------------------------------------------
Job name                                          Last execution status
start-GigabitEthernet1/0/1                                 Successful
start-GigabitEthernet1/0/2                                 Successful

Schedule name        : STOP-pc1/pc2
Schedule type        : Run on every Mon Tue Wed Thu Fri at 18:00:00
Start time           : Wed Sep 28 18:00:00 2011
Last execution time  : Wed Sep 28 18:00:00 2011
Last completion time : Wed Sep 28 18:00:01 2011
Execution counts     : 1
------------------------------------------------------------------------
Job name                                          Last execution status
shutdown-GigabitEthernet1/0/1                              Successful
shutdown-GigabitEthernet1/0/2                              Successful
```

スケジュールログの情報を表示します。

[Switch] display scheduler logfile

```
Logfile Size: 16054 Bytes.

Job name        : start-GigabitEthernet1/0/1
Schedule name   : START-pc1/pc2
Execution time  : Wed Sep 28 08:00:00 2011
Completion time : Wed Sep 28 08:00:02 2011
-------------------------------- Job output ----------------------------------
<Switch> system-view
System View: return to User View with Ctrl+Z.
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] undo shutdown

Job name        : start-GigabitEthernet1/0/2
Schedule name   : START-pc1/pc2
Execution time  : Wed Sep 28 08:00:00 2011
Completion time : Wed Sep 28 08:00:02 2011
-------------------------------- Job output ----------------------------------
<Switch> system-view
System View: return to User View with Ctrl+Z.
[Switch] interface gigabitethernet 1/0/2.
[Switch-GigabitEthernet1/0/2] undo shutdown

Job name        : shutdown-GigabitEthernet1/0/1
Schedule name   : STOP-pc1/pc2
Execution time  : Wed Sep 28 18:00:00 2011
Completion time : Wed Sep 28 18:00:01 2011
-------------------------------- Job output ----------------------------------
<Switch> system-view
System View: return to User View with Ctrl+Z.
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] shutdown
```

```
Job name         : shutdown-GigabitEthernet1/0/2
Schedule name    : STOP-pc1/pc2
Execution time   : Wed Sep 28 18:00:00 2011
Completion time : Wed Sep 28 18:00:01 2011
-------------------------------- Job output ---------------------------------
<Switch>system-view
System View: return to User View with Ctrl+Z.
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] shutdown
```

14.16. 装置の再起動

14.16.1. 装置の再起動について

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ができます。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 から即時再起動ができます。
- 再起動の間、装置は以下の動作を行います。
  a. 内蔵する全てのチップをリセットします。
  b. BootROM を使用し、ソフトウェアのスタートアップの確認・ソフトウェアの展開・ソフトウェアイメージの読み込みを行います。
  c. システムの初期化を実施します。
- 電源 ON/OFF による再起動ができます。この方法はデータの喪失を行う可能性があり、最も推奨できない方法です。

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。

14.16.2. 制限とガイドライン

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。

データ保護のため、ファイルを操作している場合、再起動は行われません。

14.16.3. CLI による装置の即時再起動

I. 前提条件

CLI による装置の即時再起動はすべての view で実行できます。

1. 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を確認するには、**display startup** コマンドを使用してください。**display startup** コマンドの詳細は、Chapter 1 *Fundamentals Command References* の”*Configuration file management commands*”を参照してください。
2. システム起動時に使用されるスタートアップファイルを確認するには、**display boot-loader** コマンドを使用してください。メインブートファイルの読み込みに失敗するか、ブートファイルが存在しない場合、装置は **reboot** コマンドで再起動ができません。**display boot-loader** コマンド

の詳細は、Chapter 1 *Fundamentals Command References* の”*Software upgrade commands*”を参照してください。

3. 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、Chapter 1 *Fundamentals Command References* の”*Configuration file management commands*”を参照してください。

II. 設定手順

操作	コマンド	補足
装置を再起動する	**reboot** [**slot** *slot-number*] [**force**]	user viewで実行可能です。

force キーワードは、ソフトウェアの確認を行わず、すぐさま装置を再起動します。**force** キーワードを指定しないと再起動できないときのみ使用してください。

14.16.4. 装置のスケジュール再起動

I. 制限とガイドライン

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

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

II. 設定手順

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

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

14.17. 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、装置はアラームやログで通知します。
- CPU 使用率のモニタリングが有効である場合、設定した間隔で CPU 使用率をサンプリングします。**display cpu-usage history** コマンドを使用すると、CPU 使用率履歴の統計情報を表示できます。

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
2. system view に移行する	**system-view**	―

操作	コマンド	補足
CPU 使用率のしきい値を設定する	**monitor cpu-usage threshold** *severe-threshold* **minor-threshold** *minor-threshold* **recovery-threshold** *recovery-threshold* ［ **slot** *slot-number* ［ **cpu** *cpu-number* ］ ］	デフォルト： severe CPU使用率アラームしきい値は99% minor CPU使用率アラームしきい値は80% CPU使用率回復しきい値は60%
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
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
user view に戻る	**quit**	ー
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。
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。

14.18. 電源オフアラームの設定

I. 制限とガイドライン

この機能は、電源が冗長構成となっている装置で使用できます。電源のどちらか一方がオフになった際に、SNMP 通知または Syslog メッセージで電源オフアラームを発することができます。

II. 設定手順

電源オフアラームの SNMP もしくは Syslog メッセージを有効にする場合、user view で以下のコマンドを実行します。

操作	コマンド	補足
system view に移行する	**system-view**	ー
電源オフアラームの送信元インタフェースを指定する	**dying-gasp source** *interface-type* { *interface-number* | *interface-number.subnumber* }	デフォルト：設定なし
SNMP 通知先ホストの設定を行う場合	**dying-gasp host** { *ip-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*] **snmp-trap version**{ **v1** | **v2c** | **v3** [**authentication** | **privacy**] } **securityname** *security-string*	デフォルト：設定なし

操作	コマンド	補足
Syslog メッセージの宛先ホストを設定する場合	**dying-gasp host** { *ip-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*] **syslog**	デフォルト：設定なし

14.19. 装置管理の情報表示と維持

すべての view で **display** コマンドを実行し、user view で **reset** 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使用率のヒストリー統計情報を図で表示する.	**display cpu-usage history** [**job** *job-id*] [**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** [**usb**] [**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*]
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*]
電源ユニットの状態を表示する	**display power** [**slot** *slot-number* [*power-id*]]
スケジュール自動実行機能の設定状態を表示する	**display scheduler job** [*job-name*]
スケジュール自動実行機能のログ情報を表示する	**display scheduler logfile**
スケジュールリブート機能の設定状態を確認する	**display scheduler reboot**
スケジュール自動実行機能の情報を表示する	**display scheduler schedule** [*schedule-name*]
システムバージョンを表示する	**display version**
スケジュール自動実行機能のログ情報をクリアする	**reset scheduler logfile**

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 について……15-1
15.2. Python スクリプトの実行……15-1
15.3. Python shell への移行……15-1
15.4. Comware 7 python 拡張 API のインポートと使用……15-1
15.4.1. import comware コマンドを使用したインポートと使用……15-2
15.4.2. from comware import コマンドを使用したインポートと使用……15-2
15.5. Python shell の終了……15-3
15.6. Python 使用例……15-3
15.6.1. Python スクリプトを使用した装置設定例……15-3

15章 Python

15.1. Pythonについて

本装置は Python インタプリタを実装しています。Python インタプリタは以下の機能をサポートします。

- Auto Config 機能の為の Python スクリプトの実行。
- 以下の機能を使用して装置を設定する為の Python shell への移行。
  - Python 2.7 コマンド。
  - Python 2.7 標準 API。
  - Comware 7 python 拡張 API。詳細は、"Comware 7 python 拡張 API"を参照してください。

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**	―

15.4. 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。

15.4.1. import comware コマンドを使用したインポートと使用

I. 設定手順

操作	コマンド	補足
1. user view から Python shell に移行する	**python**	―
2. Comware 7 Python 拡張 API をインポートする	**import comware**	―
3. Comware 7 python 拡張 API 機能を実行する	**comware.**api	―

II. 設定例

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>
```

15.4.2. from comware import コマンドを使用したインポートと使用

I. 設定手順

操作	コマンド	補足
1. user view から Python shell に移行する	**python**	―
2. Comware 7 Python 拡張 API をインポートする	**from comware import** *api-name*	―
3. Comware 7 python 拡張 API 機能を実行する	*api-function*	―

II. 設定例

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. 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()**	―

15.6. Python使用例

15.6.1. Python スクリプトを使用した装置設定例

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. 設定手順

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. 設定の確認

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
```

目次

このセクションのページは **1-x-x** です。

16 章 Comware 7 python 拡張 API……16-1
16.1. CLI……16-1
16.2. get_error……16-2
16.3. get_output……16-2
16.4. get_self_slot……16-3
16.5. get_slot_info……16-3
16.6. get_slot_range……16-4
16.7. get_standby_slot……16-4
16.8. Transfer……16-5

16章 Comware 7 python 拡張 API

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

16.1. 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。

I. Syntax

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

II. Parameters

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。

III. Usage guidelines

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。

IV. Returns

CLI オブジェクト

V. Examples

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')
```

VI. Sample output

<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>
```

16.2. 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。

I. Syntax

Transfer.get_error()

II. Returns

エラー情報(エラー情報が無ければ、None が返ります。)

III. Examples

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()
```

IV. Sample output

```
"Timeout was reached”
```

16.3. 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。

I. Syntax

CLI.get_output()

II. Returns

コマンド実行時の出力が返ります。

III. Examples

#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()
```

IV. Sample output

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

16.4. get_self_slot

get_self_slot を使用して、マスタ装置のメンバ ID を取得します。

I. Syntax

get_self_slot()

II. Returns

リストオブジェクト(フォーマットは[-1,*slot-number*])。*slot-number* がマスタ装置のメンバ ID を示します。

III. Examples

マスタ装置のメンバ ID 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
>>> comware.get_self_slot()
```

IV. Sample output

[-1,1]

16.5. get_slot_info

get_slot_info を使用して、メンバ装置情報を取得します。

I. Syntax

get_slot_info()

II. Returns

辞書オブジェクト(フォーマットは{'Slot': *slot-number,* 'Status': *'status'*, 'Chassis': chassis-number, 'Role': *'role'*, 'Cpu': *CPU-number* })。*slot-number* は装置のメンバ ID を示します。*status* はメンバ装置のステータスを示します。chassis-number と CPU-number は 0 固定です。*role* はメンバ装置の役割を示します。

III. Examples

メンバ装置情報を取得します。

<Switch> python

```
Python 2.7.3 (default)
[GCC 4.4.1] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> import comware
>>> comware.get_slot_info(1)
```

IV. Sample output

```
{'Slot': 1, 'Status': 'Normal', 'Chassis': 0, 'Role': 'Master', 'Cpu': 0}
```

16.6. get_slot_range

get_slot_range を使用して、使用可能なメンバ ID の範囲を取得します。

I. Syntax

get_slot_range()

II. Returns

辞書オブジェクト(フォーマットは{'MaxSlot': *max-slot-number*, 'MinSlot': *min-slot-number* })。*max-slot-number* はメンバ ID の最大値を示します。*min-slot-number* はメンバ ID の最小値を示します。

III. Examples

使用可能な IRF メンバ ID の範囲を取得します。

<Switch> python

```
Python 2.7.3 (default)
[GCC 4.4.1] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> import comware
>>> comware. get_slot_range()
```

IV. Sample output

```
{'MaxSlot': 20, 'MinSlot': 1}
```

16.7. get_standby_slot

get_standby_slot を使用して、スタンバイ装置のメンバ ID を取得します。

I. Syntax

get_standby_slot()

II. Returns

以下のフォーマットでリストオブジェクトが返ります。

- [ ]—IRF スタックにスタンバイ装置がありません。
- [[-1,*slot-number*]]—IRF スタックに一つのスタンバイ装置があります。
- [[-1,*slot-number1*],[-1,*slot-number2*],...]—IRF スタックに複数のスタンバイ装置があります。

slot-number はスタンバイ装置のメンバ ID です。

III. Examples

メンバ装置のメンバ ID 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
>>> comware.get_standby_slot()
```

IV. Sample output

```
[[-1, 1], [-1, 2]]
```

16.8. 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。

I. Syntax

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

II. Parameters

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。

vrf: 本パラメータは未サポートです。Null('')を指定してください。

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。

III. Returns

Transfer object

IV. Examples

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='')
```

V. Sample output

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

目次

このセクションのページは **1-x-x** です。

17 章 Auto Config 17-1
17.1. 概要 17-1
17.2. サーバベース Auto Config の使用 17-1
17.2.1. サーバベース Auto Config について 17-1
17.2.2. 設定作業リスト 17-2
17.2.3. ファイルサーバの設定 17-2
17.2.4. コンフィグレーションファイルの準備 17-2
17.2.5. スクリプトファイルの準備 17-4
17.2.6. DHCP サーバの設定 17-4
17.2.7. DNS サーバの設定 17-6
17.2.8. ゲートウェイの設定 17-6
17.2.9. Auto Config で使用するインタフェースの準備 17-6
17.2.10. Auto Config の起動と完了 17-7
17.3. USB ベース Auto Config の使用 17-7
17.3.1. USB ベース Auto Config について 17-7
17.3.2. Auto Config の USB ディスクの準備 17-8
17.3.3. USB ベース Auto Config の設定と使用 17-9
17.4. サーバベースの自動設定例 17-10
17.4.1. TFTP サーバを使用した Auto Config の設定例 17-10

17章 Auto Config

17.1. 概要

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とき、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と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。

Auto Config は以下の表の方法を使用して実行できます。

図 17-1 Auto Config の実行方法

実行方法	コンフィグレーションファイル保存場所	シナリオ
サーバベース Auto Config	ファイルサーバ	設定対象の機器用に、事前にコンフィグレーションファイルを用意する。機器そのものは地理的に離れていてもよい。

正常に起動すると(システムステータス LED が緑に点灯)、装置は自動的に Auto Config プロセスに入り、システムステータス LED は緑色で点滅します。

Auto Config プロセスが完了すると、システムステータス LED は点滅を停止し、緑色で点灯します。

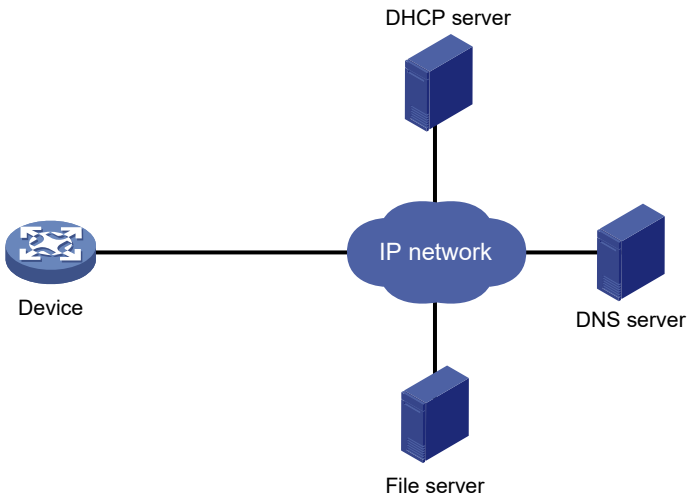
17.2. サーバベース Auto Configの使用

17.2.1. サーバベース Auto Config について

図 17-2 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。
- TFTP サーバー 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。
- 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。

図 17-2 ネットワーク図



17.2.2. 設定作業リスト

作業リスト
(必須設定項目) ファイルサーバの設定
(必須設定項目) Auto Configの為のファイル準備 • コンフィグレーションファイルの準備 • スクリプトファイルの準備
(必須設定項目) DHCPサーバの設定
(オプション設定項目) DNSサーバの設定
(オプション設定項目) ゲートウェイの設定
(必須設定項目) Auto Configに使用するインタフェースの準備
(必須設定項目) Auto Configの開始と完了

17.2.3. ファイルサーバの設定

コンフィグレーションを TFTP サーバから受信する機器の為、ファイルサーバ上の TFTP サービスを有効にください。

17.2.4. コンフィグレーションファイルの準備

I. コンフィグレーションファイルのタイプ

表 17-1 に記載されているコンフィグレーションファイルのタイプが使用できます。

表 17-1 コンフィグレーションファイルのタイプ

コンフィグレーションファイルのタイプ	適用先	ファイル名の要件	ファイルサーバの種類
専用コンフィグレーションファイル	それぞれに異なった設定内容を持つ装置。	*File name*.cfg コンフィグレーション内で指定されたホスト名をファイル名に使用してください。 尚、ファイル名にはスペースは含めないでください。	TFTPサーバ
共通コンフィグレーションファイル	全ての設定、または部分的に設定が共通となる装置群。	*File name*.cfg	TFTPサーバ
デフォルトコンフィグレーションファイル	その他の装置。 スタートアップ時に使用する共通コンフィグレーションのみを含みます。	device.cfg	TFTPサーバ

II. 必要なコンフィグレーションファイルタイプの決定とコンフィグレーションファイルの準備

1. どのようなタイプのコンフィグレーションファイルを用意するか決定します。
2. それぞれに異なったコンフィグレーションを必要とする装置の為に、異なったコンフィグレーション部分に関して個別のコンフィグレーションファイルを用意し、ファイルサーバに保存します。
3. 全ての設定が共通または部分的に共通の設定を持つ装置の為に、共通となる部分のコンフィグレーションを含むファイルを用意し、ファイルサーバに保存します。
4. TFTP を使用する場合、装置のスタートアップに必要な共通コンフィグレーションを device.cfg ファイルとしてファイルサーバに保存することができます。このファイルは、装置を使用する時に他の一切のコンフィグレーションの変更を必要としない場合にのみ、装置に適用されます。

III. TFTP サーバ上のホスト名ファイルの準備

DHCP サーバ上でコンフィグレーションファイル名の割り当てを行わない場合、TFTP サーバ上のホスト名ファイルを変更する方法を使うことができます。ホスト名ファイルは Auto Config を適用する装置のホスト名と IP アドレスの対応表を含みます。

以下のようにホスト名ファイルを準備します。

1. network.cfg というファイル名でホスト名ファイルを作成します。
2. ip host host-name ip-address の形式で、一行ずつ対応表を作成します。以下が作成例です。

```
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:

ホスト名ファイルに記載するホスト名はコンフィグレーションファイルに記載するホスト名と同一でなければなりません。

17.2.5. スクリプトファイルの準備

I. スクリプトファイルについて

Auto Config では、スクリプトファイルを使用します。

スクリプトには、Python スクリプト(.py ファイル)を使用します。Python スクリプトの詳細は“Python"を参照してください。

装置は、専用スクリプトファイルと共通スクリプトファイルを使用できます。デフォルトスクリプトファイルは使用できません。これらの詳細は表 17-1 を参照してください。

スクリプトファイルを使用する際、ホスト名と IP アドレスを対応付けるホスト名ファイルは使用できません。

II. 設定手順

- 全ての設定が共通または部分的に共通の設定を持つ装置の為に、共通となる部分のコンフィグレーションを含むスクリプトファイルを作成します。
- その他の装置の為に、装置毎のコンフィグレーションを含むスクリプトファイルを装置毎に作成します。

17.2.6. DHCP サーバの設定

I. DHCP サーバについて

DHCP サーバは、Auto Config を適用する装置の為に以下の項目の割り当てを行います。

- IP アドレス
- コンフィグレーションファイルまたはスクリプトファイルのパス

II. 制限とガイドライン

- 個別に異なるコンフィグレーションファイルを使用する装置の為、DHCP サーバに以下の設定を行ってください。
  - DHCP アドレスプールの作成。
  - スタティックアドレスバインディングの設定。
  - コンフィグレーションファイルまたはスクリプトファイルの設定。

  アドレスプールは 1 つの設定ファイルのみを使用できるため、アドレスプールに対して 1 つのスタティックアドレスバインディングのみを設定できます。
- 同じ設定ファイルを準備した装置の場合、次のいずれかの方法を使用します。
  - 方法 1:
    - 装置用の DHCP アドレスプールを作成します。
    - 設定は、アドレスプール内の各装置のスタティックアドレスバインディングです。
    - 装置の設定ファイルを指定します。

- 方法 2:
  - 装置用の DHCP アドレスプールを作成します。
  - 動的割当てのサブネットを指定します。
  - TFTP サーバを指定します。
  - 装置の設定ファイルを指定します。

- サブネット上のすべての装置が同じ設定ファイルまたはスクリプトファイルを共有している場合は、DHCP サーバで次のタスクを実行します。
  - 設定動的アドレス割り当て。
  - デバイスの設定ファイルまたはスクリプトファイルを指定します。

  設定ファイルには、デバイスの共通設定のみを含めることができます。 装置の管理者は、装置の起動後に構成を変更する方法を提供できます。

III. TFTP ファイルサーバを使用するときの DHCP サーバーの設定

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
3. 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*	—
4. アドレスプールを設定する	• アドレスプールのプライマリサブネットを設定する：**network** *network-address* [*mask-length* | **mask** *mask*] • 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できます。ただし、1つのIPアドレスは1つのクライアントにのみ割り当てることができます。 DHCPクライアントの割り当てドを変更する場合、割り当てを一度削除したのち再度設定する必要があります。
5. TFTP サーバを設定する	• 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*	デフォルト：設定なし 名前を設定する場合、ネットワークにDNSサーバが必要です。

操作	コマンド	補足
6. 設定あるいはスクリプトファイルの名前を指定する	**bootfile-name** *bootfile-name*	デフォルト：設定なし

17.2.7. DNS サーバの設定

DNS サーバは、以下の場合に必要です。

- TFTP サーバにホスト名ファイルがありません。

  装置は、DNS サーバに IP アドレスを指定してホスト名を取得する必要があります。次に、装置は TFTP サーバから *host name*.**cfg** フォーマットのコンフィグレーションファイルを取得できます。

- DHCP サーバは、DHCP 応答メッセージを介して TFTP サーバドメイン名を割り当てます。 装置は、TFTP サーバの IP アドレスを取得するためにドメイン名を使用する必要があります。

17.2.8. ゲートウェイの設定

自動的に構成され、自動的に設定のサーバが異なるネットワークセグメントに常駐する場合は、次のタスクを実行する必要があります。

- ゲートウェイを展開し、装置がサーバと通信できることを確認します。
- ゲートウェイ上の DHCP リレーエージェント機能を設定します。
- ゲートウェイ上の UDP ヘルパー機能を設定します。

  このタスクは、デバイスがブロードキャストパケットを使用して TFTP サーバに要求を送信する場合に必要です。 デバイスは、次の状況で、ブロードキャストパケットを使用して TFTP サーバに要求を送信します。

  - DHCP 応答には、TFTP サーバの IP アドレスまたはドメイン名が含まれていません。
  - TFTP サーバの IP アドレスまたはドメイン名が無効です。

  UDP ヘルパーは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、ユニキャストパケットをファイルサーバに転送します。UDP ヘルパーの詳細は、セクション 3 *アクセス オペレーションマニュアル*の“*UDP ヘルパー*”を参照してください。

17.2.9. Auto Config で使用するインタフェースの準備

装置は、インタフェースを Auto Config で選択するために次の手順を使用します。

1. レイヤ 2 でマネジメント Ethernet インタフェースの状態を識別します。状態がアップしている場合、装置マネジメント管理 Ethernet インタフェースを使用します。
2. 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アップ状態デフォルト VLAN の VLAN インタフェースを使用します。
3. すべてのレイヤ 3 イーサネットインタフェースを並べ替えます。アップ状態のインタフェースタイプのアルファベット順で、次にインタフェース数字の昇順で並べ替えます。 インタフェースでは、最初のインタフェースタイプのインタフェース間で最小のインタフェース番号を使用します。

4. レイヤ 3 イーサネットインタフェースがない場合アップ状態デバイスは 30 秒待機し、手順 1 に進みます。

高速の自動装置設定の場合、各装置のマネジメント Ethernet インタフェースのみをネットワークに接続します。

17.2.10. Auto Config の起動と完了

1. 自動的に構成されるデバイスの電源を入れます。

   装置がローカルの設定ファイルをローカルで検出しない場合は、設定の自動プロセスを起動して設定ファイルを取得します。

   - 装置が設定ファイルを取得し、ファイルを正常に実行すると、自動設定プロセスが終了します。
   - 1 回の試行に失敗すると、デバイスは最大試行回数に達するまで再試行します。 プロセスを停止するには、<Ctrl+C>または<Ctrl+D>キーを押下します。

   装置が設定ファイルの取得に失敗した場合、装置は設定をロードせずに起動します。

2. 設定を保存します。

   save

   装置は取得した設定ファイルをローカルに保存しません。 設定を保存しない場合、装置は再起動後に自動的に設定機能を使用する必要があります。save コマンドの詳細は Chapter 1 *Fundamentals Command Reference* の“*Configuration file management commands*”を参照してください。

17.3. USBベース Auto Configの使用

17.3.1. USB ベース Auto Config について

USB ベース Auto Config により、装置は接続された USB ディスクから起動時にコンフィグレーションファイルを取得できます。

コンフィグレーションファイルを取得すると、装置はそのファイルとメインに指定しているスタートアップコンフィグレーションファイルを比較します。

- 2 つのファイルの設定が同じ場合、装置は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読み込み、USB ベース Auto Config プロセスが終了します。
- 2 つのファイルの設定が異なる場合、装置は次の操作を実行します。

  a. 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が、取得したコンフィグレーションファイルと同じ名前を使用している場合、装置はファイルのベース名に**_bak** を追加して、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の名前を変更します。

  b. 取得したコンフィグレーションファイルをローカルに保存します。

     フラッシュメモリ内のスタートアップ以外のコンフィグレーションファイルが、取得したコンフィグレーションファイルと同じ名前を使用している場合、装置はプロンプトを表示せずに既存のファイルに上書きします。

  c. 取得したコンフィグレーションファイルをロードします。

– 取得したコンフィグレーションファイル内のコマンドがすべて正常にロードされると、装置は取得したコンフィグレーションファイルをメインスタートアップコンフィグレーションファイルとして設定します。
– 取得したコンフィグレーションファイル内のコマンドのロードに失敗すると、ローカルのコンフィグレーションファイルを検索します。

  コンフィグレーションファイルが見つかると、装置はコンフィグレーションファイルをロードします。

  コンフィグレーションファイルが見つからない場合、装置は設定をロードせずに Auto Config プロセスを終了します。デフォルトコンフィグで起動します。

メモ:

- USB ベース Auto Config では、装置起動中に USB からのコンフィグ読み込みにモードが変わるため、読み込みモード切替後に自動的に再起動し直します。起動中の“Cryptographic algorithms tests passed.”メッセージ表示後に、自動的に再起動します。
- USB の cfg ファイルには使用するすべてのコマンド(display saved-configuration と同じ内容)を設定してください。本機能では cfg ファイルの中身が、1 つのコマンドだけ書かれている場合でもロードが実行されますが、その場合、NEC 推奨のデフォルト設定がロードされません。

17.3.2. Auto Config の USB ディスクの準備

1. パーティションが 1 つしかない USB ディスクを準備します。
2. **display device manuinfo** コマンドで装置のシリアル番号を表示します。

```
<QX-S5324GT-4X1C>display device manuinfo
 Slot 1 CPU 0:
DEVICE_NAME           : QX-S5324GT-4X1C
DEVICE_SERIAL_NUMBER  : 210235A3Q1M195A0000X
MAC_ADDRESS           : 4CE9-E497-DB93
MANUFACTURING_DATE    : 2019-05-24
VENDOR_NAME           : NEC
PRODUCT ID            : QX-S5324GT-4X1C
Fan 1:
DEVICE_SERIAL_NUMBER  : NONE
Fan 2:
DEVICE_SERIAL_NUMBER  : NONE
Power 1:
DEVICE_NAME           : PSR150-A1
DEVICE_SERIAL_NUMBER  : 210231A0EXH181000161
```

```
MANUFACTURING_DATE    : 2018-01-17
VENDOR_NAME           : NEC
```

このコマンドの詳細については、コマンドマニュアルのセクション 1 *はじめに* “*装置管理*”を参照してください。

3. **210235A3Q1M195A0000X.cfg** または **autodeploy.cfg** という名前のコンフィグレーションファイルを作成し、USB ディスク上のファイルシステムのルートディレクトリにファイルを保存します（シリアル番号は装置ごとに異なります）。

   210235A3Q1M195A0000X.cfg と **autodeploy.cfg** の 2 つのファイルが USB ディスクに存在している場合、**210235A3Q1M195A0000X.cfg** の設定をロードします。

17.3.3. USB ベース Auto Config の設定と使用

1. 装置で USB ベース Auto Config を有効にします。USB ベース Auto Config には、装置の再起動が必要です。実行コンフィグレーションを保存して、再起動後に USB ベース Auto Config 機能が有効になるようにします。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. USB ベース Auto Config を有効にします。	**autodeploy udisk enable**	デフォルト：有効
3. 設定を保存します。	**save**	―

2. IRF スタック構成では、IRF スタック物理インタフェースをシャットダウンして、IRF スタックユニットを分割します。IRF スタックを構成したままでは使用できません。
3. USB ディスクを装置の USB インタフェースに接続します。IRF スタックの場合はマスタ装置に接続します。

   USB ディスクは **usba0:**として識別されます。
4. 装置を再起動します。
5. コンフィグレーションファイルが正しくロードされていることを確認するには、**display current-configuration** コマンドを使用します。

   USB ベース Auto Config が失敗すると、装置は失敗した内容をログに記録します。USB ディスクのルートディレクトリにある”使用したファイル名”**.log** という名前のファイルにログが保存されます。ログが保存されている場合は、内容を確認して問題を解決してください。

   例えば、autodeploy.cfg という名前のコンフィグレーションファイルに、装置に存在しないインタフェース名(GigabitEthernet1/0/100)が書かれていた場合、コンフィグのロードに失敗して autodeploy.cfg.log ファイルには以下の情報が記録されます。

```
Command interface GigabitEthernet1/0/100 fails to recover configuration.
```

6. 次回の再起動時に装置が USB ベース Auto Config を開始しないように、USB ディスクを取り外してください。

7. IRF スタックユニットを分割した場合は、シャットダウンした IRF スタック物理インタフェースを元に戻します。他のメンバが IRF スタックユニットに参加し、マスタ装置のコンフィグレーションファイルを実行していることを確認します。

17.4. サーバベースの自動設定例

17.4.1. TFTP サーバを使用した Auto Config の設定例

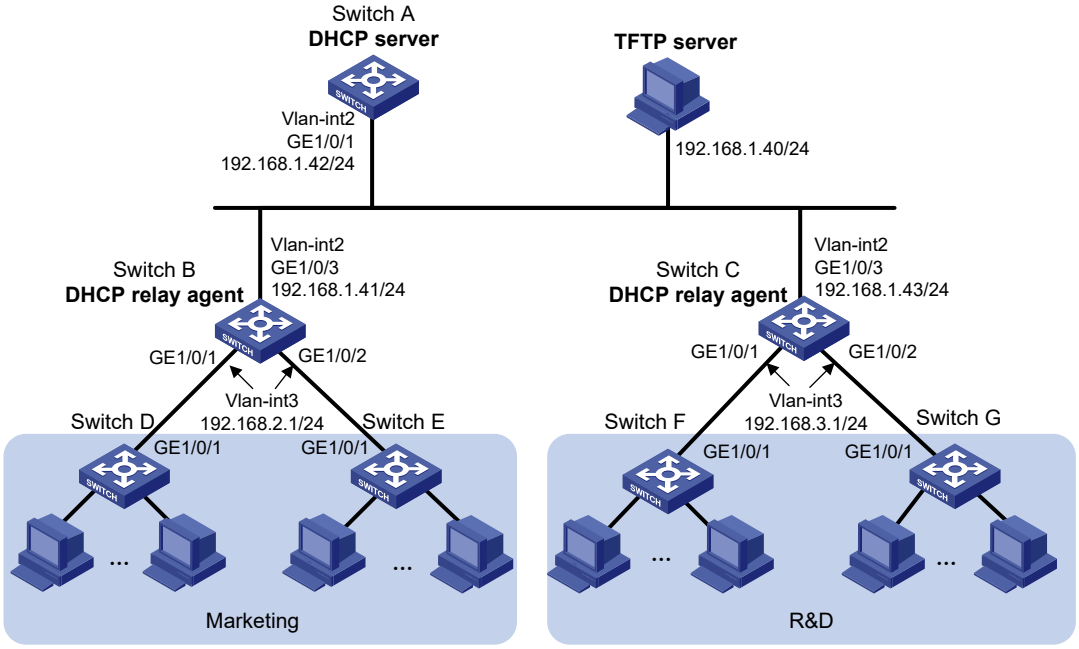
I. ネットワーク要件

図 17-3 に示すように、ゲートウェイ(Switch B と Switch C)を介して、企業の 2 つの部門をネットワークに接続しています。 アクセスデバイス Switch D、Switch E、Switch F、および Switch G には設定ファイルがありません。

設定のファイルを入手して次の設定タスクを完了できるように、サーバとゲートウェイを設定のサーバとゲートウェイに接続します。

- アクセスデバイスの管理者が、それぞれのアクセスデバイスに Telnet 接続して管理できるようにします。
- ログイン時に、管理者がそれぞれのユーザ名とパスワードを入力するように要求します。

図 17-3 ネットワーク図



II. 設定手順

1. DHCP サーバを設定します。

   #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。

   <SwitchA> system-view

   [SwitchA] vlan 2

[SwitchA-vlan2] port gigabitethernet 1/0/1

[SwitchA-vlan2] quit

[SwitchA] interface vlan-interface 2

[SwitchA-Vlan-interface2] ip address 192.168.1.42 24

[SwitchA-Vlan-interface2] quit

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

Marketing 部門のクライアントに 192.168.2.0/24 の IP アドレスを割り当てるようにアドレスプール market を設定します。TFTP サーバ、ゲートウェイ、クライアントのコンフィグレーションファイルを設定します。

[SwitchA] dhcp server ip-pool market

[SwitchA-dhcp-pool-market] network 192.168.2.0 24

[SwitchA-dhcp-pool-market] tftp-server ip-address 192.168.1.40

[SwitchA-dhcp-pool-market] gateway-list 192.168.2.1

[SwitchA-dhcp-pool-market] bootfile-name market.cfg

[SwitchA-dhcp-pool-market] quit

R&D 部門のクライアントに 192.168.3.0/24 の IP アドレスを割り当てるようにアドレスプール rd を設定します。TFTP サーバ、ゲートウェイ、クライアントのコンフィグレーションファイルを設定します。

[SwitchA] dhcp server ip-pool rd

[SwitchA-dhcp-pool-rd] network 192.168.3.0 24

[SwitchA-dhcp-pool-rd] tftp-server ip-address 192.168.1.40

[SwitchA-dhcp-pool-rd] gateway-list 192.168.3.1

[SwitchA-dhcp-pool-rd] bootfile-name rd.cfg

[SwitchA-dhcp-pool-rd] quit

DHCP リレーエージェントにスタティックルートを設定します。

[SwitchA] ip route-static 192.168.2.0 24 192.168.1.41

[SwitchA] ip route-static 192.168.3.0 24 192.168.1.43

[SwitchA] quit

2. ゲートウェイ Switch B を設定します。

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。

<SwitchB> system-view

[SwitchB] vlan 2

[SwitchB-vlan2] port gigabitethernet 1/0/3

[SwitchB-vlan2] quit

[SwitchB] interface vlan-interface 2

[SwitchB-Vlan-interface2] ip address 192.168.1.41 24

[SwitchB-Vlan-interface2] quit

[SwitchB] vlan 3

[SwitchB-vlan3] port gigabitethernet 1/0/1
[SwitchB-vlan3] port gigabitethernet 1/0/2
[SwitchB-vlan3] quit
[SwitchB] interface vlan-interface 3
[SwitchB-Vlan-interface3] ip address 192.168.2.1 24
[SwitchB-Vlan-interface3] quit
DHCP を有効にします。
[SwitchB] dhcp enable
VLAN インタフェース 3 で DHCP サーバを有効にします。
[SwitchB] interface vlan-interface 3
[SwitchB-Vlan-interface3] dhcp select relay
DHCP サーバのアドレスを設定します。
[SwitchB-Vlan-interface3] dhcp relay server-address 192.168.1.42

3. ゲートウェイ Switch C を設定します。

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。
<SwitchC> system-view
[SwitchC] vlan 2
[SwitchC-vlan2] port gigabitethernet 1/0/3
[SwitchC-vlan2] quit
[SwitchC] interface vlan-interface 2
[SwitchC-Vlan-interface2] ip address 192.168.1.43 24
[SwitchC-Vlan-interface2] quit
[SwitchC] vlan 3
[SwitchC-vlan3] port gigabitethernet 1/0/1
[SwitchC-vlan3] port gigabitethernet 1/0/2
[SwitchC-vlan3] quit
[SwitchC] interface vlan-interface 3
[SwitchC-Vlan-interface3] ip address 192.168.3.1 24
[SwitchC-Vlan-interface3] quit
DHCP を有効にします。
[SwitchC] dhcp enable
VLAN インタフェース 3 で DHCP サーバを有効にします。
[SwitchC] interface vlan-interface 3
[SwitchC-Vlan-interface3] dhcp select relay
DHCP サーバのアドレスを設定します。
[SwitchC-Vlan-interface3] dhcp relay server-address 192.168.1.42

4. TFTP サーバを設定します。

TFTP サーバで、コンフィグレーションファイル market.cfg を作成します。

```
#
 sysname Market
#
 telnet server enable
```

```
#
vlan 3
#
local-user market
 password simple market
 service-type telnet
 quit
#
interface Vlan-interface3
 ip address dhcp-alloc
 quit
#
interface gigabitethernet 1/0/1
 port access vlan 3
 quit
#
user-interface vty 0 63
 authentication-mode scheme
 user-role network-admin
#
return
```

TFTP サーバで、コンフィグレーションファイル rd.cfg を作成します。

```
#
 sysname RD
#
 telnet server enable
#
vlan 3
#
local-user rd
 password simple rd
 service-type telnet
 quit
#
interface Vlan-interface3
 ip address dhcp-alloc
 quit
#
interface gigabitethernet 1/0/1
 port access vlan 3
 quit
#
user-interface vty 0 63
 authentication-mode scheme
 user-role network-admin
#
return
```

TFTP サービスを開始し､2 つのコンフィグレーションファイルが格納される作業ディレクトリを指定します。(詳細は省略します。)

TFTP サーバと DHCP リレーエージェントが互いに通信できることを確認します。(詳細は省略します。)

III. 設定の確認

1. Switch D、Switch E、Switch F、Switch G の電源を ON にします。
2. アクセスデバイスが起動したら、Switch A 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
192.168.2.2      3030-3066-2e65-3233-  May 6 05:21:25 2013   Auto(C)
                 642e-3561-6633-2d56-
                 6c61-6e2d-696e-7465-
                 7266-6163-6533
192.168.2.3      3030-3066-2e65-3230-  May 6 05:22:50 2013   Auto(C)
                 302e-3232-3033-2d56-
                 6c61-6e2d-696e-7465-
                 7266-6163-6533
192.168.3.2      3030-6530-2e66-6330-  May 6 05:23:15 2013   Auto(C)
                 302e-3335-3131-2d56-
                 6c61-6e2d-696e-7465-
                 7266-6163-6531
192.168.3.3      3030-6530-2e66-6330-  May 6 05:24:10 2013   Auto(C)
                 302e-3335-3135-2d56-
                 6c61-6e2d-696e-7465-
                 7266-6163-6532
```

3. Switch A から 192.168.2.2 に Telnet を行います。

<SwitchA> telnet 192.168.2.2

4. プロンプトに従ってユーザ market とパスワード market を入力します。(詳細は省略します。)

Switch D または Switch E にログインしています。

目次

このセクションのページは **1-x-x** です。

18 章 Web コンソールによるログイン……18-1
18.1. HTTP ログインの設定……18-1
18.2. HTTPS ログインの設定……18-2
18.2.1. 制限とガイドライン……18-2
18.2.2. 設定作業リスト……18-3
18.3. Web ログインの表示と維持……18-5
18.4. Web ログインの設定例……18-5
18.4.1. HTTP ログインの設定例……18-5

18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。

18.1. 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**	―
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9 *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

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

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

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

18.2.1. 制限とガイドライン

- HTTPS サービスと SSL VPN サービスが同じポート番号を使用する場合は、同じ SSL サーバポリシーを使用する必要があります。異なる SSL サーバポリシーを使用する場合は、どちらか一方のみを有効にできます。
- HTTPS サービスと SSL VPN サービスの両方で使用される SSL サーバポリシーを変更するには、以下の手順で実行する必要があります。手順通りに設定が行われなかった場合、新しい設定は有効になりません。
  1. HTTPS サービスと SSL VPN サービスを無効にします。
  2. SSL サーバポリシーを変更します。
  3. HTTPS サービスと SSL VPN サービスを再度有効にします。
- 別の SSL サーバポリシーを HTTPS サービスに関連付けるには、以下の手順で実行する必要があります。手順通りに設定が行われなかった場合、新しい SSL サーバポリシーは有効になりません。
  1. HTTP サービスと HTTPS サービスを無効にします。

2. 新しい SSL サーバポリシーを関連付けます。
3. HTTP サービスと HTTPS サービスを再度有効にします。

- SSL サーバポリシーを HTTPS サービスに関連付けた後に HTTP サービスが自己署名証明書を使用するには、次の手順を実行する必要があります。

1. HTTP サービスと HTTPS サービスを無効にします。
2. undo ip https ssl-server-policy コマンドを実行して、既存の SSL サーバポリシーアソシエーションを削除します。
3. HTTP サービスと HTTPS サービスを再度有効にします。

- HTTPS サービスを有効にすると、SSL ハンドシェイク ネゴシエーションプロセスがトリガーされます。
  - □ デバイスにローカル証明書がある場合、SSL ハンドシェイク ネゴシエーションは成功し、HTTPS サービスが起動します。
  - □ デバイスにローカル証明書がない場合は、証明書適用プロセスが開始されます。証明書適用プロセスに時間がかかるため、SSL ハンドシェイク ネゴシエーションが失敗し、HTTPS サービスが開始されない場合があります。この問題を解決するには、HTTPS サービスが有効になるまで ip https enable コマンドを再度実行します。

18.2.2. 設定作業リスト

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）HTTPS サービスに SSL サーバポリシーを適用する	**ip https ssl-server-policy** *policy-name*	デフォルト：SSLサーバポリシーは関連付けられていません。HTTPサービスは自己署名証明書を使用します。
3. （オプション設定項目）HTTPS サービスにアクセスコントロールポリシーを適用する	**ip https certificate access-control-policy** *policy-name*	デフォルト：証明書ベースのアクセスコントロールポリシーは適用されません。証明書ベースのアクセスコントロールポリシーの詳細は*QXシリーズWeb認証オペレーションマニュアル(V7)*の“*PKI*”を参照してください。

操作	コマンド	補足
4. 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。 1. 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。 2. 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。
5. （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
6. （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
7. （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9 *セキュリティ”AAA”* を参照してください。
8. 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
9. 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。
10. 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
11. 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

18.3. 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* }

18.4. Webログインの設定例

18.4.1. HTTP ログインの設定例

I. ネットワーク要件

図 18-1 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 18-1 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 IE 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。

QX-S5300G シリーズ Ethernet スイッチ

オペレーションマニュアル

2.IRF スタック

本マニュアルは以下に示す章で構成されています。

01-IRF スタックの設定

目次

このセクションのページは **2-x-x** です。

1 章 IRF スタック 1-1
1.1. 概要 1-1
1.1.1. IRF スタックネットワークモデル 1-1
1.1.2. IRF スタックの利点 1-1
1.1.3. 基本コンセプト 1-2
1.1.4. IRF スタックネットワークトポロジ 1-4
1.1.5. Master の選定 1-5
1.1.6. インタフェースの命名規則 1-5
1.1.7. ファイルシステム命名規則 1-6
1.1.8. 設定の同期メカニズム 1-7
1.1.9. マルチアクティブの検知の処理 1-7
1.1.10. MAD メカニズム 1-9
1.2. 制限とガイドライン 1-14
1.2.1. IRF スタックのハードウェアの互換性 1-14
1.2.2. IRF スタックのソフトウェア 1-14
1.2.3. IRF スタック物理インタフェースの選択 1-15
1.2.4. IRF スタックのトランシーバモジュールとケーブルの選定 1-15
1.2.5. IRF スタックポートの接続 1-15
1.2.6. IRF スタック物理インタフェースの制限とガイドライン 1-16
1.3. IRF スタック設定作業リスト 1-17
1.4. IRF スタックユニットのセットアップの計画 1-17
1.5. IRF スタックユニットの設定 1-18
1.5.1. IRF スタックユニット設定作業リスト 1-18
1.5.2. 各 IRF スタックメンバ装置へのメンバ ID の割り当て 1-18
1.5.3. 各メンバ装置のプライオリティの設定 1-19
1.5.4. IRF スタックポートと物理インタフェースへの関連付け 1-19
1.5.5. IRF スタック物理インタフェースの接続 1-21
1.5.6. IRF スタックユニットのアクセス 1-21
1.6. MAD の設定 1-22
1.6.1. 制限とガイドライン 1-22
1.6.2. LACP MAD の設定 1-22
1.6.3. BFD MAD の設定 1-23
1.6.4. ARP MAD の設定 1-27
1.6.5. MAD によるシャットダウンアクションからのサービスインタフェースの除外の設定 1-30
1.6.6. IRF スタックユニットの回復 1-30
1.7. IRF スタックユニットの IRF スタックの設定の最適化 1-31
1.7.1. メンバ装置の説明の設定 1-31
1.7.2. IRF スタックの bridge MAC アドレスの設定 1-31
1.7.3. ソフトウェア同期用のソフトウェアオートアップグレードの有効化 1-32
1.7.4. IRF スタックリンクダウン検出遅延の設定 1-33
1.7.5. IRF スタック物理インタフェースを持つ拡張インタフェースカードの取り外し 1-34
1.7.6. IRF スタック物理インタフェースを持つ拡張インタフェースカードの交換 1-34
1.8. IRF スタックの表示と維持 1-35

1.9. IRF スタックの設定例 ····· 1-35
1.9.1. LACP MAD を使用する場合の IRF スタックの設定例 ····· 1-35
1.9.2. BFD MAD を使用する場合の IRF スタックの設定例 ····· 1-41
1.9.3. ARP MAD を使用する場合の IRF スタックの設定例 ····· 1-46

1章 IRF スタック

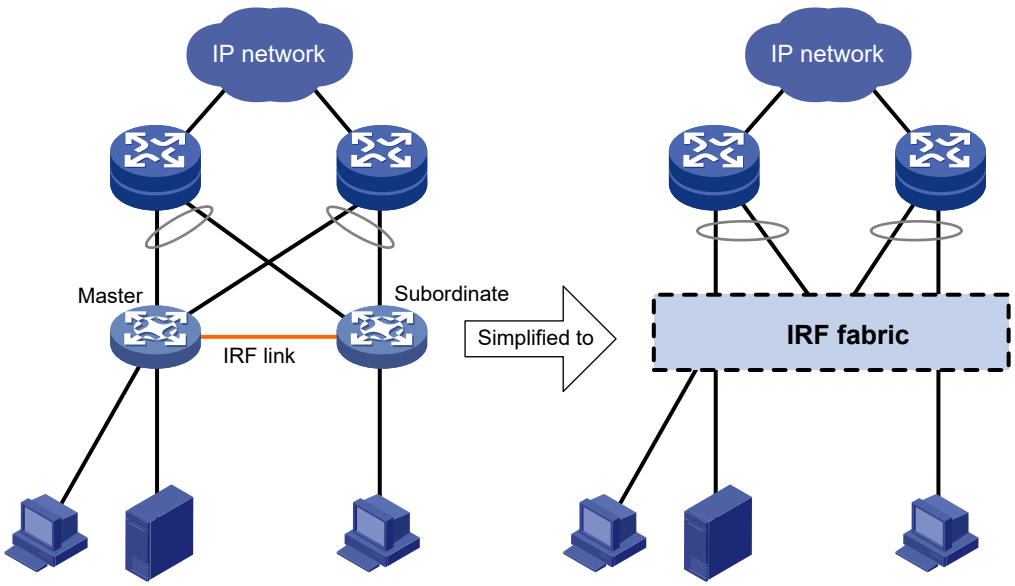
1.1. 概要

IRF(Intelligent Resilient Framework)スタック機能は、同一レイヤの複数の装置を IRF スタックポートで相互接続することにより、仮想的に 1 つの装置とすることができます。データセンタクラスの有効性、柔軟性を提供します。IRF スタック仮想化技術は複数の装置の電力、装置間の動作、管理、連続したメンテナンスを一括して行うことができます。

1.1.1. IRF スタックネットワークモデル

図 1-1 に 2 つのメンバ装置がある IRF スタックユニットを示します。上位レイヤおよび下位レイヤのユーザには、1 つの装置として見えます。

図 1-1 IRF スタックアプリケーションシナリオ



1.1.2. IRF スタックの利点

IRF スタックは以下の利点があります。

- **簡素化されたトポロジと容易な管理**—IRF スタックユニットは 1 つのノードとして、ネットワーク上で 1 つの IP アドレスでアクセス可能です。IRF スタックユニットのすべてのメンバ装置を管理するために、この IP アドレスを使用し、メンバ装置にログインすることができます。加えて IRF スタックメンバ装置でスパニングツリーを動作させる必要がありません。
- **1:N 冗長性**—IRF スタックユニット全体を管理し、制御するため、IRF スタックで 1 つのメンバ装置が Master として動作します。Master をバックアップする間、ほかのすべてのメンバは

サービスを処理します。Master が故障したとき、ほかのメンバ装置はサービスを中断することなく、メンバ装置の中から新しい Master を選定します。

- **IRF スタックリンクアグリゲーション**–負荷分散されたリンクアグリゲート IRF スタック接続を作成するため、隣接したメンバ装置間で、IRF スタックポートに複数の物理リンクを割り当てることができます。
- **マルチシャーシリンクアグリゲーション**－IRF スタックユニットと IRF スタックメンバを経由して上流あるいは下流の装置間で物理リンクを集約するために、Ethernet リンクアグリゲーション機能を使用することができます。
- **ネットワークのスケーラビリティと信頼性**－IRF スタックユニットの処理能力はすべてのメンバ装置の全処理能力と同一です。ネットワークのトポロジを変更することなく、メンバ装置を追加することで容易に、ポート、ネットワーク帯域幅、IRF スタックユニットの処理能力を増加することができます。

1.1.3. 基本コンセプト

I. IRF スタックメンバ役割

IRF スタックは、Master と standby（ここでは subordinate と呼ばれます）の 2 つのメンバの役割(ロール)を使用します。

装置は IRF スタックユニットを形成するとき、IRF スタックユニットを管理、制御するため、Master を選定し、ほかの装置は Master をバックアップします。Master 装置が故障したとき、ほかの装置が自動的に新しい Master を選定します。Master の選定についての詳細は、セクション 2 *IRF スタック オペレーションマニュアル*の"*IRF スタックの概要*"の"*Master の選定*"を参照してください。

II. IRF スタックメンバ ID

IRF スタックユニットでは、メンバ装置を識別し、管理するためにメンバ ID を使用します。メンバ ID 情報は、IRF スタックユニットのインタフェースとファイルを識別するため、インタフェースをインタフェース番号とファイルのパスの最初の部分が含まれます。2 つの装置が同じ IRF スタックメンバ ID を持つとき、IRF スタックユニットを形成することはできません。装置の IRF スタックメンバ ID がすでに IRF スタックユニットで使用されている場合、装置は IRF スタックに加入することができません。

III. メンバプライオリティ

メンバプライオリティで IRF スタックの役割を決めます。高いプライオリティを設定したメンバ装置が Master になりやすくなります。

IV. IRF スタックポート

IRF スタックポートは IRF スタックメンバ装置間の接続を行うための論理的なインタフェースです。IRF が有効な各装置は 2 つの IRF スタックポートをサポートします。

IRF スタックポートは IRF スタックポート *n*/1、IRF スタックポート *n*/2 と記載され、*n* は装置のメンバ ID です。本書では、2 つの IRF スタックポートを IRF スタックポート 1、IRF スタックポート 2 と表記します。

IRF スタックポートを使用するため、最小限 1 つの IRF スタック物理ポートを IRF スタックポートに結びつける必要があります。IRF スタックポートに割り当てられた IRF スタック物理ポートは自動的にアグリゲート IRF スタックリンクを形成します。IRF スタックのすべての IRF スタック物理ポートがダウンした場合、IRF スタックポートはダウンします。

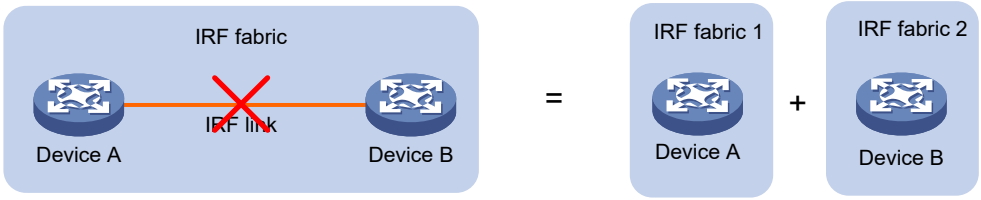
V. IRF スタック物理ポート

IRF スタック物理ポートは IRF スタックメンバ装置に接続し、IRF スタックポートに結びつける必要があります。IRF スタック物理ポートは、IRF スタックメンバ装置間の IRF スタックプロトコルパケットと、IRF スタックメンバ装置を通過するデータパケットを転送します。

VI. IRF スタックの分裂

図 1-2 に示すように、IRF スタックユニットで障害が発生した際、2 つ以上の IRF スタックユニットに分裂します。分裂した IRF スタックは同一 IP アドレスで動作するため、ネットワークのルーティングと転送の問題を引き起こします。マルチアクティブコリジョンを早急に検知するため、最小限 MAD メカニズムを設定してください。(セクション 2 *IRF スタック オペレーションマニュアル*の "*IRF スタック*"の“MAD の設定”を参照してください。)

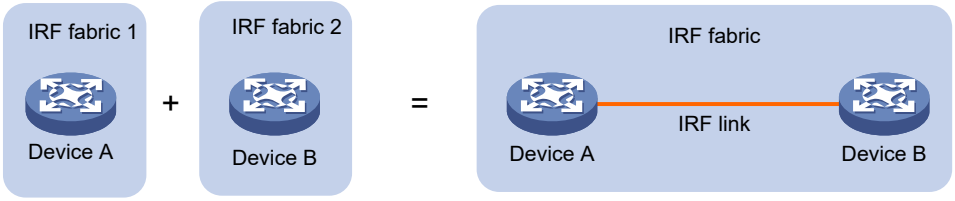
図 1-2 IRF スタックの分裂



VII. IRF スタックの結合

IRF スタックの結合とは、図 1-3 のように分裂した 2 つの IRF スタックユニットを再結合したり、2 つの独立な IRF スタックユニットを接続します。

図 1-3 IRF スタックの結合



VIII. MAD

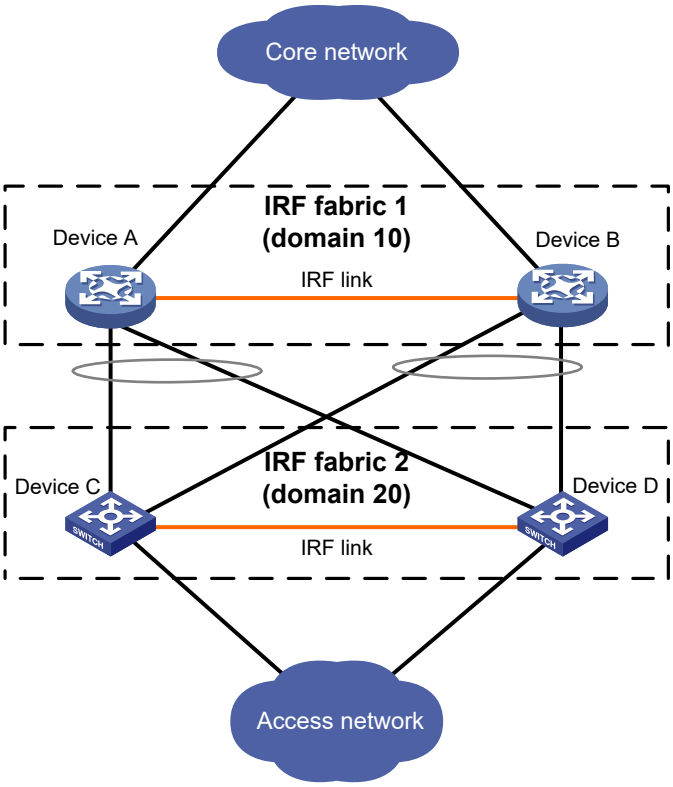
IRF スタックリンクに障害が発生すると、同一 IP アドレスが含まれる同一レイヤ 3 の設定で動作する 2 つの IRF スタックユニットに分裂します。IP アドレスの衝突とネットワークの問題を防ぐため、IRF スタックは複数の IRF スタックユニットを識別し、衝突を処理し、故障から回復する MAD（multi-active detection）メカニズムを使用します。

IX. IRF スタックドメイン ID

IRF スタックユニットは 1 つの IRF スタックドメインを形成します。IRF は IRF スタックユニットを識別するために IRF スタックドメイン ID を使用し、IRF スタックユニットが互いに干渉しないようにします。

図 1-4 に示すように、Device A と Device B は IRF 1 を形成しています。Device C と Device D は IRF 2 を形成しています。各 IRF スタックユニットは LACP MAD のリンクを持っています。メンバ装置が MAD 用の拡張 LACP パケットを受信したとき、パケットがローカル IRF スタックユニットから受信したのかどうかを調べるため、パケットのドメイン ID を確認します。それにより、Device は正しくパケットを処理することができます。

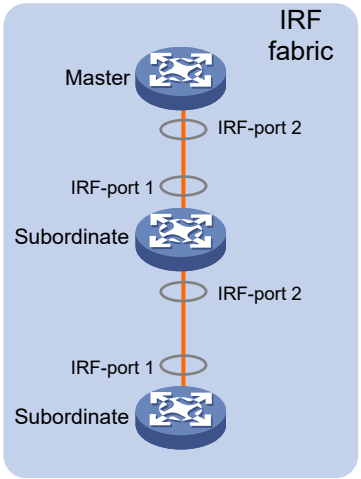
図 1-4 2 つの IRF スタックドメインによるネットワーク



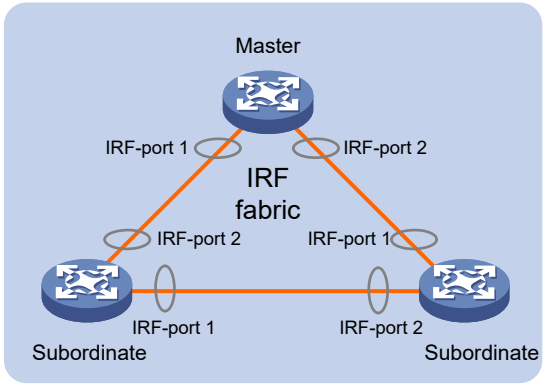
1.1.4. IRF スタックネットワークトポロジ

IRF スタックは、デイジーチェーン構成、またはリング構成のトポロジを構成することができます。リング構成は信頼性のある構成となります(図 1-5 を参照してください。)。リング構成では 1 つのリンクが故障しても、IRF スタックの分裂を起こさず、IRF スタックサービスに影響を与えないでデイジーチェーン構成になります。

図 1-5 デイジーチェーン構成とリング構成



Daisy-chain topology



Ring topology

1.1.5. Master の選定

Master の選定は以下の状況下で IRF スタックユニットのトポロジの変更があるたびに行われます。

- IRF スタックユニットが確立されました。
- Master 装置の故障や取り外しが行われました。
- IRF スタックユニットが分裂しました。
- 独立した IRF スタックユニットが結合しました。

🕮 **メモ：**

Master の選定は分裂した 2 つの IRF スタックユニットを結合するときには行われません。結合した IRF スタックユニットの Master 装置の詳細はセクション 2 *IRF スタック オペレーションマニュアル*の"*IRF スタック*"の“*故障回復*”を参照してください。

Master の選定は降順で以下のルールを使用します。

1. 新しい IRF スタックメンバのプライオリティが高くても現在の Master が有効となります。

   IRF スタックユニットが形成中で、すべての IRF スタックメンバがそれぞれ Master と認識している場合、このルールは省略されます。

2. より高いプライオリティを持つ IRF スタックメンバが有効となります。すべての IRF スタックメンバが同一のプライオリティである場合、このルールは省略されます。
3. システムの稼動時間がもっとも長いメンバ装置が有効となります。

   スタートアップから 10 分以内である場合、稼働時間は同時とみなされます。これらのメンバ装置は次の tiebreaker が適用されます。

4. もっとも低い CPU MAC アドレスを持つメンバ装置が有効になります。

新しい IRF スタックユニットをセットアップするため、subordinate (Standby)メンバ装置は、Master の選定が行われた後、再起動する必要があります。

IRF スタックユニットの結合を行う間、Master の選択に失敗した IRF スタックユニットのメンバは手動で再起動する必要があります。

1.1.6. インタフェースの命名規則

インタフェース名は *chassis-number/slot-number/port-index* のフォーマットで命名されます。

- *chassis-number*–スイッチの IRF スタックメンバ ID です。デフォルトは 1 です。スイッチが IRF スタックユニットの一部かどうかにかかわらず、常に IRF スタックメンバ ID が適用されます。スイッチが 1 台である場合、スタンドアロン（1 台構成）の IRF スタック構成であると認識します。
- *slot-number*–装置のフロントパネルあるいは背面にある拡張インタフェースカードのスロット番号です。
  - フロントパネルのスロット番号は 0 です。

- 背面にある拡張インタフェーススロットに搭載されている拡張インタフェースカードのスロット番号は 1 です。

- *interface-index*–装置のインタフェースのインデックスです。インタフェースのインデックスは装置で有効なポート数に依存します。インタフェースのインデックスを識別する場合、装置のポートインデックスマークを参照してください。

例：

スタンドアロンのスイッチにて GigabitEthernet 3/0/1 は装置の最初のポートを示します。リンクタイプをトランクに設定します。

<Switch> system-view

[Switch] interface gigabitethernet 3/0/1

[Switch-GigabitEthernet3/0/1] port link-type trunk

1.1.7. ファイルシステム命名規則

スタンドアロンの IRF スタックユニットの装置のファイルシステムにアクセスするには、記憶媒体の名前を用いることができます。

複数の装置から構成される IRF スタックユニットでは、Master のファイルシステムにアクセスするため、記憶媒体の名前を用いることができます。ほかの IRF スタックメンバのファイルシステムに、**slot***member-ID#storage-device-name* のフォーマットを用いて、アクセスすることができます。

記憶媒体の命名規則の詳細はセクション 1 *はじめに オペレーションマニュアルの“ファイルシステム管理”*を参照してください。

例：

- Master 装置に搭載されているフラッシュのルートディレクトリ直下の **test** フォルダにアクセスするには、以下のステップを実行してください。

  <Master> mkdir test

  Creating directory flash:/test... Done.

  <Master> cd test

  <Master> dir

  Directory of flash:/test

  The directory is empty.

  514048 KB total (48140 KB free)

- IRF スタックメンバ 3 に搭載されているフラッシュのルートディレクトリ直下の **test** フォルダにアクセスするには、以下のステップを実行してください。

  <Master> mkdir slot3#flash:/test

  Creating directory slot3#flash:/test... Done.

  <Master> cd slot3#flash:/test

  <Master> dir

  Directory of slot3#flash:/test

  The directory is empty.

  514048 KB total (48140 KB free)

1.1.8. 設定の同期メカニズム

IRF スタックは厳密なカレントコンフィグレーション同期メカニズムを使用します。IRF スタックユニットで、すべての装置は Master のカレントコンフィグレーションを取得し稼働させます。設定の変更は自動的に Master から残された装置に伝番されます。これらの装置のコンフィグレーションファイルは保持されますが、コンフィグレーションファイルは適用されません。IRF スタックユニットから削除されたのち、自身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を使用して起動します。

装置を IRF スタックユニットにメンバとして追加する前に、装置の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をバックアップしてください。

メンバ装置の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は、Master とメンバで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に同一のファイル名を使用する場合、上書きされる可能性があります。バックアップファイルを使用すると、IRF スタックユニットからメンバを削除した後に元の設定を復元できます。

コンフィグレーション管理の詳細はセクション 1 *はじめに オペレーションマニュアル*の"*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。

1.1.9. マルチアクティブの検知の処理

マルチアクティブの処理は検知、衝突処理、故障回復があります。

I. 検知処理

IRF スタックは LACP、BFD、ARP を拡張することによって MAD メカニズムを提供します。

MAD メカニズムはドメイン ID とアクティブ ID(Master のメンバ ID)で各 IRF スタックユニットを識別します。もし複数のアクティブ ID をドメイン内で検知すると、MAD は IRF スタックの衝突や分裂が起こったと判断します。

MAD メカニズムの詳細は、セクション 2 *IRF スタック オペレーションマニュアル*の"*IRF スタック*"の"*MAD メカニズム*"を参照してください。

II. 衝突処理

MAD がマルチアクティブ衝突を検出したとき、MAD は 1 つの IRF スタックユニットを除いたすべての IRF スタックユニットを Recovery 状態にします。Recovery 状態に変更していない IRF スタックはトラフィックを転送することができます。Recovery 状態の IRF スタックユニットは非アクティブで、トラフィックを転送することができません。

LACP MAD、BFD MAD は、以下の手順でマルチアクティブ衝突を処理します。

LACP MAD は、以下の手順でマルチアクティブ衝突を処理します。

1. それぞれの IRF スタックでメンバ数を比較します。
2. メンバ数がもっとも多い IRF スタックユニットを除いた IRF スタックユニットを Recovery 状態にします。
3. メンバ数が同じ場合、LACP MAD は Master のメンバ ID を比較します。
4. もっとも数字の小さい Master のいる IRF スタックユニットを除いた IRF スタックユニットを Recovery 状態にします。

5. Recovery 状態となった IRF スタックユニットで、以下のポートを除いたすべての IRF スタック物理ポートをシャットダウンします。
   - IRF スタック物理インタフェース
   - **mad exclude interface** コマンドで指定されたポート

対照的に ARP MAD は、IRF スタックユニットのメンバ数を比較しません。MAD メカニズムは以下の処理でマルチアクティブ衝突を行います。

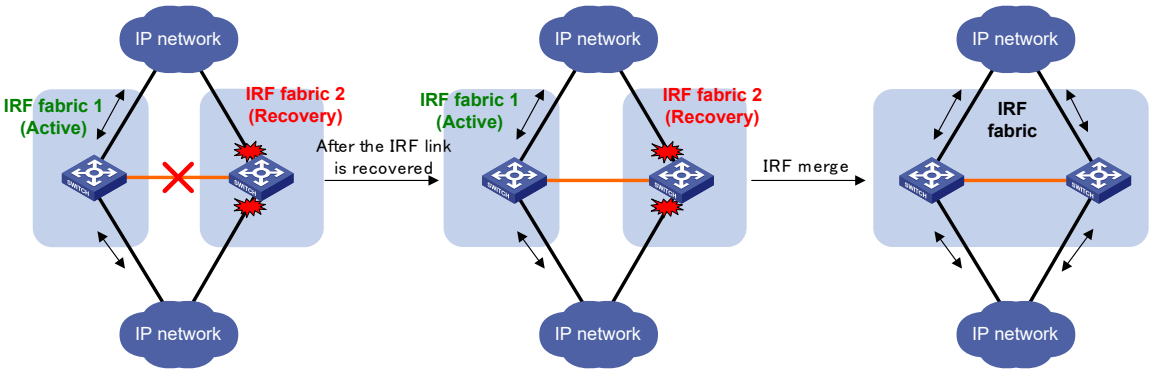
1. IRF スタックユニットの Master のメンバ ID を比較します。
2. もっとも数字の小さい Master のいる IRF スタックユニットを除いた IRF スタックユニットを Recovery 状態にします。
3. Recovery 状態となった IRF スタックユニットのネットワークポートに LACP MAD、BFD MAD と同様の設定をします。

III. 故障回復

2 つの分割された IRF スタックユニットを結合するため、故障した IRF スタックリンクを修復し、IRF スタックリンクの故障を取り除きます。

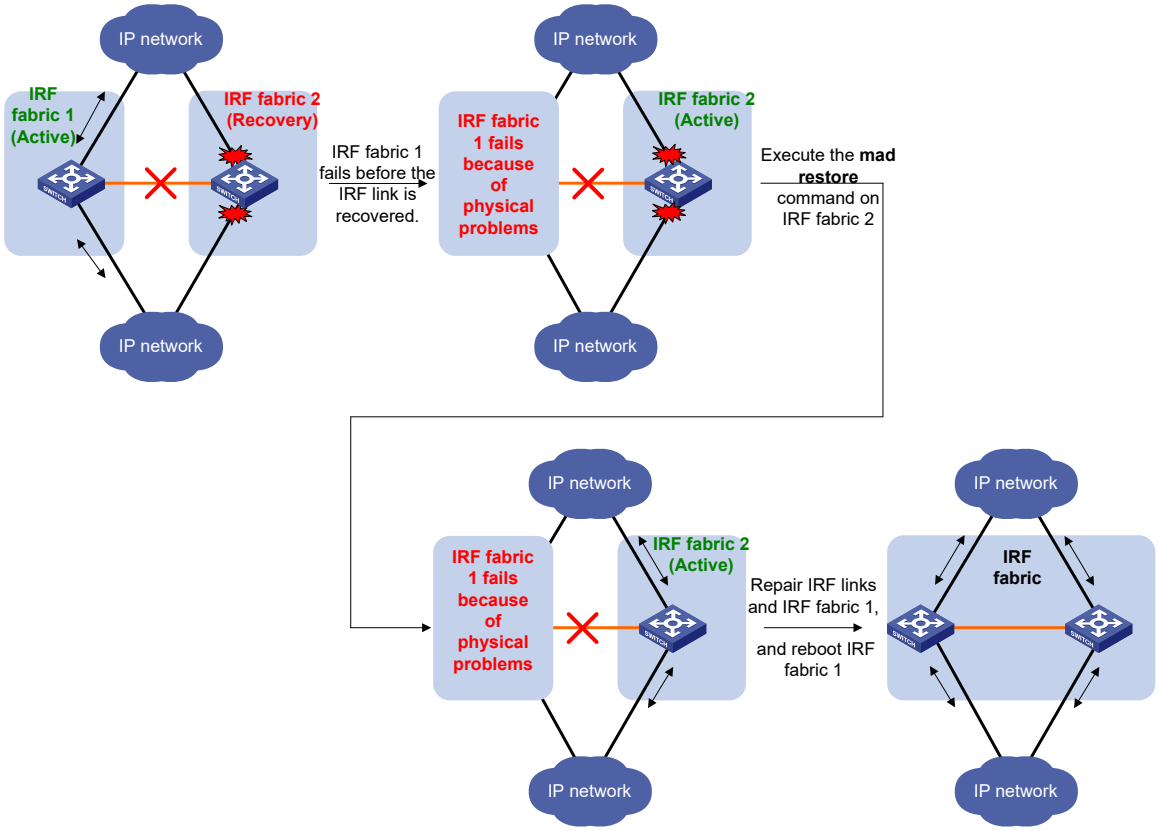
分裂した IRF スタックユニット間で故障した IRF スタックリンクが回復したとき、アクティブでない IRF スタックユニットのすべてのメンバ装置は subordinate(Standby)メンバとしてアクティブの IRF スタックユニットに加入します。そして MAD によってシャットダウンされたネットワークポートは、図 1-6 に示すようにもとの状態に戻ります。

図 1-6 IRF スタックユニットの回復



IRF スタックリンクが回復する前にアクティブ状態の IRF スタックユニットが、故障した場合(図 1-7 を参照してください)、アクティブ状態でない IRF スタックユニットを回復するため、**mad restore** コマンドを実行してください。このコマンドはアクティブ状態でない IRF スタックユニットを Detect 状態に変更し、MAD によってシャットダウンとなったすべてのネットワークポートをアクティブ状態に変更します。IRF スタックリンク障害が回復したのち、IRF スタックが結合されます。

図 1-7 IRF スタックリンクが回復する前にアクティブ状態の IRF スタックユニットが故障した場合



1.1.10. MAD メカニズム

IRF スタックは LACP、BFD、ARP を拡張することで MAD メカニズムを提供します。

表 1-1 に MAD メカニズムとアプリケーションの比較を示します。

表 1-1 MAD 機能の比較

MAD 機能	長所	短所	アプリケーション
LACP MAD	• 検知速度が速いです。 • MAD 専用の IRF スタック物理ポートあるいはレイヤ 3 インタフェースが不必要です。	拡張LACPをサポートする中継装置が必要です。	IRFスタックユニットと上流または下流装置との間でリンクアグリゲーションを使用します。
BFD MAD	• 検知速度が速いです。 • 中継装置を使用する場合、ベンダの制限はありません。	ユーザトラフィックの転送に使用しないMAD専用ポートやレイヤ3インタフェースが必要です。	• さまざまなネットワーク構成に適用されます。 • 中継装置を使用しない場合、お互いのスイッチが近くに設置され少数のメンバで構成される

MAD 機能	長所	短所	アプリケーション
			IRF スタックユニットに適します。
ARP MAD	• 中継装置が不要です。 • 中継装置を使用する場合、ベンダの制限はありません。 • MAD 専用の IRF スタック物理ポートが不必要です。	• 検知速度が BFD MAD や LACP MAD より遅いです。 • ARP MAD リンクで共通の Ethernet ポートを使用している場合、スパニングツリー機能の有効化が必要です。	共通のEthernetポートを使用している場合、リンクアグリゲーションを使用せず、スパニングツリーを有効化するIPv4ネットワークに適します。

II. LACP MAD

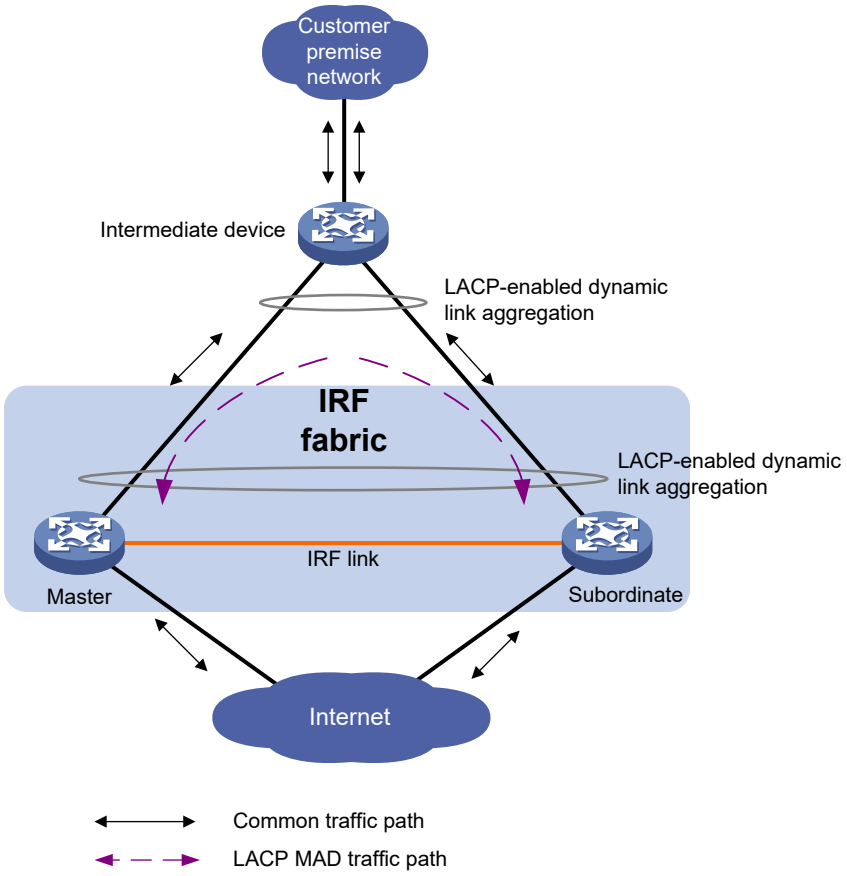
図 1-8 に示すように、LACP MAD は以下の要件があります。

- 各 IRF スタックメンバは中間装置（対向装置）とリンクしている必要があります。
- すべてのリンクはダイナミックリンクアグリゲーショングループを形成する必要があります。
- 中間装置は拡張 LACP をサポートする必要があります。

IRF スタックメンバ装置は、IRF スタックユニットのドメイン ID とアクティブ ID を含んだ拡張 LACP データユニット(LACPDU)を送信します。中間装置は、1 つの IRF スタックメンバ装置からの拡張 LACP データユニットをほかのすべての IRF スタックメンバ装置に転送します。

- すべての IRF スタックメンバ装置が送信する拡張 LACPDU 内のドメイン ID とアクティブ ID が同じならば、IRF スタックユニットが正常に動作していると判断します。
- ドメイン ID が同じであってもアクティブ ID が異なる場合、IRF スタックが分裂していると判断します。この場合、LACP MAD はセクション 2 *IRF スタック オペレーションマニュアル*の“*IRF スタック*”の”*衝突処理*”に説明した衝突処理を行います。

図 1-8 LACP MAD シナリオ



III. BFD MAD

BFD MAD は BFD を使用することでマルチアクティブ衝突を検知します。

BFD MAD は共通あるいはマネジメント Ethernet ポートを使用することができます。

マネジメント Ethernet ポートを使用する場合、中継装置が必要です。以下の要件に従うかどうか確認してください。

- 各 IRF スタックのメンバ装置は中継装置に接続する BFD MAD リンクがあります。
- 各 IRF スタックのメンバ装置はマスタ装置のマネジメント Ethernet ポートの MAD IP アドレスが割り当てられます。

共通 Ethernet ポートを使用する場合、以下の要件に従うかどうか確認してください。

- 各 IRF スタックのメンバ装置が中継装置に接続する BFD MAD リンクがあるか、すべてのメンバ装置が互いに BFD MAD リンクがあります。
- 中継装置がない場合、すべてのメンバ装置は互いに BFD MAD リンクがある必要があります。IRF スタックユニットに 2 つ以上のメンバ装置がある場合、IRF スタックメンバ装置に接続するため、中継装置を使用することを推奨します。IRF スタックメンバをフルメッシュにした場合、ブロードキャストループを発生する可能性があります。
- BFD MAD リンクの各ポートは BFD MAD で使用する VLAN インタフェースに割り当てられます。各メンバ装置は VLAN インタフェースの MAD IP アドレスが割り当てられます。

BFD MAD リンクあるいは BFD MAD VLAN は専用のリンクが必要です。ほかの目的で BFD MAD リンクあるいは BFD MAD VLAN を使用しないでください。

メモ:

- BFD MAD リンクに接続されているポートに同じ VLAN を割り当ててください。
- IRF スタックユニットのすべてのマネジメント Ethernet ポートで、マスタのマネジメント Ethernet ポートのみがアクセス可能です。

図 1-9 に、中継装置を使用する一般的な BFD MAD シナリオを示しています。中継装置で、BFD MAD リンク上のポートを同じ VLAN に割り当てます。

図 1-10 に、中継装置を使用しない一般的な BFD MAD シナリオを示します。

BFD MAD では、Master は、送信元 IP アドレスとして MAD IP アドレスを使用して、他のメンバデバイスとの BFD セッションを確立しようと試みます。

- IRF スタックユニットが結合されている場合、Master の MAD IP アドレスのみが有効になります。 Master は他のメンバと BFD セッションを確立できません。 **display bfd session** コマンドを実行すると、BFD セッションの状態は **Down** になります。
- IRF スタックユニットが分裂すると、分裂した IRF スタックユニット内の Master の IP アドレスが有効になります。Master は BFD セッションを確立できます。**display bfd session** コマンドを実行すると、2 つのデバイス間の BFD セッションの状態は Up になります。

図 1-9 中継装置を使用する一般的な BFD MAD シナリオ

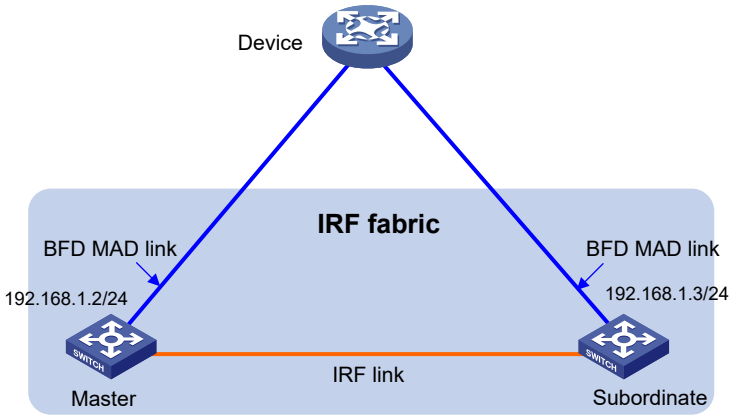
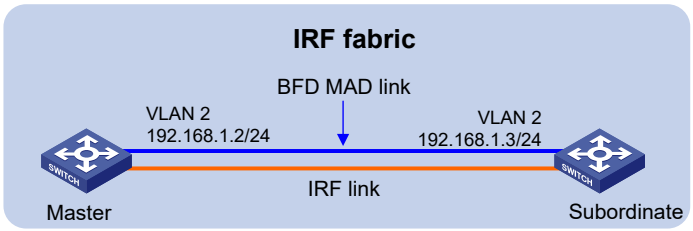


図 1-10 中継装置を使用しない一般的な BFD MAD シナリオ



IV. ARP MAD

ARP MAD は、IRF ドメイン ID とアクティブ ID を含んだ拡張 ARP パケットによってマルチアクティブ衝突を検知します。

ARP MAD は共通 Ethernet ポート、マネジメント Ethernet ポートで使用することができます。

マネジメント Ethernet ポートを使用する場合、ARP MAD は中継装置で動作する必要があります。以下の要件に従ってください。

- 各メンバ装置のマネジメント Ethernet ポートを中継装置に接続してください。
- 中継装置で ARP MAD に使用するポートは同一 VLAN にしてください。

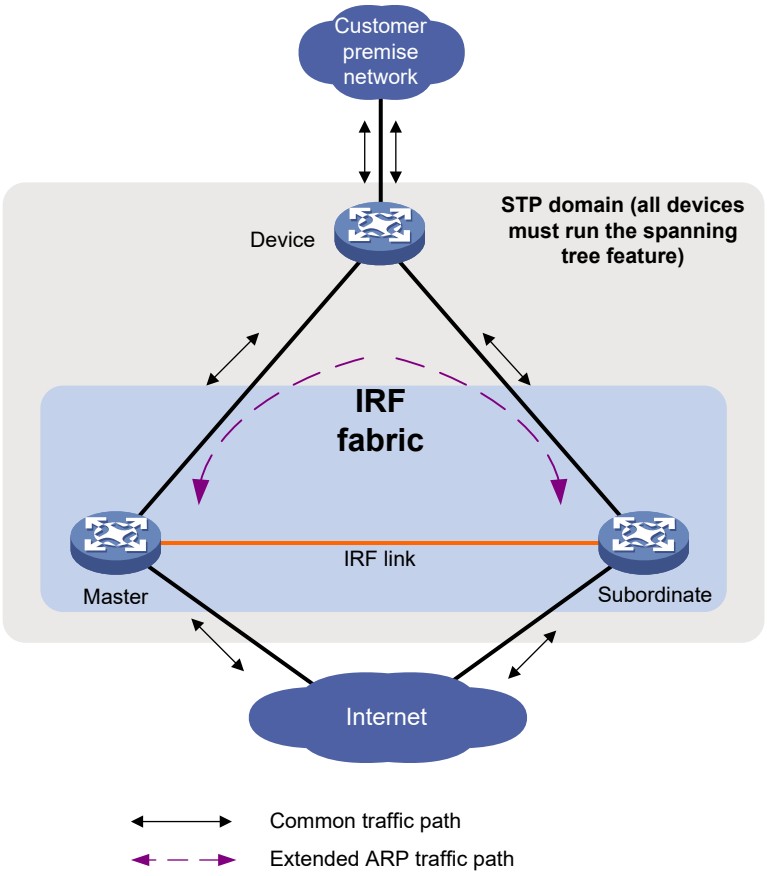
共通 Ethernet ポートを使用する場合、中継装置への接続に関わらず、ARP MAD が動作することができます。以下の要件に従ってください。

- 中継装置を使用する場合、図 1-11 に示すように各メンバ装置を中継装置に接続してください。IRF スタックユニットと中継装置間でスパニングツリー機能を動作させてください。この状態ではデータリンクは使用することができます。
- 中継装置を使用しない場合、各 IRF スタックメンバ装置をほかのメンバ装置に接続してください。この状態では IRF スタックリンクは ARP MAD として使用することができません。

各 IRF スタックメンバは、受信した拡張 ARP パケットに含まれるドメイン ID とアクティブ ID を比較します。

- ドメイン ID が異なる場合、異なる IRF スタックメンバユニットからの拡張 ARP パケットと判断し、MAD メカニズムの処理を継続しません。
- ドメイン ID が同じ場合、装置はアクティブ ID を比較します。
  - アクティブ ID が異なる場合、IRF スタックユニットが分裂していると判断します。
  - アクティブ ID が同じ場合、IRF スタックユニットは正常に動作していると判断します。

図 1-11 ARP MAD シナリオ



1.2. 制限とガイドライン

1.2.1. IRF スタックのハードウェアの互換性

QX-S5300G シリーズ Ethernet スイッチは、QX-S5300G シリーズの装置でのみ IRF スタックユニットを形成することができます。

メモ:

QX-S5300G シリーズは最大 9 台の装置で IRF スタックを形成することができます。NEC では最大 6 台の装置で IRF スタックを形成することを推奨します。

1.2.2. IRF スタックのソフトウェア

すべての IRF スタックメンバは、同じソフトウェアバージョンを使用してください。すべてのメンバ装置でソフトウェアオートアップグレード機能ができることを確認してください。

1.2.3. IRF スタック物理インタフェースの選択

IRF スタック物理インタフェースとして以下のポートを使用します。

- 10GBASE-T autosensing Ethernet ポート
- SFP+ポート
- QSFP+ポート

メモ:

QSFP+ポートを 10-GE 4 ポートとして分割したインタフェースは IRF スタック物理インタフェースとして使用することはできません

1.2.4. IRF スタックのトランシーバモジュールとケーブルの選定

トランシーバモジュールとケーブルを選択するとき、以下の制限とガイドラインに従ってください。

- 短い距離で通信するために 10GE ポートを接続する場合、カテゴリ-6 以上のツイストペアケーブルを使用してください(カテゴリ-6、カテゴリ-6A を含みます)。
- 短い距離で通信するために SFP+/QSFP+ポートを接続する場合、SFP+/QSFP+ 銅線ケーブルを使用してください。
- 長い距離で通信する場合、SFP+/QSFP+ポートを接続する場合、SFP+/QSFP+光ファイバケーブルを使用します。
- トランシーバモジュールは、IRF スタックリンクの対向ポートと同じタイプを使用してください。

SFP+/QSFP+ポート、SFP+/QSFP+ 銅線ケーブル（DAC）、SFP+/QSFP+ トランシーバモジュールの詳細は、*QX-S5300G シリーズ Ethernet スイッチ インスタレーションマニュアル*を参照してください。

メモ:

本装置に使用するトランシーバモジュールとケーブルは、NEC 指定の SFP+/QSFP+ トランシーバモジュール、SFP+/QSFP+ケーブル（DAC）を使用してください。
なお、サポートする SFP+/QSFP+ トランシーバモジュールと SFP+/QSFP+ケーブル（DAC）は、変更する可能性があります。

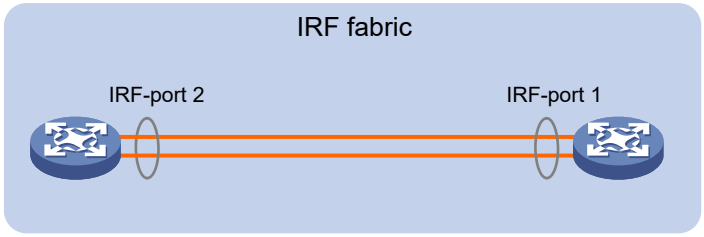
1.2.5. IRF スタックポートの接続

2 つの隣接する IRF スタックメンバを接続するとき、以下の制限とガイドラインに従ってください。

- 一方のメンバの IRF スタックポート 1 の IRF スタック物理インタフェースを他方の IRF スタックポート 2 の IRF スタック物理インタフェースに接続してください。

- 一方のメンバ装置の両方の IRF スタックポートの IRF スタック物理インタフェースをほかの装置の両方の IRF スタックポートの IRF スタック物理インタフェースに接続しないでください。

図 1-12 IRF スタック物理インタフェースの接続



1.2.6. IRF スタック物理インタフェースの制限とガイドライン

I. コマンドの制限

IRF スタックポートに関連付けられている物理インタフェースでは以下のコマンドのみ実行することができます。

- 以下のインタフェースコマンド
  - **description**
  - **flow-interval**
  - **shutdown**

  詳細は Chapter 3 *Layer 2 - LAN Switching Command References* の“*Ethernet interface commands*”を参照してください。
- MAC アドレステーブルの **mac-address static source-check enable** コマンドを実行することができます。詳細は Chapter 3 *Layer 2 - LAN Switching Command References* の“*MAC address table commands*”を参照してください。
- 以下の LLDP コマンド
  - **lldp admin-status**
  - **lldp check-change-interval**
  - **lldp enable**
  - **lldp encapsulation snap**
  - **lldp notification remote-change enable**
  - **lldp tlv-enable**

  詳細は Chapter 3 *Layer 2 - LAN Switching Command References* の“*LLDP commands*”を参照してください。

IRF スタック物理インタフェースで **mirroring-group reflector-port** コマンドを実行したとき、物理インタフェースと IRF スタックポート間のバインディングが削除されます。インタフェースが IRF スタックポートのメンバインタフェースだけになる場合、IRF スタックの分裂を避けるため、リフレクタポートとして物理インタフェースを設定しないでください。コマンドの詳細は Chapter 11 *Network Management and Monitoring Command References* の“*Port mirroring commandss*”を参照してください。

II. IRF スタック物理インタフェースのループ除去メカニズムと SNMP のモニタリング

IRF スタックメンバ装置がパケットを転送する前に、送信元と宛先の物理インタフェースと IRF スタックトポロジにもとづいて、フォワーディングパス上にループが存在するかどうかを識別します。ループが存在する場合、装置はループパスの送信元インタフェース上のパケットを破棄します。このループ除去メカニズムは、IRF スタック物理インタフェース上で大量のブロードキャストパケットを削除します。 SNMP ツールを使用するときにパケット廃棄の SNMP 通知を減らすには、IRF スタック物理インタフェースでパケット転送を監視しないでください。

1.3. IRFスタック設定作業リスト

IRF スタック設定作業リスト
1. IRF スタックユニットの設定
2. MAD の設定 IRFスタックユニットで少なくとも1つのMADメカニズムを設定してください。 MADの互換性についての詳細はセクション2 *IRFスタック オペレーションマニュアル*の“*IRF スタック*”の“*MADメカニズムの互換性*”を参照してください。 • LACP MAD の設定 • BFD MAD の設定 • ARP MAD の設定 • MAD によるシャットダウンアクションからのサービスインタフェースの除外 この機能は、IRFスタックユニットが**Recovery**状態に移行するときに、管理またはその他の特別な目的のためのシャットダウンアクションからサービスインタフェースを除外します。 • IRF スタックの回復
3. （オプション設定項目）IRF スタックユニットの IRF スタックの設定の最適化 • メンバ装置の説明の設定 • IRF スタックの bridge MAC アドレスの設定 • ソフトウェア同期用のソフトウェアオートアップグレードの有効化 この機能は、Masterの現在のソフトウェアイメージを、IRFスタックユニットに結合しようとしている装置と自動的に同期します。 • IRF スタックリンクダウン検出遅延の設定 • IRF スタック物理インタフェースを持つ拡張インタフェースカードの取り外し • IRF スタック物理インタフェースを持つ拡張インタフェースカードの交換

1.4. IRFスタックユニットのセットアップの計画

IRF スタックユニットを構成するとき、以下の点を検討してください。

- ハードウェアの互換性と制限事項
- IRF スタックユニットの大きさ
- Master 装置
- IRF スタック物理インタフェース
- メンバ ID とプライオリティの割り当て計画

- IRF スタックユニットのトポロジとケーブル計画
- IRF スタック物理インタフェース

1.5. IRFスタックユニットの設定

重要:
IRF を構築する際は以下に注意をしてください。
・system view の設定はすべての IRF スタックメンバで同じ設定にすることを推奨します(物理インタフェース設定や slot 設定を除く)。

1.5.1. IRF スタックユニット設定作業リスト

IRF スタックユニット設定作業リスト
1. 各メンバ ID、プライオリティ、IRF スタック物理インタフェースの設定 a. 各 IRF スタックメンバ装置へのメンバ ID の割り当て b. （オプション設定項目）各メンバ装置のプライオリティの設定 c. IRF スタックポートと物理インタフェースへの関連付け メンバID、プライオリティ、IRFスタック物理インタフェースがinterface rangeで設定する場合、この作業をスキップしてください。
2. IRF スタック物理インタフェースの接続
3. IRF スタックユニットのアクセス

1.5.2. 各 IRF スタックメンバ装置へのメンバ ID の割り当て

I. 制限とガイドライン

IRF スタックユニットを設定するには、それぞれのメンバ装置に固有なメンバ ID を割り当てる必要があります。

予期せぬ設定の変更やパケットロスを避けるため、IRF スタックユニットの構築後はメンバ ID を変更しないでください。

新しいメンバ ID は、再起動することによって有効になります。装置が再起動したのち、設定が保存されていたかどうかにかかわらず物理的なリソース（物理的なネットワークポートを含む）に関連するすべてのメンバ ID の設定は削除されます。

IRF スタックユニットでは、IRF スタックメンバ ID を変更すると、望ましくない設定変更やデータ損失が発生する可能性があります。これを行う前に、設定をバックアップし、ネットワークへの影響を十分に理解しておく必要があります。

II. 設定手順

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

操作	コマンド	補足
2. メンバ装置にメンバ ID を設定する	**irf member** *member-id* **renumber** *new-member-id*	デフォルト：1
3. (オプション設定項目) 設定を保存する	**save**	IRFスタックポートにIRFスタック物理インタフェースを関連づけたり、メンバプライオリティを割り当てた場合は、再起動する前に設定を保存してください。
4. 装置を再起動する	**reboot** [**slot** *slot-number*] [**force**]	—

1.5.3. 各メンバ装置のプライオリティの設定

I. IRF スタックメンバ装置のプライオリティの設定

IRF スタックメンバプライオリティは、IRF スタックの Master に選ばれる可能性を示します。プライオリティがより高いほど、可能性は高くなります。

メンバプライオリティを変更すると、次回に Master を選ぶ際の選定に影響を及ぼしますが、すぐに Master の選定が発生することはありません。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. 装置のプライオリティを指定する	**irf member** *member-id* **priority** *priority*	デフォルト：1

1.5.4. IRF スタックポートと物理インタフェースへの関連付け

I. 制限とガイドライン

セクション 2 *IRF スタック オペレーションマニュアル*の“*IRF スタック*”の“*IRF スタック物理インタフェースの選択*”に記載されているように IRF スタック物理インタフェースとして物理インタフェースを選択します。

物理インタフェースを IRF スタックポートに関連づけた後、**irf-port-configuration active** コマンドを使用して IRF スタックポートの設定をアクティブにする必要があります。 次の状況では、IRF スタックポート設定が自動的にアクティブになります。

- デバイスが起動するコンフィグレーションファイルには、IRF スタックポートのバインディングが含まれています。
- IRF スタックユニットが形成された後、IRF スタックポート(UP 状態)に物理インタフェースを追加しています。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. interface view あるいは interface range view に移行する	• interface view に移行する: **interface** *interface-type interface-number* • interface range view に移行する: **interface range** { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-24> **interface range name** *name* [**interface** { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-24>]	IRFスタック物理インタフェースの範囲をシャットダウンするため、interface range viewに移行します。 IRFスタック物理インタフェースをシャットダウンするため、interface viewに移行します。
3. インタフェースまたはインタフェース範囲をシャットダウンする	**shutdown**	デフォルト : すべてのポートはup
4. system view に戻る	**quit**	ー
5. IRF port view に移行する	**irf-port** *member-id/port-number*	ー
6. 各 IRF スタック物理インタフェースに IRF スタックポートを関連づける	**port group interface** *interface-type interface-number*	デフォルト : 全ポート関連づけなし リンクの冗長性のため、複数のIRFスタック物理インタフェースをIRFスタックポートに割り当てる場合、このコマンドを繰り返してください。 1つの論理ポートに最大4ポートのIRFスタック物理インタフェースを関連づけることができ、装置として最大8ポートまでを関連づけることができます。
7. system view に戻る	**quit**	ー

操作	コマンド	補足
8. interface view あるいは interface range view に移行する	• interface view に移行する: **interface** *interface-type interface-number* • interface range view に移行する: **interface range** { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-24> **interface range name** *name* [**interface** { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-24>]	IRFスタック物理インタフェースの範囲をシャットダウンするため、interface range viewに移行します。 IRFスタック物理インタフェースをシャットダウンするため、interface viewに移行します。
9. インタフェースまたはインタフェース範囲を有効にする	**undo shutdown**	デフォルト : すべてのポートはup
10. system view に戻る	**quit**	—
11. 設定を保存する	**save**	IRFスタックポートの設定を有効にするとIRFスタックが結合し、再起動します。データの削除を防ぐため、操作を行う前に設定を保存してください。
12. IRF スタックポートの設定を有効にする	**irf-port-configuration active**	—

1.5.5. IRF スタック物理インタフェースの接続

制限に従う IRF スタックポートの接続は、IRF スタックの物理インタフェースと、トポロジとケーブル接続方式にもとづいています。 装置はマスタ選定を行います。 Master の選定に失敗したメンバデバイスは自動的に再起動し、Master 装置で IRF スタックユニットを形成します。

1.5.6. IRF スタックユニットのアクセス

IRF スタックが形成されると、1 つのスイッチとして操作することできます。Master の CLI で、すべての IRF スタックメンバの設定と管理を行うことができます。すべての設定は、IRF スタックメンバに自動的に反映されます。

IRF スタックユニットにアクセスする場合、以下の方法があります。

- **ローカルログイン**–メンバ装置のコンソールポートを用いてログインします

- **リモートログイン**–Telnet や SNMP を用いてメンバ装置のレイヤ 3 インタフェースにログインします。

IRF スタックユニットにログインするとき、どのメンバ装置からログインしても、実際には、IRF スタックの Master にログインします。

詳細は、セクション 1 *はじめに オペレーションマニュアル*の"*ログイン*"を参照してください。

1.6. MADの設定

1.6.1. 制限とガイドライン

I. MAD メカニズムの互換性

ベストプラクティスとして、IRF スタックユニットでの MAD メカニズムですくなくとも 1 つを、IRF スタックの分裂を迅速に検出するために設定します。 MAD メカニズムは異なるコリジョン処理プロセスを使用するため、IRF スタックユニットで複数の MAD メカニズムを構成する際には、次の制限とガイドラインに従ってください。

- LACP MAD を ARP MAD と一緒に設定しないでください。
- BFD MAD を ARP MAD と一緒に設定しないでください。

II. IRF スタックドメイン ID の割り当て

2 つの IRF スタックユニット間で LACP MAD、ARP MAD が動作する場合、各 IRF スタックユニットに一意の IRF スタックドメイン ID を割り当ててください。（BFD MAD では必須ではありません。）

IRF スタックユニットは 1 つの IRF スタックドメイン ID のみを持つことができます。

irf domain コマンド、**mad enable** コマンド、 **mad arp enable** コマンドを使用して IRF スタックドメイン ID を変更することができます。これらのコマンドを使用して設定された IRF スタックドメイン ID は、たがいに上書きされます。

III. MAD によるサービスインタフェースのシャットダウンからの除外

IRF スタックユニットが Recovery 状態に遷移するとき、ポートがシャットダウンにならないようにするため、**mad exclude interface** コマンドを使用します。Recovery 状態の IRF スタックユニットでポートをアップ状態にする場合、**undo shutdown** コマンドの代わりにコマンドを使用します。**mad restore** コマンドは Recovery 状態の IRF スタックユニットをアクティブにします。

1.6.2. LACP MAD の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. IRF スタックユニットにドメイン ID を割り当てる	**irf domain** *domain-id*	デフォルト：0

操作	コマンド	補足
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*	中継装置でもこの操作を行ってください。
4. ダイナミックアグリゲーションモードでアグリゲーショングループを設定する	**link-aggregation mode dynamic**	デフォルトでは、アグリゲーショングループはスタティックモードです。 LACP MADはダイナミックアグリゲートインタフェースでのみ有効です。 中継装置でもこの操作を行ってください。
5. LACP MAD を有効にする	**mad enable**	デフォルト：無効
6. system view に戻る	**quit**	—
7. interface view あるいは interface range view に移行する	• interface view に移行する: **interface** *interface-type interface-number* • interface range view に移行する: **interface range** { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-24> **interface range name** *name* [**interface** { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-24>]	アグリゲーショングループにポート範囲を割り当てるためにinterface range viewに移行してください。 アグリゲーショングループに1つずつポートを割り当てるためにinterface viewに移行してください。
8. ポートまたはポート範囲を指定のアグリゲーショングループに割り当てる	**port link-aggregation group** *number*	中継装置でもこの操作を行ってください。

1.6.3. BFD MAD の設定

I. 制限とガイドライン

BFD MAD を設定する前に、BFD MAD リンク方式を選択してください。セクション 2 *IRF スタックオペレーションマニュアル*の“*IRF スタック*”の“*概要*”の“*BFD MAD*”を参照してください。

BFD MAD を設定した後、BFD MAD のリンクを接続してください。

VLAN インタフェースで BFD MAD を設定するとき、以下の制限とガイドラインに従ってください。

カテゴリ	制限とガイドライン
BFD MAD VLAN	• VLAN インタフェース 1 で、BFD MAD を有効にすることはできません。 • 中継装置を使用する場合、以下の作業を行ってください。 　○ IRF スタックユニットと中継装置の両方で BFD MAD の VLAN と VLAN インタフェースを作成してください。 　○ IRF スタックユニットと中継装置の両方で BFD MAD の VLAN に BFD MAD のポートを関連付けてください。 　○ IRF スタックユニットで BFD MAD VLAN の VLAN インタフェースを作成してください。 　○ ネットワークの IRF スタックユニットは異なる BFD MAD の VLAN を使用してください。 • 正しいトラフィックの転送を行うため、BFD MAD VLAN は BFD MAD リンクのポートのみを使用してください。もし BFD MAD リンクのポートでない場合、BFD MAD VLAN からのポートを取り除いてください。たとえば **port trunk permit vlan all** コマンドですべての VLAN にポートが割り当てられている場合、BFD MAD VLAN からポートを除外するため、**undo port trunk permit** コマンドを使用してください。
BFD MAD VLANと機能の互換性	BFD MAD のVLANをほかの用途で使用しないでください。 • BFD MAD で使用される VLAN インタフェースでは **mad bfd enable** コマンドと **mad ip address** コマンドのみ設定できます。もしほかの機能を設定する場合、BFD MAD とインタフェースのほかの機能の両方は正常に動作しない可能性があります。 • BFD MAD の VLAN のポートでは、スパニングツリー機能を無効にしてください。MAD 機能はスパニングツリー機能と同時に使用することはできません。
MAD IP address	• BFD MAD を有効にした VLAN インタフェースで MAD の IP アドレスを設定する場合、**ip address** コマンドの代わりに **mad ip address** コマンドを使用してください。 • すべての MAD IP アドレスは、同じサブネット上にある必要があります。

マネジメント Ethernet インタフェースで BFD MAD を設定するとき、以下の制限とガイドラインに従ってください。

カテゴリ	制限とガイドライン
BFD MADのマネジメントEthernetポート	各IRFスタックメンバデバイス上のマネジメントEthernetポートを、中継装置の共通Ethernetポートに接続します。
BFD MAD VLAN	• 中継装置で BFD MAD 用の VLAN を作成し、BFD MAD で使用するポートを割り当ててください。IRF スタックユニットで BFD MAD が有効なマネジメント Ethernet ポートに VLAN を割り当てる必要はありません。 • ネットワークの IRF スタックユニットは異なる BFD MAD の VLAN を使用してください。 • 中継装置で BFD MAD VLAN に BFD MAD リンクのポートのみ

カテゴリ	制限とガイドライン
	が存在することを確認してください。
MAD IP address	• BFD MAD を有効にした VLAN インタフェースで MAD の IP アドレスを設定する場合、**ip address** コマンドの代わりに **mad ip address** コマンドを使用してください。 • BFD MAD が有効な VLAN インタフェースのすべての MAD IP アドレスは、同じサブネット上にある必要があります。

II. VLAN インタフェースでの BFD MAD 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）IRF スタックユニットにドメイン ID を割り当てる	**irf domain** *domain-id*	デフォルト： 0
3. BFD MAD 時に稼動する VLAN を作成する	**vlan** *vlan-id*	デフォルト：VLAN 1のみ存在します。 VLANインタフェース1で BFD MADを有効にしないでください。 中継装置がある場合、このステップを繰り返してください。
4. system view に戻る	**quit**	ー
5. interface view あるいは interface range view に移行する	• interface view に移行する: **interface** *interface-type interface-number* • interface range view に移行する: **interface range** { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-24> **interface range name** *name* [**interface** { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-24>]	BFD MAD VLANのポート範囲を割り当てるために interface range viewに移行してください。 BFD MAD VLANに1つずつポートを割り当てるために interface viewに移行してください。

操作	コマンド	補足
6. BFD MAD VLAN にポートまたはポート範囲を割り当てる	• アクセスポートとして割り当てる: **port access vlan** *vlan-id* • トランクポートとして割り当てる: **port trunk permit vlan** *vlan-id* • ハイブリッドポートとして割り当てる: **port hybrid vlan** *vlan-id* { **tagged** | **untagged** }	ポートタイプによって1つのコマンドを選択してください。 デフォルト : アクセスポート 中継装置がある場合、このステップを繰り返してください。
7. system view に戻る	**quit**	—
8. VLAN interface view に移行する	**interface vlan-interface** *vlan-interface-id*	—
9. BFD MAD を有効にする	**mad bfd enable**	デフォルト：無効
10. メンバ装置の VLAN インタフェースに MAD IP アドレスを割り当てる	**mad ip address** *ip-address* { *mask* | *mask-length* } **member** *member-id*	デフォルト：設定なし VLANインタフェースの各メンバ装置にMAD IPアドレスを割り当てる場合、操作を繰り返してください。

III. マネジメント Ethernet ポートを使用した BFD MAD 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）IRF スタックユニットにドメイン ID を割り当てる	**irf domain** *domain-id*	デフォルト： 0
3. system view に戻る	**quit**	—
4. management Ethernet interface view に移行する	**interface m-gigabitethernet** *interface-number*	IRFスタックユニットのすべてのマネジメントEthernetポートのうち、Masterのマネジメントポートのみにアクセスできます。
5. BFD MAD を有効にする	**mad bfd enable**	デフォルト：無効
6. メンバ装置の VLAN インタフェースに MAD IP アドレスを割り当てる	**mad ip address** *ip-address* { *mask* | *mask-length* } **member** *member-id*	デフォルト：設定なし

1.6.4. ARP MAD の設定

I. 制限とガイドライン

中継装置を使用する場合、ARP MAD リンクとして共通のデータリンクを使用することができます。中継装置を使用しない場合、IRF スタックメンバ装置間で専用の ARP MAD リンクを設定してください。

VLAN インタフェースで ARP MAD を設定するとき、以下の制限とガイドラインに従ってください。

カテゴリ	制限とガイドライン
ARP MAD VLAN	• VLAN インタフェース 1 で、ARP MAD を有効にすることはできません。 • 中継装置を使用する場合、IRF スタックユニットと中継装置の両方で以下の作業を行ってください。 　○ IRF スタックユニットと中継装置の両方で ARP MAD の VLAN を作成してください。 　○ IRF スタックユニットと中継装置の両方で ARP MAD リンクのポートを ARP MAD の VLAN に割り当ててください。 　○ IRF スタックユニットで ARP MAD の VLAN インタフェースを作成してください。 • ARP MAD の VLAN はほかの目的で使用しないでください。
ARP MADと機能	中継装置を使用する場合、以下の要件を確認してください。 • IRF スタックユニットと中継装置の間でスパニングツリー機能を動作させてください。転送状態の ARP MAD リンクが 1 つのみ存在することを確認してください。詳細はセクション 3 *アクセス オペレーションマニュアル*の “*STP*” を参照してください。 • IRF スタックユニットから Master が離脱した際に bridge MAC アドレスが即座に変更されるように IRF スタックユニットを設定してください。 • IRF スタックユニットに中継装置がある場合、分裂を間違って検知しないように ARP MAD を有効にした IRF スタックユニットと異なるドメイン ID を割り当ててください。

マネジメント Ethernet ポートを使用する ARP MAD を設定するとき、以下の制限とガイドラインに従ってください。

カテゴリ	制限とガイドライン
ARP MADのマネジメントEthernetポート	中継装置の共通EthernetポートをIRFスタックユニットのマネジメントEthernetポートに接続してください。
ARP MAD VLAN	中継装置でARP MADのVLANを作成してください。 VLANにARP MADで使用するポートを割り当ててください。 IRFスタックユニットではマネジメントEthernetポートをVLANに割り当てる必要はありません。
ARP MAD and feature configuration	• IRF スタックユニットから Master が離脱した際に bridge MAC アドレスが即座に変更されるように IRF スタックユニ

カテゴリ	制限とガイドライン
	ットを設定してください。 • IRF スタックユニットに中継装置がある場合、分裂を間違って検知しないように ARP MAD を有効にした IRF スタックユニットと異なるドメイン ID を割り当ててください。

II. VLAN インタフェースでの ARP MAD の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. IRF スタックユニットにドメイン ID を割り当てる	**irf domain** *domain-id*	デフォルト： 0
3. Bridge MAC アドレスのオーナが離脱したときすぐに IRF スタック Bridge MAC アドレスを変更できるように設定する	**undo irf mac-address persistent**	デフォルトでは、Bridge MACアドレスのオーナが離脱した後、6分間はBridge MACアドレスを保持します。
4. ARP MAD 時に稼動する VLAN を作成する	**vlan** *vlan-id*	デフォルト：VLAN 1のみ存在します。 VLANインタフェース1でARP MADを有効にしないでください。 中継装置がある場合、このステップを繰り返してください。
5. system view に戻る	**quit**	ー
6. interface view あるいは interface range view に移行する	• interface view に移行する: **interface** *interface-type interface-number* • interface range view に移行する: **interface range** { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-24> **interface range name** *name* [**interface** { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-24>]	ARP MAD VLANのポート範囲を割り当てる場合 interface range viewに移行してください。 ARP MAD VLANに1つずつポートを割り当てる場合 interface viewに移行してください。

操作	コマンド	補足
7. ARP MAD の VLAN にポートを割り当てる	• アクセスポートとして割り当てる: **port access vlan** *vlan-id* • トランクポートとして割り当てる: **port trunk permit vlan** *vlan-id* • ハイブリッドポートとして割り当てる: **port hybrid vlan** *vlan-id* { **tagged** | **untagged** }	ポートタイプによって1つのコマンドを選択してください。 デフォルト : アクセスポート 中継装置がある場合、このステップを繰り返してください。
8. system view に戻る	**quit**	—
9. VLAN interface view に移行する	**interface vlan-interface** *vlan-interface-id*	—
10. 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* }	デフォルト：設定なし
11. ARP MAD を有効にする	**mad arp enable**	デフォルト：無効

III. マネジメント Ethernet ポートでの ARP MAD の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. IRF スタックユニットにドメイン ID を割り当てる	**irf domain** *domain-id*	デフォルト： 0
3. Master の離脱時すぐに IRF スタック Bridge MAC アドレスを変更できるように設定する	**undo irf mac-address persistent**	デフォルトでは、Master離脱後、6分間はBridge MACアドレスを保持します。
4. management Ethernet interface view に移行する	**interface m-gigabitethernet** *interface-number*	IRFスタックユニットのすべてのマネジメントEthernetポートは、Master装置のマネジメントEthernetポートのみアクセス可能です。
5. 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* }	デフォルト：設定なし
6. ARP MAD を有効にする	**mad arp enable**	デフォルト：無効

1.6.5. MAD によるシャットダウンアクションからのサービスインタフェースの除外の設定

I. MAD によるシャットダウンアクションからのサービスインタフェースの除外

IRF スタックユニットが Recovery 状態に移行するとき、以下のサービスインタフェースを除いてネットワークのすべてのポートが自動的にシャットダウンします。

- IRF スタック物理インタフェース
- BFD MAD で使用するインタフェース
- アグリゲートインタフェースがシャットダウンから除外されている場合、アグリゲートインタフェースのメンバインタフェース

管理やほかの特別な目的のため、シャットダウン動作からネットワークポートを除外することができます。たとえば以下のようなことができます。

- シャットダウンアクションからポートを除外して、管理装置からポートに telnet することができます。
- シャットダウンアクションから VLAN インタフェースやレイヤ 2 ポートを除外して、VLAN インタフェースにログインすることができます。

II. 制限とガイドライン

レイヤ 2 ポートが複数のメンバ装置に提供されている場合、シャットダウンアクションから VLAN インタフェースとレイヤ 2 ポートを除外しないでください。シャットダウンアクションから VLAN インタフェースとレイヤ 2 ポートを除外した場合、IRF スタックユニットがアクティブ状態でもアクティブでない状態でも、VLAN インタフェースが有効となるため IP アドレス衝突を招く可能性があります。

III. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. IRF スタックユニットが Recovery 状態になるときシャットダウンアクションから除外するネットワークポートを設定する	**mad exclude interface** *interface-type interface-number*	デフォルト： Recovery状態のIRFスタックユニットのすべてのネットワークポートがシャットダウン（IRFスタック物理インタフェースとコンソールポートを除きます）

1.6.6. IRF スタックユニットの回復

I. IRF スタックユニットの回復

IRF スタックユニットの分裂の場合、IRF スタックのリンクが回復する前にアクティブな IRF スタックユニットが分裂した場合、非アクティブの IRF スタックユニットでこの処理を行い、IRF スタックユニットを回復します。手動で IRF スタックユニットを回復する場合、非アクティブな IRF スタックユニットの MAD によってシャットダウンされたすべてのサービスインタフェースが UP 状態になります。

II. 設定手順

操作	コマンド
1. system view に移行する	**system-view**
2. アクティブ状態でない IRF スタックユニットを回復する	**mad restore**

1.7. IRFスタックユニットのIRFスタックの設定の最適化

1.7.1. メンバ装置の説明の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. メンバ装置の説明を設定する	**irf member** *member-id* **description** *text*	デフォルト：設定なし

1.7.2. IRF スタックの bridge MAC アドレスの設定

重要:
IRF スタックの bridge MAC アドレスを変更すると一時的にトラフィックの通信の中断が発生します。

I. IRF スタックの bridge MAC アドレス

デフォルトで IRF スタックユニットを確立させた装置は、Bridge MAC アドレスとして Master 装置の Bridge MAC アドレスを使用します。この Bridge MAC アドレスは、たとえば LACP のように IRF スタックユニットを識別するためにレイヤ 2 プロトコルで使用され、LAN で固有な値でなければなりません。

IRF スタックユニットが結合されると、IRF スタックは IRF スタック Bridge MAC アドレスを無視し、IRF スタックユニット内の各メンバデバイスの Bridge MAC アドレスをチェックします。 2 つのメンバ装置が同じ Bridge MAC アドレスを持つ場合、IRF スタックの結合は失敗します。

IRF スタックユニットを結合した後、結合された IRF スタックユニットは IRF スタック bridge MAC アドレスとして Master の選定に選ばれた IRF スタックユニットの Bridge MAC アドレスを使用します。

IRF スタックユニットの IRF スタック Bridge MAC アドレスを設定する場合、以下の方法を使用できます。

- IRF スタック Bridge MAC アドレスの保持を設定します。

この機能は、IRF スタックユニットの MAC アドレスを IRF スタックとして継続できる時間を指定します。時間が満了すると、IRF スタックユニットは現在の Master の Bridge MAC アドレスを IRF スタック Bridge MAC アドレスとして使用します。

II. 制限とガイドライン

IRF スタック Bridge MAC アドレスを設定するとき、以下の制限とガイドラインに従ってください。

- ARP MAD でスパニングツリー機能を使用している場合、**undo irf mac-address persistent** コマンドを使用して IRF スタック Bridge MAC アドレスの永続使用を無効にする必要があります。IRF スタック Bridge MAC アドレスとして MAC アドレスを指定しないでください。
- IRF スタックユニットで複数の装置のアグリゲートリンクがある場合、**undo irf mac-address persistent** コマンドを使用しないでください。衝突が発生し、トラフィックの中断が発生する可能性があります。

III. IRF スタック Bridge MAC アドレスの保持の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. IRF スタック bridge MAC の保持を設定する	• Master が変更しても、Bridge MAC アドレスを保持する **irf mac-address persistent always** • Master の離脱後、6 分間は Bridge MAC アドレスを保持する **irf mac-address persistent timer** • Master の離脱後、すぐに Bridge MAC アドレスを変更する **undo irf mac-address persistent**	デフォルトでは、Master離脱後、6分間はBridge MACアドレスを保持します。 **irf mac-address persistent timer**コマンドは、装置の再起動、一時的なリンク障害、または意図的リンク切断によって引き起こされる不要なブリッジMACアドレスの変更を回避します

1.7.3. ソフトウェア同期用のソフトウェアオートアップグレードの有効化

I. IRF スタックのソフトウェアオートアップグレード

ソフトウェアオートアップグレード機能は、Master の現在のソフトウェアを IRF スタックユニットに参加しようとする装置と自動的に同期します。

IRF スタックユニットに加わるには、Master のソフトウェアと同じソフトウェアを使用する必要があります。

装置を IRF スタックユニットに追加するとき、ソフトウェアオートアップグレード機能は加入しようとする装置のソフトウェアを IRF スタックの Master のソフトウェアと比較します。ソフトウェアが異なる場合、装置は自動で以下の処理を行います。

1. 装置は自動的に Master からソフトウェアをダウンロードします。
2. 新しいソフトウェアとしてダウンロードしたソフトウェアを設定します。
3. 再起動し、そして再び IRF スタックユニットに加わります。

オートアップグレード機能が無効である場合、IRF スタックユニットに装置を追加する前、装置のソフトウェアを手動でアップグレードしてください。

II. 制限とガイドライン

複数のユーザがいる環境でソフトウェアオートアップグレードを正常に行うため、オートアップグレード中に再起動を行わないようにしてください。ソフトウェアオートアップデートの状態を information center に出力することができます。(詳細はセクション 11 *システム管理 オペレーションマニュアル*の"*Information Center*"を参照してください。)

IRF スタックユニットに加えようとする装置に新しいソフトウェアを格納するための十分な空き容量があることを確認してください。

もし十分なメモリ容量がない場合、装置は現在のソフトウェアを自動的に削除します。それでもメモリ容量が不十分な場合は、スイッチは自動更新を完了できません。手動で再起動を行い、BootWare メニューでいくつかのファイルを削除してください。

III. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. ソフトウェアオートアップグレード機能を有効にする	**irf auto-update enable**	デフォルト：有効

1.7.4. IRF スタックリンクダウン検出遅延の設定

I. IRF スタックリンクダウン検出遅延

リンクが短時間で状態変化する間、IRF スタックの分裂、結合が頻繁に発生しないようにするため、IRF スタックポートでリンクダウンのイベント通知を遅延させるように設定します。

IRF スタックリンク状態が up から down に変更したとき、IRF スタックポートはすぐに IRF スタックユニットに通知しません。Link-delay 時間後、IRF スタックリンク状態が down の状態である場合、IRF スタックポートは IRF スタックユニットに通知します。

IRF スタックポートは up 状態のイベントに対しては遅延させません。IRF スタックリンク状態が down から up に変更したとき、すぐに IRF スタックユニットに通知します。

II. 制限とガイドライン

IRF スタックの Link-delay が上位レイヤプロトコル(たとえば、CFD)のタイムアウトの設定よりも短いことを確認してください。この上位プロトコルのタイムアウトの時間は、上位レイヤプロトコルでリンクがダウンしたと認識する間隔です。もし Link-delay がプロトコルのタイムアウト時間より長い場合、不必要な再計算が発生する可能性があります。

以下の状況では Link-delay を 0 秒に設定してください。

- IRF スタックユニットが Master/ subordinate(Standby)あるいは IRF スタックリンクの素早い切り替えが必要である場合

- RRPP、BFD あるいは GR が使用されている場合
- IRF スタックの IRF スタック物理インタフェースをシャットダウンする、あるいは IRF スタックメンバ装置を再起動する場合(操作を完了したのち、ネットワークの状況に従って遅延を再設定します。)

III. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. Link-delay を設定する	**irf link-delay** *interval*	デフォルト：500ミリ秒

> 🕮 **メモ:**
>
> **undo irf link-delay** コマンドを実行すると、**display current-configuration** コマンドには **undo irf link-delay** と表示され、4000 ミリ秒の遅延時間でリンクダウンイベントを報告します。デフォルト値に戻す場合は、**irf link-delay** 500 コマンドを実行してください。

1.7.5. IRF スタック物理インタフェースを持つ拡張インタフェースカードの取り外し

1. 次のいずれかのタスクを実行して、一時的なパケット損失を排除します。
   - 拡張インタフェースカードの IRF スタック物理インタフェースからケーブルを取り外します。
   - **shutdown** コマンドを使用して、カード上の IRF スタック物理インタフェースをシャットダウンします。
2. 拡張インタフェースカードを取り外します。

1.7.6. IRF スタック物理インタフェースを持つ拡張インタフェースカードの交換

I. 古い拡張インタフェースカードから別の種類の拡張インタフェースカードへの交換

1. **shutdown** コマンドを使用して、古い拡張インタフェースカードの IRF スタック物理インタフェースをシャットダウンします。
2. 物理インタフェースを含む IRF スタックポートのバインディングを削除します。
3. 古い拡張インタフェースカードを取り外し、交換用拡張インタフェースカードを取り付けます。
4. **display device** コマンドを使用して、交換用拡張インタフェースカードが正しく取り付けられていることを確認します。

5. IRF スタックポートのバインディングを再設定します。セクション 2 *IRF スタック オペレーションマニュアル*の“*IRF スタック*”の“*IRF スタックポートと物理インタフェースへの関連付け*”を参照してください。
6. **irf-port-configuration active** コマンドを使用して IRF スタックポートの設定をアクティブにします。

   バインディングを追加するときに IRF スタックポートが UP 状態になっている場合、このステップをスキップできます。

II. 古い拡張インタフェースカードから同一種類の拡張インタフェースカードへの交換

1. **shutdown** コマンドを使用して、古い拡張インタフェースカードの IRF スタック物理インタフェースをシャットダウンします。
2. 古い拡張インタフェースカードを取り外し、交換用拡張インタフェースカードを取り付けます。
3. **display device** コマンドを使用して、交換用拡張インタフェースカードが正しく取り付けられていることを確認します。
4. インタフェースカードの起動後に **undo shutdown** コマンドを使用して物理インタフェースを起動します。

1.8. IRFスタックの表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
すべてのIRFスタックメンバの情報を表示する	**display irf**
IRFスタックユニットのトポロジ情報を表示する	**display irf topology**
IRFスタックのリンク情報を表示する	**display irf link**
IRFスタックの設定を表示する	**display irf configuration**
MAD設定を表示する	**display mad** [**verbose**]

1.9. IRFスタックの設定例

この章では異なる MAD を使用する場合の IRF スタックユニットの設定例を示します。

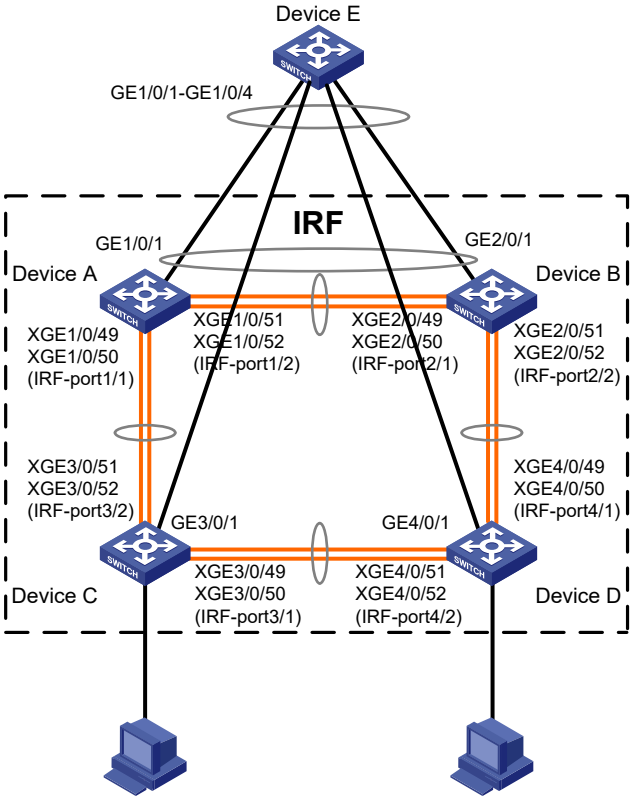
1.9.1. LACP MAD を使用する場合の IRF スタックの設定例

I. ネットワーク要件

図 1-13 に示すように、エンタープライズネットワークのアクセスレイヤで 4 台の IRF スタックユニットを設定します。

拡張 LACP をサポートする Device E に複数の装置を接続させるため、IRF スタックに LACP MAD を設定してください。

図 1-13 ネットワーク図



II. 設定手順

1. Device A を設定します。

   # interface range コマンドで IRF スタックリンクに使用する IRF スタック物理インタフェースをシャットダウンします。interface range コマンドについてはセクション 3 *アクセス オペレーションマニュアル*の“*Interface range*”を参照してください。

   <Switch> system-view

   [Switch] interface range ten-gigabitethernet 1/0/49 to ten-gigabitethernet 1/0/52

   [Switch-if-range] shutdown

   [Switch-if-range] quit

   # Ten-GigabitEthernet 1/0/49 と Ten-GigabitEthernet 1/0/50 を IRF スタックポート 1/1 に関連づけます。

   [Switch] irf-port 1/1

   [Switch-irf-port1/1] port group interface ten-gigabitethernet 1/0/49

   [Switch-irf-port1/1] port group interface ten-gigabitethernet 1/0/50

   [Switch-irf-port1/1] quit

   # Ten-GigabitEthernet 1/0/51 と Ten-GigabitEthernet 1/0/52 を IRF スタックポート 1/2 に関連づけます。

[Switch] irf-port 1/2

[Switch-irf-port1/2] port group interface ten-gigabitethernet 1/0/51

[Switch-irf-port1/2] port group interface ten-gigabitethernet 1/0/52

[Switch-irf-port1/2] quit

物理インタフェースを UP にし、設定を保存します。

[Switch] interface range ten-gigabitethernet 1/0/49 to ten-gigabitethernet 1/0/52

[Switch-if-range] undo shutdown

[Switch-if-range] quit

[Switch] save

IRF スタックポートの設定を有効にします。

[Switch] irf-port-configuration active

2. Device B を設定します。

Device B のメンバ ID を 2 に変更し、変更を有効にするため、装置を再起動します。

<Switch> system-view

[Switch] irf member 1 renumber 2

Renumbering the member ID may result in configuration change or loss. Continue? [Y/N]:y

[Switch] quit

<Switch> reboot

図 1-13 に示すように Device B を Device A に接続し、Device B にログインします。(詳細は省略します。)

IRF スタック物理インタフェースをシャットダウンします。

<Switch> system-view

[Switch] interface range ten-gigabitethernet 2/0/49 to ten-gigabitethernet 2/0/52

[Switch-if-range] shutdown

[Switch-if-range] quit

Ten-GigabitEthernet 2/0/51 と Ten-GigabitEthernet 2/0/52 を IRF スタックポート 2/1 に関連づけます。

[Switch] irf-port 2/1

[Switch-irf-port2/1] port group interface ten-gigabitethernet 2/0/49

[Switch-irf-port2/1] port group interface ten-gigabitethernet 2/0/50

[Switch-irf-port2/1] quit

Ten-GigabitEthernet 2/0/49 と Ten-GigabitEthernet 2/0/50 を IRF スタックポート 2/2 に関連づけます。

[Switch] irf-port 2/2

[Switch-irf-port2/2] port group interface ten-gigabitethernet 2/0/51

[Switch-irf-port2/2] port group interface ten-gigabitethernet 2/0/52

[Switch-irf-port2/2] quit

物理インタフェースを UP にし、設定を保存します。

[Switch] interface range ten-gigabitethernet 2/0/49 to ten-gigabitethernet 2/0/52

[Switch-if-range] undo shutdown

[Switch-if-range] quit

[Switch] save

IRF スタックポートの設定を有効にします。

[Switch] irf-port-configuration active

2 台の装置は Master 選定を行い、選定されなかった 1 台は Master とともに IRF スタックを形成するために再起動します。

3. Device C を設定します。

Device C のメンバ ID を 3 に変更し、再起動します。

<Switch> system-view

[Switch] irf member 1 renumber 3

Renumbering the member ID may result in configuration change or loss. Continue? [Y/N]:y

[Switch] quit

<Switch> reboot

図 1-13 に示すように Device C を Device A に接続し、Device C にログインします。(詳細は省略します。)

IRF スタック物理インタフェースをシャットダウンします。

<Switch> system-view

[Switch] interface range ten-gigabitethernet 3/0/49 to ten-gigabitethernet 3/0/52

[Switch-if-range] shutdown

[Switch-if-range] quit

Ten-GigabitEthernet 3/0/49 と Ten-GigabitEthernet 3/0/50 を IRF スタックポート 3/1 に関連づけます。

[Switch] irf-port 3/1

[Switch-irf-port3/1] port group interface ten-gigabitethernet 3/0/49

[Switch-irf-port3/1] port group interface ten-gigabitethernet 3/0/50

[Switch-irf-port3/1] quit

Ten-GigabitEthernet 3/0/51 と Ten-GigabitEthernet 3/0/52 を IRF スタックポート 3/2 に関連づけます。

[Switch] irf-port 3/2

[Switch-irf-port3/2] port group interface ten-gigabitethernet 3/0/51

[Switch-irf-port3/2] port group interface ten-gigabitethernet 3/0/52

[Switch-irf-port3/2] quit

物理インタフェースを UP にし、設定を保存します。

[Switch] interface range ten-gigabitethernet 3/0/49 to ten-gigabitethernet 3/0/52

[Switch-if-range] undo shutdown

[Switch-if-range] quit

[Switch] save

IRF スタックポートの設定を有効にします。

[Switch] irf-port-configuration active

Device C を IRF スタックユニットに加入させるため再起動します。

4. Device D を設定します。

Device D のメンバ ID を 4 に変更し、再起動します。

<Switch> system-view

[Switch] irf member 1 renumber 4

Renumbering the member ID may result in configuration change or loss. Continue? [Y/N]:y

[Switch] quit

<Switch> reboot

図 1-13 に示すように Device D を Device B、Device C に接続し、Device D にログインします。(詳細は省略します。)

IRF スタック物理インタフェースをシャットダウンします。

<Switch> system-view

[Switch] interface range ten-gigabitethernet 4/0/49 to ten-gigabitethernet 4/0/52

[Switch-if-range] shutdown

[Switch-if-range] quit

Ten-GigabitEthernet 4/0/49 と Ten-GigabitEthernet 4/0/50 を IRF スタックポート 4/1 に関連づけます。

[Switch] irf-port 4/1

[Switch-irf-port4/1] port group interface ten-gigabitethernet 4/0/49

[Switch-irf-port4/1] port group interface ten-gigabitethernet 4/0/50

[Switch-irf-port4/1] quit

Ten-GigabitEthernet 4/0/51 と Ten-GigabitEthernet 4/0/52 を IRF スタックポート 4/2 に関連づけます。

[Switch] irf-port 4/2

[Switch-irf-port4/2] port group interface ten-gigabitethernet 4/0/51

[Switch-irf-port4/2] port group interface ten-gigabitethernet 4/0/52

[Switch-irf-port4/2] quit

物理インタフェースを UP にし、設定を保存します。

[Switch] interface range ten-gigabitethernet 4/0/49 to ten-gigabitethernet 4/0/52

[Switch-if-range] undo shutdown

[Switch-if-range] quit

[Switch] save

IRF スタックポートの設定を有効にします。

[Switch] irf-port-configuration active

Device C は IRF スタックユニットに加入させるため再起動します。4 台の IRF スタックユニットが形成されます。

5. IRF スタックユニットの LACP MAD を設定します。

IRF スタックユニットのドメイン ID に 1 を設定します。

<Switch> system-view

[Switch] irf domain 1

#ダイナミックアグリゲーションインタフェースを作成し、LACP MAD を有効にします。

[Switch] interface bridge-aggregation 2

[Switch-Bridge-Aggregation2] link-aggregation mode dynamic

[Switch-Bridge-Aggregation2] mad enable

```
You need to assign a domain ID (range: 0-4294967295)
[Current domain is: 1]:
The assigned domain ID is: 1
MAD LACP only enable on dynamic aggregation interface.
```

[Switch-Bridge-Aggregation2] quit

Ten-GigabitEthernet 1/0/1、Ten-GigabitEthernet 2/0/1、Ten-GigabitEthernet 3/0/1、Ten-GigabitEthernet 4/0/1 にアグリゲートインタフェースを割り当てます。

[Switch] interface range gigabitethernet 1/0/1 gigabitethernet 2/0/1 gigabitethernet 3/0/1 gigabitethernet 4/0/1

[Switch-if-range] port link-aggregation group 2

[Switch-if-range] quit

6. 中継装置として Device E を設定します。

⚠ **重要:**

中継装置が IRF スタックユニットの中にある場合、正しい分裂の検出を行うため、IRF スタックユニットとは異なるドメイン ID を IRF スタックユニットに割り当ててください。間違った検出は IRF スタックの分裂を引き起こします。

ダイナミックアグリゲーションインタフェースを作成します。

<Switch> system-view

[Switch] interface bridge-aggregation 2

[Switch-Bridge-Aggregation2] link-aggregation mode dynamic

[Switch-Bridge-Aggregation2] quit

Ten-GigabitEthernet 1/0/1 ～ Ten-GigabitEthernet 1/0/4 にアグリゲートインタフェースを割り当てます。

[Switch] interface range gigabitethernet 1/0/1 to gigabitethernet 1/0/4

[Switch-if-range] port link-aggregation group 2

[Switch-if-range] quit

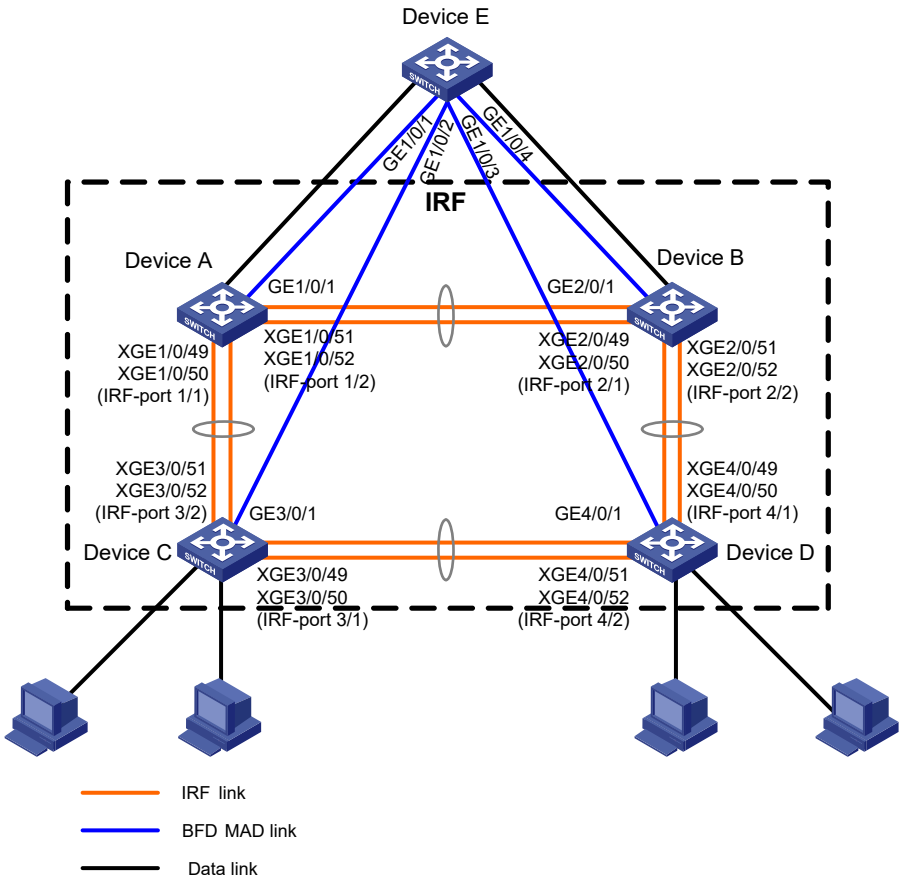
1.9.2. BFD MAD を使用する場合の IRF スタックの設定例

I. ネットワーク要件

図 1-14 に示すように、エンタープライズネットワークのコアレイヤで 4 台の IRF スタックユニットを設定します。

- IRF スタックユニット内で BFD MAD を設定し、各メンバ装置と中継装置との間で BFD MAD リンクが確立するようにしてください。
- BFD MAD とスパニングツリーの 2 つの機能は併用できないので、BFD MAD に使用するポートではスパニングツリー機能を無効にしてください。

図 1-14 ネットワーク図



II. 設定手順

1. Device A を設定します。

   # IRF スタックリンクに使用する IRF スタック物理インタフェースをシャットダウンします。

   <Switch> system-view

   [Switch] interface range ten-gigabitethernet 1/0/49 to ten-gigabitethernet 1/0/52

   [Switch-if-range] shutdown

   [Switch-if-range] quit

Ten-GigabitEthernet 1/0/49 と Ten-GigabitEthernet 1/0/50 を IRF スタックポート 1/1 に関連づけます。

[Switch] irf-port 1/1

[Switch-irf-port1/1] port group interface ten-gigabitethernet 1/0/49

[Switch-irf-port1/1] port group interface ten-gigabitethernet 1/0/50

[Switch-irf-port1/1] quit

Ten-GigabitEthernet 1/0/51 と Ten-GigabitEthernet 1/0/52 を IRF スタックポート 1/2 に関連づけます。

[Switch] irf-port 1/2

[Switch-irf-port1/2] port group interface ten-gigabitethernet 1/0/51

[Switch-irf-port1/2] port group interface ten-gigabitethernet 1/0/52

[Switch-irf-port1/2] quit

物理インタフェースを UP にし、設定を保存します。

[Switch] interface range ten-gigabitethernet 1/0/49 to ten-gigabitethernet 1/0/52

[Switch-if-range] undo shutdown

[Switch-if-range] quit

[Switch] save

IRF スタックポートの設定を有効にします。

[Switch] irf-port-configuration active

2. Device B を設定します。

Device B のメンバ ID を 2 に変更し、再起動します。

<Switch> system-view

[Switch] irf member 1 renumber 2

Renumbering the member ID may result in configuration change or loss. Continue? [Y/N]:y

[Switch] quit

<Switch> reboot

図 1-14 に示すように Device B を Device A に接続し、Device B にログインします。(詳細は省略します。)

IRF スタック物理インタフェースをシャットダウンします。

<Switch> system-view

[Switch] interface range ten-gigabitethernet 2/0/49 to ten-gigabitethernet 2/0/52

[Switch-if-range] shutdown

[Switch-if-range] quit

Ten-GigabitEthernet 2/0/49 と Ten-GigabitEthernet 2/0/50 を IRF スタックポート 2/1 に関連づけます。

[Switch] irf-port 2/1

[Switch-irf-port2/1] port group interface ten-gigabitethernet 2/0/49

[Switch-irf-port2/1] port group interface ten-gigabitethernet 2/0/50

[Switch-irf-port2/1] quit

Ten-GigabitEthernet 2/0/51 と Ten-GigabitEthernet 2/0/52 を IRF スタックポート 2/2 に関連づけます。

[Switch] irf-port 2/2

[Switch-irf-port2/2] port group interface ten-gigabitethernet 2/0/51

[Switch-irf-port2/2] port group interface ten-gigabitethernet 2/0/52

[Switch-irf-port2/2] quit

物理インタフェースを UP にし、設定を保存します。

[Switch] interface range ten-gigabitethernet 2/0/49 to ten-gigabitethernet 2/0/52

[Switch-if-range] undo shutdown

[Switch-if-range] quit

[Switch] save

IRF スタックポートの設定を有効にします。

[Switch] irf-port-configuration active

2 台の装置は Master 選定を行い、選定されなかった 1 台は Master とともに IRF スタックユニットを形成するために再起動します。

3. Device C を設定します。

Device C のメンバ ID を 3 に変更し、再起動します。

<Switch> system-view

[Switch] irf member 1 renumber 3

Renumbering the member ID may result in configuration change or loss. Continue? [Y/N]:y

[Switch] quit

<Switch> reboot

図 1-14 に示すように Device C を Device A に接続し、Device C にログインします。(詳細は省略します。)

IRF スタック物理インタフェースをシャットダウンします。

<Switch> system-view

[Switch] interface range ten-gigabitethernet 3/0/49 to ten-gigabitethernet 3/0/52

[Switch-if-range] shutdown

[Switch-if-range] quit

Ten-GigabitEthernet 3/0/49 と Ten-GigabitEthernet 3/0/50 を IRF スタックポート 3/1 に関連づけます。

[Switch] irf-port 3/1

[Switch-irf-port3/1] port group interface ten-gigabitethernet 3/0/49

[Switch-irf-port3/1] port group interface ten-gigabitethernet 3/0/50

[Switch-irf-port3/1] quit

Ten-GigabitEthernet 3/0/51 と Ten-GigabitEthernet 3/0/52 を IRF スタックポート 3/2 に関連づけます。

[Switch] irf-port 3/2

[Switch-irf-port3/2] port group interface ten-gigabitethernet 3/0/51

[Switch-irf-port3/2] port group interface ten-gigabitethernet 3/0/52

[Switch-irf-port3/2] quit

物理インタフェースを UP にし、設定を保存します。

[Switch] interface range ten-gigabitethernet 3/0/49 to ten-gigabitethernet 3/0/52

[Switch-if-range] undo shutdown

[Switch-if-range] quit

[Switch] save

IRF スタックポートの設定を有効にします。

[Switch] irf-port-configuration active

Device C を IRF スタックユニットに加入させるため再起動します。

4. Device D を設定します。

Device D のメンバ ID を 4 に変更し、再起動します。

<Switch> system-view

[Switch] irf member 1 renumber 4

Renumbering the member ID may result in configuration change or loss. Continue? [Y/N]:y

[Switch] quit

<Switch> reboot

図 1-14 に示すように Device D を Device B、Device C に接続し、Device D にログインします。(詳細は省略します。)

IRF スタック物理インタフェースをシャットダウンします。

<Switch> system-view

[Switch] interface range ten-gigabitethernet 4/0/49 to ten-gigabitethernet 4/0/52

[Switch-if-range] shutdown

[Switch-if-range] quit

Ten-GigabitEthernet 4/0/49 と Ten-GigabitEthernet 4/0/50 を IRF スタックポート 4/1 に関連づけます。

[Switch] irf-port 4/1

[Switch-irf-port4/1] port group interface ten-gigabitethernet 4/0/49

[Switch-irf-port4/1] port group interface ten-gigabitethernet 4/0/50

[Switch-irf-port4/1] quit

Ten-GigabitEthernet 4/0/51 と Ten-GigabitEthernet 4/0/52 を IRF スタックポート 4/2 に関連づけます。

[Switch] irf-port 4/2

[Switch-irf-port4/2] port group interface ten-gigabitethernet 4/0/51

[Switch-irf-port4/2] port group interface ten-gigabitethernet 4/0/52

[Switch-irf-port4/2] quit

物理インタフェースを UP にし、設定を保存します。

[Switch] interface range ten-gigabitethernet 4/0/49 to ten-gigabitethernet 4/0/52

[Switch-if-range] undo shutdown

[Switch-if-range] quit

[Switch] save

IRF スタックポートの設定を有効にします。

[Switch] irf-port-configuration active

Device D を IRF スタックユニットに加入させるため再起動します。4 台の IRF スタックユニットが形成されます。

5. IRF スタックユニットの BFD MAD を設定します。

VLAN3 を作成し、Ten-GigabitEthernet 1/0/1、Ten-GigabitEthernet 2/0/1、Ten-GigabitEthernet 3/0/1、Ten-GigabitEthernet 4/0/1 を VLAN3 に割り当てます。

[Switch] vlan 3

[Switch-vlan3] port gigabitethernet 1/0/1 gigabitethernet 2/0/1 gigabitethernet 3/0/1 gigabitethernet 4/0/1

[Switch-vlan3] quit

VLAN インタフェース 3 を作成し、各メンバ装置の VLAN インタフェースに MAD IP アドレスを設定します。

[Switch] interface vlan-interface 3

[Switch-Vlan-interface3] mad bfd enable

[Switch-Vlan-interface3] mad ip address 192.168.2.1 24 member 1

[Switch-Vlan-interface3] mad ip address 192.168.2.2 24 member 2

[Switch-Vlan-interface3] mad ip address 192.168.2.3 24 member 3

[Switch-Vlan-interface3] mad ip address 192.168.2.4 24 member 4

[Switch-Vlan-interface3] quit

Ten-GigabitEthernet 1/0/1、Ten-GigabitEthernet 2/0/1、Ten-GigabitEthernet 3/0/1、Ten-GigabitEthernet 4/0/1 のスパニングツリー機能を無効にします。

[Switch] interface range gigabitethernet 1/0/1 gigabitethernet 2/0/1 gigabitethernet 3/0/1 gigabitethernet 4/0/1

[Switch-if-range] undo stp enable

[Switch-if-range] quit

6. 中継装置として Device E を設定します。

VLAN3 を作成し、BFD MAD パケットを転送するように Ten-GigabitEthernet 1/0/1 ～ Ten-GigabitEthernet 1/0/4 を VLAN 3 に割り当てます。

<DeviceE> system-view

[DeviceE] vlan 3

[DeviceE-vlan3] port gigabitethernet 1/0/1 to gigabitethernet 1/0/4

[DeviceE-vlan3] quit

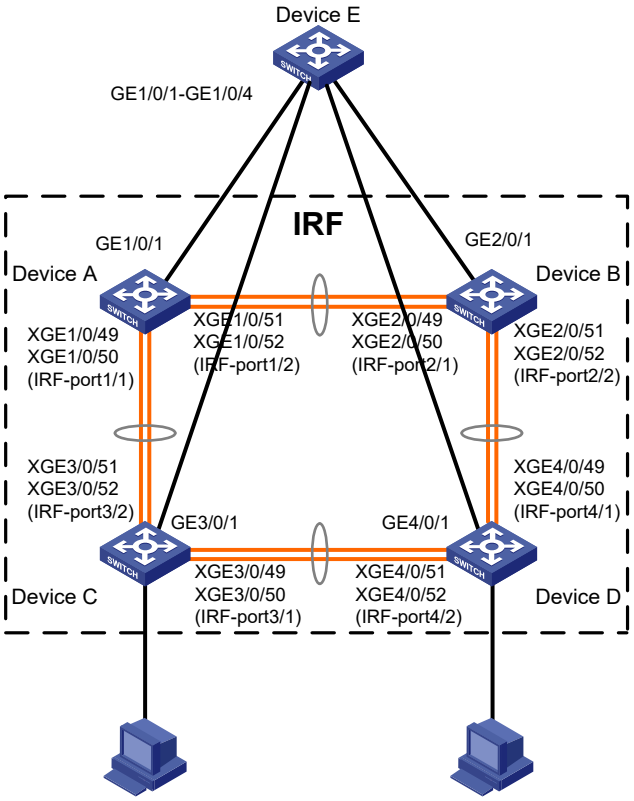
1.9.3. ARP MAD を使用する場合の IRF スタックの設定例

I. ネットワーク要件

図 1-15 に示すように、エンタープライズネットワークで 4 台の IRF スタックユニットを設定します。

- IRF スタックユニットで ARP MAD を設定し ARP MAD パケットを転送するように Device E につながるリンクを使用します。
- ループが発生しないように、スパニングツリー機能を Device E と IRF スタックユニットの間で実行します。

図 1-15 ネットワーク図



II. 設定手順

1. Device A を設定します。

   # IRF スタック接続に使用する IRF スタック物理インタフェースをシャットダウンします。

   <Switch> system-view

   [Switch] interface range ten-gigabitethernet 1/0/49 to ten-gigabitethernet 1/0/52

   [Switch-if-range] shutdown

   [Switch-if-range] quit

   # Ten-GigabitEthernet 1/0/49 と Ten-GigabitEthernet 1/0/50 を IRF スタックポート 1/1 に関連づけます。

   [Switch] irf-port 1/1

[Switch-irf-port1/1] port group interface ten-gigabitethernet 1/0/49

[Switch-irf-port1/1] port group interface ten-gigabitethernet 1/0/50

[Switch-irf-port1/1] quit

Ten-GigabitEthernet 1/0/51 と Ten-GigabitEthernet 1/0/52 を IRF スタックポート 1/2 に関連づけます。

[Switch] irf-port 1/2

[Switch-irf-port1/2] port group interface ten-gigabitethernet 1/0/51

[Switch-irf-port1/2] port group interface ten-gigabitethernet 1/0/52

[Switch-irf-port1/2] quit

物理インタフェースを UP にし、設定を保存します。

[Switch] interface range ten-gigabitethernet 1/0/49 to ten-gigabitethernet 1/0/52

[Switch-if-range] undo shutdown

[Switch-if-range] quit

[Switch] save

IRF スタックポートの設定を有効にします。

[Switch] irf-port-configuration active

2. Device B を設定します。

Device B のメンバ ID を 2 に変更し、再起動します。

<Switch> system-view

[Switch] irf member 1 renumber 2

Renumbering the member ID may result in configuration change or loss. Continue? [Y/N]:y

[Switch] quit

<Switch> reboot

図 1-15 に示すように Device B を Device A に接続し、Device B にログインします。(詳細は省略します。)

IRF スタック物理インタフェースをシャットダウンします。

<Switch> system-view

[Switch] interface range ten-gigabitethernet 2/0/49 to ten-gigabitethernet 2/0/52

[Switch-if-range] shutdown

[Switch-if-range] quit

Ten-GigabitEthernet 2/0/49 と Ten-GigabitEthernet 2/0/50 を IRF スタックポート 2/1 に関連づけます。

[Switch] irf-port 2/1

[Switch-irf-port2/1] port group interface ten-gigabitethernet 2/0/49

[Switch-irf-port2/1] port group interface ten-gigabitethernet 2/0/50

[Switch-irf-port2/1] quit

Ten-GigabitEthernet 2/0/51 と Ten-GigabitEthernet 2/0/52 を IRF スタックポート 2/2 に関連づけます。

[Switch] irf-port 2/2

[Switch-irf-port2/2] port group interface ten-gigabitethernet 2/0/51

[Switch-irf-port2/2] port group interface ten-gigabitethernet 2/0/52

[Switch-irf-port2/2] quit

物理インタフェースを UP にし、設定を保存します。

[Switch] interface range ten-gigabitethernet 2/0/49 to ten-gigabitethernet 2/0/52

[Switch-if-range] undo shutdown

[Switch-if-range] quit

[Switch] save

IRF スタックポートの設定を有効にします。

[Switch] irf-port-configuration active

2 台の装置は Master 選定を行い、選定されなかった 1 台は Master とともに IRF スタックユニットを形成するために再起動します。

3. Device C を設定します。

Device C のメンバ ID を 3 に変更し、再起動します。

<Switch> system-view

[Switch] irf member 1 renumber 3

Renumbering the member ID may result in configuration change or loss. Continue? [Y/N]:y

[Switch] quit

<Switch> reboot

図 1-15 に示すように Device C を Device A に接続し、Device C にログインします。(詳細は省略します。)

IRF スタック物理インタフェースをシャットダウンします。

<Switch> system-view

[Switch] interface range ten-gigabitethernet 3/0/49 to ten-gigabitethernet 3/0/52

[Switch-if-range] shutdown

[Switch-if-range] quit

Ten-GigabitEthernet 3/0/49 と Ten-GigabitEthernet 3/0/50 を IRF スタックポート 3/1 に関連づけます。

[Switch] irf-port 3/1

[Switch-irf-port3/1] port group interface ten-gigabitethernet 3/0/49

[Switch-irf-port3/1] port group interface ten-gigabitethernet 3/0/50

[Switch-irf-port3/1] quit

Ten-GigabitEthernet 3/0/51 と Ten-GigabitEthernet 3/0/52 を IRF スタックポート 3/2 に関連づけます。

[Switch] irf-port 3/2

[Switch-irf-port3/2] port group interface ten-gigabitethernet 3/0/51

[Switch-irf-port3/2] port group interface ten-gigabitethernet 3/0/52

[Switch-irf-port3/2] quit

物理インタフェースを UP にし、設定を保存します。

[Switch] interface range ten-gigabitethernet 3/0/49 to ten-gigabitethernet 3/0/52

[Switch-if-range] undo shutdown

[Switch-if-range] quit

[Switch] save

IRF スタックポートの設定を有効にします。

[Switch] irf-port-configuration active

Device C を IRF スタックユニットに加入させるため再起動します。

4. Device D を設定します。

Device D のメンバ ID を 4 に変更し、再起動します。

<Switch> system-view

[Switch] irf member 1 renumber 4

Renumbering the member ID may result in configuration change or loss. Continue? [Y/N]:y

[Switch] quit

<Switch> reboot

図 1-15 に示すように Device D を Device B、Device C に接続し、Device D にログインします。(詳細は省略します。)

IRF スタック物理インタフェースをシャットダウンします。

<Switch> system-view

[Switch] interface range ten-gigabitethernet 4/0/49 to ten-gigabitethernet 4/0/52

[Switch-if-range] shutdown

[Switch-if-range] quit

Ten-GigabitEthernet 4/0/49 と Ten-GigabitEthernet 4/0/50 を IRF スタックポート 4/1 に関連づけます。

[Switch] irf-port 4/1

[Switch-irf-port4/1] port group interface ten-gigabitethernet 4/0/49

[Switch-irf-port4/1] port group interface ten-gigabitethernet 4/0/50

[Switch-irf-port4/1] quit

Ten-GigabitEthernet 4/0/51 と Ten-GigabitEthernet 4/0/52 を IRF スタックポート 4/2 に関連づけます。

[Switch] irf-port 4/2

[Switch-irf-port4/2] port group interface ten-gigabitethernet 4/0/51

[Switch-irf-port4/2] port group interface ten-gigabitethernet 4/0/52

[Switch-irf-port4/2] quit

物理インタフェースを UP にし、設定を保存します。

[Switch] interface range ten-gigabitethernet 4/0/49 to ten-gigabitethernet 4/0/52

[Switch-if-range] undo shutdown

[Switch-if-range] quit

[Switch] save

IRF スタックポートの設定を有効にします。

[Switch] irf-port-configuration active

Device D を IRF スタックユニットに加入させるため再起動します。4 台の IRF スタックユニットが形成されます。

5. IRF スタックの ARP MAD を設定します。

グローバルでスパニングツリー機能を有効にします。ARP MAD の VLAN を MST region の MSTI 1 に割り当てます。

<Switch> system-view

[Switch] stp global enable

[Switch] stp region-configuration

[Switch-mst-region] region-name arpmad

[Switch-mst-region] instance 1 vlan 3

[Switch-mst-region] active region-configuration

[Switch-mst-region] quit

Bridge MAC アドレスオーナが離脱するとすぐに Bridge MAC アドレスを変更するよう IRF スタックユニットを設定します。

[Switch] undo irf mac-address persistent

IRF スタックユニットのドメイン ID を 1 に設定します。

[Switch] irf domain 1

VLAN3 を作成し、Ten-GigabitEthernet 1/0/1、Ten-GigabitEthernet 2/0/1、Ten-GigabitEthernet 3/0/1、Ten-GigabitEthernet 4/0/1 を VLAN3 に割り当てます。

[Switch] vlan 3

[Switch-vlan3] port gigabitethernet 1/0/1 gigabitethernet 2/0/1 gigabitethernet 3/0/1 gigabitethernet 4/0/1

[Switch-vlan3] quit

VLAN インタフェース 3 を作成し、IP アドレスを割り当てます。インタフェースで ARP MAD を有効にします。

[Switch] interface vlan-interface 3

[Switch-Vlan-interface3] ip address 192.168.2.1 24

[Switch-Vlan-interface3] mad arp enable

```
You need to assign a domain ID (range: 0-4294967295)
[Current domain is: 1]:
The assigned domain ID is: 1
```

6. 中継装置として Device E を設定します。

重要:

中継装置が IRF スタックユニットの中にある場合、正しい分裂の検出を行うため、IRF スタックユニットとは異なるドメイン ID を IRF スタックユニットに割り当ててください。間違った検出は IRF スタックの分裂を引き起こします。

グローバルでスパニングツリー機能を有効にします。ARP MAD の VLAN を MST region の MSTI 1 に割り当てます。

<DeviceE> system-view

[DeviceE] stp global enable

[DeviceE] stp region-configuration

[DeviceE-mst-region] region-name arpmad

[DeviceE-mst-region] instance 1 vlan 3

[DeviceE-mst-region] active region-configuration

[DeviceE-mst-region] quit

VLAN3 を作成し、ARP MAD のパケットを転送するため Ten-GigabitEthernet 1/0/1 ～ Ten-GigabitEthernet 1/0/4 を VLAN3 に割り当てます。

[DeviceE] vlan 3

[DeviceE-vlan3] port gigabitethernet 1/0/1 to gigabitethernet 1/0/4

[DeviceE-vlan3] quit

QX-S5300G シリーズ Ethernet スイッチ

オペレーションマニュアル

3. 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-Private VLAN

12-Voice VLAN

13-QinQ

14-VLAN マッピング

15-LLDP

16-L2PT

目次

このセクションのページは **3-x-x** です。

1 章 Ethernet インタフェース 1-1
1.1. 概要 1-1
1.2. マネジメント Ethernet インタフェースの設定 1-1
1.3. Ethernet インタフェースの命名ルール 1-2
1.4. Ethernet インタフェースの共通設定 1-2
1.4.1. コンボインタフェースの設定 1-2
1.4.2. 40-GE インタフェースの分割と 10-GE 分割インタフェースの結合 1-3
1.4.3. Ethernet インタフェースの基本設定 1-4
1.4.4. ジャンボフレームの設定 1-5
1.4.5. Ethernet インタフェースの抑制の設定 1-6
1.4.6. ストーム制御機能の設定 1-7
1.4.7. Ethernet インタフェースの一般的なフロー制御の設定 1-8
1.4.8. Ethernet インタフェースの節電機能の有効化 1-8
1.4.9. 統計情報のポーリング間隔の設定 1-9
1.4.10. Ethernet インタフェースのループバックテストの実行 1-10
1.5. Layer 2 Ethernet インタフェースの設定 1-11
1.5.1. 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オプション設定 1-11
1.5.2. Ethernet インタフェースの MDI モードの設定 1-12
1.5.3. Ethernet インタフェースのストーム抑止の設定 1-13
1.5.4. Ethernet インタフェースのケーブル接続テスト 1-14
1.6. Ethernet インタフェースの表示と維持 1-15

1章 Ethernet インタフェース

1.1. 概要

装置は Ethernet インタフェース、マネジメント Ethernet インタフェース、コンソールインタフェース、USB インタフェースをサポートしています。装置の種類によってサポートするインタフェースが異なります。インタフェースタイプと番号については、*QX-S5300G シリーズ Ethernet スイッチインスタレーションマニュアル*を参照してください。

この章ではマネジメント Ethernet インタフェースと Ethernet インタフェースの設定方法について記載します。

1.2. マネジメントEthernetインタフェースの設定

I. マネジメント Ethernet インタフェース

マネジメント Ethernet インタフェースは RJ-45 コネクタを使用します。PC に接続し、ソフトウェアのダウンロードやデバッグを行うために、接続します。またリモートからのシステム管理のために NMS に接続することができます。

装置の種類によってマネジメント Ethernet インタフェースのサポートが異なります。詳細は*QX-S5300G シリーズEthernet スイッチインスタレーションマニュアル*を参照してください。

IRF スタックユニットの各メンバ装置はマネジメント Ethernet インタフェースがあります。マネジメントリンクのバックアップを行うため、以下の作業を行います。

1. マスタ装置のマネジメント Ethernet インタフェースに PC を接続します。
2. メンバ装置の同一のインタフェース番号のマネジメント Ethernet インタフェースに PC を接続します。

2 つのマネジメント Ethernet インタフェースは以下のように動作します。

- IRF スタックユニットに複数のマネジメント Ethernet インタフェースがある場合マスタ装置のマネジメント Ethernet インタフェースのみがマネジメントトラフィックを処理します。
- マスタ装置のマネジメント Ethernet インタフェースが故障した場合、メンバ装置のマネジメント Ethernet インタフェースはマネジメントトラフィックの処理を行います。
- マスタ装置のマネジメント Ethernet インタフェースが回復した場合、マスタ装置が再度、マネジメントトラフィックの処理を行います。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. management Ethernet interface view に移行する	**interface M-GigabitEthernet** *interface-number*	—

操作	コマンド	補足
3. (オプション設定項目) インタフェースの説明を設定する	**description** *text*	デフォルト：**M-GigabitEthernet0/0/0 Interface**
4. (オプション設定項目) 通信モードを設定する	**duplex { auto | full | half }**	デフォルト：auto
5. (オプション設定項目) 通信速度を設定する	**speed { 10 | 100 | 1000 | auto }**	デフォルト：auto
6. (オプション設定項目) マネジメント Ethernet インタフェースを無効にする	**shutdown**	デフォルト：up

1.3. 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**–IRF スタックメンバ ID です。IRF スタックがない場合、A はデフォルトで 1 となります。
- **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。拡張インタフェースカード 1 は 1 となります。拡張インタフェースカード 2 は 2 となります。
- **C**–インタフェース番号です。

40-GE インタフェースから分割した 10-GE 分割インタフェースは A/B/C:D のフォーマットで指定されます。A/B/C は 40-GE インタフェースのインタフェース番号で、D は 10-GE 分割インタフェースの番号です。範囲は 1～4 です。40-GE インタフェースの分割方法については、セクション 3 *アクセス オペレーションマニュアル*の"*Ethernet インタフェース*"の"*40-GE インタフェースの分割と 10-GE 分割インタフェースの結合*"を参照してください。

1.4. Ethernetインタフェースの共通設定

この章はレイヤ 2 Ethernet インタフェースの共通設定について記載します。

レイヤ 2 Ethernet インタフェースの設定についてはセクション 3 *アクセス オペレーションマニュアル*の”*Ethernet インタフェース*”の” *レイヤ2 Ethernet インタフェースの設定*”を参照してください。

1.4.1. コンボインタフェースの設定

I. コンボインタフェース

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（fiber）か RJ-45 ポート（copper）を選択します。RJ-45 ポートと、SFP 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。

SFP ポートと、RJ-45 ポートは別の interface view となります。SFP ポートあるいは RJ-45 ポートのどちらかを有効にし、インタフェースの速度や通信モードのような、ポートの属性を設定します。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. 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** { auto | **copper** | **fiber** }	デフォルト：auto

メモ:

V7.2.16 を含むそれ以降のバージョンで、**combo enable** コマンドに **auto** が追加されました。あわせて、**combo enable auto** がデフォルト設定になります。

V7.1.8 を含むそれ以前は、**combo enable copper** がデフォルトになります。

1.4.2. 40-GE インタフェースの分割と 10-GE 分割インタフェースの結合

I. 40-GE インタフェースの分割と 10-GE 分割インタフェースの結合

40-GE QSFP+インタフェースは 1 つのインタフェースとして使用することができます。40-GE QSFP+インタフェースはポート密度、コスト削減、ネットワークの拡張性を向上させるため、4 つの 10-GE 分割インタフェースに分割することができます。

たとえば、40-GE インタフェース FortyGigE 1/0/1 を 4 つの 10-GE 分割インタフェース（Ten-GigabitEthernet 1/0/1:1 through Ten-GigabitEthernet 1/0/1:4）に分割することができます。

高帯域幅が必要となる場合、4 つの 10-GE 分割インタフェースを 1 つの 40-GE インタフェースに結合することができます。

II. 制限とガイドライン

- 40-GE インタフェースを 4 つの 10-GE 分割インタフェースに分割した場合、専用の 1-to-4 ケーブル（40G QSFP+/10G*4 SFP+ Copper ケーブル(DAC)）が必要です。4 つの 10-GE 分割インタフェースを結合した後、専用の 1-to-4 ケーブル（40G QSFP+/10G*4 SFP+ Copper ケーブル(DAC)）を、専用の 1-to-1 ケーブル（40G QSFP+ Copper ケーブル（DAC））あるいは 40-GE トランシーバモジュールに交換する必要があります。詳細は *QX-S5300G シリーズ Ethernet スイッチインスタレーションマニュアル*を参照してください。
- インタフェースタイプを変更した場合、設定を適用するために装置の再起動は必要ありません。インタフェースの分割、結合の情報は **display interface brief** コマンドを実行してください。

III. 40-GE QSFP+インタフェースから 10-GE 分割インタフェースへの分割

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. 40-GE interface view に移行する	**interface** *interface-type interface-number*	—

操作	コマンド	補足
3. 40-GE インタフェースを 4 つの 10-GE 分割インタフェースに分割する	**using tengige**	デフォルト：40-GEインタフェースは分割されていません。

IV. 4 つの 10-GE 分割インタフェースを 1 つの 40-GE インタフェースに結合

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. 40-GE インタフェースから分割した 10-GE 分割インタフェースのいずれかの view に移行する	**interface** *interface-type interface-number*	—
3. 4 つの 10-GE 分割インタフェースを 40-GE インタフェースに結合する	**using fortygige**	デフォルト：40-GEインタフェースは分割されていません。

1.4.3. Ethernet インタフェースの基本設定

I. Ethernet インタフェースの基本設定

以下の通信モードのいずれかを使用して Ethernet インタフェースを設定することができます。

- **Full-duplex mode**—インタフェースは同時に送受信できます。
- **Half-duplex mode**—インタフェースは同時に送信あるいは受信のみを行うことができます。
- **Autonegotiation mode**—インタフェースは対向先と通信モードのネゴシエートを行います。

Ethernet インタフェースの通信速度を設定する、あるいは対向先と自動的にネゴシエートすることができます。100Mbps/1000Mbps インタフェースでは、**speed** コマンドのオプションを使用してオートネゴシエーションを設定することができます。2 つの端末間は有効なオプションからのみ通信速度を選択できます。詳細はセクション 3 *アクセス オペレーションマニュアル*の “*Ethernet インタフェース*”の“*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オプション設定*”を参照してください。

II. 制限とガイドライン

shutdown コマンドはループバックテストの Ethernet インタフェースで設定することはできません。

III. 設定手順

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. 説明を設定する	**description** *text*	デフォルト：*interface-name* Interface たとえば“GigabitEthernet1/0/1 Interface”です。
4. 通信モードを設定する	**duplex** { **auto** | **full** | **half** }	デフォルト：**auto** 1000Mbps、10000Mbpsで動作するRJ-45ポート、光ファイバポートは**half**をサポートしていません。
5. 通信速度を設定する	**speed** { **10** | **100** | **1000** | **10000** | **40000** | **auto** }	デフォルト：**auto**
6. Ethernet インタフェースを有効にする	**undo shutdown**	デフォルト：up

1.4.4. ジャンボフレームの設定

I. ジャンボフレーム

ファイル転送のような 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。1536 バイト以上のフレームはジャンボフレームと呼ばれます。

このようなフレームが 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)にされているとき、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とき、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。

II. 設定手順

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** [*size*]	デフォルト：10000バイトのジャンボフレームが可能です。 *size*パラメータを複数設定した場合、最後に行った設定が適用されます。

1.4.5. Ethernet インタフェースの抑制の設定

I. 物理状態の変更抑制

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どちらかで動作します。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、ログの作成、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、システムは CPU に変更を通知します。

II. 制限とガイドライン

RRPP、STP、MSTP、RSTP、PVST、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。

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することができます。

複数回の設定を行った場合、最後の設定が適用されます。

インタフェースで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することができます。リンクアップイベントとリンクダウンイベントで **link-delay** コマンドを複数設定した場合、最後に行った設定が適用されます。

III. 設定手順

V7.2.16 以降

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。

V7.1.8 以前

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. Ethernet インタフェースの抑制を設定する	**link-delay** [**msec**]*delay-time* [**mode** { **up** | **updown** }]	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。 リンクダウンイベントのみを抑制する場合、**mode**パラメータを指定しないでください。 リンクアップイベントのみを抑制する場合、**mode up** パラメータを指定してください。 リンクダウン、リンクアップの両方を抑制する場合、**mode updown**パラメータを指定してください。

1.4.6. ストーム制御機能の設定

I. ストーム制御機能

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とき、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。

ストーム抑制とストーム抑止の両方でインタフェースのトラフィックを抑制することができます。ストーム抑制はトラフィックを抑制するため、ハードウェアのチップを使用します。ストーム抑止はトラフィックを制御するためソフトウェアを使用します。ストーム抑制はストーム抑止に比べて装置への影響が少なくなります。

II. 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。ストーム抑止のコマンドについては、セクション 3 *アクセス オペレーションマニュアル*の "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 で設定するとき、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、装置の表示画面を参照してください。

III. 設定手順

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

操作	コマンド	補足
2. Ethernet interface view に移行する	**interface** *interface-type interface-number*	—
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。

1.4.7. Ethernet インタフェースの一般的なフロー制御の設定

I. 一般的なフロー制御

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、トラフィックが混雑した際に、受信エンドから Pause フレームを送信エンドに通知して、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。

- 混雑が発生したとき、インタフェースはピアにフロー制御フレームを送信します。
- インタフェースはピアからフロー制御フレームを受信したとき、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。

II. 設定手順

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

1.4.8. Ethernet インタフェースの節電機能の有効化

I. Ethernet インタフェースの節電機能

オートパワーダウン機能が有効なインタフェースで一定期間ダウンしているとき、以下のことを行います。

- 装置は自動的にインタフェースへの電力供給を停止します。
- インタフェースはパワーセーブモードになります。

一定期間は装置のチップの仕様に依存します。一定期間の設定はできません。

インタフェースがアップするとき、以下のことを行います。

- 装置は自動的にインタフェースへの電力供給を回復します。

- インタフェースは通常のモードに戻ります。

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。

II. 制限とガイドライン

光ファイバのトランシーバモジュールで動作するポートで未サポートです。

III. Ethernet インタフェースのオートパワーダウンの設定

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. オートパワーダウンを有効にする	**port auto-power-down**	デフォルト：無効

IV. Ethernet インタフェースの EEE 省電力機能の有効化

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. 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

1.4.9. 統計情報のポーリング間隔の設定

I. 統計情報のポーリング間隔

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。

インタフェースの統計情報を削除するには、**reset counters interface** コマンドを使用します。

II. Ethernet インタフェースで統計情報のポーリング間隔の設定

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. 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

1.4.10. Ethernet インタフェースのループバックテストの実行

I. ループバックテスト

インタフェース機能が正常に動作しているか確認するため、Ethernet インタフェースでループバックテストを行うことができます。

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。もし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。

II. 制限とガイドライン

- インタフェースでループバックテストを有効にしたのち、インタフェースは、パケットの転送を行いません。
- ループバックテスト中は、パケットの転送を行いません。
- 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** コマンド、**duplex** コマンド、**mdix-mode** コマンド、**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 2 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。

III. 設定手順

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

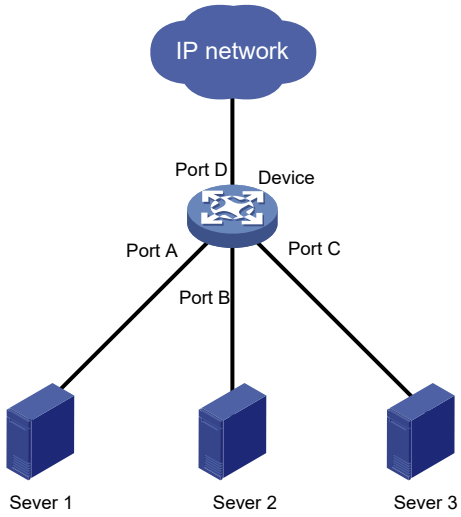
1.5. Layer 2 Ethernetインタフェースの設定

1.5.1. 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オプション設定

I. オートネゴシエーションの通信速度のオプション設定

デフォルトで通信速度のオートネゴシエーションは、両方のエンドがサポートする最高速度でピアとネゴシエートすることができます。ネゴシエーションの速度オプションリストを絞り込むことができます。

図 1-1 通信速度のオートネゴシエーションアプリケーションシナリオ



通信速度のオートネゴシエーションアプリケーションシナリオを図 1-1 に示します。

- デバイス上のすべてのインタフェースが速度で動作しているオートネゴシエーション モードで、最高速度は 1000Mbps です。
- ポート D は、サーバのインターネットへのアクセスを提供します。

サーバの各サーバの伝送レートが 1000Mbps である場合、ポート D のトータルの伝送レートを超過します。

ポート D の輻輳を避けるために、ポート A、ポート B、およびポート C のインタフェースの速度ネゴシエーションに使用できる唯一のオプションとして 100Mbps を設定します。結果として、サーバに接続された各インタフェースの伝送レートは 100Mbps に制限されます。

II. 制限とガイドライン

speed コマンドと **speed auto** コマンドを両方設定した場合、最後に行った設定が適用されます。

III. 設定手順

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

操作	コマンド	補足
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のオプション設定を行う	**speed auto** { **10** | **100** | **1000** } *	デフォルト：設定なし

1.5.2. 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、光ファイバのトランシーバモジュールで動作する SFP ポート、SFP+ポート、QSFP+ポートに設定できません。

I. MDIX モード

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、物理イーサネットインタフェースのピン 4、5、7、および 8 では有効になりません。

- 10Mbps または 100Mbps で動作するインタフェースの 4、5、7、および 8 は、信号を受信または送信しません。
- 1000Mbps 以上で動作するインタフェースのピン 4、5、7、8 は、信号を受信して送信します。

II. 制限とガイドライン

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とき、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 AutoMDIX に設定してください。

III. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. 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**

1.5.3. Ethernet インタフェースのストーム抑止の設定

I. ストーム抑止

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どちら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し、すべてのトラフィックの転送を行いません。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を転送しません。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とき、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上限を超過した後、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。ストーム制御機能のコマンドについては、セクション 3 *アクセス オペレーションマニュアル*の"*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。

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. 制限とガイドライン

トラフィック抑制結果を決定するために、同じタイプのトラフィックに対してストーム抑制とともにストーム抑止を設定しないでください。

III. 設定手順

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

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** } *max-pps-values min-pps-values*	デフォルト：無効
5. トラフィックが上限を超過したとき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：上限を超過したときあるいは下回ったときトラップを送信します。

1.5.4. Ethernet インタフェースのケーブル接続テスト

メモ:

ケーブル接続テストは、光ファイバのトランシーバモジュールで動作する SFP ポート、SFP+ポート、QSFP+ポートに設定できません。

ケーブル接続テストは通信速度 10Mbps、100Mbps では動作しません。

I. Ethernet インタフェースのケーブル接続テスト

この機能は Ethernet インタフェースのケーブルの接続をテストし、5 秒内にケーブルテスト結果を表示します。

テスト結果はケーブルの物理状態、物理パラメータが含まれます。検出に失敗した場合、失敗したケーブルセグメントの長さを含めた結果が表示されます。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. Ethernet interface view に移行する	**interface** *interface-type interface-number*	—

操作	コマンド	補足
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**	—

1.6. 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インタフェースの動作情報およびステータス情報を表示する	**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*]
指定されたEthernetインタフェースで廃棄した統計情報を削除する	**reset ethernet statistics** [**slot** *slot-number*]

目次

このセクションのページは **3-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. 概要……2-1
2.1.1. ループバックインタフェース……2-1
2.1.2. Null インタフェース……2-1
2.2. ループバックインタフェースの設定……2-2
2.3. NULL インタフェースの設定……2-2
2.4. 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. 概要

2.1.1. ループバックインタフェース

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レイヤ状態とリンクレイヤプロトコルは、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。
  - 認証ルールあるいはセキュリティサーバで、装置が作成したパケットの許可/禁止のルールを設定するとき、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。

2.1.2. Null インタフェース

NULL インタフェースは、論理的インタフェースで、常に UP しています。しかし、データパケットを転送したり、IP アドレスやリンクレイヤプロトコルを設定したりできません。NULL インタフェースをスタティックルートのネクストホップとして具体的なネットワークセグメントに指定した場合、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。

2.2. ループバックインタフェースの設定

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

2.3. NULLインタフェースの設定

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

2.4. 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クリアする	**reset counters interface loopback** [*interface-number*]

操作	コマンド
NULLインタフェースをクリアする	**reset counters interface null** [**0**]

目次

このセクションのページは **3-x-x** です。

3 章 interface range 3-1
3.1. 概要 3-1
3.2. 制限とガイドライン 3-1
3.3. 設定手順 3-2
3.4. interface range の表示と維持 3-2

3章 interface range

3.1. 概要

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をまとめて実行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 interface range を設定した場合、稼働中の設定に保存されません。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、**interface range name** コマンドを使用します。

3.2. 制限とガイドライン

interface range view で interface range 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。

- 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リスト（アルファベットでソートします）でサポートされるコマンドのみ有効です。
- インタフェースを interface range の最初のインタフェースとして設定する前に、
- **interface** *interface-type interface-number* コマンドを使用して interface view の view に移行できることを確認してください。
- アグリゲートインタフェースと、アグリゲートインタフェースのメンバインタフェースの両方を interface range に割り当てないでください。一部のコマンドはアグリゲートインタフェースと、アグリゲートインタフェースのメンバインタフェースの両方で実行したのち、アグリゲーションを中断します。
- 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。
- interface range view で interface range を実行したのち、以下の状況の 1 つが発生する可能性があります。
    - 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 interface range view のメンバインタフェースでの実行に失敗したことを示します。
        - interface range の最初のメンバインタフェースで実行が失敗した場合、ほかのメンバインタフェースでコマンドは実行しません。
        - interface range の最初以外のメンバインタフェースで実行が失敗した場合、ほか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 system view に戻ります。以下を示します。

– コマンドは system view と interface view の両方でサポートします。
– interface range view のメンバインタフェースで実行が失敗し、system view で成功します。
– コマンドは後続のメンバインタフェースで実行しません。

各メンバインタフェースの interface view の設定を確認するため、**display this** コマンドを使用することができます。加えて、system view で設定を行う必要がない場合、設定を削除するため、**undo** コマンドを使用します。

3.3. 設定手順

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>]	—
3. （オプション設定項目）interface range の最初のインタフェースで使用可能なコマンドを表示する	interface rangeのプロンプトで(?)を実行する	—
4. インタフェースを設定するため有効なコマンドを使用する	有効なコマンドはインタフェースによって異なります。	—
5. （オプション設定項目）設定を確認する	**display this**	—

3.4. interface range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
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 **3-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. MAC アドレスエントリベースのフレームの転送 ····· 4-3
4.3.2. 制限とガイドライン ····· 4-3
4.3.3. 設定要件 ····· 4-4
4.3.4. スタティック/ダイナミック MAC アドレスエントリの追加/変更 ····· 4-4
4.3.5. ブラックホール MAC アドレスエントリの追加/変更 ····· 4-5
4.3.6. マルチポートユニキャスト MAC アドレスエントリの追加/変更 ····· 4-5
4.4. 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 ····· 4-6
4.5. MAC アドレス学習の無効化 ····· 4-7
4.5.1. MAC アドレス学習の無効化 ····· 4-7
4.5.2. グローバルでの MAC アドレス学習の無効化 ····· 4-7
4.5.3. インタフェースでの MAC アドレス学習の無効化 ····· 4-7
4.5.4. VLAN での MAC アドレス学習の無効化 ····· 4-8
4.6. インタフェースで学習可能な MAC アドレス数の設定 ····· 4-8
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 ····· 4-9
4.7.1. 未知のフレームの転送の設定 ····· 4-9
4.7.2. 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 ····· 4-9
4.8. MAC アドレスの移動の通知の有効化 ····· 4-9
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 ····· 4-11
4.10. スタティック送信元チェックの無効化 ····· 4-11
4.11. MAC アドレステーブルの SNMP 通知の有効化 ····· 4-12
4.12. MAC アドレステーブルの表示と維持 ····· 4-13
4.13. MAC アドレステーブルの設定例 ····· 4-13
4.13.1. MAC アドレステーブルの設定例 ····· 4-13

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とき、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。

- もしエントリがある場合、出力インタフェースへパケットを転送します。
- もし見つからない場合、入力したインタフェースを除いたインタフェースのすべて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に入力された送信元 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。

インタフェース(例：ポート A)にフレームが到着すると、装置は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. その 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。
    - その MAC アドレスに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。
    - その MAC アドレスに対応するエントリがない場合、MAC-SOURCE とポート A のエントリに追加します。

この送信元 MAC アドレスの学習を行った後に MAC-SOURCE 宛のフレームを受信したとき、装置は以下の処理を行います。

3. MAC アドレステーブルから MAC-SOURCE を検索します。
4. ポート A からフレームを転送します。

装置は、不明な送信元 MAC アドレスのフレームを受信したとき、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とき、装置は正規ユーザのフレームかハッカーからの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 に接続されているとき、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とき、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** – スタティックエントリは、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。
- **マルチポートエントリ** – マルチポートユニキャストエントリは複数のポートによる特定のユニキャスト宛先 MAC アドレスのフレームを送信するため、手動で追加されます。エージアウトしません。マルチポートユニキャストエントリは動的に学習したエントリよりも優先します。

スタティック、ブラックホール、マルチポートユニキャスト 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。

この章はスタティック、ダイナミック、ブラックホール、マルチポートユニキャスト MAC アドレスエントリを含むユニキャスト MAC アドレスエントリの設定についてのみ記載します。スタティックマルチキャスト MAC アドレスエントリの詳細は、セクション 6 *マルチキャスト オペレーションマニュアル*の"*マルチキャストルーティングと転送*"を参照してください。

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 • スタティック/ダイナミック MAC アドレスエントリの追加/変更 • ブラックホール MAC アドレスエントリの設定 • マルチポートユニキャスト MAC アドレスエントリの追加/変更
(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

作業リスト
(オプション設定項目) MACアドレス学習の設定 • MAC アドレス学習の無効化 • インタフェースで学習可能な MAC アドレス数の設定 • 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)スタティック送信元チェックの無効化
(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

4.3. MACアドレスエントリの設定

4.3.1. MAC アドレスエントリベースのフレームの転送

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と同じかどうかに関係なく、宛先MACアドレスに従ってフレームを転送します。
マルチポートユニキャストMACアドレスエントリ	• フレームの MAC アドレスを学習し、動的 MAC アドレスエントリを生成しますが、生成されたダイナミック MAC アドレスエントリは有効になりません。 • マルチポートユニキャスト MAC アドレスエントリにもとづいて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、もと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. 制限とガイドライン

手動で設定された動的 MAC アドレスエントリは、MAC アドレスに対して異なる出力インタフェースが存在する学習済みエントリを上書きします。

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、マルチポートユニキャスト 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。

装置の予約済み MAC アドレスは、スタティック、ダイナミック、ブラックホール、またはマルチポートユニキャスト MAC アドレスとして設定できません。装置の予約済み MAC アドレスは、装置のブリッジ MAC アドレスからブリッジ MAC アドレスプラス 103 までのアドレスです。

4.3.3. 設定要件

インタフェースで MAC アドレスエントリを手動で設定する前に、VLAN エントリの VLAN が作成されていることを確認してください。

4.3.4. スタティック/ダイナミック MAC アドレスエントリの追加/変更

I. 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。

II. 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/変更

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. 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。

4.3.5. ブラックホール MAC アドレスエントリの追加/変更

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。

4.3.6. マルチポートユニキャスト MAC アドレスエントリの追加/変更

I. マルチポートユニキャスト MAC アドレスエントリの設定

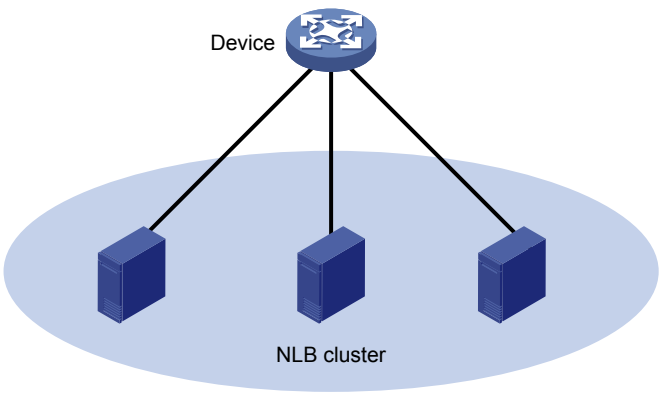
ユニキャスト宛先 MAC アドレスを複数のポートに割り当てるため、マルチポートユニキャスト MAC アドレスエントリを設定することができます。エントリにマッチする宛先 MAC アドレスのフレームは複数のポートに送信されます。

たとえば、NLB ユニキャストの場合、以下となります。

- クラスタ内のすべてのサーバは自身のアドレスとしてクラスタの MAC アドレスを使用します。
- クラスタ向けのフレームはグループの各サーバに転送されます。

この場合、サーバに接続された装置でマルチポートユニキャスト MAC アドレスを設定することができます。装置はクラスタ内のサーバに接続されたすべてのポートを通してサーバ向けのフレームを転送することができます。

図 4-1 NLB クラスタ



グローバルあるいはインタフェースでマルチポートユニキャスト MAC アドレスエントリを設定することができます。

II. グローバルでのマルチポートユニキャスト MAC アドレスエントリの設定

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

操作	コマンド	補足
2. マルチポートユニキャスト MAC アドレスエントリを追加あるいは削除する	**mac-address multiport** *mac-address* **interface** *interface-list* **vlan** *vlan-id*	デフォルト：設定なし すでにVLANが作成済みで、インタフェースにVLANが割り当てられていることを確認してください。

III. インタフェースでのマルチポートユニキャスト MAC アドレスエントリの設定

操作	コマンド	補足
1. system view へ移行する	**system-view**	—
2. interface view へ移行する	• Ethernet interface view へ移行する: **interface** *interface-type interface-number* • aggregate interface view へ移行する: **interface bridge-aggregation** *interface-number*	—
3. インタフェースにマルチポートユニキャスト MAC アドレスエントリを追加する	**mac-address multiport** *mac-address* **vlan** *vlan-id*	デフォルト：設定なし すでにVLANが作成済みで、インタフェースにVLANが割り当てられていることを確認してください。

4.4. 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

I. ダイナミック MAC アドレスエントリのエージングタイマ

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。もし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ます。MAC アドレステーブルリソースが枯渇する可能性があります。MAC アドレステーブルは最新のネットワーク変更に対応するためにエントリを更新できない場合があります。

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及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。

不必要なエージング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。

II. 設定手順

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 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**はエージングタイマを無効にします。

4.5. MACアドレス学習の無効化

4.5.1. 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。装置が攻撃者から攻撃をうけたとき、MAC アドレステーブルが満たされないようにするため、MAC アドレスの学習を無効にします。たとえば、攻撃者からの異なる送信元 MAC アドレスの大量のフレームを学習しないように装置で MAC アドレスの学習を無効にすることができます。

MAC アドレス学習が無効であるとき、装置は早急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。

4.5.2. グローバルでの MAC アドレス学習の無効化

I. 制限とガイドライン

グローバルで MAC アドレス学習を無効にすると、すべてのインタフェースで MAC アドレス学習が無効になります。

II. 設定手順

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

4.5.3. インタフェースでの MAC アドレス学習の無効化

I. 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とき、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。

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 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

4.5.4. VLAN での MAC アドレス学習の無効化

I. 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とき、VLAN ごとに MAC アドレス学習を無効にすることができます。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. VLAN view に移行する	**vlan** *vlan-id*	—
3. 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

4.6. インタフェースで学習可能なMACアドレス数の設定

I. インタフェースで学習可能な MAC アドレス数

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。

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*	—

操作	コマンド	補足
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。

4.7.1. 未知のフレームの転送の設定

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。

4.7.2. 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

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の有効化

I. MAC アドレスの移動の通知の有効化

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 アドレスのパケットを受信します。
- 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。

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 MAC アドレスの移動情報を表示することができます。装置が起動した後、MAC アドレスの記録を表示する場合、**display mac-address mac-move** コマンドを使用します。

インタフェースから MAC アドレスの移動が頻繁に移動することをシステムが検出するとき、インタフェースをダウンさせるため、インタフェースで MAC アドレスの移動の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。

II. 制限とガイドライン

MAC アドレス移動通知を設定した後、システムは information center モジュールにログメッセージのみを送信します。装置が **snmp-agent trap enable mac-address** コマンドを使用して設定されている場合、SNMP モジュールに SNMP 通知も送信されます。

III. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
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
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を設定する	**mac-address notification mac-move suppression threshold** *threshold-value*	デフォルト：3
4. （オプション設定項目）MAC アドレスの抑制間隔を設定する	**mac-address notification mac-move suppression interval** *interval-value*	デフォルト：30秒
5. 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*	—
6. 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

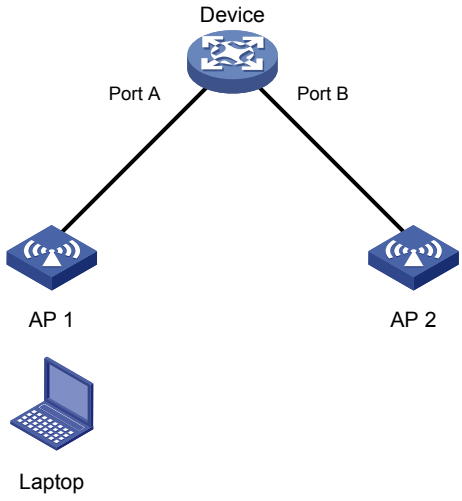
4.9. MACアドレスの移動によるARPクイックアップデートの有効化

I. MAC アドレスの移動による ARP クイックアップデート

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 4-2 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 が変更したとき、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 4-2 ARP クイックアップデートアプリケーションシナリオ



II. 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. スタティック送信元チェックの無効化

I. スタティック送信元チェック

デフォルトでスタティック送信元チェックはインタフェースで有効です。受信フレームが以下の条件に一致しているか確認します。

- フレームの送信元 MAC アドレスがスタティック MAC アドレスエントリと同一です。
- フレームの入力インタフェースがエントリの出力インタフェースと異なります。

フレームが両方の条件に一致している場合、装置はフレームを廃棄します。

この機能が無効である場合、装置は受信フレームのチェックを行いません。フレームが条件に一致しているかどうかにかかわらずフレームを転送することができます。

II. 制限とガイドライン

VLAN インタフェースの MAC アドレスから送信されたトラフィックを正しく転送するため、VLAN のレイヤ 2 インタフェースでスタティック送信元チェック機能を無効にする必要があります。

III. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. 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* • IRF physical interface view に移行する: **interface** *interface-type interface-number*	—
3. スタティック送信元チェック機能を無効にする	**undo mac-address static source-check enable**	—

4.11. MACアドレステーブルのSNMP通知の有効化

I. SNMP アドレステーブルの SNMP 通知

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 通知を無効にしたのち、装置は Information Center モジュールにログメッセージの送信のみを行います。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、セクション 10 *システム管理 オペレーションマニュアル*の”*SNMP*”、”*Information Center*”を参照してください。

II. 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. 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** [**mac-move**]	デフォルト：無効

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アドレスの移動記録を表示する	**display mac-address mac-move** [**slot** *slot-number*]
MACアドレスの統計情報を表示する	**display mac-address statistics**

4.13. MACアドレステーブルの設定例

4.13.1. MAC アドレステーブルの設定例

I. ネットワーク要件

図 4-3 に示すように設定します。

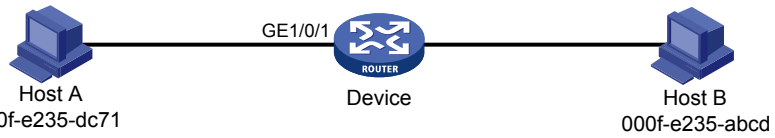
- Host A (000f-e235-dc71)は Device のインタフェース GigabitEthernet 1/0/1 に接続され、VLAN1 に属しています。
- ネットワークで一度疑わしいふるまいをした Host B (000f-e235-abcd)は VLAN1 に属しています。

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 アドレステーブルの Host A にスタティック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、Host にブラックホール 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 4-3 ネットワーク図



II. 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

III. 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 **3-x-x** です。

5 章 MAC Information 5-1
5.1. 概要 5-1
5.2. MAC Information の有効化 5-1
5.3. MAC Information モードの設定 5-1
5.4. MAC アドレス変更メッセージの送信間隔の設定 5-2
5.5. MAC Information のキュー長の設定 5-2
5.6. MAC Information の設定例 5-3
5.6.1. MAC Information の設定例 5-3

5章 MAC Information

5.1. 概要

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とき、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とき
- キューが使い果たされたとき

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。

5.2. MAC Informationの有効化

I. 制限とガイドライン

MAC Information を適用する場合、グローバルとインタフェースの両方で有効に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. 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

5.3. MAC Informationモードの設定

I. MAC Information モード

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 メッセージは監視端末の Information Center に送信します。Information Center についての詳細はセクション 10 *システム管理 オペレーションマニュアル*の "*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 NMS に SNMP トラップメッセージを送信します。SNMP についての詳細はセクション 10 *システム管理 オペレーションマニュアル*の"*SNMP*"を参照してください。

II. 設定手順

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)MAC Information モードを設定する	**mac-address information mode** { **syslog** | **trap** }	デフォルト：**trap**

5.4. MACアドレス変更メッセージの送信間隔の設定

I. MAC アドレス変更メッセージの送信間隔の設定

Syslog メッセージあるいは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。

II. 設定手順

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

5.5. MAC Informationのキュー長の設定

I. MAC Information のキュー長

MAC Information のキュー長が 0 である場合、装置は MAC アドレスの学習あるいは削除が行われた後すぐに Syslog メッセージあるいは SNMP トラップメッセージの送信を行います。

MAC Information のキュー長が 0 以外である場合、装置はキューに MAC アドレスの変更を記録します。

- 装置は、次の条件が存在する場合、最新の MAC 変更でキューに書き込まれたもっとも古い MAC アドレスの変更を上書きします。
  - MAC アドレスの変更通知間隔は期限切れになりません。

- キューは使い果たされました。

- 装置は、MAC アドレス変更通知間隔が満了した場合にのみ、syslog メッセージまたは SNMP 通知を送信します。

II. 設定手順

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

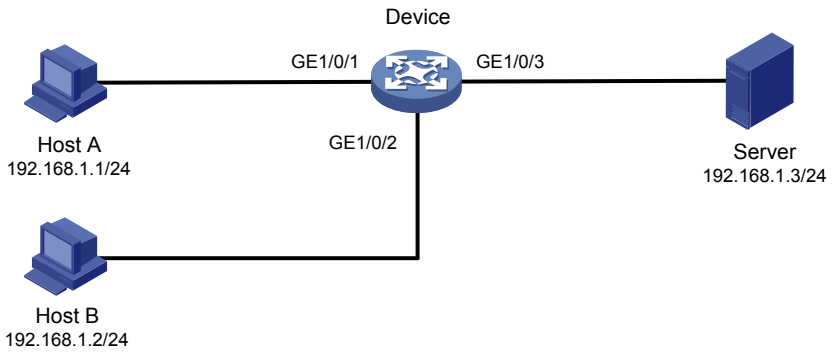
5.6. MAC Informationの設定例

5.6.1. MAC Information の設定例

I. ネットワーク要件

図 5-1 に示すように、インタフェース GigabitEthernet 1/0/2 を通してログホストの Host B に MAC アドレスの変更があった場合 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



II. 制限とガイドライン

ファイル**/etc/syslog.conf** を編集するとき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** コマンドで装置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。

III. 設定手順

1. Host B に Syslog メッセージを送信する設定を Device に行います。

   # information center を有効にします。

   <Device> system-view

[Device] info-center enable

ログホスト 192.168.1.2/24 を指定し、ロギング facility として local4 を指定します。

[Device] info-center loghost 192.168.1.2 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. Configure the log host, Host B:
3. ログホスト Host B の設定

以下のように Solaris で動作する設定を行います。同様にほかの UNIX OS の設定を行います。

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。

```
# Device configuration messages
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、**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。

4. 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 **3-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. リンクアグリゲーションアプリケーションシナリオ……6-1
6.1.2. 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、メンバポート……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. スタティックリンクアグリゲーションの動作……6-3
6.1.7. ダイナミックリンクアグリゲーション……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……6-7
6.1.9. エッジアグリゲートインタフェース……6-9
6.1.10. リンクアグリゲーショングループの負荷分散……6-9
6.2. リンクアグリゲーション設定作業リスト……6-10
6.3. アグリゲーショングループの設定……6-10
6.3.1. 制限とガイドライン……6-10
6.3.2. アグリゲーショングループの設定……6-11
6.4. アグリゲートインタフェースの設定……6-13
6.4.1. 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……6-13
6.4.2. アグリゲートインタフェースの説明の設定……6-14
6.4.3. アグリゲートインタフェースのシャットダウン……6-14
6.5. リンクアグリゲーショングループの負荷分散の設定……6-15
6.5.1. リンクアグリゲーショングループのロードシェアリングモードの設定……6-15
6.5.2. リンクアグリゲーションの local-first ロードシェアリングモードの設定……6-15
6.6. リンクアグリゲーションの表示と維持……6-16
6.7. リンクアグリゲーションの設定例……6-17
6.7.1. スタティックアグリゲーショングループの設定例……6-17
6.7.2. ダイナミックアグリゲーショングループの設定例……6-19

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、複数の物理的な Ethernet インタフェースを 1 つの論理的なリンクに集約します。リンクアグリゲーションは以下の利点があります。

- アグリゲーショングループのメンバポートにトラフィックを分配することによって帯域を増やすことができます。
- アグリゲーショングループのメンバポートがお互いをダイナミックにバックアップすることで、接続信頼性を高めることができます。メンバポートが故障したとき、自動的に他のメンバポートに切り替えられます。

6.1.1. リンクアグリゲーションアプリケーションシナリオ

図 6-1 に示すように、Device A と Device B は 3 つの物理的な Ethernet リンクによって接続されています。これらの 3 つのインタフェースは、論理的なリンクアグリゲーション 1 に集約されています。リンクアグリゲーションの帯域幅は、3 つの物理的な Ethernet インタフェースの合計の帯域幅と同一となります。同時に 3 つの Ethernet インタフェースは、それぞれ別のリンクをバックアップします。

図 6-1 リンクアグリゲーション図



6.1.2. 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、メンバポート

各リンクアグリゲーションは、論理的なアグリゲートインタフェースによって示されます。各アグリゲートインタフェースには自動的に作成されるアグリゲーショングループがあり、アグリゲーションに使用するメンバポートが含まれます。アグリゲーショングループのタイプと番号は、アグリゲートインタフェースと同じです。

I. サポートアグリゲートインタフェースのタイプ

アグリゲートインタフェースは以下のタイプがあります。

- アグリゲートインタフェースは手動で作成されます。アグリゲーショングループのメンバポートはレイヤ 2 Ethernet インタフェースでのみ設定できます。

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 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セクション 3 *アクセス オペレーションマニュアル*の"*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。

II. 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**–ノーマル物理ポートとしてトラフィックを転送することができます。次のいずれかのイベントが発生した後、LACP タイムアウトタイマの最初の満了前に LACPDU が受信されていない場合、メンバポートは Individual 状態になります。
  - 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ています。
  - メンバポートがダウンし、Unselected あるいは Selected に変わったのち、アップになりました。

エッジアグリゲートインタフェースの詳細はセクション 3 *アクセス オペレーションマニュアル*の“*リンクアグリゲーション*”の“*エッジアグリゲートインタフェース*”を参照してください。

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、ポートレート、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。

I. 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。

表 6-1 属性コンフィグレーション

機能	属性コンフィグレーション
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
QinQ	• QinQ の状態（有効/無効） • VLAN タグの TPID • VLAN トランスペアレントトランスミッション QinQについてはセクション3 *アクセス オペレーションマニュアル*の"*QinQ*"を参照してください。

機能	属性コンフィグレーション
VLANマッピング	ポートで設定されたVLANマッピングの異なるタイプです。 VLANマッピングについてはセクション3 *アクセス オペレーション マニュアル*の"*VLAN マッピング*"を参照してください。
VLAN	VLAN属性の設定は以下があります。 • VLAN ID • PVID • リンクタイプ(trunk、hybrid、access) • 動作モード（promiscuous、トランク promiscuous、ホスト、トランクセカンダリ） • IP サブネットベース VLAN の設定 • ポートベース VLAN の設定 • VLAN タグモード VLANについてはセクション3 *アクセス オペレーションマニュアル*の"*VLAN*"を参照してください。

II. 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 アドレス学習と、スパニングツリーがあります。

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** — アグリゲーションが安定します。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** — システムがメンバポートのアグリゲーションステートを自動的に管理します。管理者の管理負荷を削減することができます。ダイナミックアグリゲーションは LACP（IEEE802.3ad Link Aggregation Control Protocol）によって実装されます。ローカルシステムとピアシステムは、メンバポートの集約状態を自動的に維持します。ダイナミックリンクアグリゲーションにより、管理者の作業負荷が減少します。

6.1.6. スタティ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プロセス

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とき、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. 最も高いポート優先度
2. 全 2 重/高速

3. 半 2 重/低速

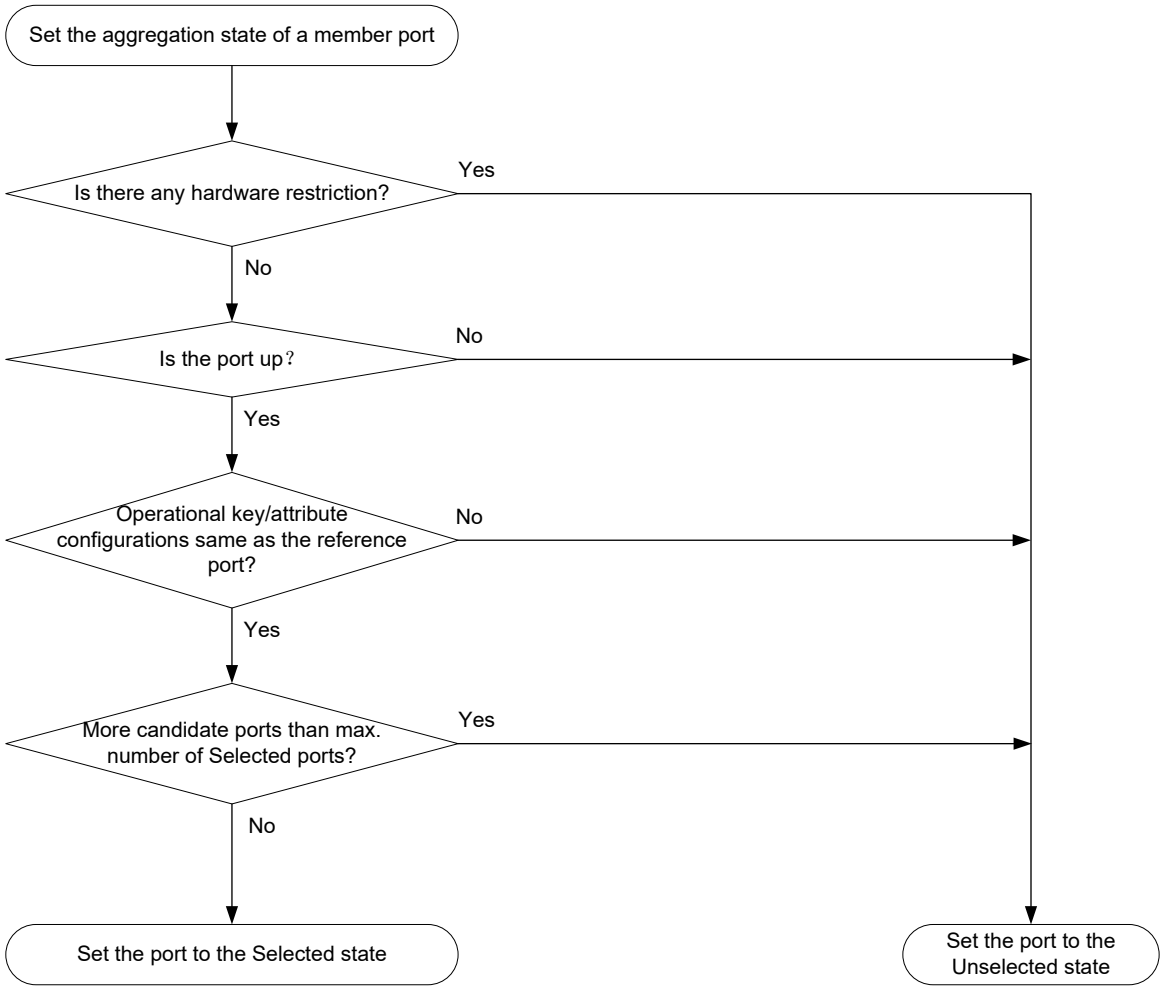
最も高い優先度のポートはリファレンスポートとして選択されます。

- もし複数のポートが同一優先度、通信モード、速度である場合、Selected ポート（可能な場合）が選択されます。複数のポートが Selected ポートである場合、ポート番号が一番小さいポートが選択されます。
- 複数のポートが同一優先度、通信モード、速度で、可能な Selected ポートがない場合、ポート番号が一番小さいポートが選択されます。

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 各メンバポートのアグリゲーションステートの設定



選択したポートの制限に達すると、新しいメンバポートの集約状態は次の条件によって変化します。

- ポートと選択されたポートが同じポートプライオリティを持つ場合、ポートは Unselected 状態になります。 このメカニズムにより、既存の選択ポートでのトラフィックの中断が防止されます。 デバイスを再起動すると、デバイスがメンバポートの集約状態を再計算することがあります。
- 次の条件が満たされると、ポートは Selected 状態になります。

- ポートと選択されたポートにはポート優先順位が異なり、ポートの優先順位が 1 つ以上選択されたポートよりも高いプライオリティが設定されています。
- ポートには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があります。

オペレーショなるキーまたは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集約状態に影響する可能性があります。

6.1.7. ダイナミックリンクアグリゲーション

I. ダイナミックリンクアグリゲーショングループへのインタフェースの割り当て方法

ダイナミックリンク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には、次のいずれかの方法を使用できます。

- 手動割り当てーダイナミックリンクアグリゲーショングループに手動でインタフェースを割り当てます。
- 自動割り当てー受信した LACPDU のピア情報に応じてダイナミックリンクアグリゲーショングループにダイナミックに参加させるために、インタフェース上で自動割り当てを有効にします。

メモ:

一方に自動割り当てを行う場合、もう一方で手動割り当てを使用する必要があります。

II. 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、他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。

III. 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	システムLACP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TLV（Type/Length/Value）フィールドでLACPDUを拡張して実装されます。IRFスタックのLACP MAD機能は拡張LACP機能を使用して実装されます。 拡張LACP機能は、IRFスタックメンバあるいは中間装置でLACP MAD機能を機能させることができます。 IRFスタック、LACP MADの詳細はセクション2 *IRFスタック オペレーションマニュアル*の”*IRFスタック*”を参照してください。

IV. 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とき、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とき、双方のポートは LACPDU を送信することができます。

V. 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、システム LACP 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
システムLACPプライオリティ	ダイナミックリンクアグリゲーションでより高いシステムLACP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。
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。

VI. 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。もしローカルメンバポートが、LACP タイムアウト間隔の 3 倍の時間以内に対向先から 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 送信レートも決まります。LACP タイムアウト間隔は以下のタイプを含みます。

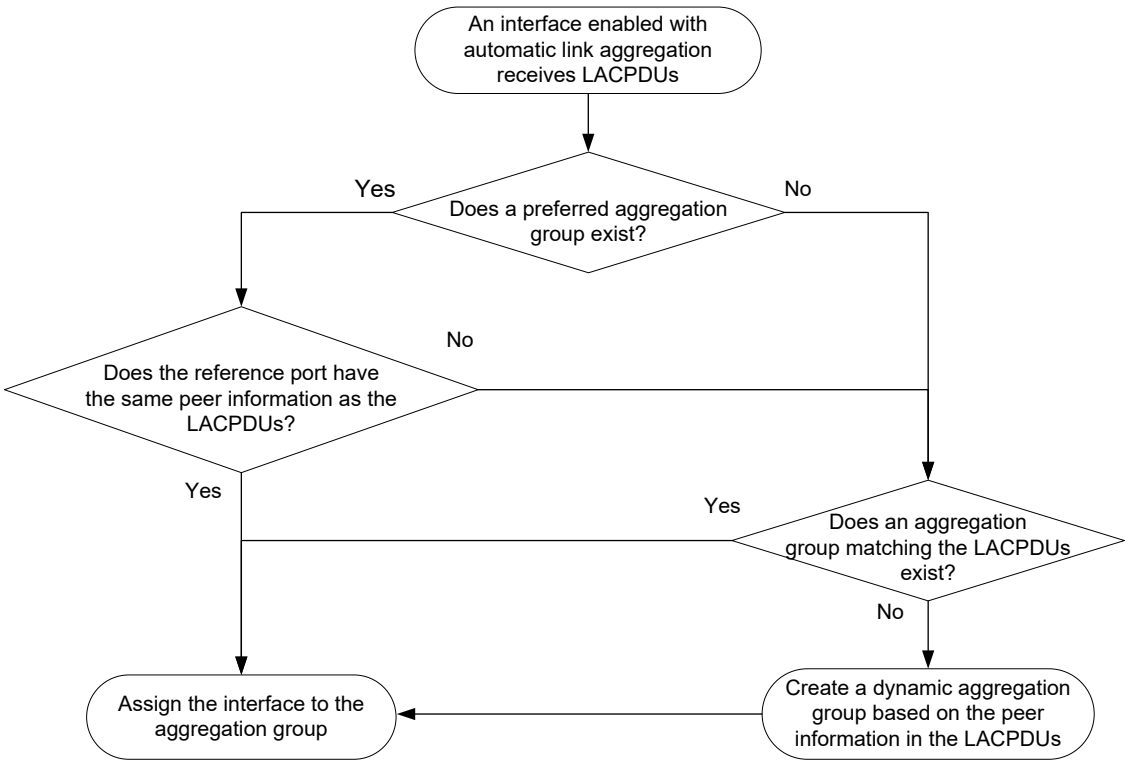
- **短いタイムアウト間隔**－タイムアウト間隔は 3 秒です。短いタイムアウト時間を設定した場合、対向先は LACPDU を早急に送信します。(1 秒ごとに 1 つの LACPDU を送信します)。
- **長いタイムアウト間隔**－タイムアウト間隔は 90 秒です。長いタイムアウト間隔を設定した場合、対向先は LACPDU を長い間隔で送信します。30 秒ごとに 1 つの LACPDU を送信します。

VII. メンバインタフェースの自動割り当て

図 6-3 に示すように、自動割り当てで有効になっているインタフェースで、アグリゲーションピアから受信した LACPDU 内のピア情報に基づいてダイナミックアグリゲーショングループを結合します。既存のダイナミックアグリゲーショングループがない場合、装置は自動的に新しいダイナミックアグリゲーショングループを作成し、装置はそのグループにインタフェースを割り当て、インタフェースの属性コンフィグレーションをアグリゲートインタフェースに同期します。

自動的に追加されたメンバポートと手動で追加されたメンバポートの両方を含むダイナミックアグリゲーショングループでは、装置は手動で追加されたメンバポートからリファレンスポートを選択します。装置は、手動で追加されたメンバポートが使用できない場合にのみ、自動的に追加されたメンバポートからリファレンスポートを選択します。

図 6-3 メンバインタフェースの自動割り当てプロセス



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 はシステム LACP プライオリティと MAC アドレスが含まれます。
   a. 2 つのシステムは 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 が小さくなります。LACP プライオリティの値が同一である場合、b)に進みます。
   b. 2 つのシステムは MAC アドレスを比較します。
      MAC アドレスが小さいとシステム ID が小さくなります。
2. 小さいシステム ID のシステムはリファレンスポートとして最も小さいポート ID のポートが選出されます。
      ポート ID はポートプライオリティとポート番号から構成されます。
   a. システムはリファレンスポートとして最も小さいプライオリティのポートが選出されます。
      ポートが同一である場合、b)に進みます。

b. システムはポート番号を比較します。

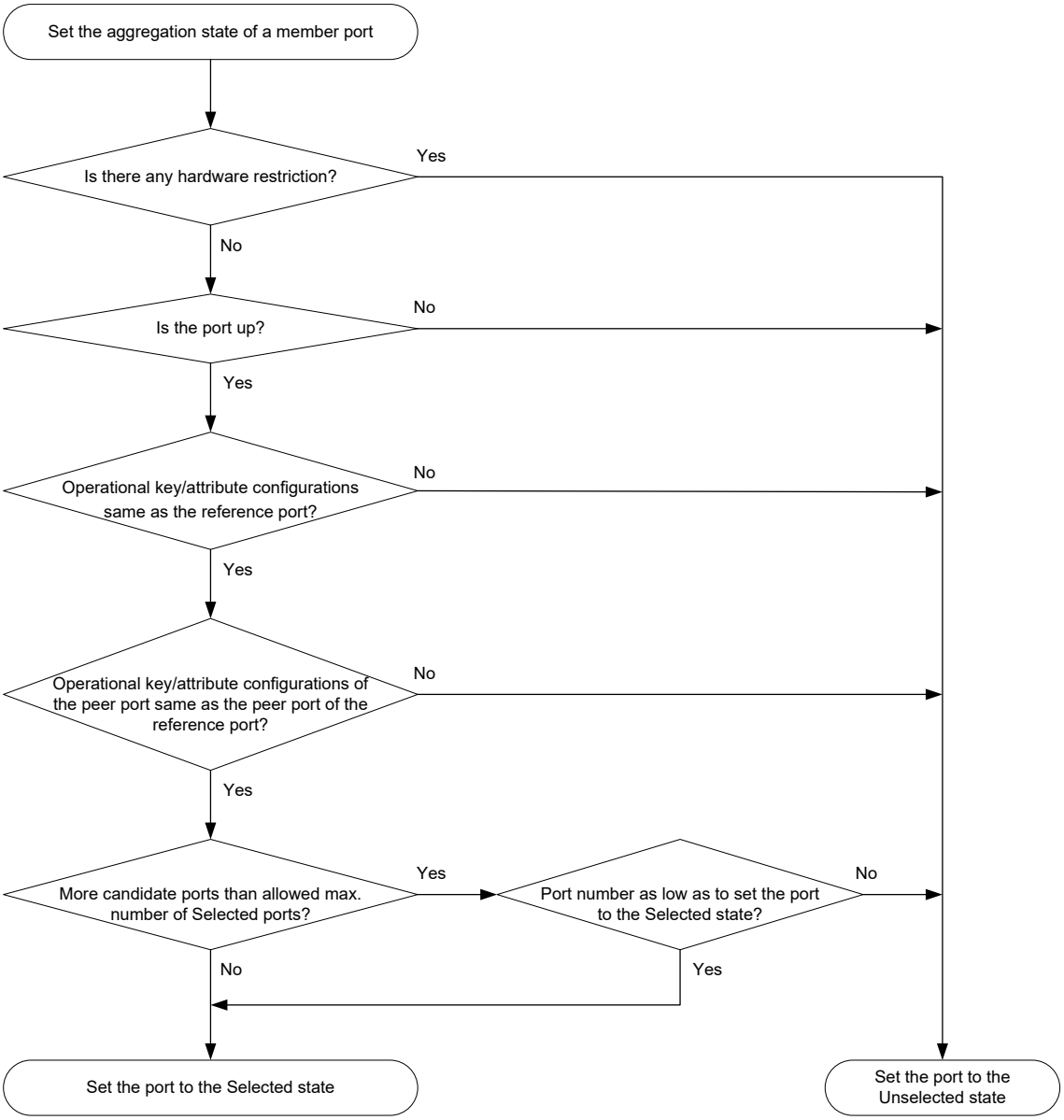
ポート番号が小さいとシステム ID が小さくなります。

最も小さい値のポートと、アグリゲートインタフェースと同一の属性コンフィグレーションを持つポートは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、もっとも小さいシステム ID のシステムは、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 6-4 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ます。システムは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とき、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 ポートとしてできる限り全 2 重で設定してください。
- 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。
- ダイナミックアグリゲーショングループで、ローカルポートのアグリゲーションステートを変更したとき、対向側のリンクアグリゲーションステートも変更されます。
- 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 ステートに置き換わります。

6.1.9. エッジアグリゲートインタフェース

ダイナミックリンクアグリゲーションがデバイス上でのみ構成されている場合、ダイナミックリンクアグリゲーションはサーバ向きのアグリゲートインタフェースで失敗します。装置は、サーバに接続されている物理ポートの 1 つだけを使用してトラフィックを転送します。

リンクの信頼性を向上させるには、アグリゲートインタフェースをエッジアグリゲートインタフェースとして構成します。この機能により、アグリゲーショングループのすべてのメンバポートがトラフィックを転送できます。メンバポートに障害が発生すると、そのトラフィックは自動的に他のメンバポートに切り替えられます。

ダイナミックリンクアグリゲーションがサーバ上で構成された後、装置はサーバから LACPDU を受信できます。 その後、装置とサーバ間のリンクアグリゲーションが正しく動作します。

エッジアグリゲートインタフェースは、ダイナミックアグリゲーショングループに対応するアグリゲートインタフェース上で構成されている場合にのみ有効です。

6.1.10. リンク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されます。

- **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。負荷分散のモードはパケットをフローで分類し、同じリンクの同一の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。
  - 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
  - 入力ポート
  - 送信元あるいは宛先 IP アドレス
- **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)リンクアグリゲーショングループの負荷分散の設定 • リンクアグリゲーショングループのロードシェアリングモードの設定 • local-first 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

6.3.1. 制限とガイドライン

I. アグリゲーショングループの制限

インタフェースで表 6-4 に示す機能を設定した場合、リンクアグリゲーショングループにインタフェースを設定することはできません。

表 6-4 アグリゲーションメンバインタフェースと互換性のない機能

インタフェース機能	参照
MACアドレス認証	セクション8 *セキュリティ オペレーションマニュアル*の“*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	セクション8 *セキュリティ オペレーションマニュアル*の“*ポートセキュリティ*”を参照してください。
802.1X	セクション8 *セキュリティ オペレーションマニュアル*の“*802.1X*”を参照してください。

II. アグリゲーションメンバポートの制限

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、アグリゲーショングループからすべてのメンバポートを削除してください。

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セクション 10 *システム管理 オペレーションマニュアル*の"*ポートミラーリング*"を参照してください。

III. 属性とプロトコルコンフィグレーションの制限

アグリゲートインタフェースで行われた属性コンフィグレーションの変更は、すべてのメンバポートに自動的に同期されます。 変更が Selected ポートに同期されない場合、ポートは Unselected に変更される可能性があります。ポートを再度選択するには、アグリゲートインタフェースまたはポート上の属性コンフィグレーションを変更できます。同期化の失敗は、アグリゲートインタフェー

スで行われた属性コンフィグレーション変更には影響しません。アグリゲートインタフェースから同期された構成は、アグリゲートインタフェースが削除された後でもメンバポート上に保持されます。

メンバポートでの属性コンフィグレーションの変更は、メンバポートの集約状態および実行中のサービスに影響を与える可能性があります。メンバポートで属性コンフィグレーション設定を変更しようとするたびに、警告メッセージが表示されます。

アグリゲートインタフェースのプロトコル構成は、現在のアグリゲートインタフェースでのみ有効です。メンバポートのプロトコル構成は、ポートがアグリゲーショングループを残す場合にのみ有効です。

IV. コンフィグレーションの整合性の要件

アグリゲートリンクの両端で同じアグリゲーションモードを構成する必要があります。

- スタティックアグリゲーションが成功した場合は、各リンクの両端のポートが同じ集約状態にあることを確認します。
- ダイナミックアグリゲーションが成功した場合:
  - リンクの両端のポートが正しいアグリゲーショングループに割り当てられていることを確認します。2 つのエンドは、各メンバポートの集約状態を自動的にネゴシエートできます。
  - 一方の端で自動インタフェース割り当てを使用する場合は、もう一方の端に手動割り当てを使用する必要があります。

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

操作	コマンド	補足
1. system view に移行する	**system-view**	―
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、自動的に作成されます。
3. system view へ戻る	**quit**	―
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* [**force**]	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。
3. ポート LACP プライオリティを設定する	**link-aggregation port-priority** *port-priority*	デフォルト：32768

メモ:

V7.2.16 を含むそれ以降のバージョンで、**port link-aggregation group** コマンドに **force** が追加されました。

II. ダイナミックアグリゲーショングループの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. システム LACP プライオリティを設定する	**lacp system-priority** *system-priority*	デフォルト：32768 システムLACPプライオリティの値を変えるとポートの状態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** *number* [**force**]	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** *port-priority*	デフォルト：32768
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を長い間隔で送信します。 ISSUの間、トラフィックの中断を防ぐため、ISSUを実行する前にshort LACPタイムアウト間隔を設定しないでください。ISSUの詳細はセクション1 *はじめに オペレーションマニュアル*の“*ISSU*”を参照してください。

メモ:

V7.2.16 を含むそれ以降のバージョンで、**port link-aggregation group** コマンドに **force** が追加されました。

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. アグリゲーショングループの Selected ポートの最小と最大数の設定

I. アグリゲーショングループの Selected ポートの最小と最大数

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とき、以下となります。
  - 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。
- 最小数のしきい値以上になったとき、以下となります。
  - 適切なメンバポートが Selected ポートに変更となります。
  - 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。

以下の操作をすることで 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 つのポートをアサインします。
- 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。

II. 制限とガイドライン

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。

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. 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 ポートの最小数を設定する	**link-aggregation selected-port minimum** *min-number*	デフォルト：設定なし
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

6.4.2. アグリゲートインタフェースの説明の設定

I. アグリゲートインタフェースの説明

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。

II. 設定手順

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**

6.4.3. アグリゲートインタフェースのシャットダウン

I. 制限とガイドライン

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されたとき、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。

II. 設定手順

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*

操作	コマンド
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. リンクアグリゲーショングループの負荷分散の設定

6.5.1. リンクアグリゲーショングループのロードシェアリングモードの設定

I. ロードシェアリングモード

⚠ 重要:
リンクアグリゲーションの負荷分散を設定すると、均等なコストルートが、バランスのとれた方法で共有トラフィックをロードするようになります。

装置は、グローバルロードシェアリングモードのみ設定できます。すべてのアグリゲーショングループに適用します。

II. グローバルでのリンクアグリゲーショングループのロードシェアリングモードの設定

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 : パケットタイプによって自動的にグローバルでのロードシェアリングモードが選択されます。

6.5.2. リンクアグリゲーションの local-first ロードシェアリングモードの設定

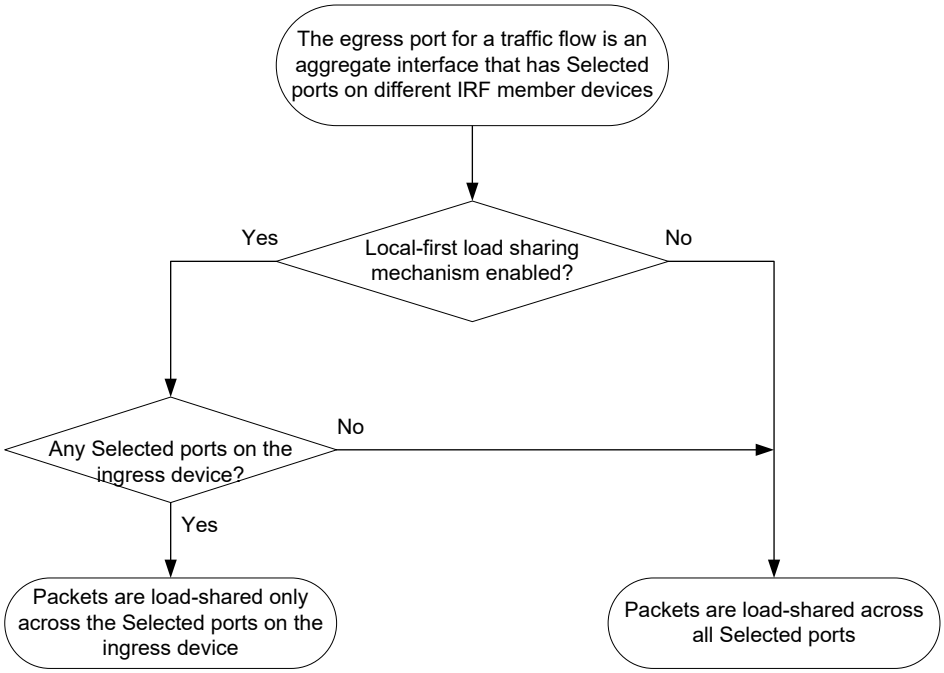
I. リンクアグリゲーションの local-first ロードシェアリングモード

拡張カードあるいは装置で、メンバポートを越えて優先的にトラフィックを配信するため、複数装置のリンクアグリゲーションで local-first ロードシェアリングを使用します。

IRF スタックユニットで異なるメンバデバイスのポートを集約するとき、図 6-5 に示すように IRF スタックのトラフィックを軽減するため、local-first ロードシェアリングを使用することができま

す。IRF スタックの詳細はセクション 2 *IRF スタック オペレーションマニュアル*の"*IRF スタックの設定*"を参照してください。

図 6-5 IRF スタックユニットの複数装置での local-first ロードシェアリング



II. グローバルでのリンクアグリゲーションの local-first ロードシェアリングモードの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. local-first ロードシェアリングを有効にする.	**link-aggregation load-sharing mode local-first**	デフォルト：有効

6.6. 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
アグリゲートインタフェースの情報を表示する	**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**
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* | **auto**]

操作	コマンド
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*]]
アグリゲートインタフェース統計情報をクリアする	**reset counters interface** [{ **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*]

6.7. リンクアグリゲーションの設定例

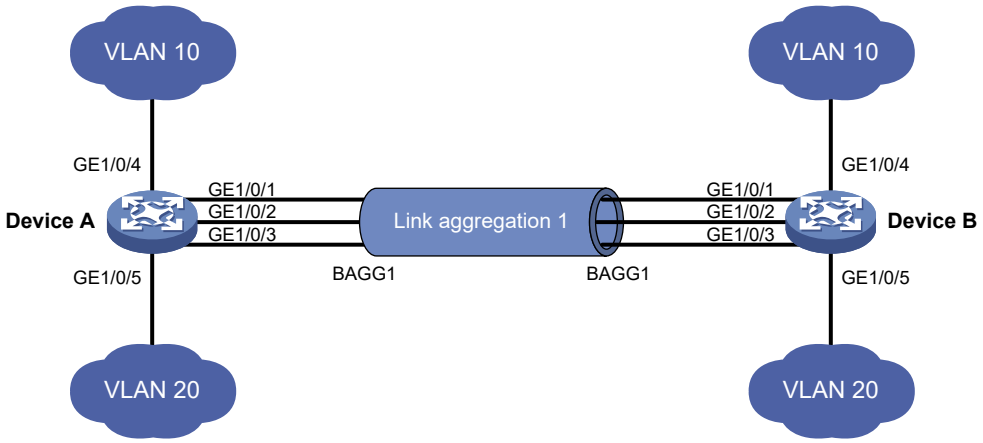
6.7.1. スタティックアグリゲーショングループの設定例

I. ネットワーク要件

図 6-6 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 6-6 ネットワーク図



II. 設定手順

1. Device A を設定します。

   # VLAN10 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

   # VLAN20 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: Shar
Management VLANs: None
  Port             Status  Priority Oper-Key
  GE1/0/1(R)       S       32768    1
  GE1/0/2          S       32768    1
```

```
GE1/0/3          S       32768    1
```

出力は以下のことを示します。

- 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す。
- アグリゲーショングループに 3 つの Selected ポートがあります。

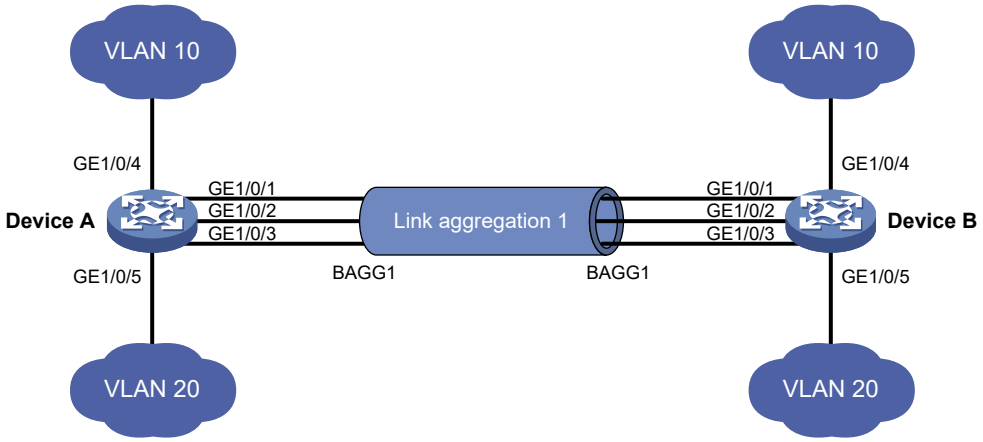
6.7.2. ダイナミックアグリゲーショングループの設定例

I. ネットワーク要件

図 6-7 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 6-7 ネットワーク図



II. 設定手順

1. Device A を設定します。

   # VLAN10 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

   # VLAN20 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
Aggregation Mode: Dynamic
Loadsharing Type: Shar
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}
```

出力は以下のことを示します。

- リンクアグリゲーション 1 はダイナミックアグリゲーショングループです。
- アグリゲーショングループは 3 つの Selected ポートがあります。

目次

このセクションのページは **3-x-x** です。

7 章 Port Isolation 7-1
7.1. 概要 7-1
7.2. アイソレーショングループへのポートの割り当て 7-1
7.3. ポートアイソレーションの表示と維持 7-2
7.4. ポートアイソレーションの設定例 7-2
7.4.1. ポートアイソレーションの設定例 7-2

7章 Port Isolation

7.1. 概要

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 トラフィックを隔離します。

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。

7.2. アイソレーショングループへのポートの割り当て

I. アイソレーショングループへのポートの割り当て

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。アイソレーショングループに追加されるポートの数に制限はありません。

II. 制限とガイドライン

- 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。
- 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。

III. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. アイソレーショングループを作成する	**port-isolate group** *group-id*	—
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*	—

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

7.3. 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*]

7.4. ポートアイソレーションの設定例

7.4.1. ポートアイソレーションの設定例

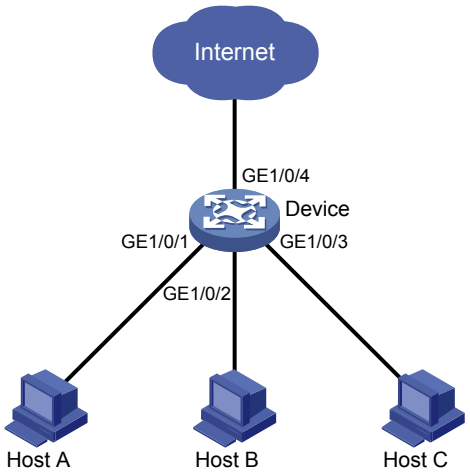
I. ネットワーク要件

図 7-1 に示すように設定します。

- LAN ユーザ Host A、Host B、Host C はそれぞれ GigabitEthernet 1/0/1、GigabitEthernet 1/0/2、GigabitEthernet 1/0/3 に接続されています。
- GigabitEthernet 1/0/4 を通してデバイスが、インタネットに接続します。

ホストはインタネットにアクセスできます。しかしホストはレイヤ 2 で互いに通信できません。

図 7-1 ネットワーク図



II. 設定手順

アイソレーショングループ 2 を作成します。

<Device> system-view

[Device] port-isolate group 2

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 2 に割り当てます。

[Device] interface gigabitethernet 1/0/1

[Device-GigabitEthernet1/0/1] port-isolate enable group 2

[Device-GigabitEthernet1/0/1] quit

[Device] interface gigabitethernet 1/0/2

[Device-GigabitEthernet1/0/2] port-isolate enable group 2

[Device-GigabitEthernet1/0/2] quit

[Device] interface gigabitethernet 1/0/3

[Device-GigabitEthernet1/0/3] port-isolate enable group 2

[Device-GigabitEthernet1/0/3] quit

III. 設定の確認

アイソレーショングループ 2 の情報を表示します。

[Device] display port-isolate group 2

```
Port isolation group information:
Group ID: 2
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 2 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 で互いに隔離されています。

目次

このセクションのページは **3-x-x** です。

8 章 STP 8-1
8.1. 概要 8-1
8.2. STP 8-1
8.2.1. STP プロトコルフレーム 8-1
8.2.2. STP の基本概念 8-3
8.2.3. STP アルゴリズムの計算プロセス 8-5
8.2.4. STP アルゴリズム計算の例 8-7
8.2.5. STP の Configuration BPDU 転送メカニズム 8-11
8.2.6. STP タイマ 8-11
8.3. RSTP 8-12
8.3.1. RSTP プロトコルフレーム 8-12
8.3.2. RSTP の基本概念 8-13
8.3.3. RSTP の動作方法 8-13
8.3.4. RSTP の BPDU 処理 8-14
8.4. PVST 8-14
8.4.1. PVST プロトコルフレーム 8-15
8.4.2. PVST の動作 8-15
8.5. MSTP 8-16
8.5.1. MSTP 機能 8-16
8.5.2. MSTP プロトコルフレーム 8-16
8.5.3. MSTP の基本概念 8-17
8.5.4. MSTP の動作 8-21
8.5.5. 装置での MSTP の実行 8-22
8.6. 高速遷移メカニズム 8-22
8.6.1. Edge ポートの高速遷移 8-23
8.6.2. Root ポートの高速遷移 8-23
8.6.3. P/A transition 8-24
8.7. プロトコルと標準 8-25
8.8. 制限とガイドライン 8-25
8.8.1. 他の機能との互換性 8-25
8.8.2. インタフェースの設定 8-25
8.9. スパニングツリー設定作業リスト 8-26
8.9.1. STP 設定作業リスト 8-26
8.9.2. RSTP 設定作業リスト 8-27
8.9.3. PVST 設定作業リスト 8-28
8.9.4. MSTP 設定作業リスト 8-30
8.10. 動作モードの設定 8-31
8.11. MST region の設定 8-32
8.12. Root Bridge と Secondary Root Bridge の設定 8-33
8.12.1. 制限とガイドライン 8-33
8.12.2. Root Bridge の設定 8-34
8.12.3. Secondary Root Bridge の設定 8-34
8.13. Bridge プライオリティの設定 8-34

8.14. MST region の最大ホップ数の設定 8-35
8.15. ネットワークダイアメータの設定 8-35
8.16. スパニングツリータイマの設定 8-36
8.17. タイムアウトファクタの設定 8-37
8.18. BPDU 最大送出レートの設定 8-38
8.19. Edge ポートの設定 8-39
8.20. Port Path Cost の設定 8-39
8.20.1. Port Path Cost 8-39
8.20.2. デフォルト Path Cost の計算時の基準指定 8-39
8.20.3. Path Cost の設定 8-41
8.21. Port priority の設定 8-42
8.22. Point-to-Point リンクの設定 8-43
8.23. MSTP パケットのフォーマット設定 8-43
8.24. ポート遷移状態情報の出力の有効化 8-44
8.25. スパニングツリー機能の有効化 8-44
8.25.1. 制限とガイドライン 8-44
8.25.2. STP/RSTP/MSTP モードでのスパニングツリー機能の有効化 8-45
8.25.3. PVST モードでのスパニングツリー機能の有効化 8-45
8.26. mCheck 機能の設定 8-45
8.26.1. mCheck 機能 8-45
8.26.2. 制限とガイドライン 8-46
8.26.3. グローバルでの mCheck の実行 8-46
8.26.4. interface view での mCheck の実行 8-46
8.27. Digest Snooping の設定 8-46
8.28. No Agreement Check の設定 8-48
8.29. TC Snooping の設定 8-50
8.30. 保護機能の設定 8-51
8.30.1. 保護機能の設定作業リスト 8-51
8.30.2. BPDU ガードの設定 8-51
8.30.3. Root ガードの有効化 8-52
8.30.4. Loop ガードの有効化 8-53
8.30.5. ポート役割の制限機能の設定 8-54
8.30.6. TC-BPDU ガードの有効化 8-54
8.30.7. BPDU ドロップ機能の有効化 8-55
8.30.8. PVST BPDU ガード機能の有効化 8-56
8.30.9. dispute ガードの無効化 8-56
8.31. TC BPDU の検出、受信イベントのログ作成の有効化 8-58
8.32. BPDU ガードによってシャットダウンされた Edge ポートの再アクティブ化の無効化 8-58
8.33. 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 8-59
8.34. スパニングツリーの表示と維持 8-60
8.35. スパニングツリー設定例 8-61
8.35.1. MSTP の設定例 8-61
8.35.2. PVST の設定例 8-65

8章 STP

8.1. 概要

スパニングツリーは、選択された冗長リンクをブロックして、standby 状態に設定することで、物理的に冗長ネットワークのループを防ぎます。

最近の STP のバージョンでは、RSTP(Rapid Spanning Tree Protocol)、MSTP(Multiple Spanning Tree Protocol)、PVST（Per-VLAN Spanning Tree）を含みます。

8.2. STP

STP (Spanning Tree Protocol)は、IEEE の 802.1d で規定されている、LAN (local area network) のループを防止するレイヤ 2 プロトコルで、一般的にレイヤ 2 のネットワークを冗長化するための 1 つの手段として使用します。ネットワークは故障時のバックアップとして冗長リンクを持ちます。しかしループはさまざまな問題を発生させます。

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。これはループしたネットワークでパケットが拡散し、無尽蔵に回り続けることを防止します。

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を含めたものを意味します。

8.2.1. STP 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。IEEE802.1d で規定される STP では、以下 2 種類の BPDU を使用します。

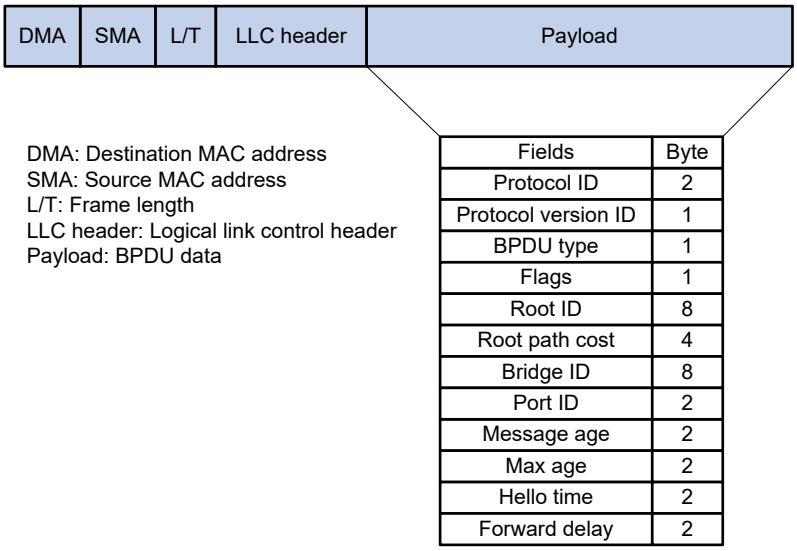
STP が有効なネットワークの装置は BPDU を交換してスパニングツリーを確立します。BPDU はスパニングツリーの計算を行うために十分な情報を含みます。

STP では、BPDU、Configuration BPDU、および TCN（トポロジ変更通知）BPDU の 2 種類が使用されます。

I. Configuration BPDU

装置は、Configuration BPDU を交換してルートブリッジを選択し、ポートの役割を決定します。図 8-1 に Configuration BPDU フォーマットを示します。

図 8-1 Configuration BPDU フォーマット



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

Configuration BPDU のペイロードは以下のフィールドがあります。

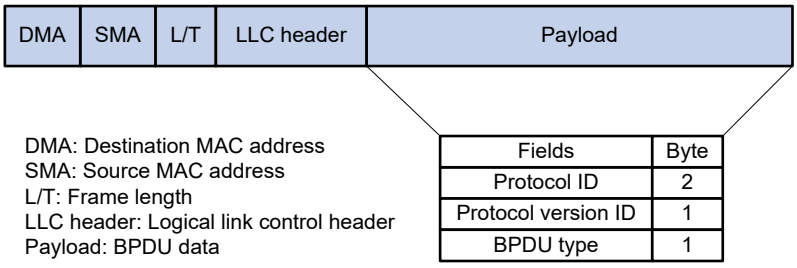
- **Protocol ID**–IEEE 802.1d で規定されています。0x0000 で固定です。
- **Protocol version ID**–スパニングツリープロトコルバージョンの ID です。STP は 0x00 です。
- **BPDU type**–BPDU のタイプです。configuration BPDU は 0x00 です。
- **Flags**–8 ビットフィールドは BPDU の目的を示します。最下位ビットは TC（Topology Change）フラグです。最上位ビットは TCA（Topology Change Acknowledge）フラグです。ほかのビットは予約済みビットです。
- **Root ID**–Root Bridge の priority と MAC アドレスで Root Bridge ID を形成します。
- **Root path cost**–Root Bridge へのパスコストです。
- **Bridge ID**–Designated bridge の priority と MAC アドレスで Designated Root Bridge ID を形成します。
- **Port ID**– Designated ポートの priority とグローバルポート番号で Designated port ID を形成します。
- **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**–ネットワーク内で転送された Configuration BPDU の有効時間です。
- **Hello time**– Configuration BPDU の転送間隔です。
- **Forward delay**–ポートでの転送遅延です。

装置はスパニングツリーの計算を行うため、root bridge ID、root path cost、designated bridge ID、designated port ID、message age、max age、hello time、forward delay を使用します。

II. TCN BPDU

装置はネットワークのトポロジの変更を通知するため、TCN BPDU を使用します。図 8-2 に TCN BPDU フォーマットを示します。

図 8-2 TCN BPDU フォーマット



TCN BPDU のペイロードは以下のフィールドがあります。

- Protocol ID– IEEE 802.1d で規定されています。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。TCN BPDU 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、非 Root Bridge が TCN BPDU を送信します。

- ポートがフォワーディング状態に移行し、ブリッジに指定されたポートが最低 1 つあります。
- ポートは、フォワーディング状態または学習状態からブロッキング状態に移行します。

非 Root Bridge は、ネットワークトポロジが変更されると、TCN BPDU を使用してルートブリッジに通知します。 Root Bridge は、その設定 BPDU に TC フラグを設定し、それを他のブリッジに転送します。

8.2.2. STP の基本概念

I. Root bridge

STP のツリーは、1 つの Root ブリッジと複数の他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 Configuration BPDU を送信します。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 port

Root Bridge 以外の装置において、Root Bridge への path cost が最も低い 1 つのポートが Root Port となります。Root Port は、Root Bridge の装置と通信を行うポートになります。なお、Root Bridge の装置には、Root Port はありません。

III. Designated bridge と designated port

分類	Designated bridge	Designated port
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の転送を行う	Designated bridgeがこのポートにBPDUを転送する
LAN	LANセグメントにBPDUを転送する	Designated bridge が、このLANセグメントにBPDUを転送する

図 8-3 に示すように、Device B と Device C は直接 LAN に接続されています。

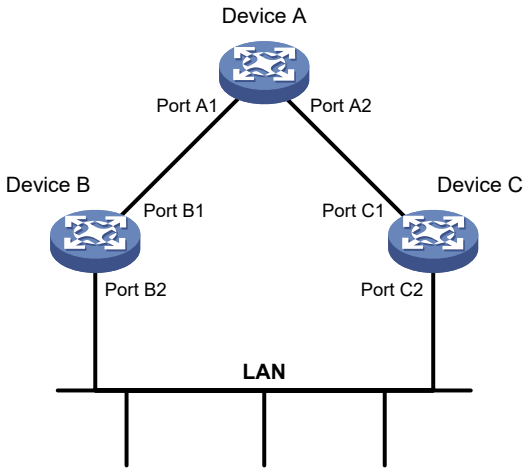
もし Device A がポート A1 を経由して Device B に BPDU を転送する場合、Designated bridge と Designated port は以下のようになります。

- Device B の Designated bridge は Device A です。
- Device B の Designated port は Device A のポート A1 です。

もし Device B が LAN に BPDU を転送する場合は以下のようになります。Designated bridge と Designated port は以下のようになります。

- LAN の Designated bridge は Device B です。
- LAN の Designated port は Device B のポート B2 です。

図 8-3 Designated bridges と designated ports



IV. ポート状態

表 8-1 に STP のポート状態を示します。

表 8-1 STP ポート状態

状態	BPDU の受信/送信	MAC アドレスの学習	ユーザデータの転送
Disabled	No	No	No
Listening	Yes	No	No
Learning	Yes	Yes	No
Forwarding	Yes	Yes	Yes
Blocking	Receive	No	No

V. Path cost

path cost 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 path cost を比較し、最も path cost 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。

8.2.3. STP アルゴリズムの計算プロセス

STP 計算では、装置は、受信した configuration BPDU の優先順位を異なるポートから比較し、root bridge、ルートポート、および designated ポートを選択します。スパニングツリーの計算が完了すると、ツリー形状のトポロジフォームが作成されます。

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、簡略化した処理の例をもとに説明します。

I. 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 Configuration BPDU を作成します。

- ポートを Designated port とします。
- 装置自身を Root Bridge とします。
- Root Path Cost を 0 とします。
- Designated Bridge ID を自身のデバイス ID とします。

II. Root bridge の選択

root bridge は以下の方法を選択することができます。

- **自動選択**–最初にネットワーク上の STP が有効な各装置は、自身が Root bridge として仮定し、Root Bridge を自身の Device ID とします。Configuration BPDU の交換を行うことによって、装置は自身の root bridge ID と、root bridge となる最も小さい root bridge ID の装置を選択するため、root bridge ID を比較します。
- **手動選択**–装置をスパニングツリーの root bridge またはセカンダリ root bridge として構成できます。
  - スパニングツリーには root bridge が 1 つしかありません。スパニングツリーの root bridge として複数のデバイスを設定すると、MAC アドレスが最も小さい装置が選択されます。
  - スパニングツリーには、1 つまたは複数のセカンダリ root bridge を設定できます。root bridge が故障するかシャットダウンされると、セカンダリ root bridge が引き継ぐことができます。 複数のセカンダリ root bridge が構成されている場合は、MAC アドレスが最も低いものが選択されます。 ただし、新しい root bridge が設定されている場合、セカンダリ root bridge は選択されません。

III. root bridge でない root port と Designated port の選択

操作	説明
1	非root bridgeの装置は、最も優先度の高いConfiguration BPDUを受信したポートをroot port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 portのpath costをもとにして、装置はほかのポートのDesignated PortのConfiguration BPDUを計算します。 • Root Bridge ID を Root Port で受信した Configuration BPDU の Root Bridge ID に書き換えます。 • Root Port Cost を Root Port で受信する Configuration BPDU の Root Port Cost に Root Port の Path Cost を加算した値に書き換えます • Designated Bridge ID をその装置の Bridge ID に書き換えます。 • Designated Port 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まります。 • 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。 ○ そのポートは Designated Port になります。 ○ ポートの Configuration BPDU を計算された Configuration BPDU に置き換えます。 ○ 書き換えた 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 を送出することを止め、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 port と Designated Port 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 最も優先度の高い 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。 • もし受信した 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。 • もし受信した 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、最も優先度の高いConfiguration BPDUを選出します。

以下に Configuration BPDU の比較順序を示します。

1. Root Bridge ID が最も小さい Configuration BPDU の優先度が最も高くなります。
2. すべての Configuration BPDU の Root Bridge ID が同じ場合には、次に Root Path Cost を比較します。Configuration BPDU の Root Path Cost とその受信ポートの Path Cost の加算値の最も小さい Configuration BPDU の優先度が高くなります。たとえば Configuration BPDU の root path cost と受信したポートの path cost が S とします。最も小さい S の Configuration BPDU が最も高い優先度となります。
3. すべての Configuration BPDU の Root Bridge ID と S が同じ場合、以下の領域を順に比較します。
   a. Designated Bridge ID
   b. Designated Port ID
   c. 受信したポートの ID

   Designated Bridge ID、Designated Port 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 bridge のとき、ツリー構造のトポロジは、root port、Designated Port が選択されます。

8.2.4. 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

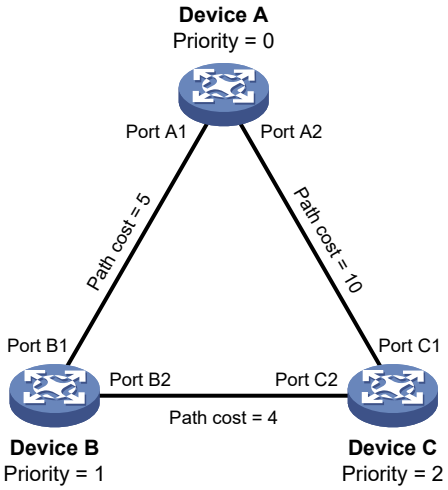


図 8-4 に示すように、Device A、Device B、Device C の優先度の値は、それぞれ 0、1、2 で、3 つの装置間のリンク path cost は、それぞれ 5、10、4 です。

I. 装置の初期状態

表 8-3 に示すように各 Configuration BPDU は root bridge ID、root path cost、designated bridge ID、Designated Port 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	Port A1	{0, 0, 0, Port A1}
	Port A2	{0, 0, 0, Port A2}
Device B	Port B1	{1, 0, 1, Port B1}
	Port B2	{1, 0, 1, Port B2}
Device C	Port C1	{2, 0, 2, Port C1}
	Port C2	{2, 0, 2, Port C2}

II. 各装置の Configuration BPDU を比較します。

表 8-4 において、各 Configuration BPDU は root bridge ID、root path cost、designated bridge ID、designated port 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} が設定を受信したメッセージより優位であることを出します。 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と検出します。 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 Bridgeおよびdesignated Bridgeが Device A であることを検出するとそれ自体をRoot Bridge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 の送信をはじめます。	• 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}
	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 Port 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 Port	• Root port (ポート B1): {0, 0, 0, ポート A1} • Designated port (ポート B2): {0, 5, 1, ポート B2}

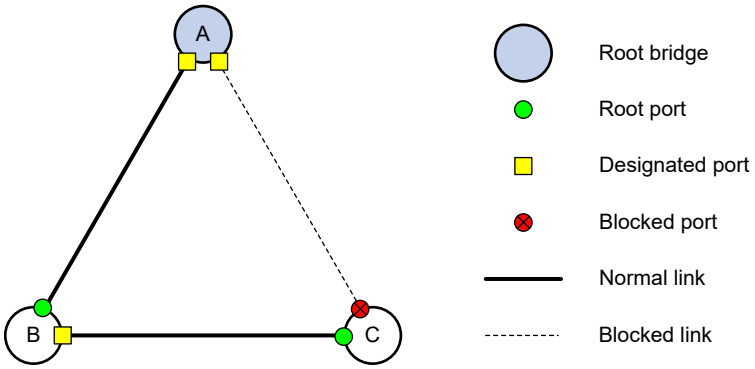
装置	比較プロセス	比較後のポートの Configuration BPDU
	のパス コスト にもとづき、ポートB2 の Configuration BPDUのdesignated {0,5,1, ポートB2} を計算します。Device B は計算したConfiguration BPDU {0,5,1, ポートB2} とポートB2 の Configuration BPDU を比較します。計算した Configuration BPDU が優位であれば ポートB2は designated Portとなります。このポートの Configuration BPDUは計算したConfiguration BPDU に置き換えられ、定期的に送信されます。	
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。 4. すべてのポートの Configuration BPDU を比較します。 5. ポート C1 の Configuration BPDU が最適な Configuration BPDU であると判断します。 6. ポート C1 を Root Port 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 Port 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 Port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 port (ポート C1): {0, 0, 0, ポート A2} • Designated port (ポート C2): {0, 10, 2, ポート C2}
	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	• ポート C1: {0, 0, 0, ポート A2} • ポート C2: {0, 5, 1, ポート B2}

装置	比較プロセス	比較後のポートの Configuration BPDU
	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。	
	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 Port 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、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の計算プロセスが新しく行われるまで、データを転送しません。	• Blocked port (ポート C1): {0, 0, 0, ポート A2} • Root port (ポート C2): {0, 5, 1, ポート B2}

III. 比較プロセス後のスパニングツリー

表 8-4 に記述した比較プロセス後は、Device A を Root Bridge 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



8.2.5. 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 Bridge とみなします。Configuration BPDU を生成し、Hello タイムの間隔で Configuration BPDU を送信します。
- Configuration BPDU を受信した Root Port 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 Port から Configuration BPDU を送信します。
- Designated Port 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 Port 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。 このとき、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 Port や Designated Port は古い通信経路でデータの転送を継続します。新しい Root Port や Designated Port 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。

8.2.6. 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ときの遅延時間です。

  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 Port や Designated Port 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 Port または Designated Port は、forwarding ステートに遷移する前に 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 time

  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。

  デフォルトでは、Hello time は 2 秒です。装置がタイムアウト期間内に Configuration BPDU を受信しない場合、スパニングツリーは再計算されます。 タイムアウト時間の計算式はタイムアウト時間=timeout factor×3×hello 時間です。

- 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。

  デフォルトでは、最大経過時間は 20 秒です。MSTP ネットワークの CIST では、装置は max age タイマを使用して、ポートが受信した Configuration BPDU が期限切れになったかどうかを判断します。 有効期限が切れている場合は、新しいスパニングツリー計算プロセスが開始されます。 最大経過時間タイマは、MSTI では有効になりません。

ポートがタイムアウト期間内に設定 BPDU を受信しない場合、ポートはリスニング状態に移行します。装置はスパニングツリーを再計算します。 フォワーディング状態に戻るにはポート 50 秒が必要です。 この期間は、max age が 20 秒、リスニング状態が 15 秒、学習状態が 15 秒です。

高速トポロジの収束を確実に行うためには、タイマ設定が次の数式を満たしていることを確認します。

- 2 × (forward delay - 1 second) ≥ max age
- Max age ≥ 2 × (hello time + 1 second)

8.3. RSTP

RSTP は、新しく選出された Root Port あるいは Designated Port を forwarding 状態にするため、STP よりも高速なネットワークの収束を行います。

8.3.1. RSTP プロトコルフレーム

RSTP BPDU は、バージョン 1 の長さフィールドが RSTP BPDU のペイロードに追加される以外は、STP BPDU と同じ形式を使用します。 RSTP BPDU と STP BPDU の違いは次のとおりです。

- **Protocol version ID**–RSTP の値は 0x02 です。
- **BPDU type**–RSTP BPDU の値は 0x02 です。
- **Flags**–8 ビットすべてが使用されます。
- **Version1 length**–値は 0x00 です。これは、バージョン 1 のプロトコル情報が存在しないことを意味します。

RSTP はトポロジ変更をアドバタイズするために TCN BPDU を使用しません。 RSTP は、トポロジ変更をアドバタイズするためにネットワークに設定された TC フラグを持つ BPDU をフラッディングします。

8.3.2. RSTP の基本概念

I. ポートの役割

ルートポートと指定ポートに加えて、RSTP は次のポートロールも使用します。

- 代替ポート–ルートポートのバックアップポートとして動作します。ルートポートがブロックされると、代替ポートが引き継ぎます。
- バックアップポート–指定ポートのバックアップポートとして動作します。指定ポートが無効な場合、バックアップポートは新しい指定ポートになります。 同じスパニングツリーデバイスの 2 つのポートが接続されているときにループが発生し、デバイスがポートの 1 つをブロックします。 ブロックされたポートはバックアップポートです。
- エッジポート–ネットワークデバイスまたはネットワークセグメントではなく、ユーザホストに直接接続します。

II. Port 状態

RSTP は、discarding 状態を使用して、STP で disabled 状態、blocking 状態、および listening 状態を置き換えます。表 8-5 に RSTP と STP のポート状態の違いを示します。

表 8-5 RSTP と STP のポート状態の違い

STP ポート状態	RSTP ポート状態	BPDUの送信	MAC アドレスの学習	ユーザデータの転送
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

8.3.3. RSTP の動作方法

RSTP 計算中に、次のイベントが発生します。

- discarding 状態のポートが代替ポートになると、そのポートはその状態を保持します。
- discarding 状態のポートがルートポートまたは指定ポートとして選択されると、フォワード遅延後に学習状態に入ります。ポートは MAC アドレスを学習し、転送状態を別の転送遅延後に入力します。
  - 新しく選出された RSTP ルートポートは、次の要件が満たされている場合、急速にフォワーディング状態に入ります。
    - デバイスの古いルートポートが転送データを停止しました。
    - アップストリーム指定ポートがデータ転送を開始しました。
  - 新しく選出された RSTP 指定ポートは、次の要件のいずれかが満たされている場合、すぐにフォワーディング状態に入ります。
    - 指定ポートは、ユーザ端末に直接接続するエッジポートとして設定されます。

– 指定ポートはポイントツーポイントリンクに接続し、直接接続されたデバイスからハンドシェイク応答を受信します。

8.3.4. RSTP の BPDU 処理

RSTP では、root bridge が RSTP BPDU を送信するのを待たずに、root bridge が指定ポートを経由して RSTP BPDU をアクティブに送信します。これにより、RSTP はリンク障害をすばやく検出できます。装置が、hello 時間の 3 倍以内のポートで RSTP BPDU を受信できない場合、装置はリンク障害が発生したと認識します。 保存された configuration BPDU が期限切れになると、装置は RSTP BPDU を設定して RSTP BPDU をフラッディングし、新しい RSTP 計算を開始します。

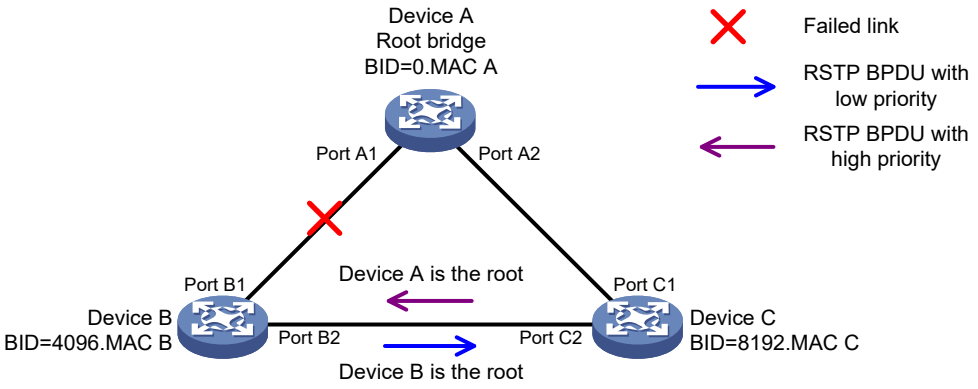
RSTP では、ブロッキング状態のポートは、自身の BPDU より優先度が低い RSTP BPDU に即座に応答できます。

図 8-6 に示すようにデバイス A がルートブリッジです。 デバイス B の優先順位がデバイス C の優先度よりも高く、デバイス C のポート C2 がブロックされています。

デバイス A とデバイス B 間のリンクが失敗すると、次のイベントが発生します。

1. デバイス B は、RSTP BPDU をデバイス C にルートブリッジとして送信します。
2. デバイス C は RSTP BPDU と自身の BPDU を比較します。
3. デバイス B からの RSTP BPDU はプライオリティが低いため、デバイス C は自身の BPDU をデバイス B に送信します。
4. デバイス B は、ポート B2 がルートポートであり、RSTP BPDU のデバイス C への送信を停止します。

図 8-6 RSTP の BPDU 処理



8.4. PVST

STP または 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を共有します。 すべての VLAN からのトラフィックはスパニングツリーに沿って転送され、VLAN ごとにポートブロックをブロックすることはできません。

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、リンクと帯域幅の使用量が増加します。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。

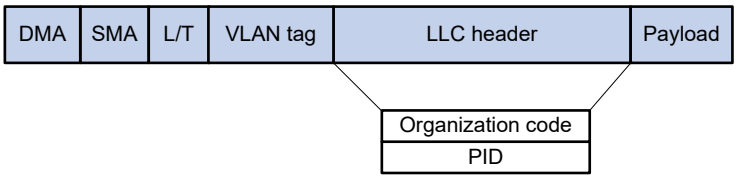
PVST 対応の NEC の装置は、Rapid PVST または PVST を実行しているサードパーティ製デバイスと通信できます。 PVST 対応の NEC の装置は、PVST 対応の NEC の装置または Rapid PVST で有効になっているサードパーティ製デバイスに接続すると、RSTP のような高速ネットワーク収束をサポートします。

8.4.1. PVST プロトコルフレーム

図 8-7 に示すように PVST BPDU は RSTP BPDU と同じフォーマットを使用していますが、以下の違いがあります。

- 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 タグを持ちます。VLAN タグは、PVST BPDU が属する VLAN を識別します。
- 組織コードおよび PID フィールドが PVST BPDU の LLC ヘッダに追加されます。

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 の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。
- トランクまたはハイブリッドポートは、デフォルト VLAN に RSTP BPDU を送信し、他の VLAN で PVST BPDU を送信します。

8.4.2. PVST の動作

PVST は、各 VLAN を MSTI にマッピングすることにより、VLAN ごとのスパニングツリーの計算を実装します。 PVST では、各 VLAN は独立して RSTP を実行して、他の VLAN のスパニングツリーに影響を与えずに独自のスパニングツリーを維持します。 このようにして、各 VLAN のループが除去され、異なる VLAN のトラフィックがリンク上で共有されます。 PVST は、スパニングツリー計算用に他の VLAN のデフォルト VLAN および PVST BPDU に RSTP BPDU を使用します。

PVST は、RSTP と同じポートの役割とポート状態を使用して、高速な移行を行います。詳細はセクション 3 *アクセス オペレーションマニュアル*の“*STP*”の“*RSTP の基本概念*“を参照してください。

8.5. MSTP

8.5.1. MSTP 機能

IEEE802.1s に基づいて開発された MSTP は、STP、RSTP、および PVST の制限を克服します。 高速ネットワーク収束をサポートするだけでなく、異なる VLAN のデータフローを別々のパスに沿って転送できます。 これにより、冗長リンクの負荷共有メカニズムが向上します。

- **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。トポロジの変更が起こった際に、新しく選出された Root Port や Designed Port は、ほかの装置または共有 LAN セグメントではなくユーザ端末に直接接続した point-to-point リンクのポートあるいは Edge Port であっても、forwarding 状態に遷移する前に 2 倍の転送遅延時間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 毎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 を許可しているとき、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。

8.5.2. MSTP 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。

図 8-8 MSTP BPDU フォーマット

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	MSTP-specific fields
MST configuration ID	51	
CIST IRPC	4	
CIST bridge ID	8	
CIST remaining ID	1	
MSTI configuration messages	LEN	

MSTP BPDU の最初の 13 フィールドは RSTP BPDU と同じです。他の 6 つのフィールドは MSTP 固有のものです。

- **Protocol version ID**－MSTP の値は 0x03 です。
- **BPDU type**－RSTP/MSTP BPDU の値は 0x02 です。
- **Root ID**－共通ルートブリッジの ID です。
- **Root path cost**－CIST 外部パスコストです。
- **Bridge ID**－IST または MSTI の regional root の ID です。
- **Port ID**－CIST 内の指定ポートの ID です。
- **Version3 length**－MSTP 固有のフィールドの長さ。 デバイスは、MSTP BPDU を受信したときの検証にこのフィールドを使用します。
- **MST configuration ID**－format セレクタ、コンフィギュレーション名、リビジョンレベル、およびコンフィギュレーションダイジェストが含まれます。 format セレクタの値は 0x00 に固定されています。他のパラメータは、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**－元のブリッジから MST region のルートまで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**－残りのホップ数です。このフィールドは、MST region のスケールを制限します。 region ルートは、残りのホップ数を最大値に設定した BPDU を送信します。 BPDU を受信する各デバイスはホップ数を 1 つずつ削除します。 ホップ数が 0 に達すると、BPDU は破棄されます。 MST region の最大ホップを超えるデバイスは、スパニングツリーの計算に参加できません。 デフォルトの残りホップ数は 20 です。
- **MSTI configuration messages**－MSTI 設定メッセージが含まれます。 各 MSTI 設定メッセージは 16 バイトです。 このフィールドには、0～64 の MSTI の設定メッセージを含めることができます。 MSTI 設定メッセージの数は、MST region の MSTI の数によって決まります。

8.5.3. 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

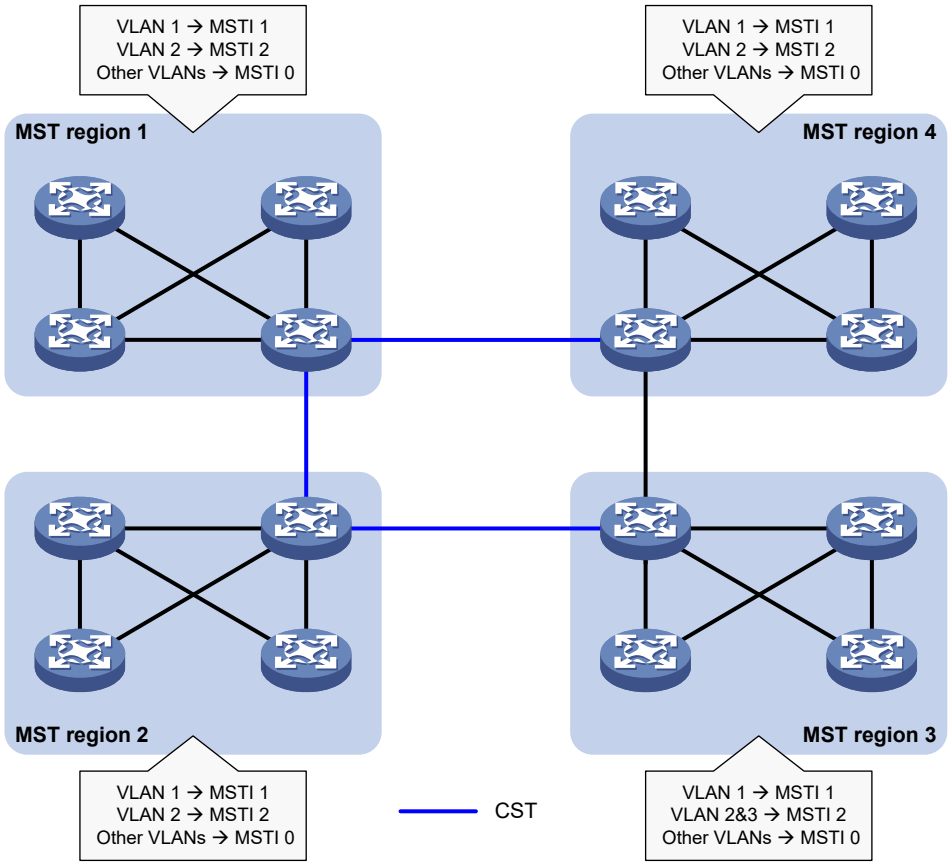
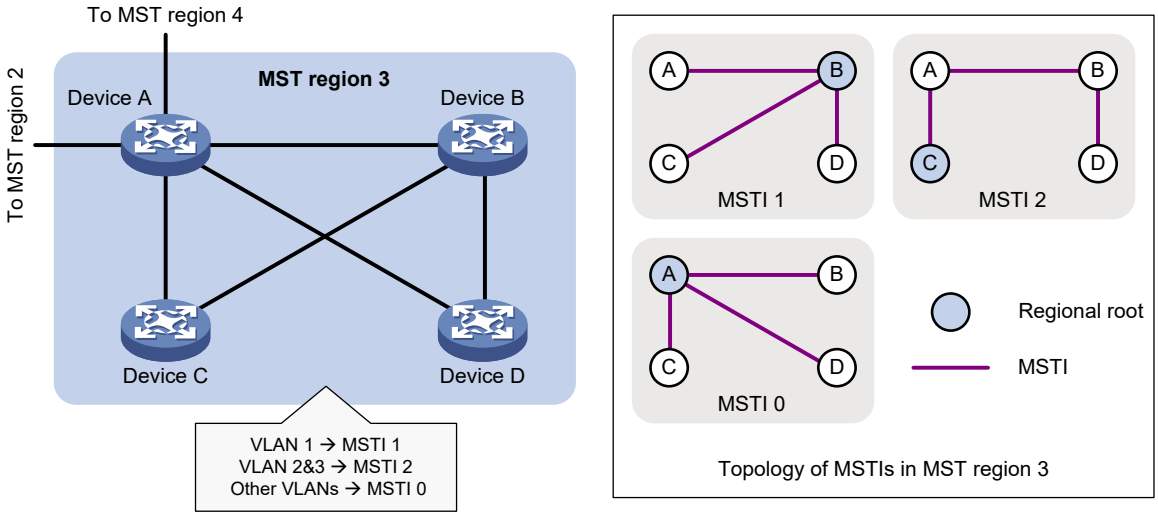


図 8-10 MST region 3 のネットワーク図とトポロジ



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-to-instance 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われます。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、MSTI 1、MSTI 2、MSTI 0 の 3 つの MSTI があります。

III. VLAN-to-instance マッピングテーブル

VLAN-to-instance 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-to-instance 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 MSTI 0 にマッピングされています。

MSTP は、VLAN-to-instance マッピング テーブルを使ってロードバランスを行います。

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 を表しています。

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 Bridge は、MST またはその MSTI の regional Root Bridge 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 bridge

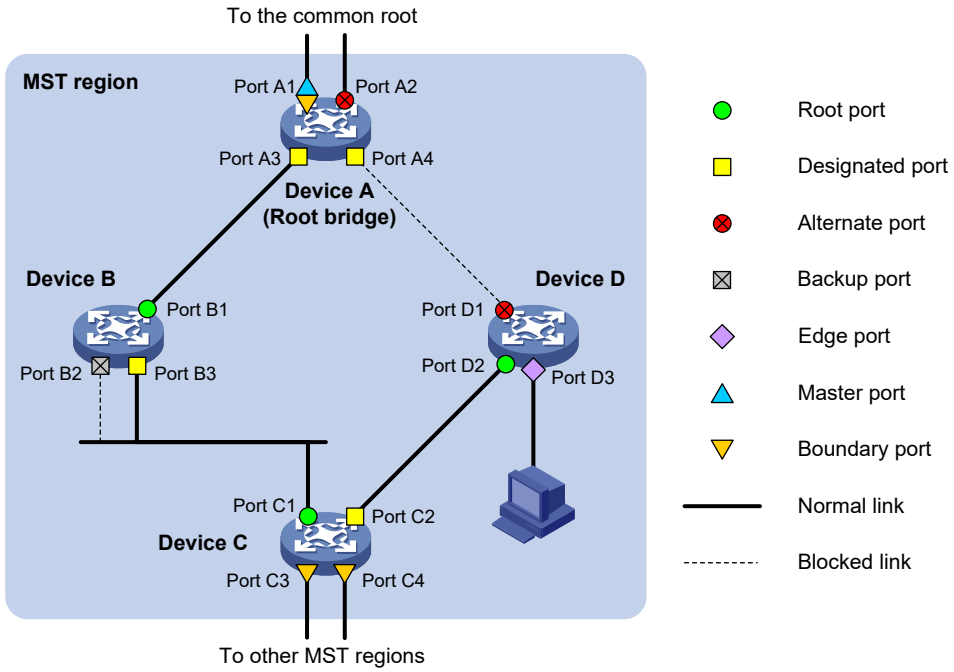
共通 Root Bridge は、CIST の root bridge です。

図 8-9 では、 MST Region 1 のスイッチが共通 Root Bridge 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 Bridge 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 bridge 用にデータを root bridge に転送します。root bridge は root port 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、即座にその代わりに Designated ポートになり、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 Bridge 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 Bridge 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 ポートは Root Port で、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 の計算を行うとき、MSTI の boundary port 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 port です。

X. ポートの状態

MSTP では、ポートは次のいずれかの状態にできます。

- **Forwarding**–ポートは BPDU を受信および送信し、MAC アドレスを学習し、ユーザートラフィックを転送します。
- **Learning**–ポートは BPDU を受信して送信し、MAC アドレスを学習しますが、ユーザートラフィックは転送しません。 学習は中間ポート状態です。
- **Discarding**–ポートは BPDU を受信して送信しますが、MAC アドレスを学習したり、ユーザートラフィックを転送したりしません。

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。“O”はポートがこの状態に対応することを表し、 “×”はポートがこの状態に対応しないことを表します

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	O	O	×	×
Learning	O	O	×	×
Discarding	O	O	O	O

8.5.4. 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 の計算

CIST の計算では、以下の処理が行われます

- 最も優先度の高いデバイスを、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 つのデバイスとみなして、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 の計算

MST Region 内では、VLAN マッピングテーブルの情報によって 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、セクション 3 *アクセス オペレーションマニュアル*の"*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:パケットは対応する MSTI に沿って転送されます。
- MST region 間:パケットは CST に沿って転送されます。

8.5.5. 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 bridge の保持
- Root bridge 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.

8.6. 高速遷移メカニズム

STP では、ポートは blocking 状態から forwarding 状態に移行する前に、転送遅延(デフォルトで 30 秒)の 2 倍待機する必要があります。 転送遅延は、hello 時間とネットワークダイアメータに関係します。 転送遅延が短すぎると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を与えます。

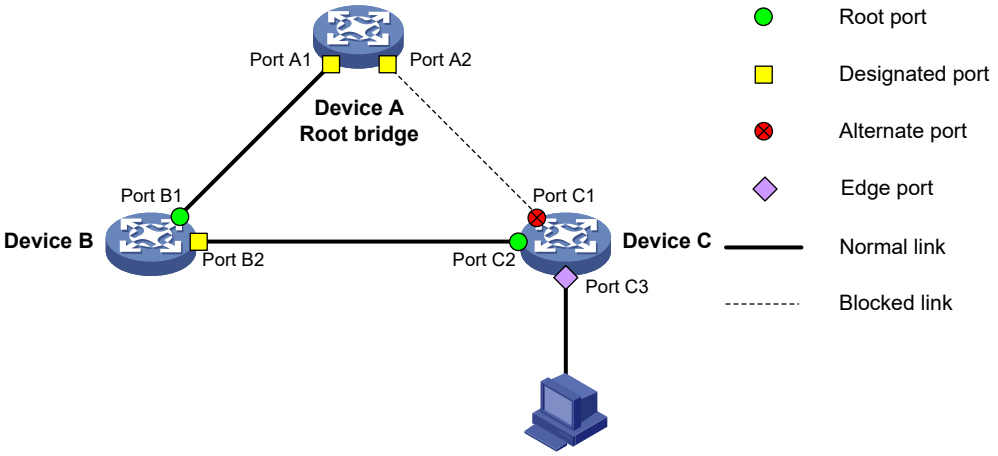
RSTP、PVST、および MSTP はすべて、高速遷移メカニズムを使用して、edge ポート、Root ポート、および designated ポートのポート状態遷移を高速化します。 指定ポートの迅速な遷移メカニズムは、P/A（proposal/agreement）_transition とも呼ばれます。

8.6.1. Edge ポートの高速遷移

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すると、ループが発生しないため、ポートは blocking 状態から forwarding 状態に即座に移行できます。

装置はポートが直接端末に接続されているかどうかを判別できないため、ポートを Edge ポートとして手動で設定する必要があります。

図 8-12 Edge ポートの高速遷移

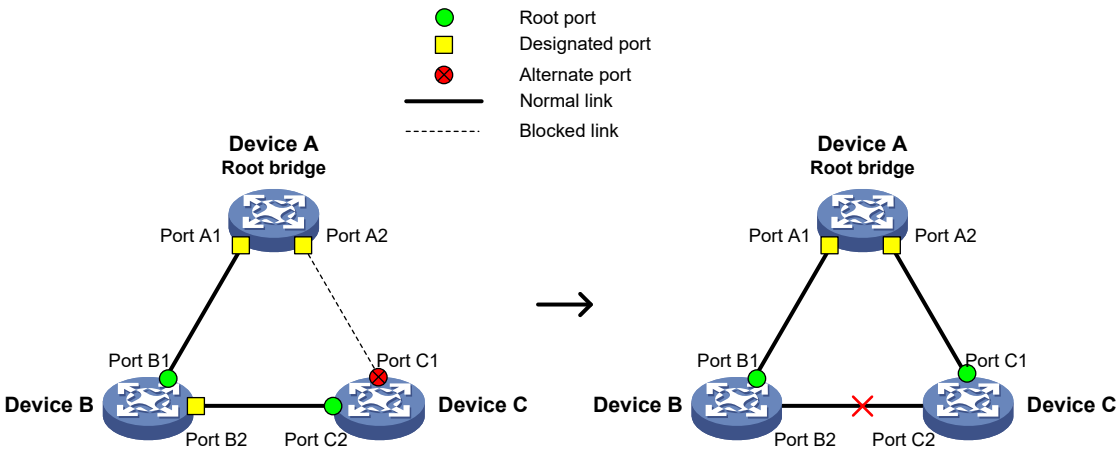


8.6.2. Root ポートの高速遷移

ルートポートがブロックされると、ブリッジは新しい root ポートとしてプライオリティが最も高い代替ポートを選択します。新しい root ポートのピアが forwarding 状態にある場合、新しい root ポートはただちに forwarding 状態に移行します。

図 8-13 に示すように、デバイス C のポート C2 がルートポートで、ポート C1 が代替ポートです。ポート C2 が blocking 状態に移行すると、ポート C1 は Root ポートとして選択され、直ちに forwarding 状態に移行します。

図 8-13 Root ポートの高速遷移



8.6.3. P/A transition

P/A transition は､指定ポートがピアとハンドシェイク後に転送状態に急速に移行することを可能にします。 P/A transition はポイントツーポイントリンクにのみ適用されます。

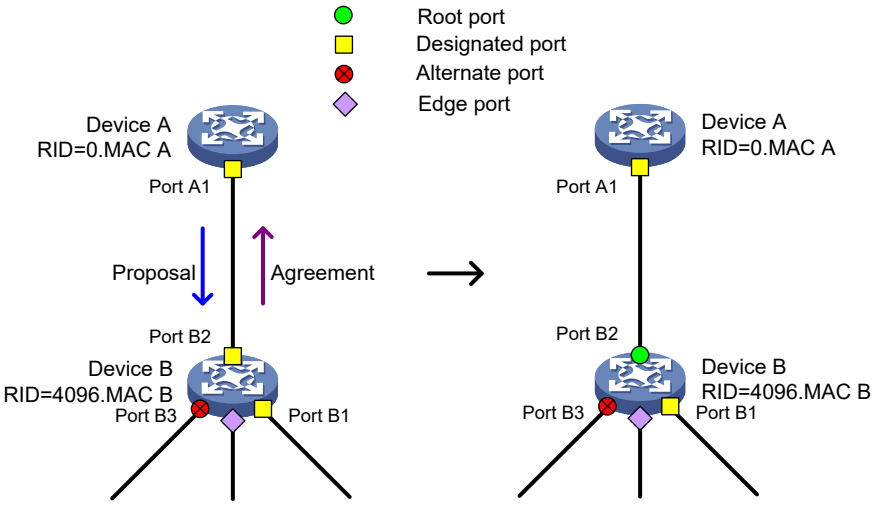
I. RSTP と PVST の P/A transition

RSTP または PVST では、新しいリンクまたはリカバリされたリンクのポートは、blocking 状態のポートです。 designated ポートの 1 つが discarding または learning 状態に遷移すると、その BPDU に proposal フラグが設定されます。ピアブリッジは BPDU を受信し、受信ポートが Root ポートかどうかを決定します。 Root ポートの場合、ブリッジは Edge ポートを除く他のポートをブロックします。 ブリッジは次に、agreement BPDU を designated ポートに返信します。 designated ポートは、agreement BPDU を受信すると直ちに forwarding 状態に移行します。 designated ポートが agreement BPDU を受信しない場合、転送遅延の 2 倍を待機して forwarding 状態に移行します。

図 8-14 に示すように P/A transition の動作を以下に示します。

1. デバイス A は、ポート A1 を介して、proposal BPDU をデバイス B に送信します。
2. デバイス B はポート B2 で proposal BPDU を受信します。 ポート B2 は Root ポートとして選択されます。
3. デバイス B は、designated ポート B1 と代替ポートポート B3 をブロックしてループを除去します。
4. Root ポート B2 はフォワーディング状態に移行し、agreement BPDU をデバイス A に送信します。
5. デバイス A の指定ポート A1 は、agreement BPDU を受信した後、直ちに forwarding 状態に移行します。

図 8-14 RSTP と PVST の P/A transition



II. MSTP の P/A transition

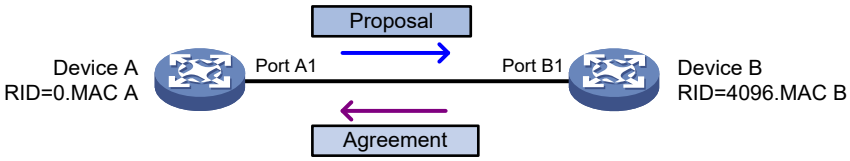
MSTP では、上流ブリッジは、proposal フラグと agreement フラグの両方を BPDU に設定します。下流ブリッジが BPDU を受信し、その受信ポートが Root ポートとして選択されている場合、ブリッジは Edge ポートを除く他のすべてのポートをブロックします。 その後、下流ブリッジは、agreement BPDU を上流ブリッジに返信します。上流ポートは、agreement BPDU を受信すると直

ちに forwarding 状態に移行します。上流ポートが agreement BPDU を受信しない場合、forwarding 状態への転送に転送遅延の 2 倍を待機します。

図 8-15 に示すように P/A transition の動作を以下に示します。

1. デバイス A は、その BPDU 内の proposal フラグと agreement フラグを設定し、ポート A1 を介してデバイス B に送信します。
2. デバイス B は BPDU を受信します。デバイス B のポート B1 が Root ポートとして選択されます。
3. デバイス B は、Edge ポート以外のすべてのポートをブロックします。
4. デバイス B の Root ポート B1 は forwarding 状態に移行し、agreement BPDU をデバイス A に送信します。
5. デバイス A のポート A1 は、契約 BPDU を受信すると直ちに forwarding 状態に移行します。

図 8-15 MSTP の P/A transition



8.7. プロトコルと標準

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*

8.8. 制限とガイドライン

8.8.1. 他の機能との互換性

スパニングツリーの設定は、RRPP、Smart Link、L2PT と同時に設定することはできません。

8.8.2. インタフェースの設定

- 一部のスパニングツリー機能は、Layer2 Ethernet interface view および aggregate interface view でサポートされています。 特に明記されていない限り、これらの view は、この文書の interface view と総称されます。 BPDU ドロップは、Layer2 Ethernet interface view でのみ設定できます。
- 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転送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。

8.9. スパニングツリー設定作業リスト

8.9.1. STP 設定作業リスト

作業リスト
root bridgeの設定: 1. (必須設定項目) 動作モードの設定 2. (オプション設定項目) Root Bridge と Secondary Root Bridge の設定 3. (オプション設定項目) Bridge プライオリティの設定 4. (オプション設定項目) STP トポロジ収束パラメータの設定 ○ ネットワークダイアメータの設定 ○ スパニングツリータイマの設定 ○ タイムアウトファクタの設定 ○ PDU 最大送出レートの設定 5. (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 6. (必須設定項目) スパニングツリー機能の有効化 7. (オプション設定項目) スパニングツリー拡張機能の設定 ○ TC snooping の設定 ○ 保護機能の設定 ○ BPDU ガードによってシャットダウンされた Edge ポートの再アクティブ化の無効化 ○ 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

作業リスト
leaf nodeの設定: 1. (必須設定項目) 動作モードの設定 2. (オプション設定項目) Bridge プライオリティの設定 3. (オプション設定項目) STP トポロジ収束パラメータの設定 o タイムアウトファクタの設定 o BPDU 最大送出レートの設定 o Port Path Cost の設定 o Port priority の設定 4. (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 5. (必須設定項目) スパニングツリー機能の有効化 6. (オプション設定項目) スパニングツリー拡張機能の設定 o TC snooping の設定 o 保護機能の設定 o BPDU ガードによってシャットダウンされた Edge ポートの再アクティブ化の無効化 o 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

8.9.2. RSTP 設定作業リスト

作業リスト
root bridgeの設定: 1. (必須設定項目) 動作モードの設定 2. (オプション設定項目) Root Bridge と Secondary Root Bridge の設定 3. (オプション設定項目) Bridge プライオリティの設定 4. (オプション設定項目) STP トポロジ収束パラメータの設定 o ネットワークダイアメータの設定 o スパニングツリータイマの設定 o タイムアウトファクタの設定 o BPDU 最大送出レートの設定 o Edge ポートの設定 o Point-to-Point リンクの設定 5. (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 6. (必須設定項目) スパニングツリー機能の有効化 7. (オプション設定項目) スパニングツリー拡張機能の設定 o mCheck 機能の設定 o TC snooping の設定 o 保護機能の設定 o BPDU ガードによってシャットダウンされた Edge ポートの再アクティブ化の無効化 o 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

作業リスト
leaf nodeの設定: 1. (必須設定項目) 動作モードの設定 2. (オプション設定項目) Bridge プライオリティの設定 3. (オプション設定項目) STP トポロジ収束パラメータの設定 o タイムアウトファクタの設定 o BPDU 最大送出レートの設定 o Edge ポートの設定 o Port Path Cost の設定 o Port priority の設定 o Point-to-Point リンクの設定 4. (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 5. (必須設定項目) スパニングツリー機能の有効化 6. (オプション設定項目) スパニングツリー拡張機能の設定 o mCheck 機能の設定 o TC snooping の設定 o 保護機能の設定 o BPDU ガードによってシャットダウンされた Edge ポートの再アクティブ化の無効化 o 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

8.9.3. PVST 設定作業リスト

作業リスト
root bridgeの設定: 1. (必須設定項目) 動作モードの設定 2. (オプション設定項目) Root Bridge と Secondary Root Bridge の設定 3. (オプション設定項目) Bridge プライオリティの設定 4. (オプション設定項目) STP トポロジ収束パラメータの設定 o ネットワークダイアメータの設定 o スパニングツリータイマの設定 o タイムアウトファクタの設定 o BPDU 最大送出レートの設定 o Edge ポートの設定 o Point-to-Point リンクの設定 5. (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 6. (必須設定項目) スパニングツリー機能の有効化 7. (オプション設定項目) スパニングツリー拡張機能の設定 o mCheck 機能の設定 o 保護機能の設定 o トポロジ変更イベントによる SNMP notification の有効化 o BPDU ガードによってシャットダウンされた Edge ポートの再アクティブ化の無効化 o 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

作業リスト
leaf nodeの設定: 1. (必須設定項目) 動作モードの設定 2. (オプション設定項目) Bridge プライオリティの設定 3. (オプション設定項目) STP トポロジ収束パラメータの設定 o タイムアウトファクタの設定 o BPDU 最大送出レートの設定 o Edge ポートの設定 o Port Path Cost の設定 o Port priority の設定 o Point-to-Point リンクの設定 4. (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 5. (必須設定項目) スパニングツリー機能の有効化 6. (オプション設定項目) スパニングツリー拡張機能の設定 o mCheck 機能の設定 o 保護機能の設定 o トポロジ変更イベントによる SNMP notification の有効化 o BPDU ガードによってシャットダウンされた Edge ポートの再アクティブ化の無効化 o 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

8.9.4. MSTP 設定作業リスト

作業リスト
root bridgeの設定: 1. (必須設定項目) 動作モードの設定 2. (必須設定項目) MST region の設定 3. (オプション設定項目) Root Bridge と Secondary Root Bridge の設定 4. (オプション設定項目) Bridge プライオリティの設定 5. (オプション設定項目) STP トポロジ収束パラメータの設定 o MST region の最大ホップ数の設定 o ネットワークダイアメータの設定 o スパニングツリータイマの設定 o タイムアウトファクタの設定 o BPDU 最大送出レートの設定 o Edge ポートの設定 o Point-to-Point リンクの設定 6. (オプション設定項目) MSTP パケットのフォーマット設定 7. (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 8. (必須設定項目) スパニングツリー機能の有効化 9. (オプション設定項目) スパニングツリー拡張機能の設定 o mCheck 機能の設定 o Digest Snooping の設定 o No Agreement Check の設定 o TC snooping の設定 o 保護機能の設定 o BPDU ガードによってシャットダウンされた Edge ポートの再アクティブ化の無効化 o 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

作業リスト
leaf nodeの設定: 1. (必須設定項目) 動作モードの設定 2. (必須設定項目) MST region の設定 3. (オプション設定項目) Bridge プライオリティの設定 4. (オプション設定項目) STP トポロジ収束パラメータの設定 ○ タイムアウトファクタの設定 ○ BPDU 最大送出レートの設定 ○ Edge ポートの設定 ○ Port Path Cost の設定 ○ Port priority の設定 ○ Point-to-Point リンクの設定 5. (オプション設定項目) MSTP パケットのフォーマット設定 6. (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 7. (必須設定項目) スパニングツリー機能の有効化 8. (オプション設定項目) スパニングツリー拡張機能の設定 ○ mCheck 機能の設定 ○ Digest Snooping の設定 ○ No Agreement Check の設定 ○ TC snooping の設定 ○ 保護機能の設定 ○ BPDU ガードによってシャットダウンされた Edge ポートの再アクティブ化の無効化 ○ 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

8.10. 動作モードの設定

I. 動作モード

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**–装置を STP で動作させます。スパニングツリーの情報交換のため、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**–装置を RSTP で動作させます。スパニングツリーの情報交換のため、RSTP BPDU を送信します。ただし、対向装置が STP で動作していることを検知すると STP BPDU を送信します。対向装置が MSTP BPDU を受信していても、このモードのポートは MSTP モードに移行しません。
- **PVST モード**–装置を PVST で動作させます。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 が有効なポートと、PVST が有効な VLAN を掛け合わせた数になります。もし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とき、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**–装置を MSTP で動作させます。スパニングツリーの情報交換のため、MSTP BPDU を送信します。ただし、対向装置が STP で動作していることを検知すると STP BPDU を送信し

ます。対向装置が RSTP BPDU を受信していても、このモードのポートは RSTP モードに移行しません。

II. 制限とガイドライン

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。

III. 設定手順

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

8.11. MST regionの設定

I. MST region

スパニングツリーの装置が物理的に接続され、以下が同じ設定の場合、スパニングツリーの装置は同じ MST region に属します。

- フォーマットセレクタ(デフォルトは 0 です。設定できません。)
- MST region 名
- MST region revision レベル
- MST region の同一 VLAN-to-instance マッピングエントリ

MST region に関連したパラメータ(特に VLAN-to-instance 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。

II. 制限とガイドライン

STP、RSTP、PVST モードでは MST region の設定は適用されません。

III. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. MST region view に移行する	**stp region-configuration**	—

操作	コマンド	補足
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-to-instance マッピングテーブルを作成する	• MSTI へのVLAN リストのマッピング : **instance** *instance-id* **vlan** *vlan-id-list* • VLAN-インスタンスマッピングテーブルの休息生成 : **vlan-mapping modulo** *modulo*	どちらかの設定を使用します。 デフォルト : すべての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**	—

8.12. Root BridgeとSecondary Root Bridgeの設定

8.12.1. 制限とガイドライン

スパニングツリーは、 計算でスパニングツリーの Root Bridge を指定できます。あるいは、Root Bridge あるいは Secondary Root Bridge として装置を指定することができます。

Root Bridge と Secondary Root Bridge を設定するとき、以下の制限とガイドラインに従ってください。

- 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 Bridge や Secondary Root Bridge は、別のスパニングツリーの Root Bridge や Secondary Root Bridge 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 Bridge や Secondary Root Bridge にすることはできません。
- 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 Bridge を指定することができます。装置を Root Bridge あるいは Secondary Root Bridge 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 Bridge 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きましては、セクション 3 *アクセス オペレーションマニュアル*の"*STP*"の" *Bridge プライオリティの設定*"を参照してください。

8.12.2. Root Bridge の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. Root Bridge 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 Bridgeとして機能しません。

8.12.3. Secondary Root Bridge 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 Bridge 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 Bridgeとして機能しません。

8.13. Bridgeプライオリティの設定

I. Bridge プライオリティ

スパニングツリーでは、Bridge プライオリティのパラメータを用いて、Root Bridge を決定します。この際に使用する Bridge 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。最も小さい値の Bridge プライオリティを設定することで、そのデバイスを Root Bridge 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 Bridge プライオリティを設定することができます。

Root Bridge の選出とき、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、最も小さい MAC アドレスの装置が Root Bridge として選択されます。Root bridge もしくは Secondary Root Bridge を指定した後、コマンドを使用してそのスイッチの Bridge Priority を変更することはできません。

II. 設定手順

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

操作	コマンド	補足
2. Bridge 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

8.14. MST regionの最大ホップ数の設定

I. MST region の最大ホップ数

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。

Configuration BPDU には、残りホップ数を管理するためのフィールド（Remaining Hops 領域）があります。スパニングツリーの Root Bridge が送信する Configuration BPDU のこのフィールドは、スパニングツリーを構成するデバイスを経由する度に、-1 します。フィールドの値が 0 である Configuration BPDU を受信した装置は、その BPDU を廃棄するため、MST Region のネットワークの最大範囲が制限できます。

II. 制限とガイドライン

この設定は Root Bridge のみ設定できます。MST region 内にある他のすべての装置は、Root Bridge 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。

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. MST Region の最大ホップ数を設定する	**stp max-hops** *hops*	デフォルト：20

8.15. ネットワークダイアメータの設定

I. ネットワークダイアメータ

ネットワークにおける任意の 2 台の装置を結ぶ最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、転送遅延、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、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 Bridge)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 Bridge でのみ有効です。

II. 設定手順

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

8.16. スパニングツリータイマの設定

I. スパニングツリータイマ

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。リンクに障害が発生すると、装置はスパニングツリーの再構築を行いますが、再構築されたスパニングツリーの BPDU がネットワーク全体に展開するまで時間を要します。そのため、Forward Delay、中間のポート状態(学習状態)を設定し、ルートポートと指定ポートが学習状態から転送状態に移行する時間を確保します。
- **Hello time**–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 Hello パケット(Configuration BPDU)を定期的に送信します。装置がタイムアウト期間内に configuration BPDU を受信しない場合、スパニングツリーは再計算されます。タイムアウト時間の計算式はタイムアウト時間=タイムアウトファクタ×3×hello 時間です。
- **Max age**–BPDU の有効期間を指定します。装置は、BPDU 内に記載されている最大エージング時間（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。

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 タイマ、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 time ＋ 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 Bridge 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。

II. 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、転送遅延は長く設定してください。転送遅延を極端に

短く設定すると一時的に冗長パスが発生してしまい、転送遅延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 タイマ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 タイマ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デバイスでの処理も大きくなります。また Hello タイマ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、デバイス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デバイス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。

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. forward delay timer 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 timer 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 timer 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

8.17. タイムアウトファクタの設定

I. タイムアウトファクタ

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とき、Root Bridge 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。もし

通常、Hello タイマの 9 倍の時間、上位の装置から Hello パケットを受信しないと、上位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。

II. 制限とガイドライン

以下の状態の場合、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。

- 安定したネットワークにおいても、上位のデバイス処理能力がビジーのときに、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。この場合、Hello パケットの監視時間の倍数を多くして、タイムアウトするまでの時間を長くすることができます。
- ネットワークの安定性を保つ必要がある場合

III. 設定手順

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

8.18. BPDU最大送出レートの設定

I. BPDU 最大送出レート

各 hello 時間内でポートが送信できる BPDU の最大数は、BPDU 送信レートと hello 時間値に等しくなります。

BPDU の送出レートが高いほど、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 送出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されたときに、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。

II. 制限とガイドライン

BPDU 伝送レートは、ポートの物理状態とネットワーク構造によって異なります。一般的なネットワークでは、デフォルト値で使用することを推奨します。

III. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. 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

8.19. Edgeポートの設定

I. Edge port ポート

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指します。Edge ポートと設定することによって、接続デバイスが 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 状態に移行させることができます。

II. 制限とガイドライン

- BPDU ガード機能が無効であるとき、Edge ポートが別のポートから BPDU を受信した場合、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 状態を早急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。

III. 設定手順

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 port を設定する	**stp edged-port**	デフォルト：非Edgeポート

8.20. Port Path Costの設定

8.20.1. Port Path Cost

Path Cost 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 Path Cost を持つことができます。Path Cost 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ので、VLAN ごとのロードバランスが可能です。

装置は自動的にデフォルト Path Cost を計算でき、一方でユーザはポートの Path Cost を設定できます。

8.20.2. デフォルト Path Cost の計算時の基準指定

I. デフォルト Path Cost の計算時の基準

Port Path Cost のデフォルト値には以下のモードがあります。以下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 Port Path Cost の対応値を使用します。
- **dot1t**–IEEE 802.1t で規定されている Port Path Cost の対応値を使用します。

- **legacy**–QX シリーズ独自の Port Path Cost の対応値を使用します。

表 8-7 リンク速度（100Mbps 以下）と Path Cost 間のマッピング

リンク速度	ポートタイプ	Path cost		
		IEEE 802.1d-1998	IEEE 802.1t	QX シリーズ独自
0	ー	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

図 8-16 リンク速度（1000Mbps）と Path Cost 間のマッピング

リンク速度	ポートタイプ	Path cost		
		IEEE 802.1d-1998	IEEE 802.1t	QX シリーズ独自
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

図 8-17 リンク速度（10Gbps）と Path Cost 間のマッピング

リンク速度	ポートタイプ	Path cost		
		IEEE 802.1d-1998	IEEE 802.1t	QX シリーズ独自
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

図 8-18 リンク速度（40Gbps）と Path Cost 間のマッピング

リンク速度	ポートタイプ	Path cost		
		IEEE 802.1d-1998	IEEE 802.1t	QX シリーズ独自
40 Gbps	単一ポート	1	500	1
	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

II. 制限とガイドライン

デバイスがデフォルト Path Cost 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 Path Cost を戻してください。

アグリゲーションリンクの Path Cost 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、Path Cost= 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 を超えたとき、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最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 Path は、最適な Path 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 Path Cost 計算の基準として、**dot1t** を使用します。
- ポートの Path Cost を手動で設定します。(セクション 3 *アクセス オペレーションマニュアル* の"*STP*"の"*Path Cost の設定*"を参照してください。)

III. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. Path Cost の計算基準を設定する	**stp pathcost-standard** { **dot1d-1998** | **dot1t** | **legacy** }	デフォルト：**legacy**

8.20.3. Path Cost の設定

I. 制限とガイドライン

ポートの Path Cost を変更したとき、ポートの役割を再計算し、状態遷移を初期化します。

II. 設定手順

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

操作	コマンド	補足
2. Ethernet あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	—
3. Path Cost 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Path Costを自動計算

8.21. Port priorityの設定

I. Port priority

Root Port を選出する際、ポートの Port Priority 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、Port Priority の高いポート（Port Priority 値が小さいポート）が Root Port に選出されます。

スパニングツリーでは異なる path ごとに異なる Port Priority 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 ベースでロードバランスが可能となります。正確なネットワーク要件にもとづいて Port Priority を設定することができます。

II. 制限とガイドライン

ポートの priority を変更したとき、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。ポートの priority を設定する前にネットワークトポロジの変更を行ってください。

III. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. Ethernet interface view あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	—
3. port 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

8.22. Point-to-Pointリンクの設定

I. Point-to-Point リンク

Point-to-Point リンクは、2 台のデバイス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 状態に移行させることができます。

II. 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二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。

III. 設定手順

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。

8.23. MSTPパケットのフォーマット設定

I. MSTP フレームのフォーマット

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。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

ポートの MSTP パケットフォーマットをポートごとに設定できます。設定後、MSTP モードで動作しているときは、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デバイスと通信します。

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ときポートは **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が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。

II. 制限とガイドライン

MSTI 数が 48 を超えたとき、ポートは IEEE 802.1s のみ送信することができます。

III. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. 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**

8.24. ポート遷移状態情報の出力の有効化

I. ポート遷移状態情報の出力

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。

II. 設定手順

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

8.25. スパニングツリー機能の有効化

8.25.1. 制限とガイドライン

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に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。

8.25.2. 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 : グローバルで無効
3. Ethernet interface view あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	—
4. 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

8.25.3. 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 : グローバルで無効
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

8.26. mCheck機能の設定

8.26.1. mCheck 機能

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。このとき、Device C は、Device B によって透過的に転送された STP BPDU を受信するとき、受信したポートは STP モードに変更します。もし 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。

8.26.2. 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。

8.26.3. グローバルでの mCheck の実行

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**

8.26.4. 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**

8.27. Digest Snoopingの設定

I. Digest Snooping

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。

- region 名
- リビジョンレベル

- VLAN-to-instance 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-to-instance 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計算される設定ダイジェストも異なるので、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には、同じ MST region で接続するポートで Digest snooping 機能を有効にします。

II. 制限とガイドライン

注意:

以下に示す状態において、グローバルで Digest Snooping を使用する場合、注意してください。

- VLAN-to-instance マッピングを変更するとき
- MST region の設定を復元するとき

VLAN-to-instance 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。

- 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-to-instance 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ときは、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。

III. 設定要件

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。

IV. 設定手順

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*	—

操作	コマンド	補足
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**	ー
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

8.28. No Agreement Checkの設定

I. No Agreement Check

RSTP と MSTP の Designated Port 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 Port 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の装置から、agreement パケットを受信したときにのみ、Designated Port 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 Port が上流の装置から 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 Port が上流の装置から 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 8-19 MSTP の designated port の高速状態遷移のメカニズム

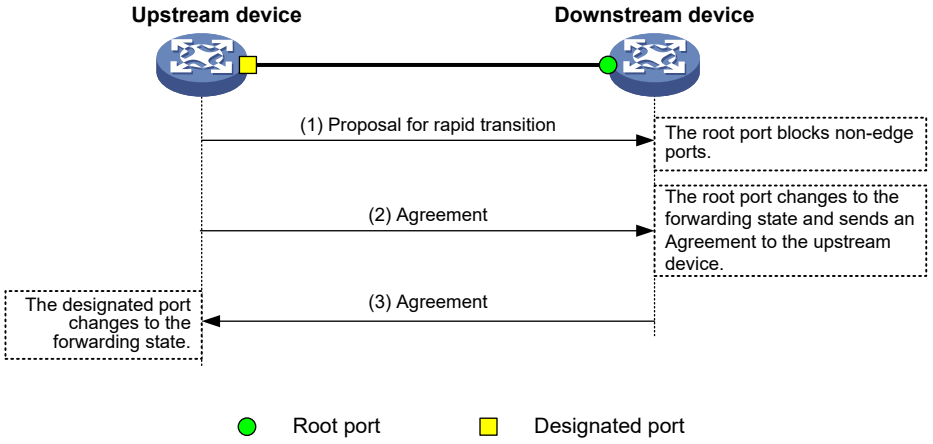
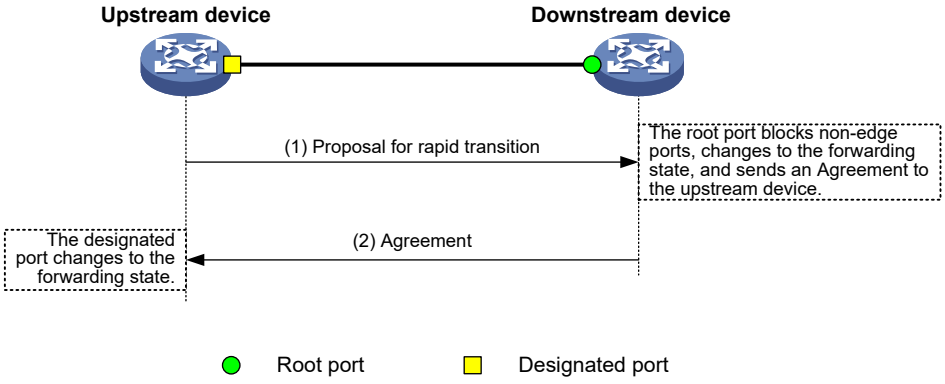


図 8-20 RSTP の designated port の高速状態遷移のメカニズム



上流装置がほかベンダの装置である場合、以下のように高速状態遷移の実行が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ている場合
- 下流装置が MSTP を使用し、RSTP モードをサポートしない場合

この場合、以下の事象が起こります。

1. 下流装置の Root Port 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 Port は転送遅延の 2 倍の時間が経過した後、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。

II. 制限とガイドライン

Root port で No Agreement Check 機能を有効にすることができます。

III. 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 台の装置で同じ region 名、リビジョンレベル、VLAN-to-instance マッピングを設定します。

IV. 設定手順

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

8.29. TC Snoopingの設定

I. TC Snooping

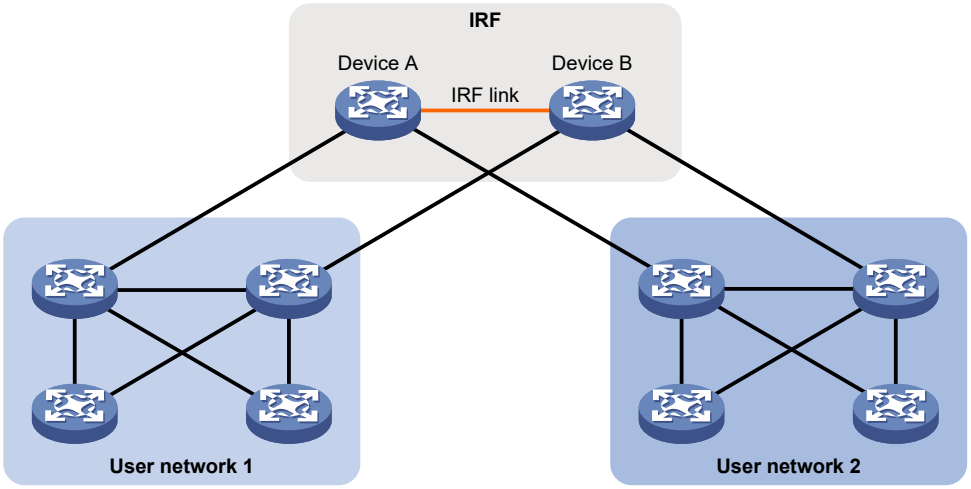
図 8-21 に示すように、IRF スタックユニットは 2 重のポートで 2 つのユーザネットワークに接続します。

以下の要件に従います。

- Device A と Device B は、IRF スタックを構成します。
- スパニングツリー機能は、Device A と Device B では無効にし、ユーザネットワーク 1 とユーザネットワーク 2 のすべての装置では有効にします。
- IRF スタックユニットはユーザネットワークにスパニングツリーの計算をせずに BPDU を送信します。

ネットワーク構成に変更が生じると、IRF スタックユニットは MAC アドレステーブルと ARP テーブルを更新するのに時間を要します。この間、ネットワークの通信断が発生します。

図 8-21 TC Snooping アプリケーションシナリオ



トラフィックの中断を防ぐため、IRF スタックユニットに TC snooping を設定することができます。ポートから TC-BPDU を受信したのち、IRF スタックユニットはポートの VLAN に関連する MAC アドレステーブルと ARP テーブルのエントリを更新します。こうして、TC snooping はネットワーク構成の変更からネットワーク内の通信断を避けることができます。ARP テーブルの詳細は、セクション 4 *IP サービス オペレーションマニュアル*の“*ARP*”を参照してください。

II. 制限とガイドライン

- 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。
- BPDU トンネリングの優先順位は TC snooping の優先順位より高いです。 ポートで BPDU トンネリングが有効になっている場合、TC snooping 機能はポートで有効になりません。
- TC snooping は PVST モードではサポートしておりません。

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. 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 を有効にする	**stp tc-snooping**	デフォルト：無効

8.30. 保護機能の設定

8.30.1. 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 • dispute ガードの無効化

8.30.2. BPDU ガードの設定

I. 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デバイスで、Edge ポートが configuration BPDU を受信すると、装置は次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、Chapter 1 *Fundamentals Command References* の"*Device management commands* "を参照してください。

II. 制限とガイドライン

BPDU ガード機能は、system view または Edge 単位で設定できます。Edge ポートは、Edge 単位の BPDU ガード設定を適用します。Edge 単位の BPDU ガード設定が使用できない場合、Edge ポートはグローバルの BPDU ガード設定を使用します。

他のデバイスまたは共有 LAN セグメントではなく、ユーザ端末に直接接続する Edge ポート上の BPDU ガードを設定します。

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、セクション 3 *アクセス オペレーションマニュアル*の"*Ethernet インタフェース*"を参照してください。

III. system view での BPDU ガードの設定

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

IV. interface view での BPDU ガードの設定

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 ガードを設定する	**stp port bpdu-protection** { **enable** | **disable** }	デフォルト: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。

8.30.3. Root ガードの有効化

I. Root ガード

Root ガードは、designated port で設定します。

スパニングツリーの Root Bridge と secondary root bridge 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 Bridge と secondary root bridge 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、不正なデバイス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。もし Root ガードが Root Bridge 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 port 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、以下の操作をします。

- すぐさま 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。

この操作は、MSTI のポートに接続されたリンクを切断することと同一です。もしポートが 2 倍の forwarding 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。

II. 制限とガイドライン

ポートで、Loop ガード機能、Root ガード機能の設定は同時に設定することはできません。

III. 設定手順

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

8.30.4. Loop ガードの有効化

I. Loop ガード

装置の Root ポートと、交代するポートで Loop ガードを設定します。

上流の装置から受信した BPDU に従って、Root ポートとほかの Blocking ポートの状態が決まります。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、ポートは上流の装置から BPDU の受信に失敗する可能性があります。この場合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。
- Blocking 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。これらを防止するための機能として、Loop ガード機能をサポートします。

Loop ガード機能が有効なポートの初期状態は、各 MSTI で Discard 状態です。ポートが BPDU を受信したとき、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。

II. 制限とガイドライン

ユーザの端末を接続したポートで Loop ガードを無効にすることはできません。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。

ポートで、Loop ガード機能、Root ガード機能、Edge ポート機能は同時に設定することはできません。

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. 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

8.30.5. ポート役割の制限機能の設定

I. ポート役割の制限

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。

ユーザアクセスネットワークの装置の bridge 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 を受信したとき、ルートポートではなく代理ポートになります。

II. 制限とガイドライン

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。

III. 設定手順

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

8.30.6. TC-BPDU ガードの有効化

I. TC-BPDU ガード

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。

II. 制限とガイドライン

NEC は TC-BPDU ガードを有効にすることを推奨します。

III. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. TC-BPDU ガードを有効にする	**stp tc-protection**	デフォルト：有効
3. (オプション設定項目) 10 秒間に転送アドレスエントリを削除する最大数を設定する	**stp tc-protection threshold** *number*	デフォルト：6

8.30.7. 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、ネットワークの他の装置に転送を行います。偽の攻撃者が捏造した BPDU をネットワークに攻撃する脆弱性を使用する可能性があります。捏造された BPDU を連続して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

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. BPDU ドロップ機能を設定する	**bpdu-drop any**	デフォルト：無効

8.30.8. PVST BPDU ガード機能の有効化

I. PVST BPDU ガード機能

この機能は装置が MSTP モードで動作しているときのみ有効です。

MSTP が有効な装置は 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 が有効な装置で 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 が有効な装置で 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。

II. 設定手順

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

8.30.9. dispute ガードの無効化

I. dispute ガード

片方向リンク障害により、Dispute ガードが開始します。上流ポートが、片方向リンク障害のために、下流の designated ポートから下位の BPDU を forwarding または learning 状態に受信すると、ループが表示されます。 Dispute ガードは、上流の designated ポートをブロックしてループを防止します。

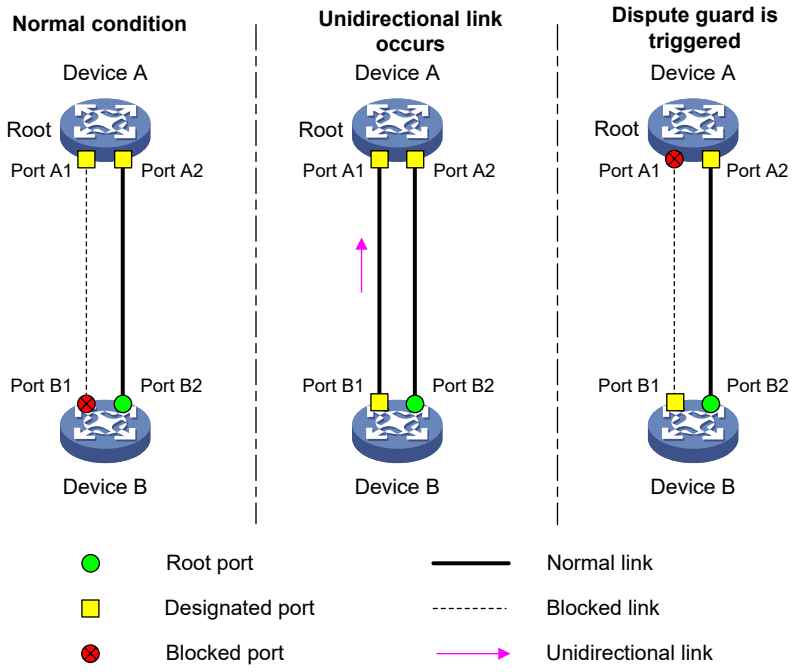
図 8-22 に示すように、通常の状態ではスパニングツリーの計算結果はです。

- デバイス A はルートブリッジで、ポート A1 は指定ポートです。
- ポート B1 がブロックされます。

ポート A1 とポート B1 の間のリンクがポート A1 からポート B1 の方向に障害が発生し、片方向になると、次のイベントが発生します。

1. ポート A1 は BPDU のみを受信でき、BPDU をポート B1 に送信できません。
2. ポート B1 は、一定期間ポート A1 から BPDU を受信しません。
3. デバイス B は、自身を root ブリッジとして決定します。
4. ポート B1 は BPDU をポート A1 に送信します。
5. ポート A1 は、受信した BPDU が自身の BPDU より下位であることを判断します。Dispute が検出されます。
6. Dispute ガードを開始し、ポート A1 を起動してブロックし、ループを防止します。

図 8-22 Dispute ガードの開始シナリオ

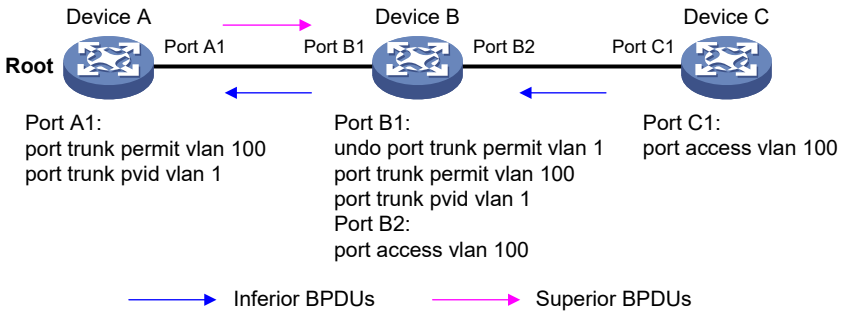


しかし、Dispute ガードはネットワーク接続を妨害する可能性があります。 VLAN ネットワークでの接続損失を回避するために、Dispute ガードを無効にできます。 図 8-23 に示すようにスパニングツリー機能はデバイス B 上で無効にされます。スパニングツリー機能はデバイス A およびデバイス C で有効になっているため、BPDU をトランスペアレントに送信します。

デバイス C のポート B1 は VLAN1 のパケットを拒否するように構成されているため、デバイス C はデバイス A から VLAN1 の優れた BPDU を受信できません。 デバイス C は、一定期間後に Root ブリッジとして自身を決定します。 次に、ポート C1 は、VLAN 100 の下位の BPDU をデバイス A に送信します。

デバイス A が下位の BPDU を受信すると、Dispute ガードはポート A1 をブロックし、トラフィックの中断を引き起こします。 サービス継続性を確保するために、デバイス A の Dispute ガードを無効にして、リンクがブロックされないようにすることができます。

図 8-23 Dispute ガードの無効化シナリオ



II. 制限とガイドライン

ネットワークに片方向リンク障害がない場合、Dispute ガードを無効にできます。

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. Dispute ガードを無効にする	**undo stp dispute-protection**	デフォルト：有効

8.31. TC BPDUの検出、受信イベントのログ作成の有効化

I. TC BPDU のイベントのログ

TC BPDU を検出したとき、あるいは受信したとき、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。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. TC BPDU を検出したとき、あるいは受信したとき、装置でログを作成する	**stp log enable tc**	デフォルト：無効

8.32. BPDUガードによってシャットダウンされたEdgeポートの再アクティブ化の無効化

I. BPDU ガードによってシャットダウンされた Edge ポートの再アクティブ化の無効化

BPDU ガードは、設定 BPDU を受信した Edge ポートをシャットダウンし、シャットダウンイベントの NMS に通知します。

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とき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できます。**shutdown-interval** のコマンドの詳細については、Chapter 1 *Fundamentals Command References* の"*Device management commands* "を参照してください。

II. 制限とガイドライン

この機能を使用すると、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 Edge ポートを再アクティブ化できなくなります。**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。 これらのポートを表示するには、**undo shutdown** コマンドを使用します。

III. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. 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無効にする	**stp port shutdown permanent**	デフォルト : 装置はポートステータス検出タイマが満了した後に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します。

8.33. 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

I. SNMP notification

この機能を有効にすると、スパニングツリーの新規ルートブリッジの選択あるいは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、セクション 10 *システム管理 オペレーションマニュアルの”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とき、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。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. スパニングツリーの新規ルートブリッジの選択あるいはトポロジ変更イベントによる SNMP notification の送信を有効にする	**snmp-agent trap enable stp** [**new-root** | **tc**]	デフォルト : • 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。

操作	コマンド	補足
		• 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。

メモ:

- **snmp-agent trap enable stp** コマンドはデフォルト状態では設定はありません(無効)。
- **snmp-agent** コマンドで SNMP 機能を有効にした場合、装置起動時に読み込むコンフィグにより **snmp-agent trap enable stp** コマンドが無効で設定される場合と有効で設定される場合があります(下記表を参照)。cfg や mdb についての詳細は”01-はじめに”の”11.1.2. カレントコンフィグレーション読み込みプロセス”を参照ください。
- STP の TRAP を使用する場合は、SNMP と STP を有効にした後で **snmp-agent trap enable stp** コマンドを設定して、**display snmp-agent trap-list** コマンドによって STP の TRAP(stp notification)が有効であることを確認してください。

読み込みコンフィグ	stp global enable 設定	
	有効	無効
default	-	有効
cfg(*1)	有効	無効
mdb	有効	有効(*2)

*1. バージョン変更時は cfg ファイルを読み込みます。
*2. stp global enable を一度も設定していない装置で保存した mdb ファイルでは無効です。デフォルトコンフィグ読み込み時に一度有効化されるため通常は有効となります。

8.34. 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
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**]
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*]

操作	コマンド
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*]
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 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**
有効なMST regionの設定情報を表示する	**display stp region-configuration**
MSTIのRoot Bridge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クリアする	**reset stp** [**interface** *interface-list*]

8.35. スパニングツリー設定例

8.35.1. MSTP の設定例

I. ネットワーク要件

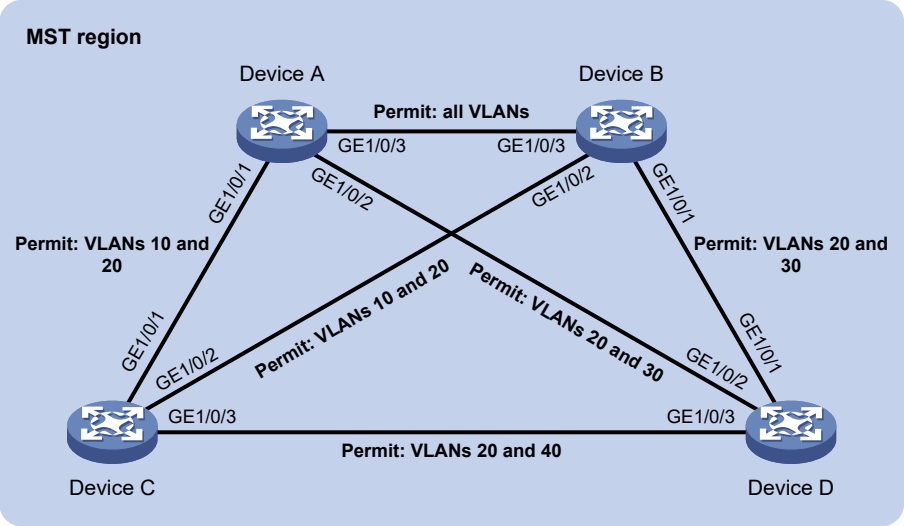
図 8-24 に示すようにすべての装置は同じ MST region にあります。Device A、Device B はディストリビューション層にあり、Device C、Device D はアクセス層にあります。

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。

- VLAN10 のパケットは MSTI1 で転送されます。
- VLAN30 のパケットは MSTI3 で転送されます。
- VLAN40 のパケットは MSTI4 で転送されます。
- VLAN20 のパケットは MSTI0 で転送されます。

VLAN10 と VLAN30 はディストリビューション層の装置のみ、VLAN40 はアクセス層の装置のみで通信します。MSIT1 と MSTI3 の Root Bridge は Device A、Device B となり、MSTI4 の Root Bridge は Device C となります

図 8-24 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 VLAN10、VLAN20、VLAN30 を作成します。
   - Device C で VLAN10、VLAN20、VLAN40 を作成します。
   - Device D で VLAN20、VLAN30、VLAN40 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、region 名 **example** を設定します。

   <DeviceA> system-view

   [DeviceA] stp region-configuration

   [DeviceA-mst-region] region-name example

   # VLAN10、VLAN30、VLAN40 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 Bridge として Device A を設定します。

   [DeviceA] stp instance 1 root primary

   # グローバルで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

VLAN10、VLAN30、VLAN40 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 Bridge として Device B を設定します。

[DeviceB] stp instance 3 root primary

グローバルで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

VLAN10、VLAN30、VLAN40 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 Bridge として Device C を設定します。

[DeviceC] stp instance 4 root primary

グローバルで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

VLAN10、VLAN30、VLAN40 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

グローバルで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

Device B が最も小さい Root Bridge ID を持っていると仮定します。結果として、Device B が MSTI 0 の Root Bridge 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、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

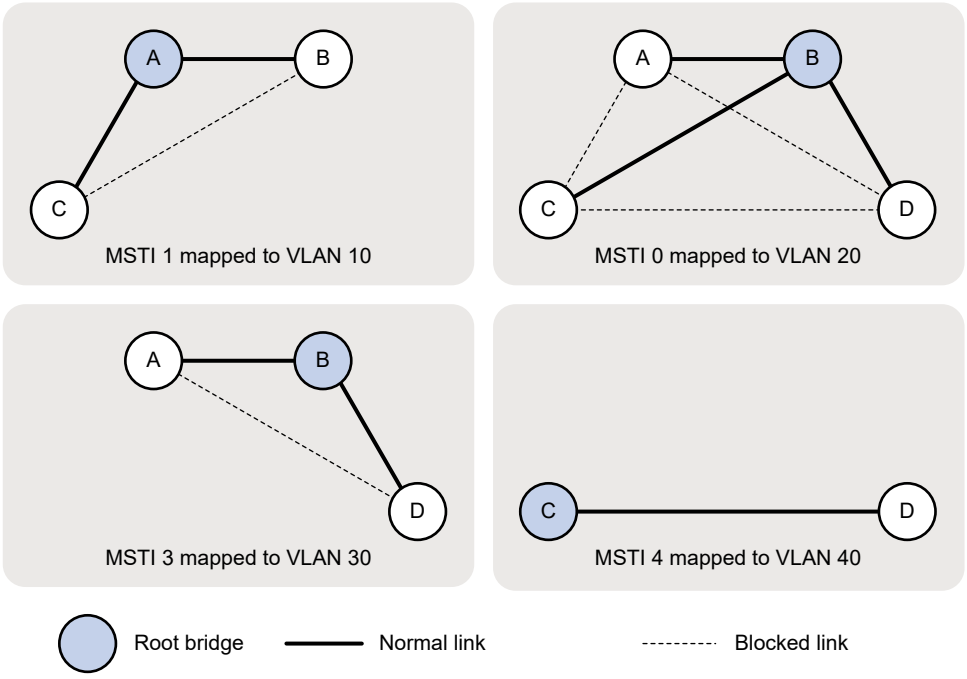
Device D のスパニングツリーの概要情報を表示します。

[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 8-25 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 8-25 異なる VLAN への MSTI のマッピングの設定



8.35.2. PVST の設定例

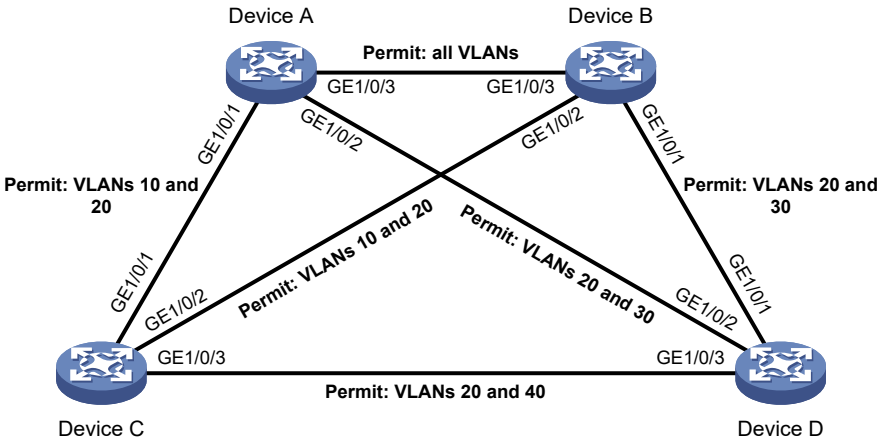
I. ネットワーク要件

図 8-26 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。
- VLAN10、VLAN20、VLAN30 はディストリビューション層のデバイスで終端され、VLAN40 はアクセス層で終端されます。
- VLAN10、VLAN20 の Root Bridge は Device A です。
- VLAN30 の Root Bridge は Device B です。
- VLAN40 の Root Bridge は Device C です。

図 8-26 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 VLAN10、VLAN20、VLAN30 を作成します。
   - Device C で VLAN10、VLAN20、VLAN40 を作成します。
   - Device D で VLAN20、VLAN30、VLAN40 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

   # VLAN10、VLAN20 の Root Bridge として Device を設定します。

   [DeviceA] stp vlan 10 20 root primary

   # グローバル、VLAN10、VLAN20、VLAN30 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

   # VLAN30 の Root Bridge として Device を設定します。

[DeviceB] stp vlan 30 root primary

グローバル、VLAN10、VLAN20、VLAN30 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

VLAN40 の Root Bridge として Device を設定します。

[DeviceC] stp vlan 40 root primary

グローバル、VLAN10、VLAN20、VLAN40 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、VLAN20、VLAN30、VLAN40 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、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
```

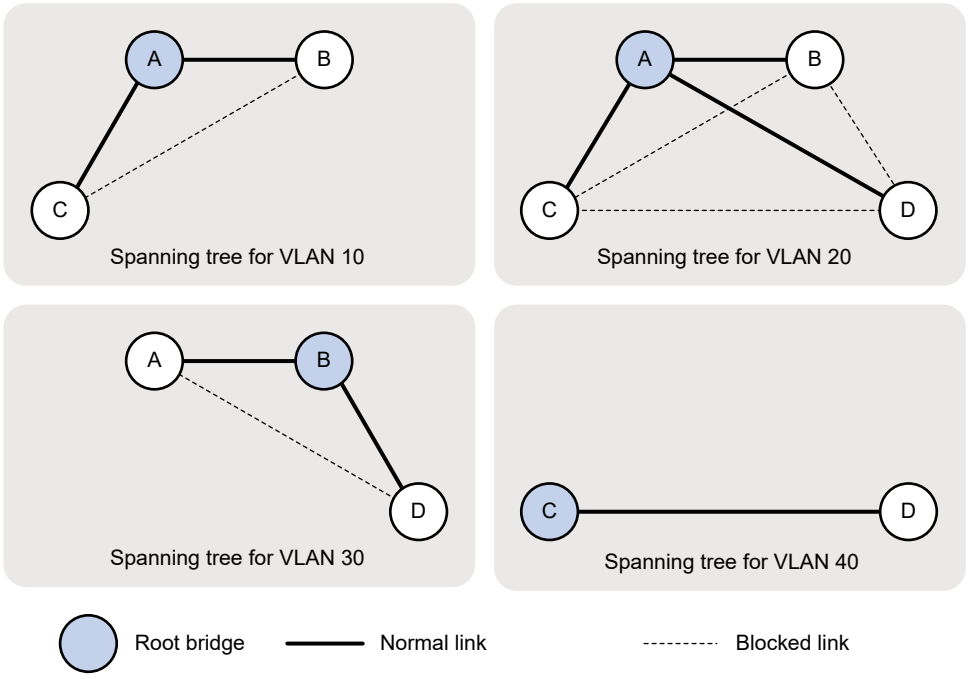
Device D のスパニングツリーの概要情報を表示します。

[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 8-27 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 8-27 VLAN スパニングツリートポロジ



目次

このセクションのページは **3-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. 制限とガイドライン 9-4
9.4.2. グローバルでのループ保護アクションの設定 9-4
9.4.3. ポート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. ループ検出の基本設定例 9-6

9章 ループ検出

9.1. 概要

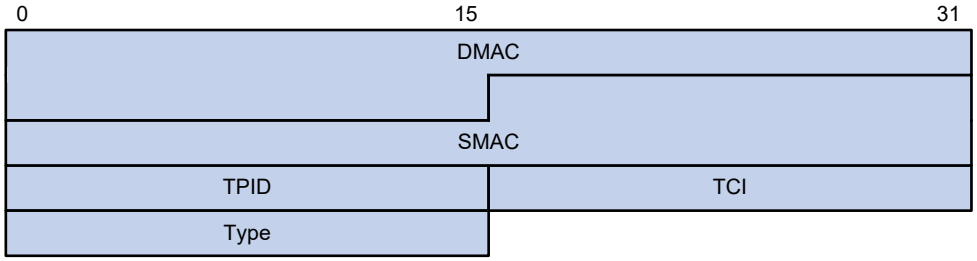
不正なネットワークの接続あるいは設定は、レイヤ 2 のループを発生させます。そこでは、ブロードキャスト、マルチキャスト、不明なユニキャストパケットが繰り返し転送され、ネットワークリソースの枯渇が発生し、ネットワークが麻痺することがあります。ループ検出機能は、ループが発生したとき、ネットワークの接続と設定に対応するように通知させるため、すぐさまログを作成します。ループ検出はネットワークの接続と設定をシャットダウンすることができます。ログは Information center で維持されます。詳細はセクション 10 *システム管理 オペレーションマニュアル*の"*Information Center*"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。

ループ検出は通常 VLAN 内で動作します。検出フレームに送信されたフレームと異なる VLAN タグが付いている場合、内部 VLAN ループが発生しています。ループを取り除くため、正しい設定の QinQ あるいは VLAN マッピングの設定を行います。QinQ の詳細はセクション 3 *アクセス オペレーションマニュアル*の”*QinQ*”、”*VLAN マッピング*”を参照してください。

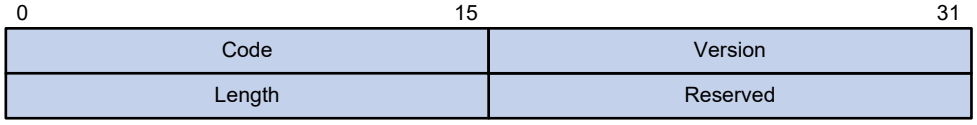
図 9-1 ループ検出のイーサネットフレームヘッダ



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。

- フレームを CPU に送信します。
- フレームが最初に受信された VLAN 内のフレームをフラッディングします。

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。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とき、CPU にフレームを送信し、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。
- **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

装置がポートでループを検出したとき、ログを作成しますが、デフォルトでポートに何らかの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 つのアクションを行う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。もし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。

シャットダウンアクションが設定された装置がポートでループを検出すると、以下のイベントが発生します。

1. 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。**shutdown-interval** コマンドの詳細はセクション 1 *はじめに オペレーションマニュアル*の”*装置管理*”を参照してください。
3. 検出タイマが満了した後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 • グローバルでのループ検出の有効化 • ポートでの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 • グローバルでのループ保護アクションの設定 • インタフェースでの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**	—
2. グローバルでループ検出を有効にする	**loopback-detection global enable vlan** { *vlan-list* | **all** }	デフォルト：有効

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**	—
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

9.4.1. 制限とガイドライン

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。グローバルの設定は、指定された VLAN のすべてのポートに適用されます。ポート毎の設定は、グローバルの設定よりも優先されます。

9.4.2. 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**	—
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：ループを検出したときアクションは実行しませんがログを出力します。

9.4.3. ポート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**	—
2. Ethernet interface view に移行する	**interface** *interface-type interface-number*	—
3. ポート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 : ループを検出したときアクションは実行しませんがログを出力します。 ポートタイプによってサポートするパラメータが異なります。詳細はChapter 3 *Layer 2 - LAN Switching Command References*の“*Loop detection commands*”を参照してください。

9.5. ループ検出間隔の設定

I. ループ検出間隔

ループ検出が有効であるとき、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ときには、システムの性能とループ検出速度を考慮してください。

II. 設定手順

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

📖 メモ:

undo loopback-detection interval-time コマンドを実行しても、デフォルト設定には戻りません。**undo** コマンドを実行した場合は、30 秒のループ検出間隔で動作する設定となります。デフォルト値に戻す場合は、**loopback-detection interval-time 5** コマンドを実行してください。

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

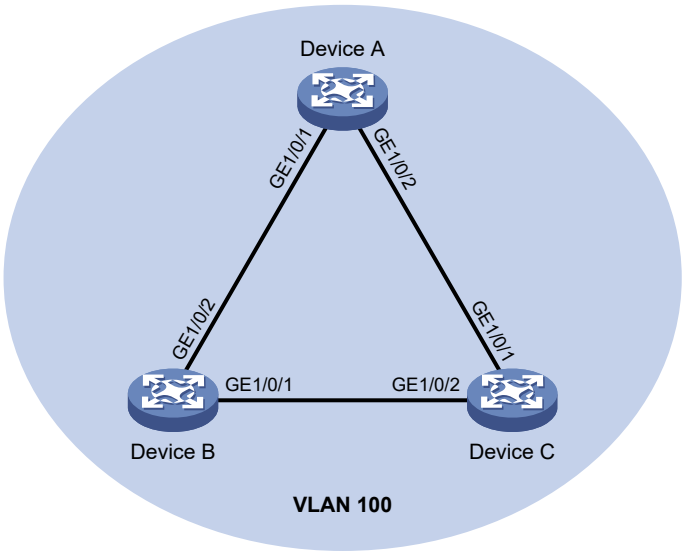
9.7.1. ループ検出の基本設定例

I. ネットワーク要件

図 9-3 に示すように、以下の動作を行うようにループ検出の設定を行います。

- Device A がログを作成します。
- ループを検出したとき、自動的にポートのシャットダウンを行います。

図 9-3 ネットワーク図



II. 設定手順

1. Device A を設定します。

   # Create 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、VLAN100 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、VLAN100 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、VLAN100 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

III. 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: Loopback exists on
GigabitEthernet1/0/1.
%Feb 24 15:04:29:667 2013 DeviceA LPDT/4/LPDT LOOPED: Loopback exists on
GigabitEthernet1/0/2.
%Feb 24 15:04:44:243 2013 DeviceA LPDT/5/LPDT RECOVERED: Loopback on GigabitEthernet1/0/1
recovered.
%Feb 24 15:04:44:248 2013 DeviceA LPDT/5/LPDT RECOVERED: Loopback on GigabitEthernet1/0/2
recovered.
```

上記の出力内容は、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 でループを検出しました。
- GigabitEthernet 1/0/1、GigabitEthernet 1/0/2 のループが取り除かれました。

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).
No loopback is detected.
```

上記の出力内容はシャットダウン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取り除か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)
...
```

上記の出力内容は、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)
...
```

上記の出力内容は、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 **3-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. VLAN タイプ 10-2
10.1.3. ポートベース VLAN 10-2
10.1.4. MAC ベース VLAN 10-3
10.1.5. IP サブネットベース VLAN 10-6
10.1.6. プロトコルベース VLAN 10-6
10.1.7. VLAN 間のレイヤ 3 通信 10-6
10.1.8. プロトコルと標準 10-6
10.2. VLAN の設定 10-7
10.2.1. 制限とガイドライン 10-7
10.2.2. VLAN の作成 10-7
10.3. ポートベース VLAN 10-8
10.3.1. 制限とガイドライン 10-8
10.3.2. アクセスポート VLAN の設定 10-8
10.3.3. トランクポート VLAN の設定 10-9
10.3.4. ハイブリッドポートの VLAN の設定 10-9
10.4. MAC ベース VLAN の設定 10-10
10.4.1. 制限とガイドライン 10-10
10.4.2. スタティック MAC ベース VLAN の割り当て 10-10
10.4.3. ダイナミック MAC ベース VLAN の割り当て 10-11
10.4.4. サーバ割り当て MAC ベース VLAN 10-13
10.5. IP サブネットベース VLAN の設定 10-13
10.6. プロトコルベース VLAN 10-14
10.7. VLAN インタフェースの設定 10-15
10.7.1. 制限とガイドライン 10-15
10.7.2. VLAN インタフェースの設定作業リスト 10-16
10.7.3. 設定要件 10-16
10.7.4. VLAN インタフェースの作成 10-16
10.8. VLAN の表示と維持 10-16
10.9. VLAN 設定例 10-17
10.9.1. ポートベース VLAN の設定例 10-17
10.9.2. MAC ベース VLAN 設定例 10-19
10.9.3. IP サブネットベース VLAN 設定例 10-21
10.9.4. プロトコルベース VLAN 設定例 10-23

10章 VLAN

10.1. 概要

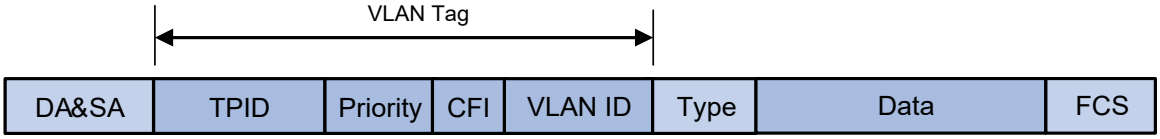
VLAN（Virtual Local Area Network）テクノロジは、物理 LAN を複数の論理 LAN に分割します。次の利点があります。

- **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ます。
- **ブロードキャストトラフィックの分離**－各 VLAN はブロードキャストパケットの送信を制限するブロードキャストドメインです。
- **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、同じ VLAN に割り当てることができます。

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 10-1 に示すように IEEE802.1Q では、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。

図 10-1 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。詳細はセクション 7 *ACL and QoS オペレーションマニュアル*の" *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とき、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。

  Ethernet のフィールドは常に 0 です。

- **VLAN ID**–フレームが属する 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とき、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。詳細はセクション 3 *アクセス オペレーションマニュアル* の"*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. VLAN タイプ

以下の VLAN タイプが利用可能です。

- ポートベース VLAN
- MAC ベース VLAN
- IP サブネットベース VLAN
- プロトコルベース VLAN

ポートで VLAN のすべてのタイプが設定されている場合、デフォルトではポートは以下の順番でパケットの処理を行います。

- MAC ベース VLAN
- IP サブネットベース VLAN
- プロトコルベース VLAN
- ポートベース VLAN

10.1.3. ポートベース VLAN

ポートベース VLAN はポートに VLAN を割り当てます。VLAN を割り当てられたポートはその 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。以下の条件の場合に使用します。
  - 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するときに使用します。
- **トランク**－トランクポートは複数の VLAN に属することができ、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

るとき、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 をも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**ー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。ハイブリッドポートは一般的に SVLAN タグを削除するため、one-to-two VLAN マッピングで使用されます。one-to-two VLAN マッピングの詳細は、セクション 3 *アクセス オペレーションマニュアル*の”*VLAN マッピング*”を参照してください。

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、ポート PVID からのパケットと見なします。

アクセスポートは 1 つの VLAN だけに接続できます。 アクセスポートが属する VLAN は、ポートの PVID です。 トランクまたはハイブリッドポートは、複数の VLAN と PVID 構成をサポートします。

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受信します。 • VLAN がポートで許可されていない場合廃棄します。	
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。

10.1.4. MAC ベース VLAN

MAC ベース VLAN は MAC アドレスをもとにして VLAN にホストを割り当てます。この機能は、ユーザの物理的な場所に関係なく、VLAN の設定が同一であるため、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、ポートはフレームを送信する前に、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. 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ならば、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。
  b. あいまい一致に失敗した場合、ALL-F のマスクで MAC-VLAN マッピングを検索して、完全一致モードによる検索を実行します。MAC-VLAN マッピングリストの MAC アドレスが、タグなしフレームの送信元 MAC アドレスと完全に一致している場合、対応する VLAN タグをパケットに追加します。
  c. VLAN ID に一致しない場合、システムは転送方法を決定するために以下の順番でパケットの VLAN を決定します。
     – IP サブネットベース VLAN
     – プロトコルベース VLAN
     – ポートベース VLAN
     一致すると、ポートは一致する VLAN ID を持つパケットをタグ付けします。
- タグづけフレームを受信したとき、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。
  - フレームの VLAN ID がポートで許可されている場合、ポートはフレームを転送します。
  - フレームの VLAN ID がポートで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。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。

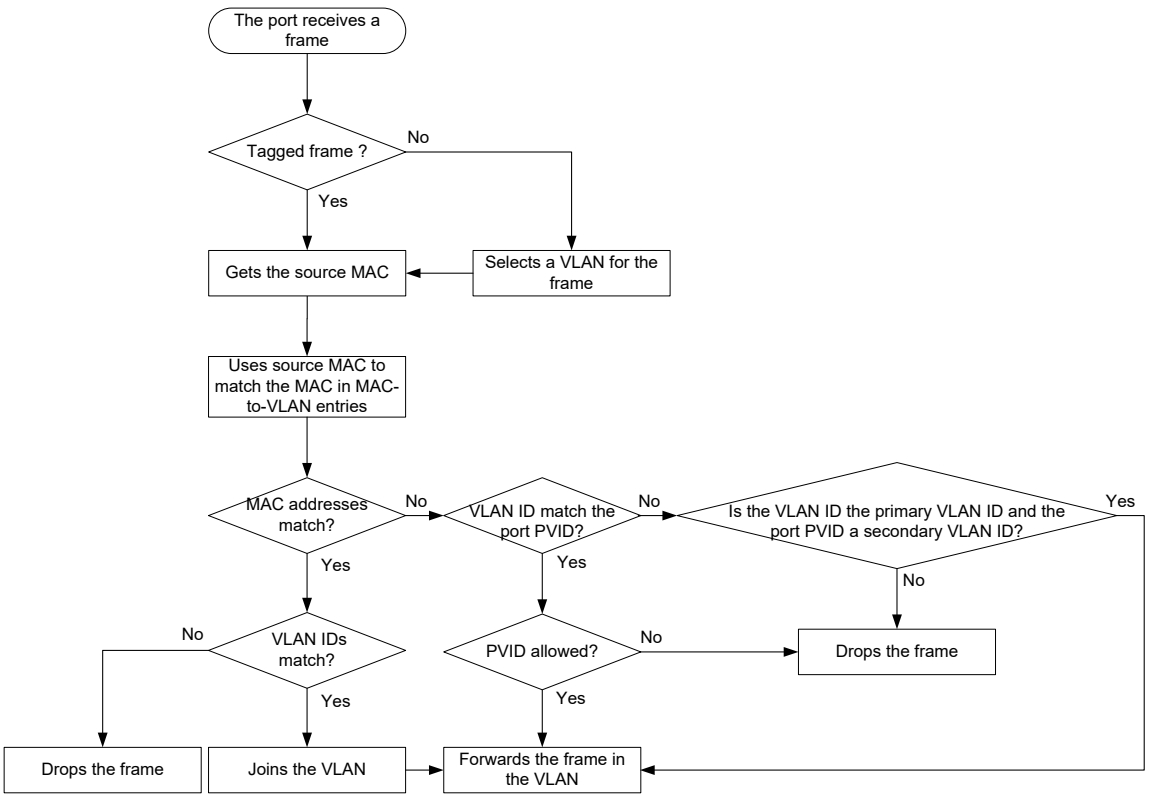
図 10-2 に示すように、ダイナミック MAC ベース VLAN の割り当てを以下のように処理します。

4. ポートでフレームを受信したとき、ポートはフレームがタグづけされているか確認します。
   - もしタグづけされている場合、ポートはフレームの送信元 MAC アドレスに通知します。
   - もしタグづ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
     – IP サブネットベース VLAN
     – プロトコルベース VLAN
     – ポートベース VLAN

選択した VLAN をフレームにタグづけしたのち、ポートはフレームの送信元 MAC アドレスに通知します。

5. ポートは MAC-VLAN エントリに一致させるため、フレームの送信元 MAC アドレスと VLAN を使用します。
   - もしフレームの送信元 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。
     - もし 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。
     - もし 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。
   - もしフレームの送信元 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。
     - もしフレームの 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。もし 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。もし VLAN が有効でない場合、ポートはフレームを廃棄します。

図 10-2 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



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。

装置でサーバ割り当て MAC ベース VLAN を設定するために、以下の処理を行います。

1. アクセス装置でサーバ割り当て 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-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とき、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。

3. 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。
4. 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とき、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 認証、MAC アドレス認証の詳細はセクション 8 *セキュリティ オペレーションマニュアル*の“*802.1X*”、“*MAC アドレス認証*”を参照してください。

10.1.5. IP サブネットベース VLAN

IP サブネットベース VLAN は、送信元 IP アドレスとサブネットマスクにもとづいてタグなしパケットを VLAN に割り当てます。

IP サブネットあるいは IP アドレスからタグなしパケットを VLAN に送信する場合、IP サブネットベース VLAN を使用します。

10.1.6. プロトコルベース VLAN

プロトコルベース VLAN はプロトコルタイプとカプセル化フォーマットにもとづいて、異なる VLAN に入力パケットを割り当てます。VLAN で有効なプロトコルは IP、IPX、AT があります。カプセル化フォーマットは Ethernet II、802.3 raw、802.2 LLC、802.2 SNAP があります。

この機能は、有効なネットワークサービスタイプを VLAN に関連づけます。ネットワーク管理と維持を容易にします。

10.1.7. VLAN 間のレイヤ 3 通信

レイヤ 3 で通信するため、異なる VLAN のホストは VLAN インタフェースを使用することができます。VLAN インタフェースは異なる VLAN 間でレイヤ 3 通信を行うために使用される仮想的な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。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 サブネットへのトラフィックを転送することが可能となります。

10.1.8. 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

- システムデフォルト VLAN として VLAN 1 を作成あるいは削除することができません。
- アプリケーションによってロックされているダイナミック VLAN またはVLAN を削除する前に、VLAN から設定を削除する必要があります。

10.2.2. VLAN の作成

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. VLAN を作成する	• VLAN を作成し、その view に移行する：**vlan** *vlan-id* • 複数の VLAN を作成し、その view に移行する： ○ VLAN を作成する：**vlan** { *vlan-id-list* | **all** } ○ VLAN view に移行する：**vlan** *vlan-id*	デフォルト： デフォルト VLAN(VLAN1)のみ
3. （オプション設定項目）VLAN の名前を設定する	**name** *text*	デフォルト：**VLAN** *vlan-id* 4桁の形式でVLAN IDを指定します。VLAN IDが4桁未満の場合、先頭に0が追加されます。たとえばVLAN 100のVLAN名は**VLAN 0100**です。
4. （オプション設定項目）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。 4桁の形式でVLAN IDを指定します。VLAN IDが4桁未満の場合、先頭に0が追加されます。たとえばVLAN 100の説明は**VLAN 0100**です。

10.3. ポートベースVLAN

10.3.1. 制限とガイドライン

- アクセスポートで **undo vlan** コマンドで PVID を削除する場合、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。
- ローカルポートとリモートポートで同じ PVID を設定することを推奨します。
- PVID からのパケットとタグなしパケットをポートで廃棄しないように、ポートを PVID に割り当ててください。

10.3.2. アクセスポート VLAN の設定

I. アクセスポートの VLAN 割り当て

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。

II. VLAN view でのアクセスポートの VLAN 割り当て

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. VLAN view 移行する	**vlan** *vlan-id*	ー
3. アクセスポートを VLAN に割り当てる	**port** *interface-list*	デフォルト：1

III. interface view でのアクセスポートの VLAN 割り当て

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	• 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*	ー
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. 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。

10.3.3. トランクポート VLAN の設定

I. トランクポートの VLAN 割り当て

トランクポートは複数の VLAN に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。

II. 制限とガイドライン

ポートリンクタイプをトランクからハイブリッド（またはハイブリッドからトランク）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、**port trunk permit vlan** コマンドでトランクポートを PVID に割り当ててください。

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 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
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

10.3.4. ハイブリッドポートの VLAN の設定

I. ハイブリッドポートの VLAN 割り当て

ハイブリッドポートは複数の VLAN に属すことができます。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。ハイブリッドポートを VLAN に割り当てる前に、対応する VLAN が作成されている必要があります。

II. 制限とガイドライン

ポートリンクタイプをトランクからハイブリッド（またはハイブリッドからトランク）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、**port hybrid vlan** コマンドでハイブリッドポートを PVID に割り当ててください。

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 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：ハイブリッドポートは、リンクタイプがアクセスであるときに、ポートが所属しているVLANのタグなしメンバです。
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：ハイブリッドポートのPVIDは、リンクタイプがアクセスであるときに、ポートが所属しているVLANのIDです。

10.4. MACベースVLANの設定

10.4.1. 制限とガイドライン

- MAC ベース VLAN は、ハイブリッドポートでのみ有効です。

10.4.2. スタティック MAC ベース VLAN の割り当て

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* [**dot1q** *priority*]	デフォルト：設定なし

操作	コマンド	補足
3. 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*	—
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ときに所属している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
7. (オプション設定項目) VLAN マッチングの優先順位を設定する	**vlan precedence mac-vlan**	デフォルト：**mac-vlan**

10.4.3. ダイナミック MAC ベース VLAN の割り当て

I. ダイナミック MAC ベース VLAN

ダイナミック MAC ベース VLAN 割り当てる場合、MAC-to-VLAN エントリを作成するときにスタティック VLAN を使用します。

MAC-VLAN エントリで指定された VLAN に加入するとき、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しません。

パケットが MAC-VLAN エントリにマッチするとき、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。

II. 制限とガイドライン

- 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。
- 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。
- MAC 学習を無効にする状態で、ダイナミック MAC ベース VLAN 割り当てを設定しないことを推奨します。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とき、ポートで受信されたパケットは CPU に転送されます。パケットの処理はもっとも高い優先度となります。MAC 学習を制限する設定は適用されません。

- MAC 学習を制限する状態で、ダイナミック MAC ベース VLAN 割り当てを設定しないことを推奨します。
- ポートで MAC アドレスエントリが最大数に到達し、ダイナミック MAC ベース VLAN 割り当てを設定した場合、ポートは次のようにパケットを処理します。
  - ポート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削除します。
- 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 MSTI で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 つを削除するとき、もう一方の動作に影響します。

III. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. MAC-VLAN エントリを作成する	**mac-vlan mac-address** *mac-address* **vlan** *vlan-id* [**dot1q** *priority*]	—
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
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 の割り当てを有効にする	**mac-vlan trigger enable**	デフォルト：無効 ポートに対するVLAN割り当ては、受信パケットの送信元MACアドレスがMAC-VLANエントリ内のMACアドレスと正確に一致する場合にのみ開始します。
7. (オプション設定項目) VLAN マッチングの優先順位を設定する	**vlan precedence mac-vlan**	デフォルト：**mac-vlan**
8. (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とき、PVIDに転送します。

10.4.4. 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 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ときに所属している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	セクション8 *セキュリティオペレーションマニュアル*の“*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. IPサブネットベースVLANの設定

I. 制限とガイドライン

この機能はハイブリッドポートでのみ有効で、タグなしパケットのみ処理します。

II. 設定手順

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

操作	コマンド	補足
3. VLAN に IP サブネットあるいは IP アドレスを割り当てる	**ip-subnet-vlan** [*ip-subnet-index*] **ip** *ip-address* [*mask*]	デフォルト：VLANはIPサブネットあるいはIPアドレスが割り当てられていません。 マルチキャストサブネットあるいはマルチキャストアドレスはVLANに関連づけることができません。
4. system view に戻る	**quit**	—
5. 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*	—
6. 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
7. IP サブネットベース VLAN にハイブリッドポートを割り当てる	**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ときに所属しているVLANのタグなしメンバです。
8. IP サブネットベース VLAN にハイブリッドポートを割り当てる	**port hybrid ip-subnet-vlan vlan** *vlan-id*	デフォルト：設定なし

10.6. プロトコルベースVLAN

I. プロトコルベース V LAN

プロトコルベース VLAN は 1 つ以上のプロトコルテンプレートがあります。プロトコルテンプレートは、入力パケットにマッチさせる一致条件として、プロトコルタイプとカプセル化フォーマットを定義します。各プロトコルテンプレートはプロトコルベース VLAN で一意のインデックスをもちます。プロトコルベース VLAN のすべてのプロトコルテンプレートは同一の VLAN ID をもちます。

ポートで、入力パケットをプロトコルベース VLAN に割り当てるため、以下の作業が必要です。

- プロトコルベース VLAN にポートを割り当てます。
- プロトコルベース VLAN のプロトコルテンプレートにポートを関連づけます。

ポートにタグなしパケットが到達したとき、ポートは以下の処理を行います。

- パケットのプロトコルタイプとカプセル化フォーマットがプロトコルテンプレートに一致した場合、ポートはプロトコルテンプレートに特定な VLAN タグをパケットにタグづけします。
- パケットのプロトコルタイプとカプセル化フォーマットがプロトコルテンプレートに一致しない場合、ポートはパケットに PVID をタグづけします。

II. 制限とガイドライン

自動モードの voice VLAN は、タグつき音声通信のみを処理します。プロトコルベース VLAN と voice VLAN の両方を VLAN に設定しないでください。

III. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. VLAN view に移行する	**vlan** *vlan-id*	VLANが存在しない場合、VLANを作成し、そのviewに移行します。
3. VLAN のプロトコルテンプレートを作成する	**protocol-vlan** [*protocol-index*] { **at** | **ipv4** | **ipv6** | **ipx** { **ethernetii** | **llc** | **raw** | **snap** } | **mode** { **ethernetii etype** *etype-id* | **llc** { **dsap** *dsap-id* [**ssap** *ssap-id*] | **ssap** *ssap-id* } | **snap etype** *etype-id* } }	デフォルト：設定なし
4. VLAN view から戻る	**quit**	―
5. 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*	―
6. 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
7. プロトコルベース VLAN にハイブリッドポートを割り当てる	**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ときに所属しているVLANのタグなしメンバです。
8. ハイブリッドポートとプロトコルベース VLAN を関連づける	**port hybrid protocol-vlan vlan** *vlan-id* { *protocol-index* [**to** *protocol-end*] | **all** }	デフォルト：設定なし

10.7. VLANインタフェースの設定

10.7.1. 制限とガイドライン

- 以下の特徴をもつセカンダリ VLAN の VLAN インタフェースを作成することはできません。
  - 同じプライマリ VLAN に関連づけられています。
  - プライマリ VLAN インタフェースの VLAN interface view でレイヤ 3 通信が有効です。

セカンダリ VLAN の詳細はセクション 3 *アクセス オペレーションマニュアル*の“*Private VLAN*”を参照してください。

10.7.2. VLAN インタフェースの設定作業リスト

作業リスト
VLANインタフェースの作成

10.7.3. 設定要件

VLAN の VLAN インタフェースを作成する前に、最初に VLAN を作成してください。

10.7.4. VLAN インタフェースの作成

操作	コマンド	補足
1. system view に移行する	**system-view**	—
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*	—
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. （オプション設定項目）VLAN インタフェースの説明を設定する	**description** *text*	デフォルト：VLANインタフェース名です。 たとえば**Vlan-interface1 Interface**です。
5. 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1つ以上のポートをアップした場合、VLANインタフェースはアップになります。VLANのすべてのポートをダウンした場合、ダウンします。

10.8. 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	**display interface vlan-interface** [*interface-number*]

操作	コマンド
る	[**brief** [**description** | **down**]]
指定したポートに関連したIPサブネットベースVLANを表示する	**display ip-subnet-vlan interface** { *interface-type interface-number1* [**to** *interface-type interface-number2*] | **all** }
IPサブネットベースVLANの情報を表示する	**display ip-subnet-vlan vlan** { *vlan-id1* [**to** *vlan-id2*] | **all** }
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** }
指定したポートに関連したプロトコルベースVLANを表示する	**display protocol-vlan interface** { *interface-type interface-number1* [**to** *interface-type interface-number2*] | **all** }
プロトコルベースVLANの情報を表示する	**display protocol-vlan vlan** { *vlan-id1* [**to** *vlan-id2*] | **all** }
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**
ポートの統計情報を削除する	**reset counters interface vlan-interface** [*interface-number*]

10.9. VLAN設定例

10.9.1. ポートベース VLAN の設定例

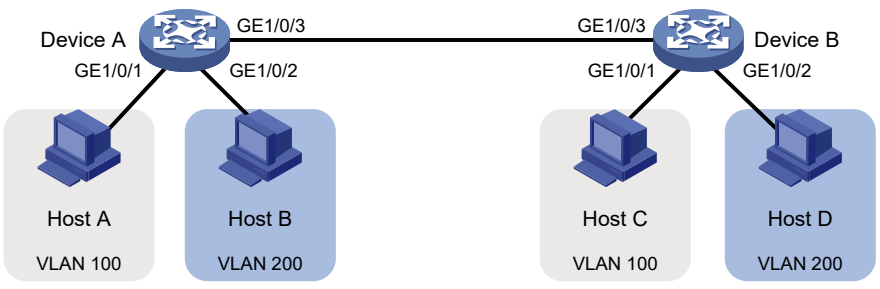
I. ネットワーク要件

図 10-3 に示すように設定します。

- Host A と Host C は Department A に属します。VLAN 100 は Department A に割り当てられます。
- Host B と Host D は Department B に属します。VLAN 200 は Department B に割り当てられます。

同じ部門内のホストのみが通信できるように、ポートベース VLAN を構成します。

図 10-3 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。（詳細は省略します）
3. host を設定します。
   a. 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。
   b. 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
```

10.9.2. MAC ベース VLAN 設定例

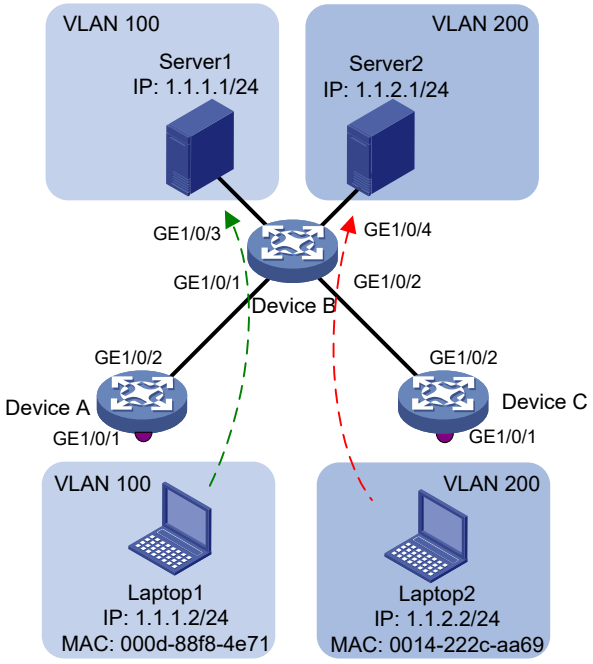
I. ネットワーク要件

図 10-4 に示すように設定します。

- Device A と Device C の GigabitEthernet 1/0/1 はミーティングルームに接続されています。Laptop 1、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ます。
- Laptop 1、Laptop 2 は異なる部門でしようされます。2 つの部門は VLAN 100、VLAN 200 を使用します。

それぞれの Laptop がミーティングルームで使用されても所属する各部門のみアクセスできるように、MAC ベース VLAN を設定します。

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、VLAN 200 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

VLAN 100 と VLAN 200 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。

VLAN100 を作成し、GigabitEthernet 1/0/13 を VLAN 100 に割り当てます。

<DeviceB> system-view

[DeviceB] vlan 100

[DeviceB-vlan100] port gigabitethernet 1/0/3

[DeviceB-vlan100] quit

VLAN200 を作成し、GigabitEthernet 1/0/4 を VLAN 200 に割り当てます。

[DeviceB] vlan 200

[DeviceB-vlan200] port gigabitethernet 1/0/4

[DeviceB-vlan200] quit

アップリンクポート GigabitEthernet 1/0/1 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

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。

[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
```

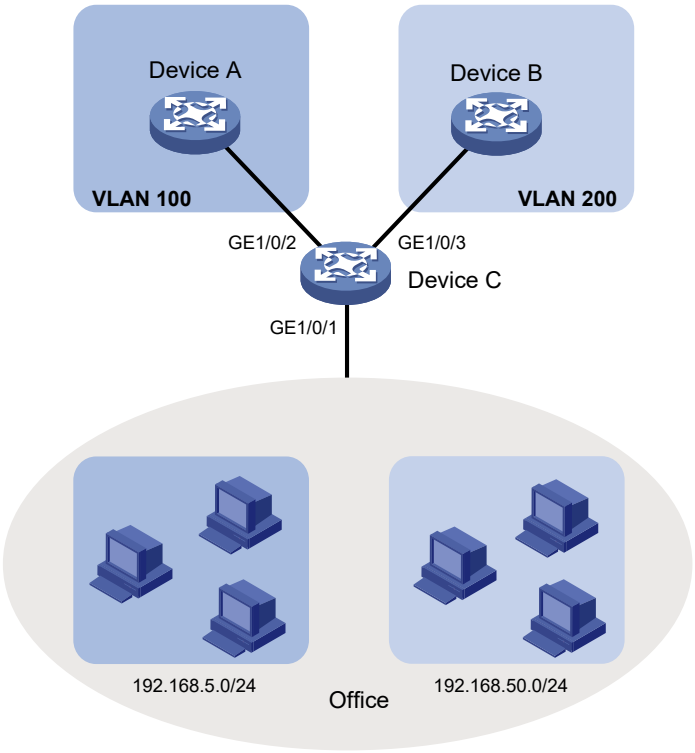
10.9.3. IP サブネットベース VLAN 設定例

I. ネットワーク要件

図 10-5 に示すように、Office の Host は異なる IP サブネットに所属します。

それぞれ VLAN 100、VLAN 200 の 192.168.5.0/24、192.168.50.0/24 からパケットを転送するため、Device C を設定します。

図 10-5 ネットワーク図



II. 設定手順

1. Device C を設定します。

IP サブネット 192.168.5.0/24 を VLAN 100 に関連づけます。

<DeviceC> system-view

[DeviceC] vlan 100

[DeviceC-vlan100] ip-subnet-vlan ip 192.168.5.0 255.255.255.0

[DeviceC-vlan100] quit

IP サブネット 192.168.50.0/24 を VLAN 200 に関連づけます。

[DeviceC] vlan 200

[DeviceC-vlan200] ip-subnet-vlan ip 192.168.50.0 255.255.255.0

[DeviceC-vlan200] quit

ハイブリッドポートとして、GigabitEthernet 1/0/2 を設定し、タグづけ VLAN メンバとして VLAN 100 に割り当てます。

[DeviceC] interface gigabitethernet 1/0/2

[DeviceC-GigabitEthernet1/0/2] port link-type hybrid

[DeviceC-GigabitEthernet1/0/2] port hybrid vlan 100 tagged

[DeviceC-GigabitEthernet1/0/2] quit

ハイブリッドポートとして、GigabitEthernet 1/0/3 を設定し、タグづけ VLAN メンバとして VLAN 200 に割り当てます。

[DeviceC] interface gigabitethernet 1/0/3

[DeviceC-GigabitEthernet1/0/3] port link-type hybrid

[DeviceC-GigabitEthernet1/0/3] port hybrid vlan 200 tagged

[DeviceC-GigabitEthernet1/0/3] quit

ハイブリッドポートとして、GigabitEthernet 1/0/1 を設定し、タグなし VLAN メンバとして VLAN 100、VLAN 200 に割り当てます。

[DeviceC] interface gigabitethernet 1/0/1

[DeviceC-GigabitEthernet1/0/1] port link-type hybrid

[DeviceC-GigabitEthernet1/0/1] port hybrid vlan 100 200 untagged

GigabitEthernet 1/0/1 を IP サブネットベース VLAN100、VLAN200 に関連づけます。

[DeviceC-GigabitEthernet1/0/1] port hybrid ip-subnet-vlan vlan 100

[DeviceC-GigabitEthernet1/0/1] port hybrid ip-subnet-vlan vlan 200

[DeviceC-GigabitEthernet1/0/1] quit

2. それぞれ VLAN100、VLAN200 からパケットを転送するため、Device A と Device B を設定します。（詳細は省略します）

III. 設定の確認

Device C ですべての IP サブネットベース VLAN の情報を表示します。

[DeviceC] display ip-subnet-vlan vlan all

```
VLAN ID: 100
 Subnet index       IP address      Subnet mask
 0                  192.168.5.0     255.255.255.0

VLAN ID: 200
 Subnet index       IP address      Subnet mask
 0                  192.168.50.0    255.255.255.0
```

GigabitEthernet 1/0/1 の IP サブネットベース VLAN の情報を表示します。

[DeviceC] display ip-subnet-vlan interface gigabitethernet 1/0/1

```
Interface: GigabitEthernet1/0/1
 VLAN ID   Subnet index    IP address       Subnet mask       Status
 100       0               192.168.5.0      255.255.255.0     Active
 200       0               192.168.50.0     255.255.255.0     Active
```

10.9.4. プロトコルベース VLAN 設定例

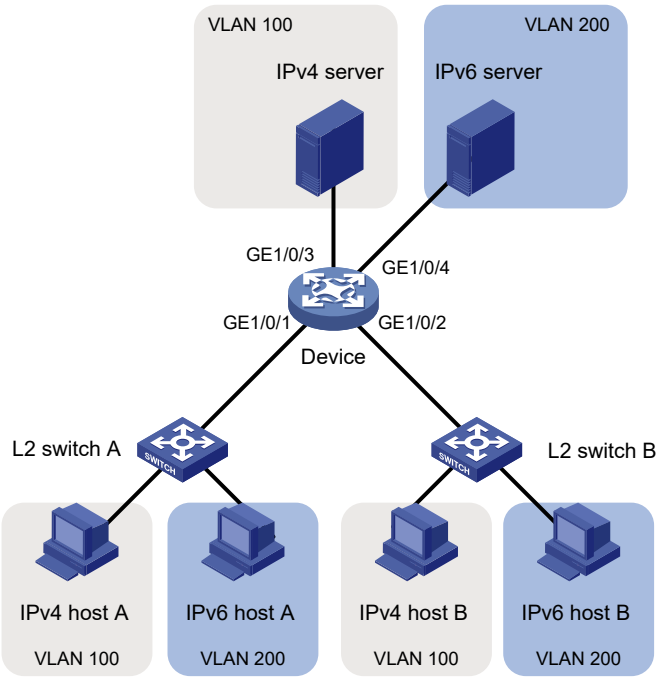
I. ネットワーク要件

図 10-6 に示すように設定します。

- 実験室の大多数の Host は IPv4 プロトコルで動作します。
- 他の Host は教育目的で IPv6 プロトコルが動作します。

レイヤ 2 で IPv4 トラフィックと IPv6 トラフィックを隔離するため、IPv4 と ARP プロトコルを VLAN 100 に関連づけ、IPv6 プロトコルを VLAN 200 に関連づけるように、プロトコルベース VLAN を設定します。

図 10-6 ネットワーク図



II. 設定手順

この例では L2 Switch と L2 Switch は工場出荷状態で使用します。

1. Device を設定します。

VLAN 100 を作成し、VLAN 100 の説明を IPv4 のプロトコル VLAN として設定します。

<Device> system-view

[Device] vlan 100

[Device-vlan100] description protocol VLAN for IPv4

GigabitEthernet 1/0/3 に VLAN 100 を割り当てます。

[Device-vlan100] port gigabitethernet 1/0/3

[Device-vlan100] quit

VLAN 200 を作成し、VLAN 200 の説明を IPv6 のプロトコル VLAN として設定します。

[Device] vlan 200

[Device-vlan200] description protocol VLAN for IPv6

GigabitEthernet 1/0/4 に VLAN 200 を割り当てます。

[Device-vlan200] port gigabitethernet 1/0/4

プロトコルベース VLAN として VLAN 200 を設定し、VLAN 200 用のインデックスが 1 の IPv6 プロトコルテンプレートを作成します。

[Device-vlan200] protocol-vlan 1 ipv6

[Device-vlan200] quit

プロトコルベース VLAN として VLAN 100 を設定し、VLAN 100 用のインデックスが 1 の IPv4 プロトコルテンプレートを作成します。インデックスが 2 の ARP プロトコルテンプレートを

作成します。（カプセル化タイプは Ethernet II で ARP のプロトコルタイプは 16 進数で 0806 です）

[Device] vlan 100

[Device-vlan100] protocol-vlan 1 ipv4

[Device-vlan100] protocol-vlan 2 mode ethernetii etype 0806

[Device-vlan100] quit

ハイブリッドポートとして GigabitEthernet 1/0/1 を設定し、タグなし VLAN メンバとして VLAN100、VLAN200 に割り当てます。

[Device] interface gigabitethernet 1/0/1

[Device-GigabitEthernet1/0/1] port link-type hybrid

[Device-GigabitEthernet1/0/1] port hybrid vlan 100 200 untagged

GigabitEthernet 1/0/1 に VLAN100 の IPv4、ARP プロトコルテンプレートを関連づけ、VLAN200 の IPv6 プロトコルテンプレートを関連づけます。

[Device-GigabitEthernet1/0/1] port hybrid protocol-vlan vlan 100 1 to 2

[Device-GigabitEthernet1/0/1] port hybrid protocol-vlan vlan 200 1

[Device-GigabitEthernet1/0/1] quit

ハイブリッドポートとして GigabitEthernet 1/0/2 を設定し、タグなし VLAN メンバとして VLAN100、VLAN200 に割り当てます。

[Device] interface gigabitethernet 1/0/2

[Device-GigabitEthernet1/0/2] port link-type hybrid

[Device-GigabitEthernet1/0/2] port hybrid vlan 100 200 untagged

GigabitEthernet 1/0/2 に VLAN100 の IPv4 プロトコルテンプレート、VLAN100 の ARP プロトコルテンプレート、VLAN200 の IPv6 プロトコルテンプレートを関連づけます。

[Device-GigabitEthernet1/0/2] port hybrid protocol-vlan vlan 100 1 to 2

[Device-GigabitEthernet1/0/2] port hybrid protocol-vlan vlan 200 1

[Device-GigabitEthernet1/0/2] quit

2. Host と Server を設定します。
   a. IPv4 Host A、IPv4 Host B、IPv4 server を同一ネットワークセグメント上に設定します。（たとえば、192.168.100.0/24 です）（詳細は省略します）
   b. IPv6 Host A、IPv6 Host B、IPv6 server を同一ネットワークセグメント上に設定します。（たとえば、2001::1/64 です）（詳細は省略します）

III. 設定の確認

1. 以下を確認します。
   - VLAN 100 の Host と Server が互いに ping できることを確認します。(詳細は省略します)
   - VLAN 200 の Host と Server が互いに ping できることを確認します。(詳細は省略します)
   - VLAN 100 の Host あるいは Server が、VLAN 200 の Host あるいは Server に ping できないことを確認します。(詳細は省略します)
2. プロトコルベース VLAN の設定を確認します。

   # Device のプロトコルベース VLAN を表示します。

[Device] display protocol-vlan vlan all

```
VLAN ID: 100
 Protocol index  Protocol type
 1               IPv4
 2               Ethernet II Etype 0x0806

VLAN ID: 200
 Protocol index  Protocol type
 1               IPv6
```

Device のポートでプロトコルベース VLAN を表示します。

[Device] display protocol-vlan interface all

```
Interface: GigabitEthernet1/0/1
 VLAN ID  Protocol index  Protocol type             Status
 100      1              IPv4                      Active
 100      2              Ethernet II Etype 0x0806  Active
 200      1              IPv6                      Active

Interface: GigabitEthernet 1/0/2
 VLAN ID  Protocol index  Protocol type             Status
 100      1              IPv4                      Active
 100      2              Ethernet II Etype 0x0806  Active
 200      1              IPv6                      Active
```

目次

このセクションのページは **3-x-x** です。

11 章 Private VLAN 11-1
11.1. 概要 11-1
11.2. 制限とガイドライン 11-2
11.3. Private VLAN 設定作業リスト 11-2
11.4. プライマリ VLAN の作成 11-2
11.5. セカンダリ VLAN の作成 11-3
11.6. プライマリ VLAN とセカンダリ VLAN の関連付け 11-3
11.7. アップリンクポートの設定 11-3
11.8. ダウンリンクポートの設定 11-4
11.9. セカンダリ VLAN 間のレイヤ 3 通信の設定 11-5
11.10. Private VLAN の表示と維持 11-6
11.11. Private VLAN 設定例 11-6
11.11.1. プロミスカスポートの設定例 11-6
11.11.2. トランクプロミスカスポートの設定例 11-10
11.11.3. トランクプロミスカスとトランクセカンダリの設定例 11-13
11.11.4. セカンダリ VLAN でのレイヤ 3 通信の 設定例 11-17

11章 Private VLAN

11.1. 概要

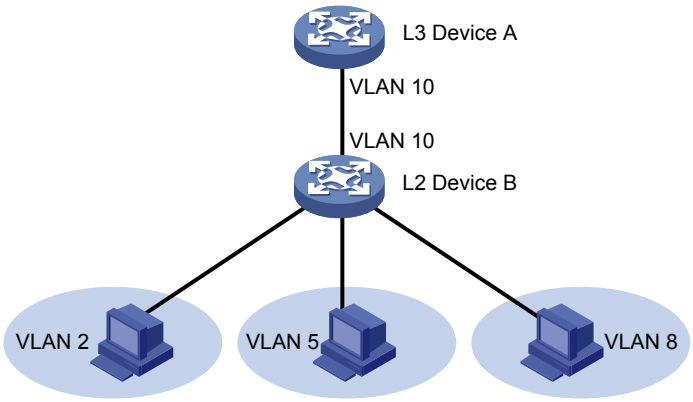
VLAN 機能はカスタマからトラフィックを隔離するための方法を提供します。ネットワークのアクセスレイヤでは、セキュリティ確保等の目的でカスタマトラフィックを隔離する必要があります。VLAN がユーザ単位に割り当てられている場合、設定に必要な VLAN の数が多くなります。

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 を関連付けできます。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 で隔離されます。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（図 11-1 では L3 Device A）ではローカルプロキシ ARP を有効にしてください。

図 11-1 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、VLAN 5、VLAN 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 11-1 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 装置上でレイヤ 3 通信を有効にするため以下の方法のうち 1 つ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 間やセカンダリ VLAN と他のネットワークの間で必要となる場合があります。

- 方法 1:
  a. セカンダリ VLAN に VLAN インタフェースを作成します。
  b. 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。
- 方法 2:
  a. 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。

b. 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。（方法 2 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。）

c. 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。

11.2. 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。

11.3. 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

11.4. 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。

11.5. 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** }	—

11.6. 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

11.7. アップリンクポートの設定

I. アップリンクポート

アップリンクポートを以下に従い設定します。図 11-1 の例では L2 Device B と L3 Device A を接続しているポートがアップリンクポートです。

- 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ます。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。

II. 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*	—

操作	コマンド	補足
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

11.8. ダウンリンクポートの設定

I. ダウンリンクポート

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（図 11-1 の例では L2 Device B と Host を接続しているポートがダウンリンクポートです。）、そのポートはホストポートとして設定してください。そのホストポートはセカンダリ 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。そのトランクセカンダリポートはセカンダリ VLAN と関連付けたプライマリ VLAN が自動的に設定されます。

II. 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*	—

操作	コマンド	補足
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。	—
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	• ホストポートに設定する：**port private-vlan host** • 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**	—
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. （オプション設定項目）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

11.9. 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

操作	コマンド	補足
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 ローカルプロキシARPの詳細はセクション4 *IPサービス オペレーションマニュアル* の“*Proxy ARP*”を参照してください。

11.10. 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*]

11.11. Private VLAN設定例

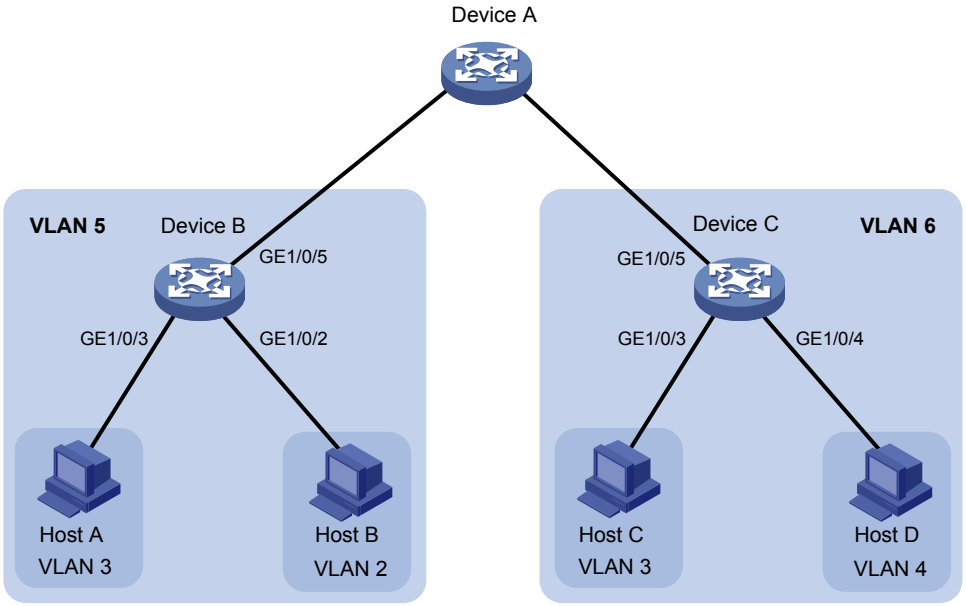
11.11.1. プロミスカスポートの設定例

I. ネットワーク要件

図 11-2 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 11-2 ネットワーク図



II. 設定手順

この設定例は Device B と Device C について記載します。

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

VLAN 2 と VLAN 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

アップリンクポート 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

ダウンリンクポート 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

ダウンリンクポート 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。

VLAN 6 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

VLAN 3 と VLAN 4 を作成します。

[DeviceC] vlan 3 to 4

セカンダリ VLAN 3、VLAN 4 をプライマリ VLAN 6 に関連づけます。

[DeviceC] vlan 6

[DeviceC-vlan6] private-vlan secondary 3 to 4

[DeviceC-vlan6] quit

アップリンクポート GigabitEthernet 1/0/5 を VLAN 6 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

ダウンリンクポート GigabitEthernet 1/0/3 を VLAN3 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

ダウンリンクポート 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 VLAN 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 とセカンダリ VLAN3 の untagged メンバです。

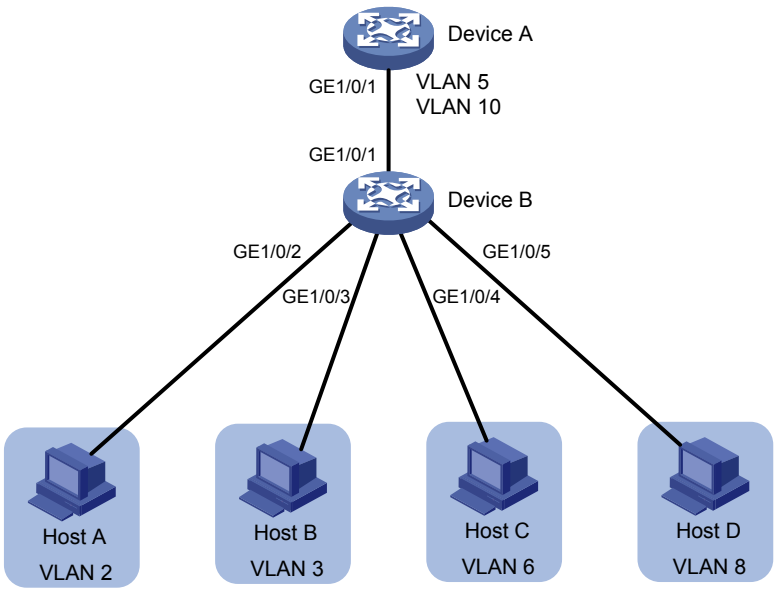
11.11.2. トランクプロミスカスポートの設定例

I. ネットワーク要件

図 11-3 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 VLAN 10 のみ認識します。

図 11-3 ネットワーク図



II. 設定手順

1. Device B を設定します。

   # VLAN5 と VLAN 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、VLAN 3、VLAN 6、VLAN 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 VLAN 2 と VLAN 3 をプライマリ VLAN 5 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 VLAN 6 と VLAN 8 をプライマリ VLAN 10 に関連付けます。

[DeviceB] vlan 10

[DeviceB-vlan10] private-vlan secondary 6 8

[DeviceB-vlan10] quit

アップリンクポート GigabitEthernet 1/0/1 を VLAN5、VLAN 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

ダウンリンクポート 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

ダウンリンクポート GigabitEthernet 1/0/3 を VLAN3 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

ダウンリンクポート GigabitEthernet 1/0/4 を VLAN6 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

ダウンリンクポート GigabitEthernet 1/0/5 を VLAN8 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、VLAN 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 VLAN 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 VLAN 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。

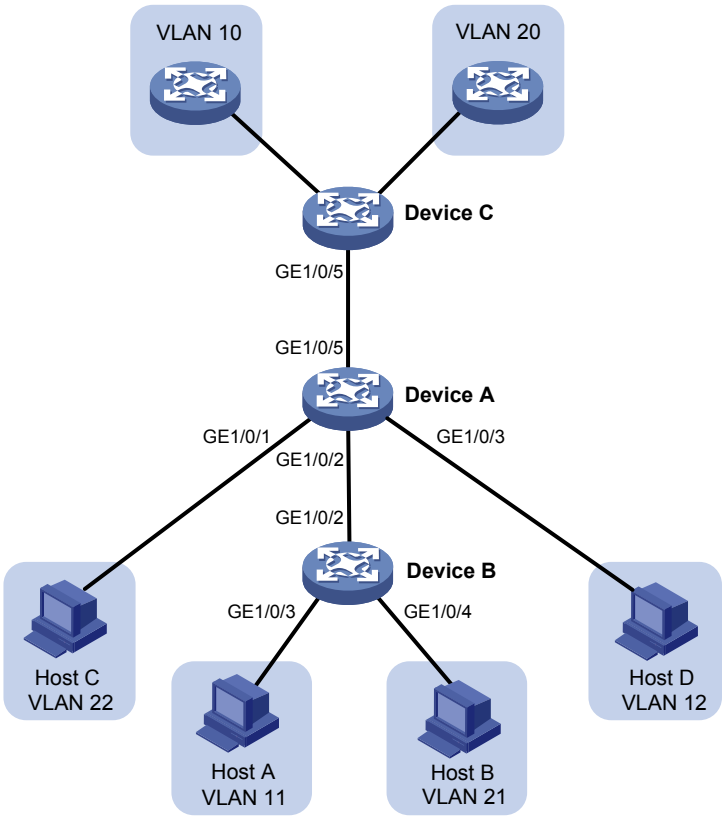
11.11.3. トランクプロミスカスとトランクセカンダリの設定例

I. ネットワーク要件

図 11-4 に示すように設定します。

- VLAN10 と VLAN 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、VLAN20 からの VLAN タグ付きパケットの転送を許可します。
- VLAN11、VLAN 12、VLAN 21、VLAN 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、VLAN 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、VLAN 12 はプライマリ VLAN10 と関連付けます。
- セカンダリ VLAN21、VLAN 22 はプライマリ VLAN20 と関連付けます。

図 11-4 ネットワーク図



II. 設定手順

1. Device A を設定します。

   # VLAN10、VLAN 20 をプライマリ 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

   # VLAN 11、VLAN 12、VLAN 21、VLAN 22 を作成します。

   [DeviceA] vlan 11 to 12

   [DeviceA] vlan 21 to 22

   # セカンダリ VLAN 11 と VLAN 12 をプライマリ VLAN 10 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 VLAN 21 と VLAN 22 をプライマリ VLAN 20 に関連付けます。

[DeviceA] vlan 20

[DeviceA-vlan20] private-vlan secondary 21 22

[DeviceA-vlan20] quit

アップリンクポート GigabitEthernet 1/0/5 を VLAN 10 と VLAN 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

ダウンリンクポート 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

ダウンリンクポート 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

ダウンリンクポート GigabitEthernet 1/0/2 を VLAN11、VLAN 21 のトランクセカンダリポートに設定します。

[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。

VLAN 11 と VLAN 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、VLAN 11、VLAN 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 を VLAN 11 に割り当てます。

[DeviceB] interface gigabitethernet 1/0/3

[DeviceB-GigabitEthernet1/0/3] port access vlan 11

[DeviceB-GigabitEthernet1/0/3] quit

GigabitEthernet 1/0/4 を VLAN 21 に割り当てます。

[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。

VLAN 10 と VLAN 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、VLAN 10 と VLAN 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。

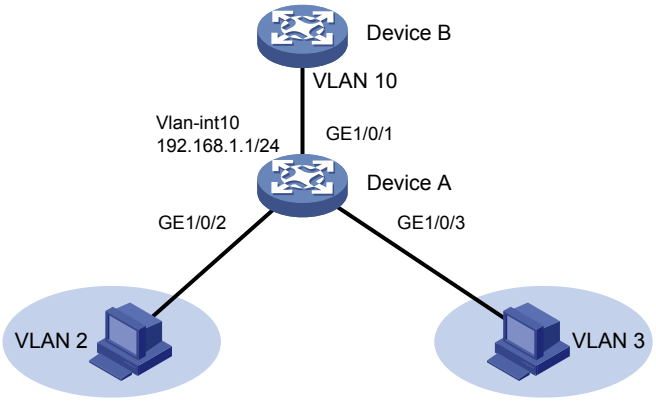
11.11.4. セカンダリ VLAN でのレイヤ 3 通信の 設定例

I. ネットワーク要件

図 11-5 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 で隔離していますが、レイヤ 3 では相互通信します。

図 11-5 ネットワーク図



II. 設定手順

VLAN10 を作成し、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

VLAN 2 と VLAN 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 VLAN 2 と VLAN 3 と関連付けます。

[DeviceA] vlan 10

[DeviceA-vlan10] private-vlan primary

[DeviceA-vlan10] private-vlan secondary 2 3

[DeviceA-vlan10] quit

アップリンクポート 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

ダウンリンクポート 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

ダウンリンクポート 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 VLAN 10 に関連付けたセカンダリ VLAN 2 と VLAN 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 VLAN 2 と VLAN 3 がレイヤ 3 で相互通信可能であることを示します。

目次

このセクションのページは **3-x-x** です。

12 章 Voice VLAN 12-1
12.1. 概要 12-1
12.1.1. 動作メカニズム 12-1
12.1.2. IP 電話の識別方法 12-1
12.1.3. IP 電話への Voice VLAN の配信 12-2
12.1.4. IP 電話のアクセス方式 12-2
12.1.5. Voice VLAN のアサインモード 12-3
12.1.6. Voice VLAN のアサインモードと IP 電話の協力 12-4
12.1.7. Voice VLAN のセキュリティモードとノーマルモード 12-5
12.2. Voice VLAN 設定作業リスト 12-6
12.3. 音声トラフィックの QoS プライオリティの設定 12-6
12.4. Voice VLAN アサインモードの設定 12-7
12.4.1. 自動 Voice VLAN アサインモードの設定 12-7
12.4.2. 手動 Voice VLAN アサインモードの設定 12-8
12.5. Voice VLAN を配信する LLDP の設定 12-10
12.5.1. Voice VLAN を配信する LLDP の設定 12-10
12.6. Voice VLAN の表示と維持 12-10
12.7. Voice VLAN の設定例 12-11
12.7.1. 自動 Voice VLAN モードの設定例 12-11
12.7.2. 手動 Voice VLAN アサインモードの設定例 12-13

12章 Voice VLAN

12.1. 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 にアサインすると、音声トラフィックのために QoS(Quality Of Service)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(統合アクセスデバイス)がありますが、本章では IP 電話（IP Phone）を用いて説明します。

12.1.1. 動作メカニズム

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。

1. ネットワーク中の IP 電話を識別し、その MAC アドレスを得ます。
2. 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。

12.1.2. 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。

I. 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 にアサインされます。

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（表 12-1 を参照してください。）を使用することができます。手動でデフォルト OUI アドレスを削除することも、新しく OUI アドレスを追加することもできます。

表 12-1 デフォルトの 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	000f-e200-0000	Aolynk phone
5	0060-b900-0000	Philips/NEC phone
6	00d0-1e00-0000	Pingtel phone

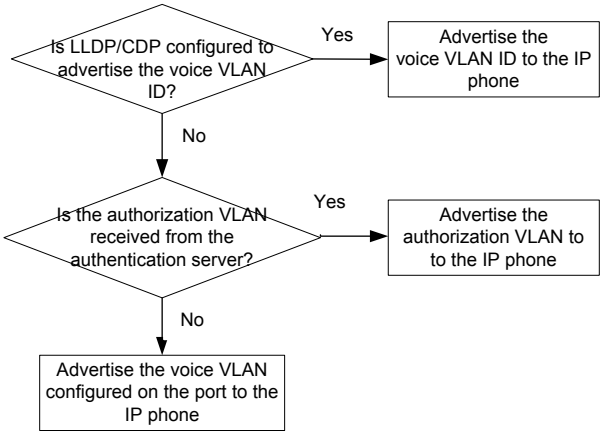
番号	OUI アドレス	ベンダ
7	00e0-7500-0000	Polycom phone
8	00e0-bb00-0000	3Com phone

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 ビットに割り当てられ、IEEE が各ベンダに割り当てるグローバルに一意な識別子です。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、MAC アドレスと **voice vlan mac-address** コマンドで設定された *mac-address* と *oui-mask* の 2 つの AND 演算の結果で求められます。

12.1.3. IP 電話への Voice VLAN の配信

図 12-1 に、IP 電話に Voice VLAN 情報を配信するフローを示します。

図 12-1 IP 電話への Voice VLAN の配信フロー



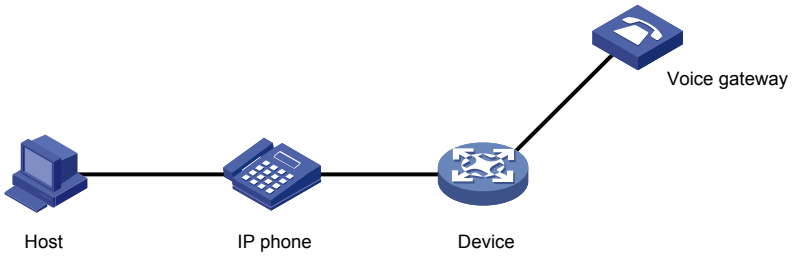
12.1.4. IP 電話のアクセス方式

I. ホストと IP 電話の直列接続

図 12-2 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 を使用します。
- 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。

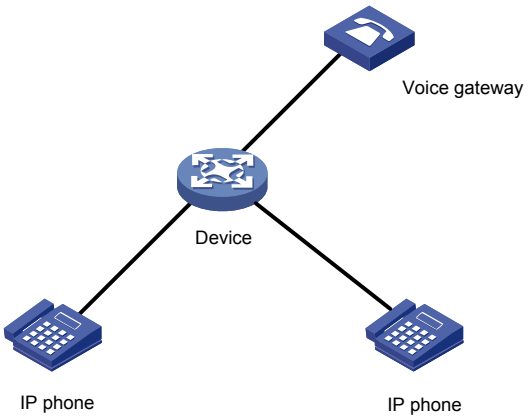
図 12-2 ホストと IP 電話が直列接続されたネットワーク



II. IP 電話の装置への接続

図 12-3 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 電話がタグの無い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 12-3 IP 電話が装置に接続されたネットワーク



12.1.5. Voice VLAN のアサインモード

ポートは、自動的あるいは手動で Voice VLAN をアサインすることができます。

I. 自動モード

図 12-2 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、装置は OUI アドレスに一致させるため、プロトコルパケットの送信元 MAC アドレスを使用します。照合が一致すれば、システムは以下の操作をします。

- システムはプロトコルパケットの受信ポートに Voice VLAN をアサインします。
- 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 のエージングタイマを開始します。

システムは、エージングタイマが超過するまでにポートでパケットを受信しない場合、Voice VLAN からポートを削除します。

装置が再起動した場合、ポートは正常に既存の音声装置に接続するため、再度 Voice VLAN に割り当てられます。Voice VLAN が正しく動作する限り、音声トラフィックによって開始されず、再割り当てが自動で行われます。

II. 手動モード

図 12-3 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、ポートは音声トラフィックを送信する Voice VLAN のみ割り当てられます。データトラフィックは音声トラフィックの送信に影響しません。手動で Voice VLAN に装置の受信ポートを割り当ててください。システムは装置の OUI アドレスとパケット内の送信元 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には、手動で行ってください。

12.1.6. Voice VLAN のアサインモードと IP 電話の協力

IP 電話は VLAN タグつ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。

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
- 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。

アクセスポートはタグパケットを送信しません。

I. タグ付き音声トラフィックの送信の設定要件

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PVIDはVoice VLANにできません。
	手動モード	ポートのPVID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します。
Hybrid	自動モード	ポートのPVIDはVoice VLANにできません。
	手動モード	ポートのPVID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します。

II. タグなし音声トラフィックの送信の設定要件

IP 電話がタグなしパケットを送信するとき、Voice VLAN アサインモードを手動に設定する必要があります。

表 12-2 手動モードにおけるタグなし音声トラフィックの送信の設定要件

ポートリンクタイプ	設定要件
Access	Voice VLANとしてポートのPVIDを設定します。
Trunk	Voice VLANとしてポートのPVIDを設定します。 ポートはVoice VLANからのパケットを転送する必要があります。
Hybrid	Voice VLANとしてポートのPVIDを設定します。 ポートはVLANタグなしのVoice VLANからのパケットを転送する必要があります。

12.1.7. 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、以下のモードで動作することができます。

- **ノーマルモード**–ポートは Voice VLAN でタグ付けされたパケットを受信し、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 はトラフィックの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 OUI アドレスと一致する音声パケットのみを受信します。他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 アドレスの確認を行うことでリソースの消費を削減します。

どちらのモードでも、装置は送信元 MAC アドレスがデバイスの OUI アドレスと一致する Voice VLAN パケットに対してのみ送信プライオリティを変更します。

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 12-3 ノーマルモードとセキュリティモードでの Voice VLAN が有効なポートのパケット処理

Voice VLAN モード	パケットタイプ	パケット処理モード
ノーマルモード	• タグなしパケット • Voice VLAN タグのパケット	ポートはMACアドレスを確認しません。すべてのパケットをVoice VLANで通過させます。
	他の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ってパケットを通過さ

Voice VLAN モード	パケットタイプ	パケット処理モード
		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、Voice VLAN で通過します。 • マッチしない場合、廃棄します。
	他の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ってパケットを通過させるか廃棄させます。

12.2. Voice VLAN設定作業リスト

作業リスト
音声トラフィックのQoSプライオリティの設定
Voice VLANアサインモードの設定 以下のいずれかの作業を行ってください。 • 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

12.3. 音声トラフィックのQoSプライオリティの設定

I. 音声トラフィックの QoS プライオリティの設定

QoS プライオリティ設定には、CoS と DSCP を含みます。装置は音声トラフィックの QoS プライオリティの設定を変更することができます。

II. 制限とガイドライン

デフォルトでは、ポートは受信パケットの 802.1p プライオリティを信用しません。受信音声 VLAN パケットのプライオリティ設定を信用するようポートを設定するには、**qos trust dot1p** コマンドを使用してプライオリティトラステッドモードをポート上の 802.1p プライオリティに設定する必要があります。プライオリティトラステッドモードの設定については、セクション 7 *ACL and QoS オペレーションマニュアル*の“*プライオリティマッピング*”を参照してください。

voice vlan qos コマンドと **voice vlan qos trust** コマンドの両方を設定した場合、最後に設定した設定が有効になります。

III. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. interface view に移行する	**interface** *interface-type interface-number*	—
3. 受信 Voice VLAN パケットの QoS プライオリティを設定する	• QoS プライオリティ設定をトラストする：**voice-vlan qos trust** • ポート CoS と DSCP を修正する：**voice-vlan qos** *cos-value dscp-value*	デフォルト：CoSは6、DSCPは46です。 ポートが受信Voice VLANパケットのQoS設定をトラストする場合、CoSとDSCPの修正はできません。

12.4. Voice VLANアサインモードの設定

12.4.1. 自動 Voice VLAN アサインモードの設定

I. 制限とガイドライン

- Voice VLAN とプロトコルベース VLAN を同時に設定しないでください。
  - ハイブリッドポートの自動モードの Voice VLAN はタグ付けされた受信音声トラフィックのみ処理します。
  - ハイブリッドポートのプロトコルベース VLAN はタグなしの受信パケットのみ処理します。プロトコルベースの VLAN については、セクション 3 *アクセス オペレーションマニュアル*の”*VLAN*”の”*プロトコルベース VLAN*”を参照してください。
- 自動 Voice VLAN アサインモードと MSTP を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。ポートに両方を設定する必要がある場合、最初にダイナミック MAC ベース VLAN を先に設定してください。逆の順序で設定すると、動作しません。設定の片方を削除すれば、もう一方の設定は動作します。

II. 設定手順

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

操作	コマンド	補足
2. (オプション設定項目)Voice VLAN のエージングタイマを設定する	**voice vlan aging** *minutes*	デフォルト：1440分 Voice VLANエージングタイマの設定は、自動Voice VLANアサインモードの時のみ実行されます。
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 12-1 に示すアドレスが登録されています。
5. interface view に移行する	**interface** *interface-type 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**	—
7. 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 設定する前にVLANが存在することを確認してください。

12.4.2. 手動 Voice VLAN アサインモードの設定

I. 制限とガイドライン

- それぞれのポートに、同時に異なる Voice VLAN を設定することができます。以下の要件が適用されているか確認してください。
  - 1 つのポートには 1 つの Voice VLAN のみ設定されています。
  - Voice VLAN は、既にスタティック VLAN として設定されています。
  - 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セクション 3 *アクセス オペレーションマニュアルの”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 を手動でポートにアサイン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. （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

操作	コマンド	補足
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 12-1 に示すアドレスが登録されています。
4. interface view に移行する	**interface** *interface-type interface-number*	—
5. 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、セクション 3 *アクセス オペレーション マニュアル*の”*VLAN*”の”*アクセスポート VLAN の設定*”を参照してください。 • トランクポートに設定する場合、セクション 3 *アクセス オペレーション マニュアル*の”*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、セクション 3 *アクセス オペレーションマニュアル*の”*VLAN*”の”*ハイブリッドポート 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PVIDになります。
7. （オプション設定項目）トランクポートあるいはハイブリッドポートの PVID として Voice VLAN を設定する	• トランクポートに設定する場合、セクション 3 *アクセス オペレーション マニュアル*の”*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、セクション 3 *アクセス オペレーションマニュアル*の”*VLAN*”の”*アクセスポート VLAN の設定*”を参照してください。	この設定は入力音声トラフィックがタグなしの場合に必要です。タグ付きの場合は必要することができません。
8. Voice VLAN を有効にする	**voice vlan** *vlan-id* **enable**	デフォルト：無効 設定する前にVLANが存在することを確認してください。

12.5. Voice VLANを配信するLLDPの設定

12.5.1. Voice VLAN を配信する LLDP の設定

I. 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。

II. 設定要件

設定する前に、グローバルとポートの両方で LLDP を有効にしてください。

III. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. interface view に移行する	**interface** *interface-type interface-number*	—
3. LLDP を設定する	**lldp tlv-enable med-tlv network-policy** *vlan-id*	デフォルト：LLDPは無効です。 **lldp tlv-enable med-tlv network-policy**コマンドの詳細はChapter 3 *Layer 2 - LAN Switching Command References*の”*LLDP commands*”を参照してください。
4. （オプション設定項目）Voice VLAN を表示する	**display lldp local-information**	配信されたVoice VLAN情報はコマンド出力のMED情報フィールドに表示されます。

12.6. 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
システムがサポートするOUIアドレスを表示する	**display voice-vlan mac-address**
Voice VLANの状態を表示する	**display voice vlan state**

12.7. Voice VLANの設定例

12.7.1. 自動 Voice VLAN モードの設定例

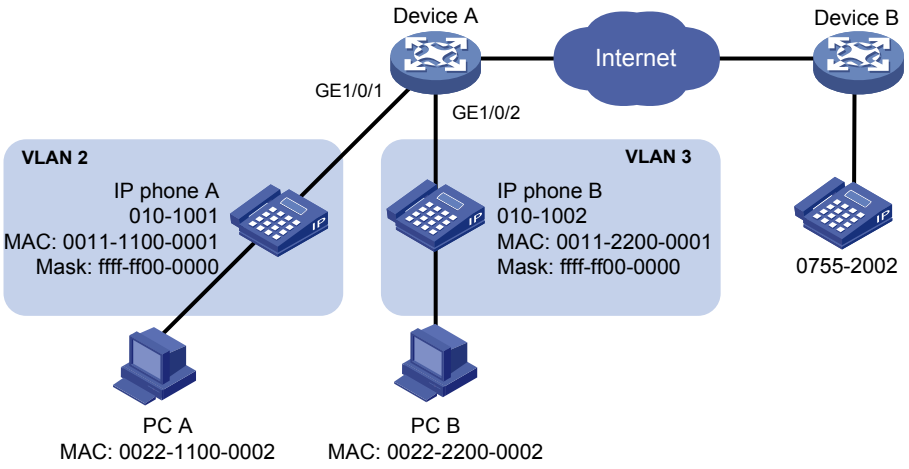
I. ネットワーク要件

図 12-4 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 VLAN2 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。
- Voice VLAN のエージングタイマを設定します。

図 12-4 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 のエージングタイマを 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 の OUI アドレス、マスク、説明を表示します。

[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  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
```

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
```

12.7.2. 手動 Voice VLAN アサインモードの設定例

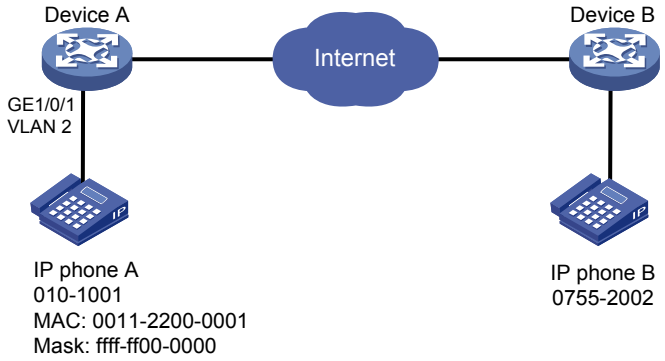
I. ネットワーク要件

図 12-5 に示すように設定します。IP 電話 A はタグなし音声トラフィックを送信します。

Device A は GigabitEthernet 1/0/1 で音声トラフィックのみを転送するように設定します。

- VLAN 2 を作成し、音声トラフィックを転送するように Voice VLAN を設定します。
- 手動 Voice VLAN サインモードを動作させるために、GigabitEthernet 1/0/1 ポートに設定をします。
- 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 12-5 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 の MAC アドレス 0011-2200-0000 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 として VLAN 2 を設定します。

[DeviceA-GigabitEthernet1/0/1] port hybrid pvid vlan 2

GigabitEthernet 1/0/1 を VLAN 2 の音声トラフィックが、タグなしで転送されるように設定します。

[DeviceA-GigabitEthernet1/0/1] port hybrid vlan 2 untagged

Voice VLAN を有効にし、GigabitEthernet 1/0/1 で 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  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
```

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 **3-x-x** です。

13 章 QinQ 13-1
13.1. 概要 13-1
13.1.1. QinQ の利点 13-1
13.1.2. QinQ の動作 13-1
13.1.3. QinQ の実装 13-2
13.1.4. プロトコルと標準 13-3
13.2. 制限とガイドライン 13-3
13.3. QinQ の有効化 13-4
13.4. VLAN トランスペアレントトランスミッションの設定 13-5
13.5. VLAN タグの TPID の設定 13-5
13.5.1. TPID 13-5
13.5.2. 制限とガイドライン 13-6
13.5.3. CVLAN タグの TPID の設定 13-7
13.5.4. SVLAN タグの TPID の設定 13-7
13.6. SVLAN タグの 802.1p プライオリティの設定 13-7
13.6.1. SVLAN タグの 802.1p プライオリティ 13-7
13.6.2. SVLAN の 802.1p プライオリティの設定要件 13-7
13.6.3. 設定作業リスト 13-8
13.6.4. トラフィッククラスの作成と、CVLAN のマッチング基準の設定 13-8
13.6.5. トラフィック動作の作成と、SVLAN タグのプライオリティマーキングアクションの設定 13-8
13.6.6. QoS ポリシーの作成 13-9
13.6.7. QoS ポリシーの適用 13-9
13.7. QinQ の表示と維持 13-9
13.8. QinQ 設定例 13-10
13.8.1. Basic QinQ 設定例 13-10
13.8.2. VLAN トランスペアレントトランスミッション設定例 13-12

13章 QinQ

この章では以下の用語を使用します。

- **CVLAN** – カスタマネットワーク VLAN（CVLAN [内部 VLAN]）は、顧客のプライベートネットワーク上で使う VLAN を示します。
- **SVLAN** – サービスプロバイダネットワーク VLAN（SVLAN[外部 VLAN]）は、サービスプロバイダが顧客の VLAN タグ付けされたトラフィックを転送する VLAN を示します。

13.1. 概要

QinQ(802.1Q-in-802.1Q)機能は、802.1Q がタグ付けされたカスタマトラフィックに 802.1Q タグを追加します。カスタマサイト間で Ethernet ネットワークを越えてレイヤ 2 通信を行うことができるようにサービスプロバイダを提供します。

13.1.1. QinQ の利点

QinQ は以下の利点があります。

- サービスプロバイダは 1 つの SVLAN を使用することで、カスタマ用に複数の CVLAN を転送することができます。
- カスタマが SVLAN との重複を気にせずに、CVLAN を設定できるようにします。
- サービスプロバイダが VLAN 割り当て方式を変更するとき、カスタマに割り当てた方式を変更しないで、保持することができます。
- カスタマが重複する CVLAN ID を使用することができます。サービスプロバイダネットワーク内の装置は CVLAN ID の代わりに SVLAN ID をもとにして転送を行います。

13.1.2. QinQ の動作

図 13-1 に示すように、QinQ フレームはサービスプロバイダネットワークを経由して以下のタグを運びます。

- **CVLAN tag** – CVLAN タグはカスタマネットワークで転送されるとき、QinQ フレームが属している VLAN を識別します。
- **SVLAN tag** – サービスプロバイダは、このタグをカスタマに割り当てます。SVLAN タグはサービスプロバイダネットワークで転送されるとき、QinQ フレームが属している VLAN を識別します。

サービスプロバイダネットワーク内のデバイスは、その SVLAN タグに基づいてタグ付きフレームを転送します。 CVLAN タグはフレームのペイロードの一部として送信されます。

図 13-1 シングルタグ付きのイーサネットフレームヘッダと 2 重タグ付きのイーサネットフレームヘッダ

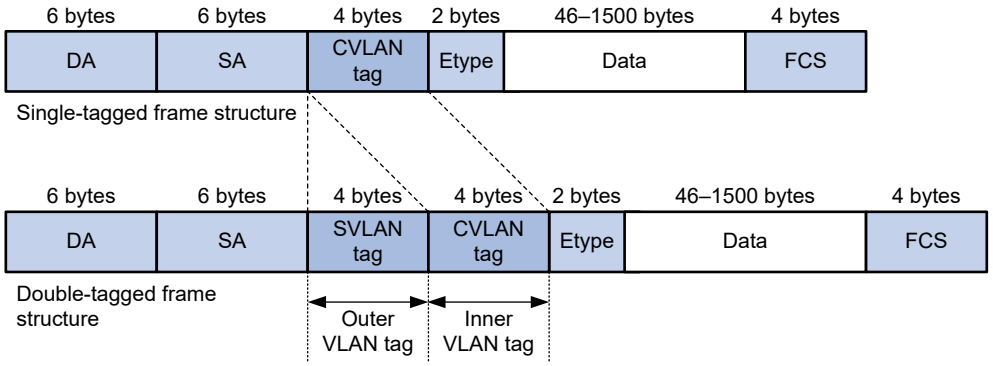
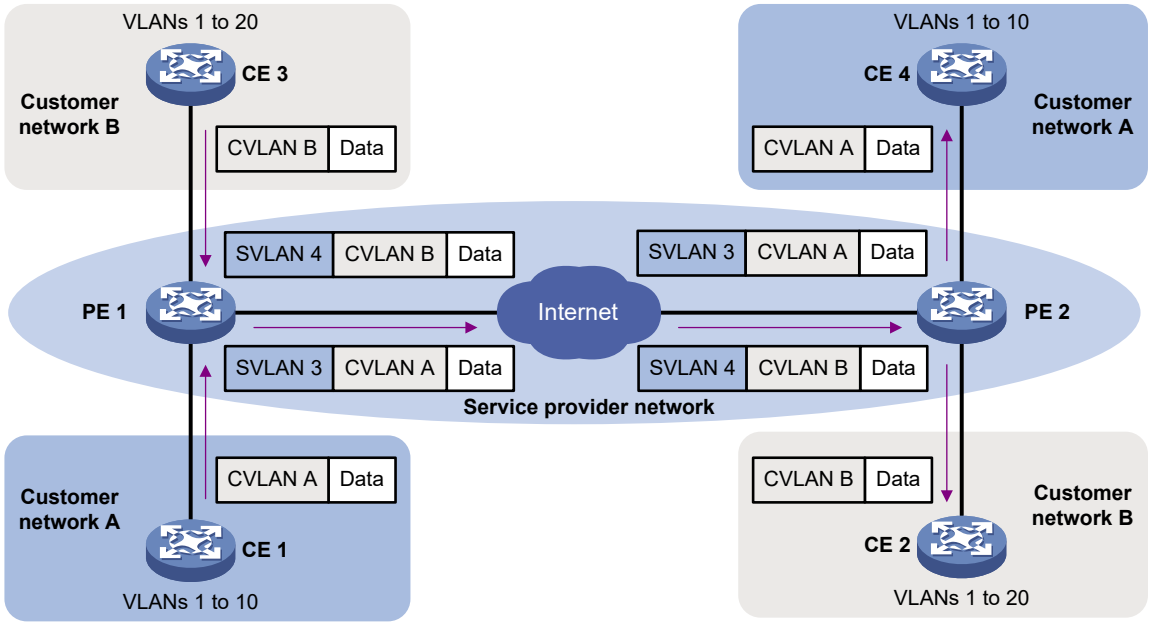


図 13-2 に示すように、カスタマ A はリモート側の CE 1 と CE 4 があります。カスタマ B はリモート側の CE 2 と CE 3 があります。2 つのカスタマの CVLAN は重複しています。サービスプロバイダはカスタマネットワーク A に SVLAN3 を割り当て、カスタマネットワーク B に SVLAN4 を割り当てます。

CE 1 からタグ付きフレームが到着したとき、PE 1 はフレームに SVLAN 3 をタグつけします。2 重のタグが付いたフレームは PE 2 に到着するまでサービスプロバイダネットワークを通過します。PE 2 はフレームの SVLAN タグを削除します。そして CE 4 にフレームを送信します。

図 13-2 一般的な QinQ アプリケーションシナリオ



13.1.3. QinQ の実装

QinQ はポートベースで設定できます。QinQ が有効になったポートのリンクタイプにはアクセス、ハイブリッド、トランクが使用できます。QinQ のタグ付けはポートのタイプと同一です。

QinQ が有効なポートはすべての入力フレーム(タグありあるいはタグなし)に PVID タグをタグ付けします。

- もし入力フレームが 1 つのタグを持っている場合、2 重タグフレームになります。
- もしフレームに 802.1Q タグがない場合、PVID のタグがつけられます。

QinQ はすべての入力フレーム(タグありあるいはタグなし)に PVID タグをタグ付けするために、最も基本的な VLAN の処理方式を提供します。拡張 VLAN 処理方式を実行するには、VLAN マッピング(セクション 3 *アクセス オペレーションマニュアル*の"*VLAN マッピング*"を参照してください)あるいは QoS ポリシーを使用します。

- 異なる CVLAN タグ用に異なる SVLAN を使用するため、one-to-two VLAN マッピングを使用します。
- 2 重タグの入力フレーム用に、SVLAN ID、CVLAN ID あるいは両方の ID を置き換える場合、two-to-two VLAN マッピングを設定します。
- CVLAN ID 以外の条件を使用して SVLAN タグありのパケットを一致させるには、QoS ネストアクションを使用します。QoS ネストアクションは、同じトラフィック動作の他のアクションとともに使用することもできます。
- SVLAN タグに 802.1p プライオリティを設定するために、QoS ポリシーを設定します。詳細はセクション 3 *アクセス オペレーションマニュアル*の"*QinQ*"の"*SVLAN タグの 802.1p プライオリティの設定*"を参照してください。

13.1.4. プロトコルと標準

- IEEE 802.1Q, *IEEE Standard for Local and Metropolitan Area Networks-Virtual Bridged Local Area Networks*
- IEEE 802.1ad, *IEEE Standard for Local and Metropolitan Area Networks-Virtual Bridged Local Area Networks-Amendment 4: Provider Bridges*

13.2. 制限とガイドライン

QinQ を設定する場合、以下の制限とガイドラインがあります。

- QinQ フレームの内部 802.1Q タグはペイロードの一部となります。QinQ フレームを正しく転送するため、QinQ フレームの転送パスの各ポートの最小 MTU を 1504 バイトに設定することを推奨します。この値はデフォルトの Ethernet インタフェースの MTU(1500 バイト)と VLAN タグ(4 バイト)の合計です。
- QinQ と VLAN マッピングが重複する場合、VLAN マッピングが適用され、QinQ は動作しません。
- QoS ポリシー、VLAN マッピング、および QinQ をポート上で重複して設定した場合、QinQ は動作しません。また、QoS ポリシー、および VLAN マッピングが重複する場合は、QoS ポリシーが優先されます。
- QinQ、two-to-two VLAN を同時に設定することはできません。QinQ が有効なポートで SVLAN タグを追加することができません。CVLAN、SVLAN ID を変更することもできません。
- 一致ルールとして VLAN ID を使用して QoS ポリシーを適用し、QinQ 対応インタフェースにネストするには、一致するパケットが VLAN タグで通過できるようにします。インタフェースで一致するパケットが VLAN タグで通過できない場合、ネストは有効になりません。

13.3. QinQの有効化

I. QinQ の有効化

PE のカスタマ側のポートで QinQ を有効にします。QinQ が有効なポートは入力フレームに PVID をタグ付けします。

II. 制限とガイドライン

ポートで QinQ を有効、無効にする間に、ポートの VLAN マッピングの設定を削除してください。VLAN マッピングの詳細はセクション 3 *アクセス オペレーションマニュアル*の“*VLAN マッピング*”を参照してください。

III. 設定手順

操作		コマンド	補足
1. system view に移行する		**system-view**	—
2. Ethernet interface view あるいは aggregate interface view に移行する		**interface** *interface-type interface-number*	—
3. リンクタイプを設定する		**port link-type** { **hybrid** | **trunk** }	デフォルト：アクセス
4. PVID からパケットを通過できるようにポートを設定する	指定した VLANにアクセスポートを割り当てる	**port access vlan** *vlan-id*	デフォルト : VLAN1に属します。 アクセスポートのPVIDは、ポートが属するVLANです。 ポートはタグなしVLANからパケットを送信します。
	タグなしの PVIDからパケットを送信するように、ハイブリッドポートを設定する	**port hybrid vlan** *vlan-id-list* **untagged**	デフォルト : ハイブリッドポートは、リンクタイプがアクセスするときにポートが属するVLANのタグなしメンバです。
	PVIDからパケットを通過できるようにトランクポートを設定する	**port trunk permit vlan** { *vlan-id-list* | **all** }	デフォルトで : VLAN1からのみパケットを通過します。
5. QinQ を有効にする		**qinq enable**	デフォルト：無効

13.4. VLANトランスペアレントトランスミッションの設定

I. トランスペアレント VLAN

カスタマ側のポートで QinQ のタグづけを行う際、VLAN(たとえばマネジメント VLAN)のトラフィックを除外することができます。この VLAN はトランスペアレント VLAN と呼ばれます。

II. 制限とガイドライン

- ポートで VLAN を処理する別の設定を行わないでください。
- 転送経路上にあるすべてのポートで VLAN を通過できることを確認してください。
- インタフェースでトランスペアレント VLAN と VLAN マッピングの両方を設定した場合、トランスペアレント VLAN は以下の VLAN を使用できません。
  - one-to-one VLAN マッピング、one-to-two VLAN マッピング、many-to-one VLAN マッピングの変更前の VLAN と変更後の VLAN
  - two-to-two VLAN マッピングの変更前の外部 VLAN と変更後の外部 VLAN

III. 設定手順

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. リンクタイプを設定する	**port link-type** { **hybrid** | **trunk** }	デフォルト：アクセス
4. ポートで PVID のパケットを許可し、通過できるようにトランスペアレント VLAN を設定する	• ハイブリッドポート: **port hybrid vlan** *vlan-id-list* { **tagged** | **untagged** } • トランクポート: **port trunk permit vlan** { *vlan-id-list* | **all** }	デフォルト： トランクポートはVLAN1のみ許可し、ハイブリッドポートはVLAN1のuntaggedメンバのみ許可します。
5. トランスペアレント VLAN を指定する	**qinq transparent-vlan** *vlan-list*	デフォルト：設定なし

13.5. VLANタグのTPIDの設定

13.5.1. TPID

TPID はフレームを 802.1Q のタグ付きフレームとして識別します。この値はベンダによって変わります。802.1Q が有効なポートで 802.1Q タグが付いた TPID はデフォルトで 0x8100 です。IEEE802.1Q

に準拠しています。複数のベンダがあるネットワークでは、802.1Q のタグ付きフレームが正しく識別できるように、TPID の設定はすべての装置で同一にする必要があります。

TPID の設定は、CVLAN TPID と SVLAN TPID を含みます。

QinQ が有効なポートは、入力するタグ付けフレームにマッチさせるため、CVLAN TPID を使用します。もし TPID が CVLAN TPID と異なる場合、入力フレームはタグなしフレームとして扱われます。

SVLAN TPID はポート毎に設定できます。サービスプロバイダ側のポートは出力するフレームの SVLAN タグの TPID を置き換えるため、そして入力するタグ付けフレームにマッチさせるため、SVLAN TPID を使用します。もし外部 VLAN タグの TPID が SVLAN TPID と異なる場合、入力フレームはタグなしフレームとして扱われます。

たとえば、PE 装置は TPID 0x8200 を使用するカスタマデバイスと、TPID 0x9100 を使用するプロバイダデバイスに接続されています。正しいパケットの処理を行うため、PE で CVLAN TPID を 0x8200、SVLAN TPID を 0x9100 として設定する必要があります。

TPID フィールドはタグなし Ethernet フレームの EtherType フィールドと同じ位置づけとなります。パケットタイプを正しく識別するため、TPID は表 13-1 に示す予約済み EtherType 値を設定することができません。

表 13-1 予約済み EtherType 値

プロトコルタイプ	値
ARP	0x0806
PUP	0x0200
RARP	0x8035
IP	0x0800
IPv6	0x86dd
PPPoE	0x8863/0x8864
MPLS	0x8847/0x8848
IPX/SPX	0x8137
IS-IS	0x8000
LACP	0x8809
LLDP	0x88cc
802.1X	0x888e
802.1ag	0x8902
Cluster	0x88a7
Reserved	0xfffd/0xfffe/0xffff

13.5.2. 制限とガイドライン

CVLAN タグの TPID 値は通常、PE で設定します。 通常、SVLAN タグの TPID 値は、PE のサービスプロバイダ側のポートで設定されます。

13.5.3. CVLAN タグの TPID の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. CVLAN タグの TPID を設定する	**qinq ethernet-type customer-tag** *hex-value*	デフォルト：0x8100

13.5.4. SVLAN タグの TPID 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 あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	ー
3. SVLAN TPID を設定する	**qinq ethernet-type service-tag** *hex-value*	デフォルト：0x8100

13.6. SVLANタグの802.1pプライオリティの設定

13.6.1. SVLAN タグの 802.1p プライオリティ

デフォルトでは、SVLAN タグの 802.1p プライオリティは、ポートのプライオリティのトラステッドモードに依存して追加されます。

- もしフレームの 802.1p プライオリティがトラステッドモードである場合、装置は CVLAN タグの 802.1p プライオリティを SVLAN にコピーします。
- もしポートプライオリティがトラステッドモードである場合、ポートは SVLAN の 802.1p プライオリティをポートプライオリティと同一に設定します。デフォルトのポートプライオリティは 0 です。

QoS ポリシー、プライオリティトラステッドモードの詳細はセクション 7 *ACL and QoS オペレーションマニュアル*の“*QoS ポリシー*”、“*プライオリティマッピング*”を参照してください。

13.6.2. SVLAN の 802.1p プライオリティの設定要件

1. QinQ を有効にしてください。詳細はセクション 3 *アクセス オペレーションマニュアル*の“*QinQ*”の“*QinQ の有効化*”を参照してください。

   CVLAN タグの CVLAN ID あるいは 802.1p プライオリティを SVLAN タグの 802.1p プライオリティに使用する場合、最初にポートで QinQ を有効にしてください。

2. 受信フレームの 802.1p プライオリティを信用するため、ポートで **qos trust dot1p** コマンドを設定してください。詳細はセクション 7 *ACL and QoS オペレーションマニュアル*の“*QoS ポリシー*”を参照してください。

   remark dot1p コマンドが設定されている場合、**qos trust dot1p** コマンドが必要です。**remark dot1p customer-dot1p-trust** コマンドが設定されている場合、**remark dot1p** コマンドはオプションです。

13.6.3. 設定作業リスト

作業リスト
トラフィッククラスの作成と、CVLANのマッチング基準の設定
トラフィック動作の作成と、SVLANタグのプライオリティマーキングアクションの設定
QoSポリシーの作成
QoSポリシーの適用

13.6.4. トラフィッククラスの作成と、CVLAN のマッチング基準の設定

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. CVLAN のマッチング基準を設定する	• CVLAN ID にマッチする: **if-match customer-vlan-id** *vlan-id-list* • 802.1p プライオリティにマッチする: **if-match customer-dot1p** *dot1p-value*&<1-8>	—

13.6.5. トラフィック動作の作成と、SVLAN タグのプライオリティマーキングアクションの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. traffic behavior を作成し、traffic behavior view に移行する	**traffic behavior** *behavior-name*	—

操作	コマンド	補足
3. SVLAN タグのプライオリティマーキングアクションを設定する	• マッチしているフレームの SVLAN タグのプライオリティを設定されたプライオリティに書き換える: **remark dot1p** *dot1p-value* • CVLAN タグの 802.1p プライオリティを SVLAN タグにコピーする: **remark dot1p customer-dot1p-trust**	—

13.6.6. QoS ポリシーの作成

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. QoS policy を作成し、QoS policy view に移行する	**qos policy** *policy-name*	—
3. トラフィッククラスを QoS ポリシーの traffic behavior に関連付けする	**classifier** *classifier-name* **behavior** *behavior-name*	—

13.6.7. QoS ポリシーの適用

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. インタフェースの入力方向に QoS ポリシーを適用する	**qos apply policy** *policy-name* **inbound**	—

13.7. QinQ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
QinQが有効なインタフェースを表示する	**display qinq** [**interface** *interface-type interface-number*]

13.8. QinQ設定例

13.8.1. Basic QinQ 設定例

I. ネットワーク要件

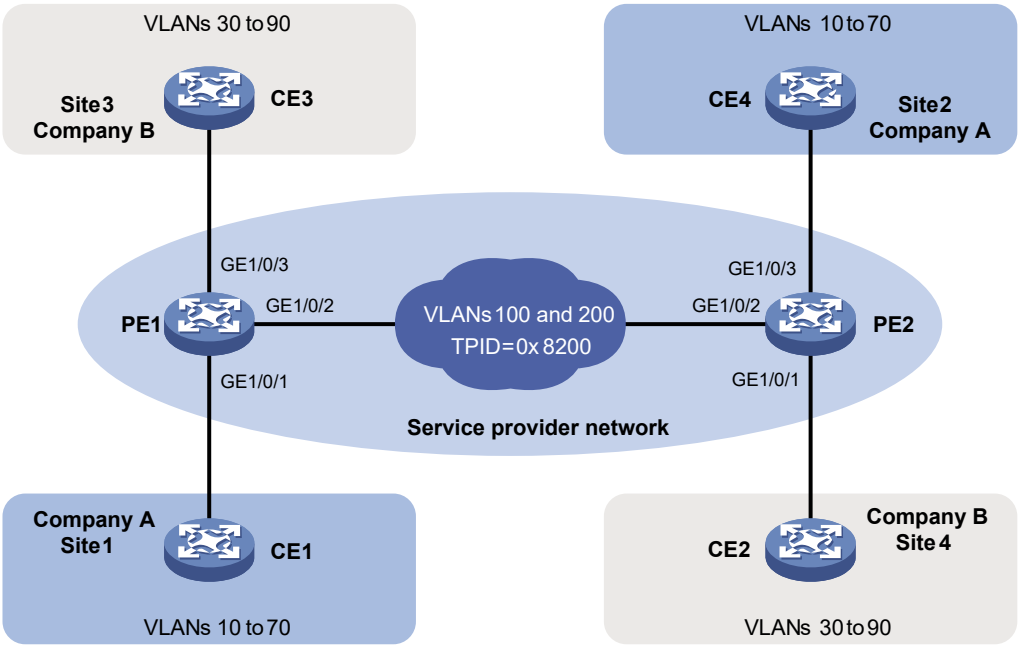
図 13-3 に示すように設定します。

- サービスプロバイダは、VLAN 100 を Company A の VLAN 10～VLAN 70 に割り当てます。
- サービスプロバイダは、VLAN 200 を Company B の VLAN 30～VLAN 90 に割り当てます。
- サービスプロバイダネットワークの PE1 と PE2 間のデバイスは TPID 0x8200 を使用します。

それぞれ VLAN 100 と VLAN 200 で Company A と Company B のトラフィックを転送するため、PE1 と PE2 の QinQ を設定します。

QinQ フレームを正しく識別するため、PE1 と PE2 のサービスプロバイダ側ポートの SVLAN TPID を 0x8200 に設定します。

図 13-3 ネットワーク図



II. 設定手順

1. PE 1 の設定

トランクポートとして GigabitEthernet 1/0/1 を設定し、VLAN 100 を割り当てます。

<PE1> system-view

[PE1] interface gigabitethernet 1/0/1

[PE1-GigabitEthernet1/0/1] port link-type trunk

[PE1-GigabitEthernet1/0/1] port trunk permit vlan 100

GigabitEthernet 1/0/1 の PVID として VLAN 100 を設定します。

[PE1-GigabitEthernet1/0/1] port trunk pvid vlan 100

GigabitEthernet 1/0/1 で QinQ を有効にします。

[PE1-GigabitEthernet1/0/1] qinq enable

[PE1-GigabitEthernet1/0/1] quit

トランクポートとして GigabitEthernet 1/0/2 を設定し、VLAN 100、VLAN 200 を割り当てます。

[PE1] interface gigabitethernet 1/0/2

[PE1-GigabitEthernet1/0/2] port link-type trunk

[PE1-GigabitEthernet1/0/2] port trunk permit vlan 100 200

GigabitEthernet 1/0/2 の SVLAN タグの TPID 値を 0x8200 に設定します。

[PE1-GigabitEthernet1/0/2] qinq ethernet-type service-tag 8200

[PE1-GigabitEthernet1/0/2] quit

トランクポートとして GigabitEthernet 1/0/3 を設定し、VLAN 200 を割り当てます。

[PE1] interface gigabitethernet 1/0/3

[PE1-GigabitEthernet1/0/3] port link-type trunk

[PE1-GigabitEthernet1/0/3] port trunk permit vlan 200

GigabitEthernet 1/0/3 の PVID として VLAN 200 を設定します。

[PE1-GigabitEthernet1/0/3] port trunk pvid vlan 200

GigabitEthernet 1/0/3 で QinQ を有効にします。

[PE1-GigabitEthernet1/0/3] qinq enable

[PE1-GigabitEthernet1/0/3] quit

2. PE 2 の設定

トランクポートとして GigabitEthernet 1/0/1 を設定し、VLAN 200 を割り当てます。

<PE2> system-view

[PE2] interface gigabitethernet 1/0/1

[PE2-GigabitEthernet1/0/1] port link-type trunk

[PE2-GigabitEthernet1/0/1] port trunk permit vlan 200

GigabitEthernet 1/0/1 の PVID として VLAN 200 を設定します。

[PE2-GigabitEthernet1/0/1] port trunk pvid vlan 200

GigabitEthernet 1/0/1 で QinQ を有効にします。

[PE2-GigabitEthernet1/0/1] qinq enable

[PE2-GigabitEthernet1/0/1] quit

トランクポートとして GigabitEthernet 1/0/2 を設定し、VLAN100、VLAN200 を割り当てます。

[PE2] interface gigabitethernet 1/0/2

[PE2-GigabitEthernet1/0/2] port link-type trunk

[PE2-GigabitEthernet1/0/2] port trunk permit vlan 100 200

GigabitEthernet 1/0/2 の SVLAN タグの TPID 値を 0x8200 に設定します。

[PE2-GigabitEthernet1/0/2] qinq ethernet-type service-tag 8200

[PE2-GigabitEthernet1/0/2] quit

トランクポートとして GigabitEthernet 1/0/3 を設定し、VLAN 100 を割り当てます。

[PE2] interface gigabitethernet 1/0/3

[PE2-GigabitEthernet1/0/3] port link-type trunk

[PE2-GigabitEthernet1/0/3] port trunk permit vlan 100

GigabitEthernet 1/0/3 の PVID として VLAN 100 を設定します。

[PE2-GigabitEthernet1/0/3] port trunk pvid vlan 100

GigabitEthernet 1/0/3 で QinQ を有効にします。

[PE2-GigabitEthernet1/0/3] qinq enable

[PE2-GigabitEthernet1/0/3] quit

3. PE1 と PE2 間のデバイスの設定

QinQ フレームのパスにある各ポートの MTU を 1504 バイト以上に設定します。(詳細は省略します)

VLAN タグを取り外すことなく VLAN 100 と VLAN 200 からのすべてのフレームを許可するように転送パスのすべてのポートを設定します。(詳細は省略します)

13.8.2. VLAN トランスペアレントトランスミッション設定例

I. ネットワーク要件

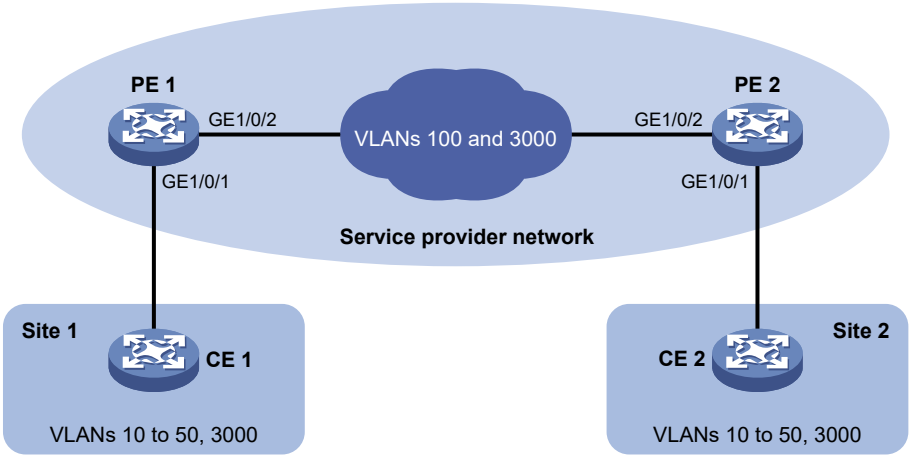
図 13-4 に示すように設定します。

- サービスプロバイダは VLAN 100 を company の VLAN 10～VLAN 50 に割り当てます。
- サービスプロバイダネットワークの company の専用 VLAN として VLAN 3000 を設定します。

サービスプロバイダネットワークを越えて CVLAN 10～CVLAN 50 のレイヤ 2 接続を提供するため、PE1 と PE2 の QinQ を設定します。

SVLAN を使用しないで VLAN 3000 内のホストが通信できるように、PE1 と PE2 の VLAN 3000 の VLAN トランスペアレントトランスミッションを設定します。

図 13-4 ネットワーク図



II. 設定手順

1. PE 1 の設定

   # トランクポートとして GigabitEthernet 1/0/1 を設定し、VLAN 100、VLAN 3000 を割り当てます。

   <PE1> system-view

   [PE1] interface gigabitethernet 1/0/1

   [PE1-GigabitEthernet1/0/1] port link-type trunk

   [PE1-GigabitEthernet1/0/1] port trunk permit vlan 100 3000

   # GigabitEthernet 1/0/1 の PVID として VLAN 100 を設定します。

   [PE1-GigabitEthernet1/0/1] port trunk pvid vlan 100

   # GigabitEthernet 1/0/1 で QinQ を有効にします。

   [PE1-GigabitEthernet1/0/1] qinq enable

   # VLAN 3000 からトランスペアレントにフレームを転送するため、GigabitEthernet 1/0/1 を設定します。

   [PE1-GigabitEthernet1/0/1] qinq transparent-vlan 3000

   [PE1-GigabitEthernet1/0/1] quit

   # トランクポートとして GigabitEthernet 1/0/2 を設定し、VLAN 100、VLAN 3000 を割り当てます。

   [PE1] interface gigabitethernet 1/0/2

   [PE1-GigabitEthernet1/0/2] port link-type trunk

   [PE1-GigabitEthernet1/0/2] port trunk permit vlan 100 3000

   [PE1-GigabitEthernet1/0/2] quit

2. PE 2 の設定

   # トランクポートとして GigabitEthernet 1/0/1 を設定し、VLAN 100、VLAN 3000 を割り当てます。

   <PE2> system-view

   [PE2] interface gigabitethernet 1/0/1

[PE2-GigabitEthernet1/0/1] port link-type trunk

[PE2-GigabitEthernet1/0/1] port trunk permit vlan 100 3000

GigabitEthernet 1/0/1 の PVID として VLAN 100 を設定します。

[PE1-GigabitEthernet1/0/1] port trunk pvid vlan 100

GigabitEthernet 1/0/1 で QinQ を有効にします。

[PE2-GigabitEthernet1/0/1] qinq enable

VLAN 3000 からトランスペアレントにフレームを転送するため、GigabitEthernet 1/0/1 を設定します。

[PE2-GigabitEthernet1/0/1] qinq transparent-vlan 3000

[PE2-GigabitEthernet1/0/1] quit

トランクポートとして GigabitEthernet 1/0/2 を設定し、VLAN 100、VLAN 3000 を割り当てます。

[PE2] interface gigabitethernet 1/0/2

[PE2-GigabitEthernet1/0/2] port link-type trunk

[PE2-GigabitEthernet1/0/2] port trunk permit vlan 100 3000

3. PE1 と PE2 間のデバイスの設定

QinQ フレームのパスにある各ポートの MTU を 1504 バイト以上に設定します。(詳細は省略します)

VLAN タグを取り外すことなく VLAN 100 と VLAN 3000 からのすべてのフレームを許可するように転送パスのすべてのポートを設定します。(詳細は省略します)

目次

このセクションのページは **3-x-x** です。

14 章 VLAN マッピング 14-1
14.1. 概要 14-1
14.1.1. VLAN マッピングのタイプ 14-1
14.1.2. VLAN マッピングアプリケーションシナリオ 14-1
14.1.3. VLAN マッピングの実装 14-3
14.2. 制限とガイドライン 14-5
14.3. VLAN マッピングの設定作業リスト 14-6
14.4. 設定要件 14-6
14.5. one-to-one VLAN マッピングの設定 14-6
14.6. one-to-two VLAN マッピングの設定 14-7
14.7. two-to-two VLAN マッピングの設定 14-8
14.8. VLAN マッピングの表示と維持 14-9
14.9. VLAN マッピングの設定例 14-10
14.9.1. one-to-one VLAN マッピングの設定例 14-10
14.9.2. one-to-two、two-to-two VLAN マッピングの設定例 14-13

14章 VLAN マッピング

14.1. 概要

VLAN マッピングはタグ付けされたトラフィックを新しい VLAN ID で再マッピングします。

14.1.1. VLAN マッピングのタイプ

NEC は以下のタイプを提供します。

- **One-to-One VLAN マッピング** — 1 つの VLAN タグを別の VLAN タグに置き換えます。
- **One-to-two VLAN マッピング** – シングルタグ付けされたパケットに外部 VLAN タグをタグ付けします。
- **Two-to-two VLAN マッピング** – SVLAN ID、CVLAN ID あるいは両方の ID を 2 重タグ付けられた入力フレームに置き換えます。

14.1.2. VLAN マッピングアプリケーションシナリオ

I. One-to-one VLAN マッピング

図 14-1 に示すように、一般的に one-to-one VLAN マッピングはブロードバンドインタネットアクセスで使用されます。

図 14-1 VLAN マッピングのアプリケーションシナリオ

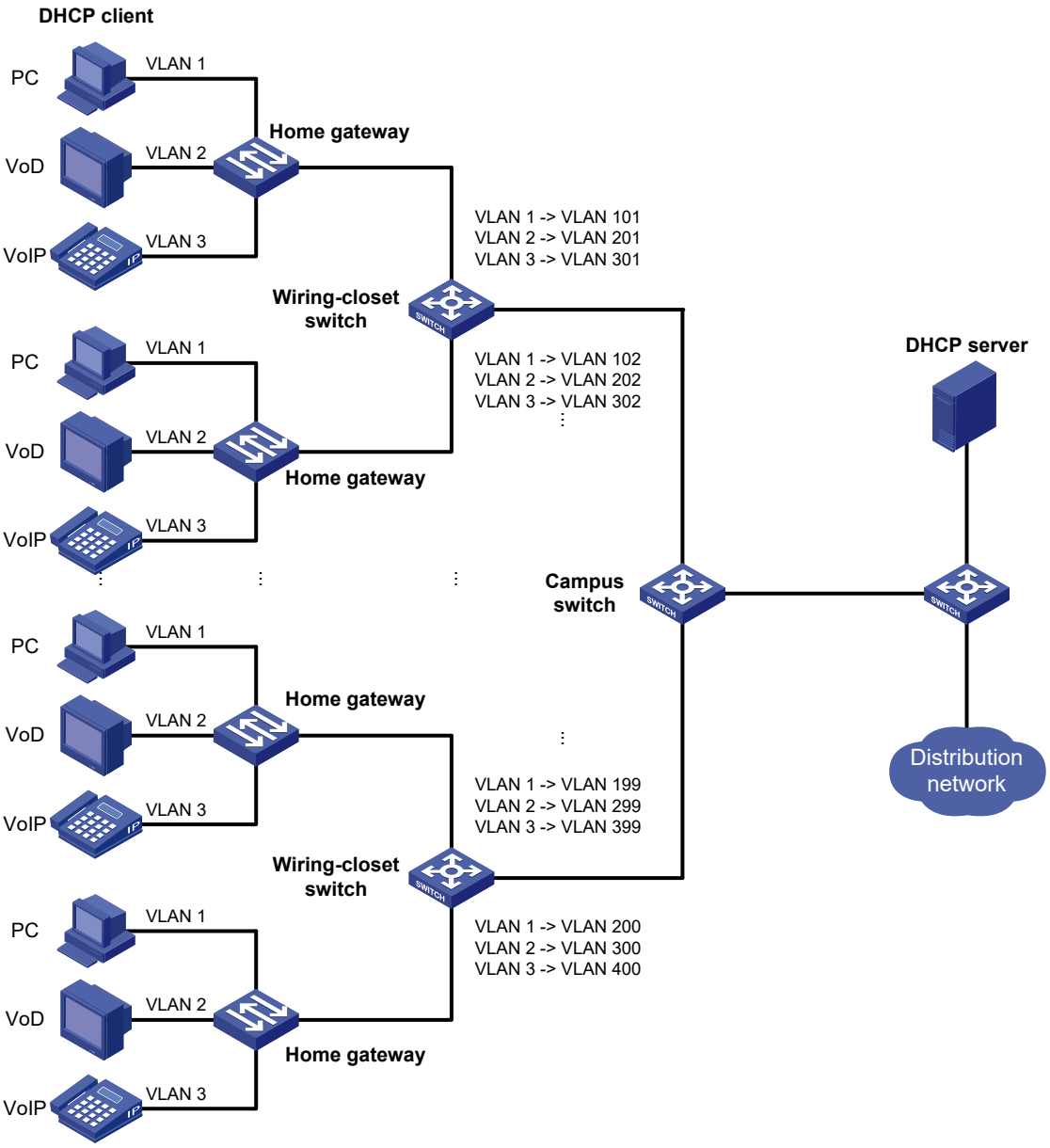


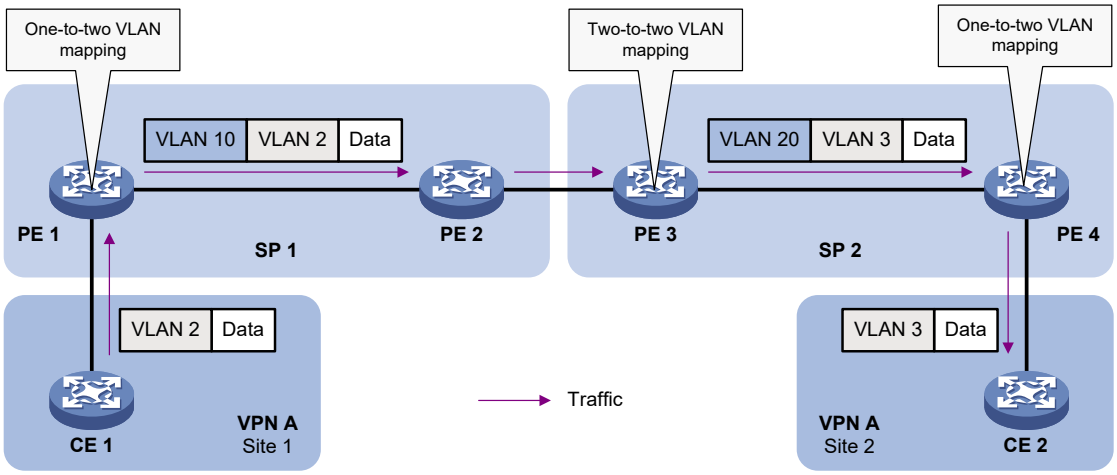
図 14-1 における、ネットワークの概要を以下に示します。

- 各ホームゲートウェイは、PC、VoD、VoIP サービスを転送するため、異なる VLAN を使用します。
- カスタマ毎に詳細にトラフィックの各タイプを分類させるため、ワイヤリングクローゼットのスイッチで one-to-one VLAN を設定します。この機能は分類した VLAN を各カスタマからのトラフィックタイプ毎に割り当てます。必要とされる VLAN のトータル数は非常に多くなります。

II. One-to-two マッピングと two-to-two VLAN マッピング

図 14-2 に示すように、One-to-two VLAN マッピングと two-to-two VLAN マッピングは一般的に、同じ VPN のリモートサイトが 2 つの SP ネットワークを越えて通信します。

図 14-2 one-to-two と two-to-two VLAN マッピングのアプリケーションシナリオ



Site 1 と Site 2 はそれぞれ VLAN2 と VLAN3 にあります。SP1 ネットワークは SVLAN10 を Site 1 に割り当てます。SP2 ネットワークは SVLAN20 を Site 2 に割り当てます。Site 1 からのパケットが PE1 に到着したとき、PE1 は one-to-two VLAN マッピングを使用して、SVLAN10 のパケットをタグ付けします。

SP1 のネットワークから 2 重タグ付けのパケットが SP2 ネットワークインタフェースに到着したとき、PE3 は以下のパケット処理を行います。

- SVLAN タグ 10 を SVLAN タグ 20 に置き換えます。
- CVLAN タグ 2 を CVLAN タグ 3 に置き換えます。

One-to-two VLAN マッピングは以下の利点があります。

- SVLAN に重複することなく CVLAN の割り当てを計画するようにカスタマネットワークを設定することができます。
- タグ付けされたパケットに VLAN タグを追加し、4094×4094 に VLAN の数を拡張します。
- SVLAN のリソースを減少させます。つまりマッピングプロセスが初期化するまえに、SP ネットワークに 4094 の VLAN が存在します。

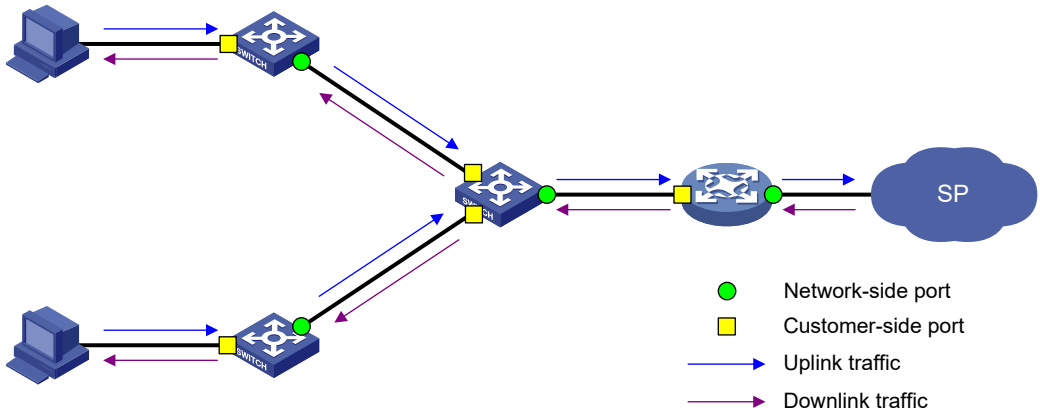
14.1.3. VLAN マッピングの実装

図 14-3 は VLAN マッピングが動作するときの、用語を説明するために、簡単なネットワークで示したものです。

基本用語を以下に示します。

- **Uplink traffic** – 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に転送されるトラフィックです。
- **Downlink traffic** – サービスプロバイダネットワークからカスタマネットワークに転送されるトラフィックです。
- **Network-side port** – サービスプロバイダに接続されたポート、あるいはサービスプロバイダに近いポートです。
- **Customer-side port** – カスタマネットワークに接続されたポート、あるいはカスタマネットワークに近いポート です。

図 14-3 VLAN マッピングの基本用語

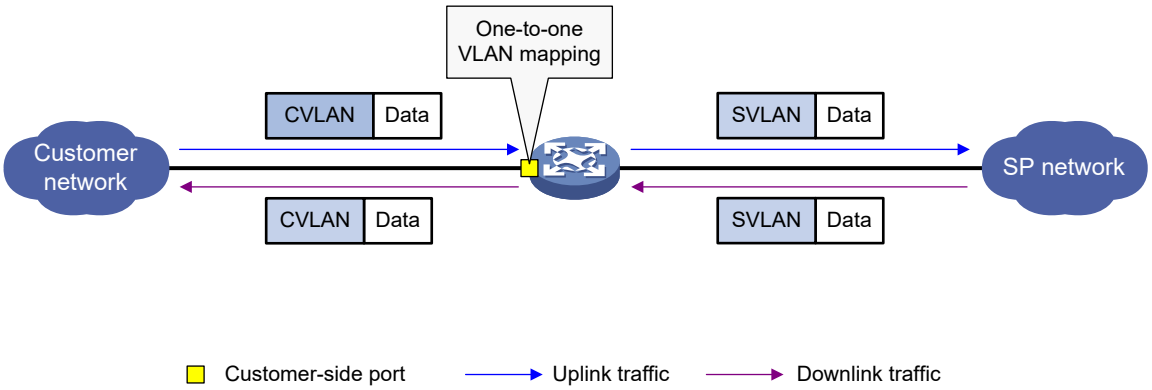


I. One-to-one VLAN マッピング

図 14-4 に示すように、one-to-one VLAN マッピングはカスタマ側ポートで実装され、VLAN タグを以下のように置き換えます。

- アップリンクトラフィック用に CVLAN を SVLAN に置き換えます。
- ダウンリンクトラフィック用に SVLAN を CVLAN に置き換えます。

図 14-4 One-to-one VLAN マッピングの実装



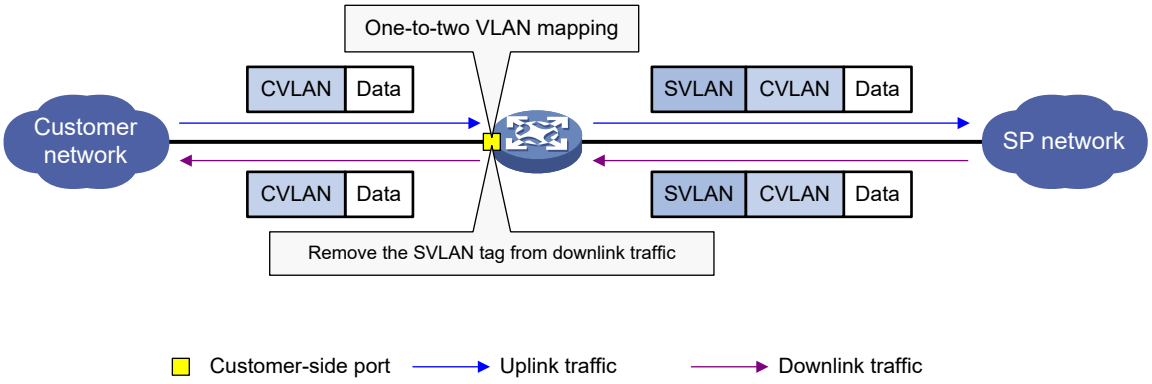
II. One-to-two VLAN マッピング

図 14-5 に示すように、one-to-two VLAN マッピングはアップリンクトラフィックように SVLAN タグを追加するため、カスタマ側ポートで実装されます。

ダウンリンクトラフィック用にカスタマネットワークに正しく送信するため、転送するまえにカスタマ側ポートの SVLAN タグを取り外すことを確認してください。以下の方法の 1 つを使用してダウンリンクトラフィックの SVLAN タグを取り外してください。

- ハイブリッドポートとしてカスタマ側ポートを設定し、タグなしメンバとして SVLAN にポートを割り当てます。
- トランクポートとしてカスタマ側ポートを設定し、PVID として SVLAN を設定します。

図 14-5 One-to-two VLAN マッピングの実装

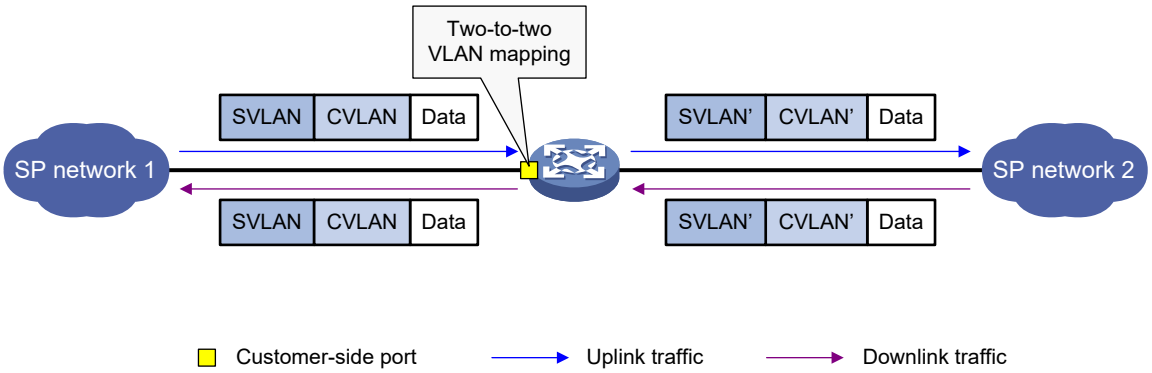


III. Two-to-two VLAN マッピング

図 14-6 に示すように、two-to-two VLAN マッピングはカスタマ側ポートで実装され、VLAN タグを以下のように置き換えます。

- アップリンクトラフィック用に CVLAN と SVLAN を CVLAN’ と SVLAN’ に置き換えます。
- ダウンリンクトラフィック用に CVLAN’ と SVLAN’ を CVLAN と SVLAN に置き換えます。

図 14-6 Two-to-two VLAN マッピングの実装



14.2. 制限とガイドライン

VLAN タグをパケットに追加するには、VLAN マッピングと QinQ の両方を設定できます。 VLAN マッピングは、設定の重複が発生した場合に有効になります。 QinQ 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 *アクセス "QinQ"*を参照してください。

パケットに VLAN タグを追加または置換するには、VLAN マッピングと QoS ポリシーの両方を設定できます。 QoS ポリシーは、設定の重複が発生した場合に有効になります。QoS ポリシーの詳細はオペレーションマニュアルのセクション 7 *ACL and QoS "QoS ポリシー"*を参照してください。

VLAN マッピングを適用したインタフェースを経由し、かつ VLAN マッピング対象の VLAN インタフェースを経由する L3 通信は未サポートです。

VLAN マッピング対象の VLAN に VLAN インタフェースを作成および IP アドレスを設定する場合は、L3 通信の経路（送受信インタフェース）には VLAN マッピングを適用しないでください。

DHCP スヌーピングとの併用はできません。

14.3. VLANマッピングの設定作業リスト

⚠ 重要:

ネットワークのデバイスで適切な VLAN マッピング方法を使用してください。

作業リスト	補足
one-to-one VLANマッピングの設定	図 14-1 に示すワイヤリングクローゼットのスイッチでone-to-one VLANマッピングを設定します。
one-to-two VLANマッピングの設定	図 14-2 に示すように、カスタマネットワークからサービスプロバイダにトラフィックが通過するPE1、PE4でone-to-two VLANマッピングを設定します。
two-to-two VLANマッピングの設定	図 14-2 に示すようにSP2ネットワークのPE3、エッジデバイスでtwo-to-two VLANマッピングを設定します。

14.4. 設定要件

VLAN マッピングを設定する前に、もとの VLAN、変換される VLAN を作成してください。

14.5. one-to-one VLANマッピングの設定

I. one-to-one VLAN マッピング

異なるホームから同じサービスタイプのトラフィックを隔離するため、ワイヤリングクローゼット(図 14-1 を参照してください)のカスタマ側ポートで one-to-one VLAN マッピングを設定します。

II. 設定手順

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

操作	コマンド	補足
2. Layer 2 Ethernet interface view あるいは Layer 2 aggregate interface view に移行する	• Layer 2 Ethernet interface view に移行する: **interface** *interface-type interface-number* • Layer 2 aggregate interface view に移行する: **interface bridge-aggregation** *interface-number*	—
3. ポートのリンクタイプを設定する	**port link-type** { **hybrid** | **trunk** }	デフォルト：アクセス
4. ポートにもとの VLAN と変換される VLAN を割り当てる	• トランクポートにもとの VLAN と変換される VLAN を割り当てる：**port trunk permit vlan** *vlan-id-list* • ハイブリッドポートにもとの VLAN と変換される VLAN を割り当てる：**port hybrid vlan** *vlan-id-list* **tagged**	デフォルト：トランクポートはVLAN 1に割り当てられています。 ハイブリッドポートはリンクタイプがアクセスするときにポートが属するVLANのタグなしメンバです。
5. one-to-one VLAN マッピングを設定する	**vlan mapping** *vlan-id* **translated-vlan** *vlan-id*	デフォルト：設定なし

14.6. one-to-two VLANマッピングの設定

I. one-to-two VLAN マッピング

図 14-2 に示すように、カスタマトラフィックが PE1、PE4 の SP ネットワークに入るエッジデバイスの one-to-two VLAN を実行します。たとえば、one-to-two VLAN マッピングは SVLAN タグを各入力パケットに追加するエッジデバイスを有効にします。

II. 制限とガイドライン

同じ CVLAN からパケットに追加できる SVLAN タグは 1 つだけです。ポート上の異なる CVLAN パケットに異なる SVLAN タグを追加するには、ポートリンクタイプをハイブリッドに設定し、複数の one-to-two VLAN マッピングを設定します。

インタフェースの MTU はデフォルトで 1500byte です。VLAN タグがパケットに追加されると 4byte のパケット長が追加されます。one-to-two VLAN マッピングを設定するとき、サービスプロバイダネットワークのインタフェースの MTU を少なくとも 1504byte にすることを推奨します。

III. 設定手順

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

操作	コマンド	補足
2. Layer 2 Ethernet interface view あるいは Layer 2 aggregate interface view に移行する	• Layer 2 Ethernet interface view へ移行する: **interface** *interface-type interface-number* • Layer 2 aggregate interface view に移行する: **interface bridge-aggregation** *interface-number*	—
3. ポートのリンクタイプを設定する	**port link-type** { **hybrid** | **trunk** }	デフォルト：アクセス
4. CVLAN にポートを割り当てる	• トランクポートに CVLAN を割り当てる：**port trunk permit vlan** *vlan-id-list* • ハイブリッドポートに CVLAN を割り当てる：**port hybrid vlan** *vlan-id-list* { **hybrid** | **trunk** }	デフォルト：トランクポートはVLAN 1に割り当てられています。 ハイブリッドポートはリンクタイプがアクセスするときにポートが属するVLANのタグなしメンバです。
5. タグなしメンバとして変換された外部 VLAN にポートを割り当てる	• トランクポートの PVID として SVLAN を設定し、SVLAN にトランクポートを割り当てる：**port trunk pvid vlan** *vlan-id* **port trunk permit vlan** { *vlan-id-list* | **all** } • タグなしメンバとして SVLAN にハイブリッドポートを割り当てる：**port hybrid vlan** *vlan-id-list* **untagged**	—
6. one-to-two VLAN マッピングを設定する	**vlan mapping nest** { **range** *vlan-range-list* | **single** *vlan-id-list* } **nested-vlan** *vlan-id*	デフォルト：設定なし

14.7. two-to-two VLANマッピングの設定

I. two-to-two VLAN マッピング

two-to-two VLAN マッピングは、図 14-2 に示すような PE3 の 2 つの SP ネットワークに接続されたエッジデバイスのカスタマ側ポートで設定します。two-to-two VLAN マッピングは、レイヤ 2 で通信する異なる VLAN の 2 つのリモートサイトが、異なる VLAN 割り当て方式を使用する 2 つの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。

II. 設定手順

操作	コマンド	補足
1. system view.に移行する	**system-view**	ー
2. Layer 2 Ethernet interface view あるいは Layer 2 aggregate interface view に移行する	• Layer 2 Ethernet interface view へ移行する: **interface** *interface-type interface-number* • Layer 2 aggregate interface view に移行する: **interface bridge-aggregation** *interface-number*	ー
3. ポートのリンクタイプを設定する	**port link-type** { **hybrid** | **trunk** }	デフォルト：アクセス
4. もとの VLAN と変換される VLAN にポートを割り当てる	• トランクポートにもとの VLAN と変換される VLAN を割り当てる：**port trunk permit vlan** *vlan-id-list* • ハイブリッドポートにもとの VLAN と変換される VLAN を割り当てる：**port hybrid vlan** *vlan-id-list* **tagged**	デフォルト：トランクポートはVLAN 1に割り当てられています。 ハイブリッドポートはリンクタイプがアクセスするときにポートが属するVLANのタグなしメンバです。
5. two-to-two VLAN マッピングを設定する	**vlan mapping tunnel** *outer-vlan-id inner-vlan-id* **translated-vlan** *outer-vlan-id inner-vlan-id*	デフォルト：設定なし

14.8. VLAN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
VLANマッピング情報を表示する	**display vlan mapping** [**interface** *interface-type interface-number*]

14.9. VLANマッピングの設定例

14.9.1. one-to-one VLAN マッピングの設定例

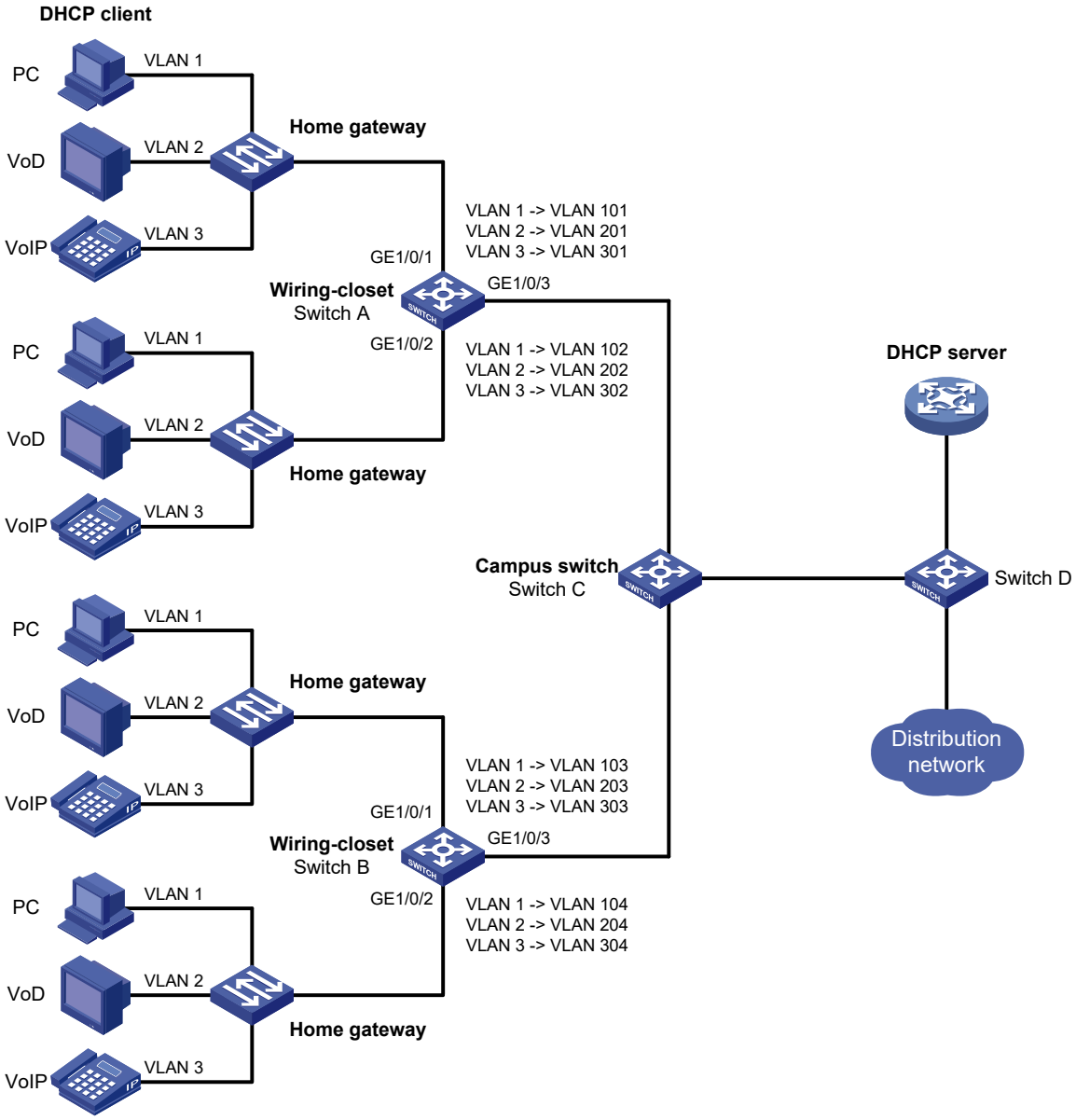
I. ネットワーク要件

図 14-7 に示すように、ネットワーク要件を記載します。

- 各ホームは、DHCP を通して IP アドレスを取得し、PC、VoD、VoIP サービスを提供します。
- ホームゲートウェイで、PC トラフィック用に VLAN1、VoD トラフィック用に VLAN2、VoIP サービス用に VLAN3 を割り当てます。

異なるホームから同じサービスタイプのトラフィックを隔離するため、ワイヤリングクローゼットスイッチで one-to-one VLAN マッピングを設定します。この機能は各ホームからのトラフィックの各タイプを 1 つの VLAN に割り当てます。

図 14-7 ネットワーク図



II. 設定手順

1. Switch A を設定します。

   # もとの VLAN を作成します。

   <SwitchA> system-view

   [SwitchA] vlan 2 to 3

   # 変換される VLAN を作成します。

   [SwitchA] vlan 101 to 102

   [SwitchA] vlan 201 to 202

   [SwitchA] vlan 301 to 302

   # トランクポートとしてカスタマ側ポート GigabitEthernet 1/0/1 を設定します。

<SwitchA> system-view

[SwitchA] interface gigabitethernet 1/0/1

[SwitchA-GigabitEthernet1/0/1] port link-type trunk

GigabitEthernet 1/0/1 を、もとの VLAN と変換される VLAN に割り当てます。

[SwitchA-GigabitEthernet1/0/1] port trunk permit vlan 1 2 3 101 201 301

それぞれ VLAN 1、VLAN 2、VLAN 3 に VLAN 101、VLAN 201、VLAN 301 をマッピングするように GigabitEthernet 1/0/1 で one-to-one VLAN マッピングを設定します。

[SwitchA-GigabitEthernet1/0/1] vlan mapping 1 translated-vlan 101

[SwitchA-GigabitEthernet1/0/1] vlan mapping 2 translated-vlan 201

[SwitchA-GigabitEthernet1/0/1] vlan mapping 3 translated-vlan 301

[SwitchA-GigabitEthernet1/0/1] quit

トランクポートとしてカスタマ側ポート GigabitEthernet 1/0/2 を設定します。

[SwitchA] interface gigabitethernet 1/0/2

[SwitchA-GigabitEthernet1/0/2] port link-type trunk

GigabitEthernet 1/0/2 を、もとの VLAN と変換される VLAN に割り当てます。

[SwitchA-GigabitEthernet1/0/2] port trunk permit vlan 1 2 3 102 202 302

それぞれ VLAN 1、VLAN 2、VLAN 3 に VLAN 102、VLAN 202、VLAN 302 をマッピングするように GigabitEthernet 1/0/2 で one-to-one VLAN マッピングを設定します。

[SwitchA-GigabitEthernet1/0/2] vlan mapping 1 translated-vlan 102

[SwitchA-GigabitEthernet1/0/2] vlan mapping 2 translated-vlan 202

[SwitchA-GigabitEthernet1/0/2] vlan mapping 3 translated-vlan 302

[SwitchA-GigabitEthernet1/0/2] quit

トランクポートとしてネットワーク側ポート GigabitEthernet 1/0/3 を設定します。

[SwitchA] interface gigabitethernet 1/0/3

[SwitchA-GigabitEthernet1/0/3] port link-type trunk

GigabitEthernet 1/0/3 を変換される VLAN に割り当てます。

[SwitchA-GigabitEthernet1/0/3] port trunk permit vlan 101 201 301 102 202 302

[SwitchA-GigabitEthernet1/0/3] quit

2. Switch A の設定と同様に Switch B を設定します。(詳細は省略します)

III. 設定の確認

Switch A のワイヤリングクローゼットスイッチの VLAN マッピング情報を表示します。

[SwitchA] display vlan mapping

```
Interface GigabitEthernet1/0/1:
  Outer VLAN    Inner VLAN    Translated Outer VLAN    Translated Inner VLAN
  1             N/A           101                      N/A
  2             N/A           201                      N/A
  3             N/A           301                      N/A
Interface GigabitEthernet1/0/2:
  Outer VLAN    Inner VLAN    Translated Outer VLAN    Translated Inner VLAN
  1             N/A           102                      N/A
```

```
2               N/A             202                 N/A
3               N/A             302                 N/A
```

14.9.2. one-to-two、two-to-two VLAN マッピングの設定例

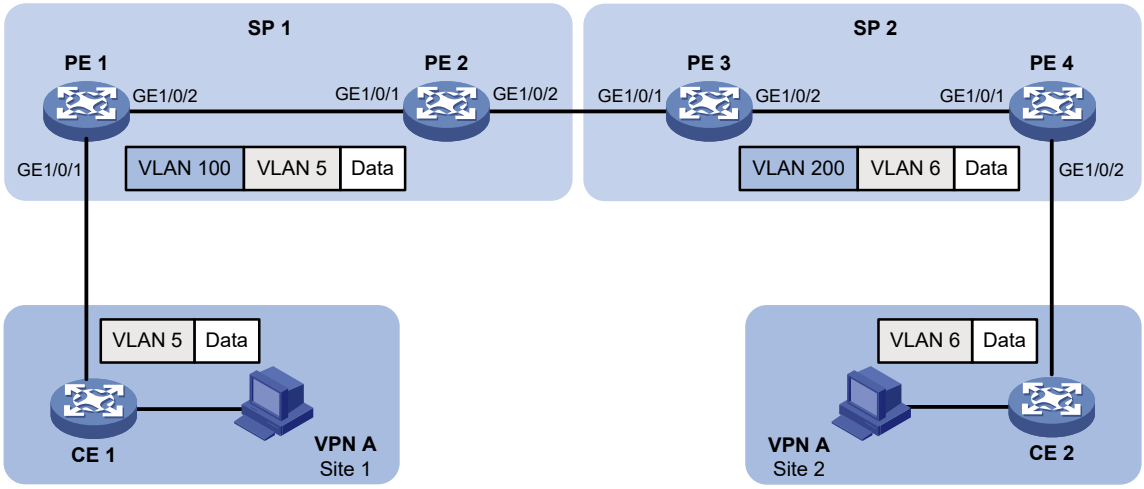
I. ネットワーク要件

図 14-8 に示すように、ネットワーク要件を記載します。

- 2 つの VPN A は、サイト 1 とサイト 2 はそれぞれ VLAN 5 と VLAN 6 があります。
- 2 つのサイトは､異なるサービスプロバイダ SP1､SP2 から異なる VPN アクセスを使用します。
- SP1 はサイト 1 とサイト 2 に VLAN 100 を割り当て、SP2 はサイト 1 とサイト 2 に VLAN 200 を割り当てます。

SP1 と SP2 ネットワーク間の通信を行うための 2 つの部門を有効にするため one-to-two、two-to-two VLAN マッピングを設定します。

図 14-8 ネットワーク図



II. 設定手順

1. PE 1 を設定します。

   # VLAN 5、VLAN 100 を作成します。

   <PE1> system-view

   [PE1] vlan 5

   [PE1-vlan5] quit

   [PE1] vlan 100

   [PE1-vlan100] quit

   # カスタマポート GigabitEthernet 1/0/1 に one-to-two VLAN を設定し、SVLAN タグ 100 を VLAN 5 からのパケットに追加します。

   [PE1] interface gigabitethernet 1/0/1

   [PE1-GigabitEthernet1/0/1] vlan mapping nest single 5 nested-vlan 100

   # ハイブリッドポートとして GigabitEthernet 1/0/1 を設定します。

[PE1-GigabitEthernet1/0/1] port link-type hybrid

タグ付けメンバとして VLAN 5 に GigabitEthernet 1/0/1 を割り当てます。

[PE1-GigabitEthernet1/0/1] port hybrid vlan 5 tagged

タグなしメンバとして VLAN 100 に GigabitEthernet 1/0/1 を割り当てます。

[PE1-GigabitEthernet1/0/1] port hybrid vlan 100 untagged

[PE1-GigabitEthernet1/0/1] quit

トランクポートとしてネットワーク側ポート GigabitEthernet 1/0/2 を設定します。

[PE1] interface gigabitethernet 1/0/2

[PE1-GigabitEthernet1/0/2] port link-type trunk

VLAN 100 に GigabitEthernet 1/0/2 を割り当てます。

[PE1-GigabitEthernet1/0/2] port trunk permit vlan 100

[PE1-GigabitEthernet1/0/2] quit

2. PE 2 を設定します。

VLAN 100 を作成します。

<PE2> system-view

[PE2] vlan 100

[PE2-vlan100] quit

トランクポートとして GigabitEthernet 1/0/1 を設定します。

[PE2] interface gigabitethernet 1/0/1

[PE2-GigabitEthernet1/0/1] port link-type trunk

VLAN 100 に GigabitEthernet 1/0/1 を割り当てます。

[PE2-GigabitEthernet1/0/1] port trunk permit vlan 100

[PE2-GigabitEthernet1/0/1] quit

トランクポートとして GigabitEthernet 1/0/2 を設定します。

[PE2] interface gigabitethernet 1/0/2

[PE2-GigabitEthernet1/0/2] port link-type trunk

VLAN 100 に GigabitEthernet 1/0/2 を割り当てます。

[PE2-GigabitEthernet1/0/2] port trunk permit vlan 100

[PE2-GigabitEthernet1/0/2] quit

3. PE 3 を設定します。

VLAN 5、VLAN 6、VLAN 100、VLAN 200 を作成します。

<PE3> system-view

[PE3] vlan 5 to 6

[PE3] vlan 100

[PE3-vlan100] quit

[PE3] vlan 200

[PE3-vlan200] quit

トランクポートとして GigabitEthernet 1/0/1 を設定します。

[PE3] interface gigabitethernet 1/0/1

[PE3-GigabitEthernet1/0/1] port link-type trunk

VLAN 100、VLAN 200 に GigabitEthernet 1/0/1 を割り当てます。

[PE3-GigabitEthernet1/0/1] port trunk permit vlan 100 200

SVLAN 100 と CVLAN5 を、SVLAN200、CVLAN6 にマッピングする GigabitEthernet 1/0/1 に two-to-two VLAN マッピングを設定します。

[PE3-GigabitEthernet1/0/1] vlan mapping tunnel 100 5 translated-vlan 200 6

[PE3-GigabitEthernet1/0/1] quit

トランクポートとして GigabitEthernet 1/0/2 を設定します。

[PE3] interface gigabitethernet 1/0/2

[PE3-GigabitEthernet1/0/2] port link-type trunk

VLAN 200 に GigabitEthernet 1/0/2 を割り当てます。

[PE3-GigabitEthernet1/0/2] port trunk permit vlan 200

[PE3-GigabitEthernet1/0/2] quit

4. PE 4 を設定します。

VLAN 6、VLAN 200 を作成します。

<PE4> system-view

[PE4] vlan 6

[PE4-vlan6] quit

[PE4] vlan 200

[PE4-vlan200] quit

トランクポートとしてネットワーク側ポート GigabitEthernet 1/0/1 を設定します。

[PE4] interface gigabitethernet 1/0/1

[PE4-GigabitEthernet1/0/1] port link-type trunk

GigabitEthernet 1/0/1 を VLAN 200 に割り当てます。

[PE4-GigabitEthernet1/0/1] port trunk permit vlan 200

[PE4-GigabitEthernet1/0/1] quit

ハイブリッドポートとしてカスタマ側ポート GigabitEthernet 1/0/2 を設定します。

[PE4] interface gigabitethernet 1/0/2

[PE4-GigabitEthernet1/0/2] port link-type hybrid

タグ付けメンバとして VLAN 6 に GigabitEthernet 1/0/2 を割り当てます。

[PE4-GigabitEthernet1/0/2] port hybrid vlan 6 tagged

タグなしメンバとして VLAN 200 に GigabitEthernet 1/0/2 を割り当てます。

[PE4-GigabitEthernet1/0/2] port hybrid vlan 200 untagged

カスタマ側ポート GigabitEthernet 1/0/2 の one-to-two VLAN マッピングを設定し、SVLAN タグ 200 を VLAN 6 からのパケットに追加します。

[PE4-GigabitEthernet1/0/2] vlan mapping nest single 6 nested-vlan 200

[PE4-GigabitEthernet1/0/2] quit

III. 設定の確認

PE 1 の VLAN マッピング情報を表示します。

[PE1] display vlan mapping

```
Interface GigabitEthernet1/0/1:
  Outer VLAN    Inner VLAN    Translated Outer VLAN    Translated Inner VLAN
  5             N/A           100                      5
```

PE 3 の VLAN マッピング情報を表示します。

[PE3] display vlan mapping

```
Interface GigabitEthernet1/0/1:
  Outer VLAN    Inner VLAN    Translated Outer VLAN    Translated Inner VLAN
  100           5             200                      6
```

PE 4 の VLAN マッピング情報を表示します。

[PE4] display vlan mapping

```
Interface GigabitEthernet1/0/2:
  Outer VLAN    Inner VLAN    Translated Outer VLAN    Translated Inner VLAN
  6             N/A           200                      6
```

目次

このセクションのページは **3-x-x** です。

15 章 LLDP 15-1
15.1. 概要 15-1
15.1.1. LLDP エージェントとブリッジモード 15-1
15.1.2. LLDP フレームフォーマット 15-2
15.1.3. LLDPDU 15-4
15.1.4. TLV 15-4
15.1.5. 管理アドレス 15-7
15.1.6. LLDP 動作モード 15-8
15.1.7. LLDP フレームの送受信 15-8
15.1.8. プロトコルと標準 15-8
15.2. 制限とガイドライン 15-9
15.3. LLDP 設定作業リスト 15-9
15.4. LLDP の有効化 15-10
15.5. LLDP 動作モードの設定 15-10
15.6. LLDP 再初期化遅延時間の設定 15-11
15.7. アドバタイズ可能な TLV の設定 15-11
15.8. 管理アドレス TLV の設定 15-14
15.9. LLDP フレームのカプセル化フォーマットの設定 15-15
15.10. LLDP フレーム転送パラメータの設定 15-15
15.11. Enabling LLDP ポーリングの有効化 15-16
15.12. CDP 互換モードの設定 15-17
15.13. LLDP トラップ、LLDP-MED トラップの設定 15-18
15.14. LLDP の表示と維持 15-19
15.15. LLDP の設定例 15-20
15.15.1. LLDP の基本的な設定例 15-20
15.15.2. CDP 互換モードの設定例 15-24

15章 LLDP

15.1. 概要

LLDP（Link Layer Discovery Protocol）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、設定を交換できるようにするスタンダードリンクレイヤプロトコルです。

LLDP では、装置は LLDPDU(LLDP データユニット)にある TLV(タイプ、長さ、値)形式のローカル装置情報を、直接接続された装置に送信します。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、セクション 10 *システム管理 オペレーションマニュアル*の”*SNMP*”を参照してください。

以下に LLDP を通してアドバタイズすることができる情報を示します。

- システム機能
- 管理 IP アドレス
- 装置 ID
- ポート ID

15.1.1. LLDP エージェントとブリッジモード

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。

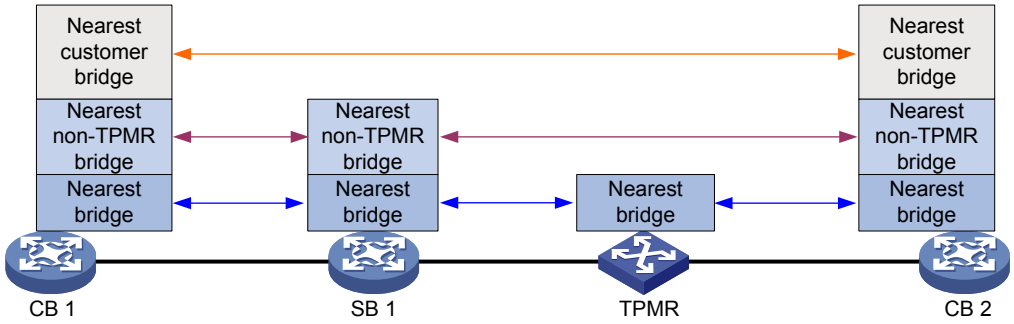
- Nearest bridge エージェント
- Nearest customer bridge エージェント
- Nearest non-TPMR bridge エージェント

  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 15-1 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持ちます。

図 15-1 LLDP 隣接関係



サポートされる LLDP エージェントのタイプは、LLDP が動作するブリッジモードによって異なります。LLDP は、カスタマブリッジ(CB)とサービスブリッジ(SB)のブリッジモードをサポートしています。

- **カスタマブリッジモード**－LLDP は最も近いブリッジエージェント、最も近い non-TPMR ブリッジエージェント、および最も近いカスタマブリッジエージェントをサポートします。 LLDP は、これらのエージェントの宛先 MAC アドレスを持つ LLDP フレームを処理し、VLAN 内の他の宛先 MAC アドレスで LLDP フレームを透過的に送信します。
- **サービスブリッジモード**－LLDP は、最も近いブリッジエージェントと最も近い非 TPMR ブリッジエージェントをサポートします。 LLDP は、これらのエージェントの宛先 MAC アドレスを持つ LLDP フレームを処理し、VLAN 内の他の宛先 MAC アドレスで LLDP フレームを透過的に送信します。

15.1.2. 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（Subnetwork Access Protocol）フレームでカプセル化されています。

I. Ethernet II にカプセル化した LLDP フレーム

図 15-2 Ethernet II にカプセル化した LLDP フレーム

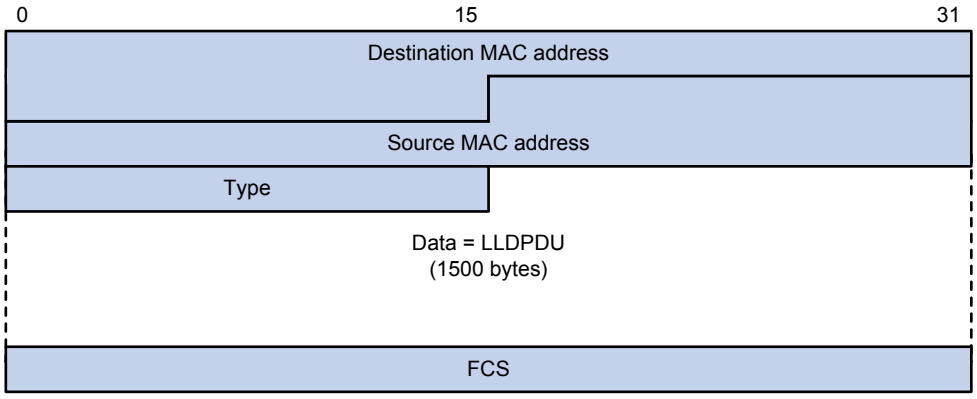


表 15-1 Ethernet II にカプセル化した LLDP フレームフィールド

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。

フィールド	説明
	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の異なるエージェントタイプによって送受信されたLLDPフレームを区別するのに役立ちます。宛先MACアドレスは以下のマルチキャストMACアドレスの1つに固定されます。 • LLDP フレーム 0x0180-C200-000E は nearest bridge 向けです。 • LLDP フレーム 0x0180-C200-0000 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。
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。

II. SNAP にカプセル化した LLDP フレーム

図 15-3 SNAP にカプセル化した LLDP フレーム

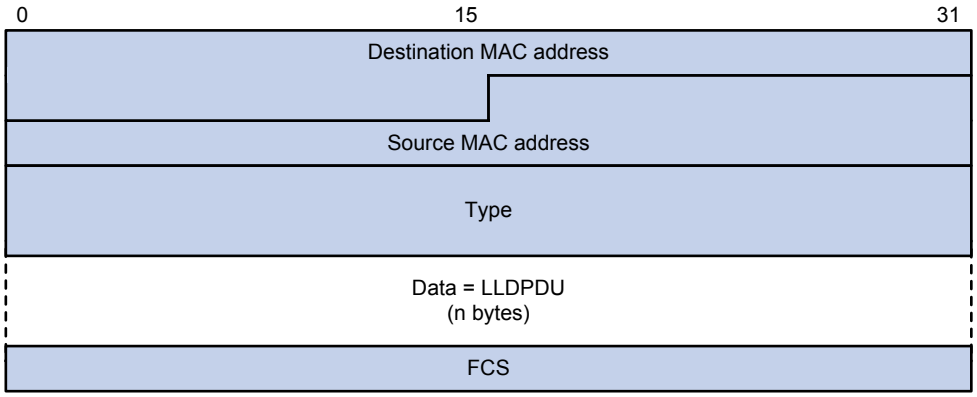


表 15-2 SNAP にカプセル化した LLDP フレームフィールド

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。

フィールド	説明
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。

15.1.3. 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 15-4 LLDPDU カプセルフォーマット

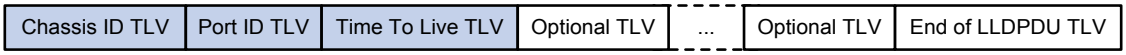


図 15-4 に示すように各 LLDPDU に、Chassis ID TLV、Port ID TLV、Time to Live TLV の必須の TLV から開始します。 必須 TLV には、最大 29 のオプションの TLV が続きます。

15.1.4. 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。

I. 基本的な管理 TLV

表 15-3 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 15-3 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。	

タイプ	説明	補足
End of LLDPDU	LLDPDUのTLVシーケンスの終端をマーキングします。	オプション
Port Description	送信するポートの説明を指定します。	
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 • インタフェース番号、アドレスに関連した OID	

II. IEEE 802.1 組織指定 TLV

表 15-4 に IEEE 802.1 組織指定 TLV タイプを示します。装置は protocol identity TLV および VID usage digest TLV を受信できますが、これらの TLV を送信することはできません。

表 15-4 IEEE 802.1 組織指定 TLV

タイプ	説明
Port VLAN ID (PVID)	ポートのVLAN識別子(PVID) を指定します。
Port And Protocol VLAN ID (PPVID)	装置がプロトコルVLANをサポートしているかどうかを示します。サポートしている場合、プロトコルのVLAN IDです。
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-S5300G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。
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。もし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。

タイプ	説明
QCN	Quantized Congestion Notificationです。 🕮 メモ： QX-S5300GシリーズはQCN TLVをサポートしていません。

III. IEEE 802.3 組織指定 TLV

表 15-5 に IEEE 802.3 組織指定 TLV タイプを示します。

Power Stateful Control TLV は IEEE P802.3at D1.0 で定義されていますが、QX-S5300G シリーズは Power Stateful Control TLV をサポートしていません。Power Stateful Control TLV を受信したのち、送信のみを行います。

表 15-5 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。 • ポートクラス(PSE あるいは PD) • 電源供給モード • PSE 電源供給のサポート状況 • PSE 電源供給の有効/無効状態 • ツイストペアの選択の制御/不制御 • 電源供給タイプ • 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 の電源供給モード • PSE/PD の優先度 • PSE/PD の電力
Energy-Efficient Ethernet	EEE（Energy Efficient Ethernet）を示します。

IV. LLDP-MED TLV

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 15-6 に LLDP-MED TLV を示します。

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。

表 15-6 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。

15.1.5. 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。

15.1.6. 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** – このモードの LLDP エージェントは LLDP フレームの送信、受信を行うことができます。
- **Tx モード** – このモードの LLDP エージェントは LLDP フレームの送信のみを行うことができます。
- **Rx モード** – このモードの LLDP エージェントは LLDP フレームの受信のみを行うことができます。
- **Disable モード** – このモードの LLDP エージェントは 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別の動作モードに変更されるたびに LLDP は初期化されます。LLDP エージェントの動作モードが別の動作モードへ変更したとき、設定可能な再初期化遅延時間を設定することで 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。

15.1.7. LLDP フレームの送受信

I. 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ときに、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 LLDP フレームを制限するためトークバケットメカニズムを使用します。トークンバケットメカニズムの詳細はセクション 7 *ACL and QoS オペレーションマニュアル*の”*トラフィックポリシング、GTS、レートリミット*”を参照してください。

LLDPは自動的に以下のいずれかのケースを用いて早急に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します。
- 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 に変更したときに早急に LLDP フレームを送信します。

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。

II. 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。LLDP フレームでアドバタイズされた Time To Live TLV の TTL が 0 になったとき、情報はすぐにエージアウトします。

15.1.8. 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*

15.2. 制限とガイドライン

LLDP を設定するとき、以下の制限とガイドラインに従ってください。

- 一部の LLDP の設定は、異なる interface view で有効です。（表 15-7 を参照してください。）

表 15-7 異なる view での LLDP の設定のサポート

操作	サポート view
LLDPの有効化	Layer 2 Ethernet interface view Management Ethernet interface view Layer 2 aggregate interface view IRF physical interface view
LLDP動作モードの設定	
アドバタイズ可能なTLVの設定	
管理アドレスTLVのアドバタイズの設定	
LLDPフレームのカプセル化フォーマットの設定	
LLDPポーリングの有効化	
LLDPトラップ、LLDP-MEDトラップの設定	

- IRF 物理インタフェースで LLDP を設定して、IRF 物理リンクの接続とリンクステータスを監視できます。 LLDP 対応の IRF 物理インタフェースは、nearest bridge エージェントのみをサポートします。

15.3. LLDP設定作業リスト

作業リスト
(必須設定項目) LLDPの有効化
(必須設定項目) LLDP動作モードの設定
(オプション設定項目) LLDP再初期化遅延時間の設定
(オプション設定項目) LLDPパケット関連の設定 • (オプション設定項目) アドバタイズ可能な TLV の設定 • 管理アドレス TLV のアドバタイズの設定 • LLDP フレームのカプセル化フォーマットの設定 • LLDP フレーム転送パラメータの設定
(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ポーリングの有効化
(オプション設定項目) LLDPトラップ、LLDP-MEDトラップの設定

15.4. LLDPの有効化

I. 制限とガイドライン

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。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. グローバルで LLDP を有効化する	**lldp global enable**	デフォルト：無効
3. interface view に移行する	**interface** *interface-type interface-number*	—
4. (オプション設定項目) LLDP を有効にする	**lldp enable**	デフォルト：有効

15.5. 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**	—
2. 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/management Ethernet interface view での設定: **lldp** [**agent nearest-customer**] **admin-status** { **disable** | **rx** | **tx** | **txrx** } • Layer 2 aggregate interface view での設定: **lldp agent nearest-customer admin-status** { **disable** | **rx** | **tx** | **txrx** } • IRF physical interface view での設定: **lldp 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。 IRF physical 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。

15.6. LLDP再初期化遅延時間の設定

I. LLDP 再初期化遅延時間

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。LLDP 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することを防ぐことができます。

II. 設定手順

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

15.7. 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. interface view に移行する	**interface** *interface-type interface-number*	—

操作	コマンド	補足
3. LLDPDU TLV を設定する(Layer 2 Ethernet interface view)	• **lldp tv-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** | **protocol-vlan-id** [*vlan-id*] | **vlan-name** [*vlan-id*] | **management-vid** [*mvlan-id*] } | **dot3-tlv** { **all** | **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** } }	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(management Ethernet interface view)	• **lldp tlv-enable** { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [*ip-address*] } | **dot1-tlv** { **all** | **link-aggregation** } | **dot3-tlv** { **all** | **mac-physic** | **max-frame-size** | **power** } | **med-tlv** { **all** | **capability** | **inventory** | **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** | **link-aggregation** } }	デフォルト： • Nearest bridge エージェントは network policy TLV を除いて LLDP TLV のすべてのタイプ(802.1 組織指定 TLV)を送信します。 • Nearest customer bridge エージェントは basic TLV、IEEE802.1 組織指定 TLV(link aggregation TLV のみ)を送信します。 • Nearest bridge エージェントは LLDP TLV のすべてのタイプ(802.3 組織指定 TLV)を送信します。
5. 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** { **protocol-vlan-id** [*vlan-id*] | **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(port VLAN ID TLV、protocol VLAN ID 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。
6. LLDPDU TLV を設定する(IRF physical interface view)	**lldp tlv-enable basic-tlv** { **port-description** | **system-capability** | **system-description** | **system-name** }	• Nearest bridge エージェントは basic TLV のすべてのタイプを送信します。 • 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。

15.8. 管理アドレスTLVの設定

I. 管理アドレス TLV

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。

隣接装置が管理アドレスを string 形式でエンコードする場合は、管理アドレスのエンコード形式を接続ポート上の string に設定します。 これにより、隣接装置との正常な通信が保証されます。

装置は、インタフェースに対する管理アドレス TLV のアドバタイズ設定を次の順序で選択します。

1. **management-address-tlv** パラメータを使用した **lldp tlv-enable** コマンドによって設定されたインタフェースベースの設定
2. インタフェースのデフォルト設定
   - デフォルトで nearest bridge エージェントと nearest customer bridge エージェントは管理アドレス TLV をアドバタイズします。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. 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. 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/management Ethernet interface view での設定: **lldp** [**agent nearest-customer**] **tlv-enable basic-tlv management-address-tlv** [*ip-address*] • Layer 2 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** • Layer 2 aggregate interface view での設定: **lldp agent nearest-customer management-address-format string**	デフォルト：数値形式

15.9. LLDPフレームのカプセル化フォーマットの設定

I. LLDP フレームのカプセル化フォーマットの設定

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。

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. SNAP に LLDPDU のカプセル化フォーマットを設定する	• Layer 2/management Ethernet interface view での設定: **lldp** [**agent nearest-customer**] **encapsulation snap** • Layer 2 aggregate interface view での設定: **lldp agent nearest-customer encapsulation snap** • IRF physical interface view での設定: **lldp encapsulation snap**	デフォルト： Ethernet II

15.10. LLDPフレーム転送パラメータの設定

I. LLDP フレーム転送パラメータの設定

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めて、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 x 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。

II. 設定手順

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

15.11. Enabling LLDPポーリングの有効化

I. LLDP ポーリング

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。

II. 設定手順

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. LLDP ポーリングの有効化を設定する	• Layer 2/management Ethernet interface view での設定: **lldp** [**agent nearest-customer**] **check-change-interval** *interval* • Layer 2 aggregate interface view での設定: **lldp agent nearest-customer check-change-interval** *interval* • IRF physical interface view での設定: **lldp check-change-interval** *interval*	デフォルト：無効

15.12. CDP互換モードの設定

I. CDP 互換モード

装置が、LLDP よりも CDP のみをサポートした Cisco 製品に接続されている場合、直接接続された製品の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、認識するために LLDP を使用します。直接接続された装置に 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。もし許可された 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、Chapter 3 *Layer 2 - LAN Switching Command References* の”*LLDP commands*”を参照してください。

装置を Cisco IP phone で動作させる場合、CDP 互換モードを有効にする必要があります。

LLDP が有効な装置が 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 IP phone の要求に応答しません。その結果、Cisco IP phone 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。装置はトラフィックの他のタイプから音声トラフィックを区別することができません。

CDP の互換モードは、Cisco IP phone からの CDP パケットを受信し、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。voice VLAN の設定の TLV に従い、IP phone 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 の詳細はセクション 3 *アクセス オペレーションマニュアル*の”*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持つ Cisco IP Phone に接続されている場合、ホストは Cisco IP Phone を介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すると、IP Phone は装置に CDP パケットを送信し、装置がユーザをログアウトできるようにします。

CDP 互換モードは以下のモードのどちらかで動作します。

- **TxRx**– CDP パケットは送受信されます。
- **Disable**–CDP パケットは送受信されません。

II. 制限とガイドライン

LLDP で CDP 互換モードの設定を行う場合、以下の制限とガイドラインに従ってください。

- 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。

a. グローバルで CDP 互換モードを有効にします。

b. 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 phone 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。

III. 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。

IV. 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/management 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

15.13. LLDPトラップ、LLDP-MEDトラップの設定

I. LLDP トラップ、LLDP-MED トラップ

LLDP トラップあるいは LLDP-MED 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とき、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。

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*	—

操作	コマンド	補足
3. LLDP トラップの送信を有効にする	• Layer 2/management Ethernet interface view での設定: **lldp** [**agent nearest-customer**] **notification remote-change enable** • Layer 2 aggregate interface view での設定: **lldp agent nearest-customer notification remote-change enable** • IRF physical interface view での設定: **lldp notification remote-change enable**	デフォルト：無効
4. system view に戻る	**quit**	ー
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

15.14. 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*] [**agent** { **nearest-bridge** | **nearest-customer** }] [**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*] [**agent** { **nearest-bridge** | **nearest-customer** | **nearest-nontpmr** }]]
ポートのLLDPのステータスを表示する	**display lldp status** [**interface** *interface-type interface-number*] [**agent** { **nearest-bridge** | **nearest-customer** }]
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*] [**agent** { **nearest-bridge** | **nearest-customer** }]

15.15. LLDPの設定例

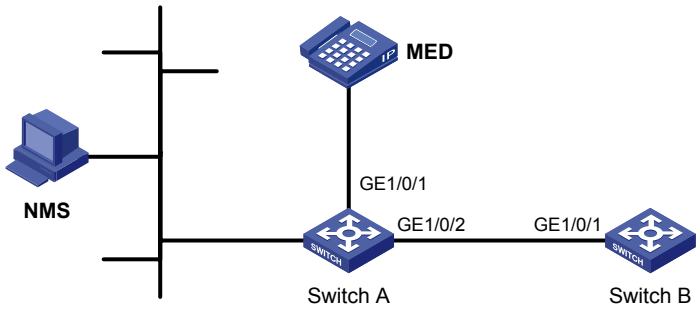
15.15.1. LLDP の基本的な設定例

I. ネットワーク要件

図 15-5 で示すように、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 15-5 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 gigabitethernet1/2

   [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 credit max            : 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 credit max            : 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
```

15.15.2. CDP 互換モードの設定例

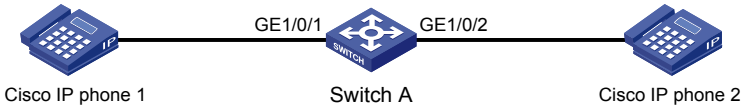
I. ネットワーク要件

図 15-6 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 IP phone に接続されています。

Switch A で voice VLAN 2 を設定します。Cisco IP phone 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 15-6 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 互換モードを設定します。

   [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 phone を検出します。
- IP phone の情報を取得します。

[SwitchA] display lldp neighbor-information

```
CDP neighbor-information of port 1[GigabitEthernet1/0/1]:
LLDP agent nearest-bridge:
 CDP neighbor index  : 1
 Chassis ID          : SEP00141CBCDBFE
 Port ID             : Port 1

CDP neighbor-information of port 2[GigabitEthernet1/0/2]:
LLDP agent nearest-bridge:
 CDP neighbor index  : 2
 Chassis ID          : SEP00141CBCDBFF
 Port ID             : Port 1
```

目次

このセクションのページは **3-x-x** です。

16 章 L2PT……16-1
16.1. 概要……16-1
16.1.1. L2PT アプリケーションシナリオ……16-1
16.1.2. サポートプロトコル……16-2
16.1.3. L2PT 動作メカニズム……16-2
16.2. L2PT 設定作業リスト……16-3
16.3. L2PT の有効化……16-4
16.3.1. 制限とガイドライン……16-4
16.3.2. Layer 2 Ethernet interface view のプロトコルでの L2PT の有効化……16-4
16.3.3. aggregate interface view のプロトコルでの L2PT の有効化……16-5
16.4. 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……16-5
16.5. L2PT の表示と維持……16-6
16.6. L2PT の設定例……16-6
16.6.1. STP での L2PT の設定例……16-6
16.6.2. LACP での L2TP の設定……16-7

16章 L2PT

16.1. 概要

L2PT（Layer 2 Protocol Tunneling）は地理的に分散されているカスタマネットワークがサービスプロバイダネットワークを経由してレイヤ 2 プロトコルパケットを送信あるいは廃棄します。

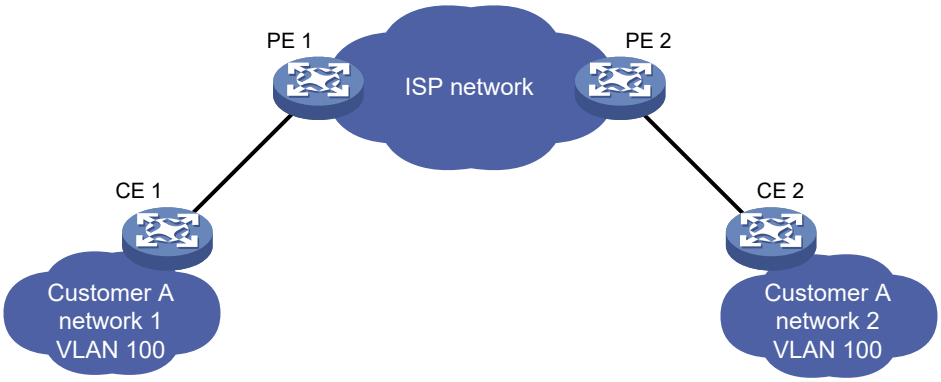
16.1.1. L2PT アプリケーションシナリオ

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 16-1 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 とネットワークに分割されています。Customer A ネットアークでレイヤ 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 16-1 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隔離します。

16.1.2. サポートプロトコル

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。

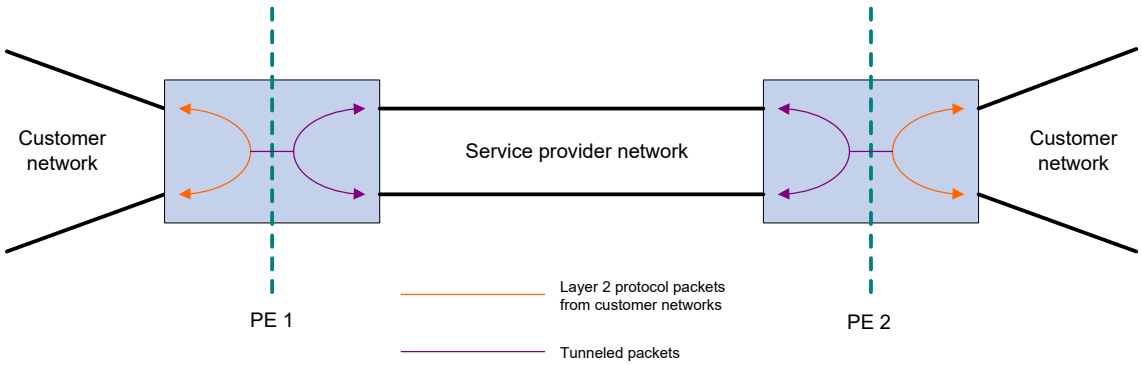
- CDP
- DLDP
- EOAM
- GVRP
- LACP
- LLDP
- MVRP
- PAgP
- PVST
- STP（STP、RSTP、MSTP を含みます）
- UDLD
- VTP

16.1.3. L2PT 動作メカニズム

図 16-2 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とき、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とき、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 16-2 L2PT 動作メカニズム

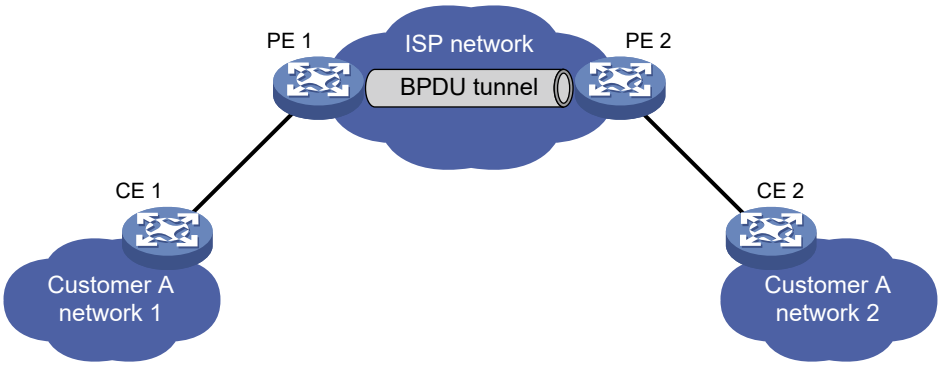


たとえば、図 16-3 に示すように PE1 はネットワーク 1 からネットワーク 2 への TP パケット（BPDU）を受信します。CE はカスタマネットワークの Edge 装置です。PE はサービスプロバイダネットワークの Edge 装置です。L2PT は以下のようにパケットを処理します。

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（デフォルトで 010f-e200-0003 です）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 16-3 L2PT ネットワーク図



16.2. L2PT設定作業リスト

作業リスト
（必須設定項目）L2PTの有効化 この機能はカスタマ側のポートにのみ設定可能です。
（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

16.3. L2PTの有効化

16.3.1. 制限とガイドライン

- 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。
  - 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。
- サービスループバックグループに加入しているポートで L2PT を有効にしないでください。ポートがグループに加入したのち、すべての設定が削除されます。

16.3.2. Layer 2 Ethernet interface view のプロトコルでの L2PT の有効化

I. 制限とガイドライン

LACP、EOAM はポイントーポイントの転送が必要です。LACP あるいは EOAM の L2PT を有効にした場合、L2PT はカスタマ側のポートに LACP あるいは EOAM パケットをマルチキャストします。その結果、2 つの CE 間の転送はポイントーポイントの転送ではありません。LACP パケットあるいは EOAM パケットのポイントーポイントの転送を行うため、VLAN などのほかの機能を設定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	**interface** *interface-type interface-number*	—
3. プロトコルの L2PT を有効にする	**l2protocol** { **cdp** | **dldp** | **eoam** | **gvrp** | **lacp** | **lldp** | **mvrp** | **pagp** | **pvst** | **stp** | **udld** | **vtp** } **tunnel dot1q**	デフォルト：無効

16.3.3. aggregate interface view のプロトコルでの L2PT の有効化

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-type interface-number*	—
3. プロトコルの L2PT を有効にする	**l2protocol** { `cdp` | `lacp` | `lldp` | **gvrp** | **mvrp** | `pagp` | **pvst** | **stp** | `udld` | **vtp** } **tunnel dot1q**	デフォルト：無効

MEMO:

cdp , **lacp** , **lldp** , **pagp** , **udld** オプションは、Version 7.2.23 を含むそれ以降のバージョンでサポートしています。
ただし、Version 7.3.21 では、上記オプションは未サポートです。

16.4. 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. トンネルパケットの宛先マルチキャスト MAC アドレス

有効なマルチキャスト 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止することができます。

III. 設定手順

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

16.5. 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*]

16.6. L2PTの設定例

16.6.1. STP での L2PT の設定例

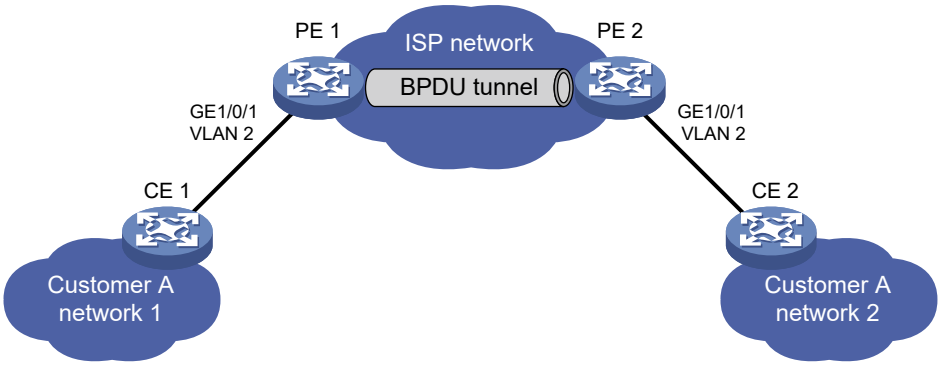
I. ネットワーク要件

図 16-4 に示すように、CE1 の MAC アドレスを f474-8802-5800、CE2 の MAC アドレスを f474-8802-5802 に設定します。Customer A ネットワークでは MSTP が有効です。デフォルトの 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ます。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 16-4 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 L2TP 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
```

16.6.2. LACP での L2TP の設定

I. ネットワーク要件

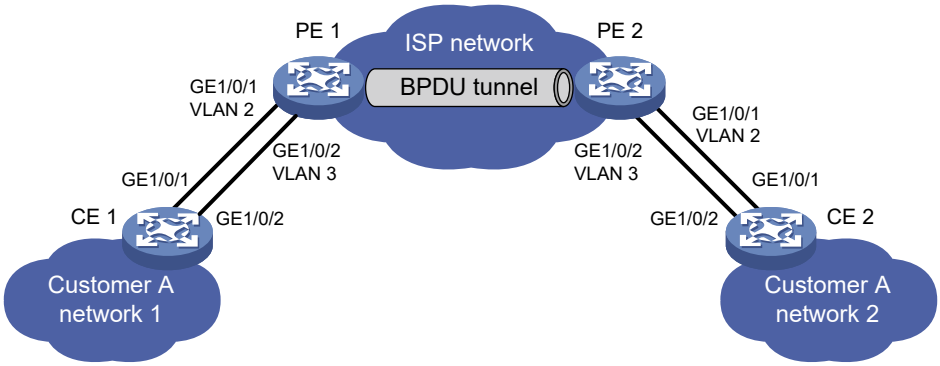
図 16-5 に示すように、CE1 の MAC アドレスを 0001-0000-0000、CE2 の MAC アドレスを 0004-0000-0000 に設定します。

以下の処理を行います。

- CE1、CE2 でリンクアグリゲーションを設定します。
- CE1 で GigabitEthernet 1/0/1 と GigabitEthernet 1/0/2 をアグリゲートインタフェースに設定し、CE2 で GigabitEthernet 1/0/1 と GigabitEthernet 1/0/2 をアグリゲートインタフェースに設定します。

- サービスプロバイダネットワークを通して、リンクアグリゲーションを行うため、CE1 と CE2 で LACP の L2PT を有効にします

図 16-5 ネットワーク図



II. 要件の分析

ネットワーク要件に適合するため、以下の処理を行います。

- リンクアグリゲーションを正常に動作させるために、アグリゲーショングループの CE1 と CE2 間のポイントーポイントの転送を行うため PE で VLAN を設定してください。
  - GigabitEthernet 1/0/1 の PVID を VLAN 2 に設定してください。GigabitEthernet 1/0/2 の PVID を VLAN 3 に設定してください。
  - PE1 の設定と同様に PE2 を設定してください。
  - CE に接続されるポートをトランクポートに設定してください。
- カスタマネットワークの VLAN タグを保持するため PE1 と PE2 の両方の GigabitEthernet 1/0/1 と GigabitEthernet 1/0/2 で QinQ を有効にしてください。
- すべての VLAN からパケットを転送するため、サービスプロバイダネットワークのすべてのポートをトランクポートに設定してください。

III. 設定手順

1. CE1 を設定します。

   # ダイナミックアグリゲーションモードで動作させるため、アグリゲーショングループ Bridge-Aggregation 1 を設定します。

   <CE1> system-view

   [CE1] interface bridge-aggregation 1

   [CE1-Bridge-Aggregation1] port link-type access

   [CE1-Bridge-Aggregation1] link-aggregation mode dynamic

   [CE1-Bridge-Aggregation1] quit

   # GigabitEthernet 1/0/1、GigabitEthernet 1/0/2 を Bridge-Aggregation 1 に割り当てます。

   [CE1] interface gigabitethernet 1/0/1

   [CE1-GigabitEthernet1/0/1] port link-aggregation group 1

   [CE1-GigabitEthernet1/0/1] quit

   [CE1] interface gigabitethernet 1/0/2

   [CE1-GigabitEthernet1/0/2] port link-aggregation group 1

[CE1-GigabitEthernet1/0/2] quit

2. CE1 の設定と同様に CE2 を設定してください。（詳細は省略します。）
3. PE1 を設定します。

VLAN 2、VLAN 3 を作成します。

<PE1> system-view

[PE1] vlan 2

[PE1-vlan2] quit

[PE1] vlan 3

[PE1-vlan3] quit

GigabitEthernet 1/0/1 をトランクポートとして設定します。VLAN 2 に割り当て、PVID を VLAN 2 に設定します。

[PE1] interface gigabitethernet 1/0/1

[PE1-GigabitEthernet1/0/1] port link-mode bridge

[PE1-GigabitEthernet1/0/1] port link-type trunk

[PE1-GigabitEthernet1/0/1] port trunk permit vlan 2

[PE1-GigabitEthernet1/0/1] port trunk pvid vlan 2

GigabitEthernet 1/0/1 で QinQ を有効にします。

[PE1-GigabitEthernet1/0/1] qinq enable

GigabitEthernet 1/0/1 で LACP の L2PT を有効にします。

[PE1-GigabitEthernet1/0/1] l2protocol lacp tunnel dot1q

[PE1-GigabitEthernet1/0/1] quit

GigabitEthernet 1/0/2 をトランクポートとして設定します。VLAN 3 に割り当て、PVID を VLAN 3 に設定します。

[PE1] interface gigabitethernet 1/0/2

[PE1-GigabitEthernet1/0/2] port link-mode bridge

[PE1-GigabitEthernet1/0/2] port link-type trunk

[PE1-GigabitEthernet1/0/2] port trunk permit vlan 3

[PE1-GigabitEthernet1/0/2] port trunk pvid vlan 3

GigabitEthernet 1/0/2 で QinQ を有効にします。

[PE1-GigabitEthernet1/0/2] qinq enable

GigabitEthernet 1/0/2 で LACP の L2PT を有効にします。

[PE1-GigabitEthernet1/0/2] l2protocol lacp tunnel dot1q

[PE1-GigabitEthernet1/0/2] quit

4. PE1 の設定と同様に PE2 を設定してください。（詳細は省略します。）

Ⅳ. 設定の確認

CE1 と CE2 で正常にリンクアグリゲーションが設定されていることを確認します。

[CE1] display link-aggregation member-port

```
Flags: A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
```

```
       D -- Synchronization, E -- Collecting, F -- Distributing,
       G -- Defaulted, H -- Expired

GigabitEthernet1/0/1:
Aggregate Interface: Bridge-Aggregation1
Local:
    Port Number: 3
    Port Priority: 32768
    Oper-Key: 1
    Flag: {ACDEF}
Remote:
    System ID: 0x8000, 0004-0000-0000
    Port Number: 3
    Port Priority: 32768
    Oper-Key: 1
    Flag: {ACDEF}
Received LACP Packets: 23 packet(s)
Illegal: 0 packet(s)
Sent LACP Packets: 26 packet(s)

GigabitEthernet1/0/2:
Aggregate Interface: Bridge-Aggregation1
Local:
    Port Number: 4
    Port Priority: 32768
    Oper-Key: 1
    Flag: {ACDEF}
Remote:
    System ID: 0x8000, 0004-0000-0000
    Port Number: 4
    Port Priority: 32768
    Oper-Key: 1
    Flag: {ACDEF}
Received LACP Packets: 10 packet(s)
Illegal: 0 packet(s)
Sent LACP Packets: 13 packet(s)
[CE2] display link-aggregation member-port
Flags: A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
       D -- Synchronization, E -- Collecting, F -- Distributing,
       G -- Defaulted, H -- Expired

GigabitEthernet1/0/1:
Aggregate Interface: Bridge-Aggregation1
Local:
    Port Number: 3
    Port Priority: 32768
    Oper-Key: 1
```

```
    Flag: {ACDEF}
Remote:
    System ID: 0x8000, 0001-0000-0000
    Port Number: 3
    Port Priority: 32768
    Oper-Key: 1
    Flag: {ACDEF}
Received LACP Packets: 23 packet(s)
Illegal: 0 packet(s)
Sent LACP Packets: 26 packet(s)

GigabitEthernet1/0/2:
Aggregate Interface: Bridge-Aggregation1
Local:
    Port Number: 4
    Port Priority: 32768
    Oper-Key: 1
    Flag: {ACDEF}
Remote:
    System ID: 0x8000, 0001-0000-0000
    Port Number: 4
    Port Priority: 32768
    Oper-Key: 1
    Flag: {ACDEF}
Received LACP Packets: 10 packet(s)
Illegal: 0 packet(s)
Sent LACP Packets: 13 packet(s)
```

QX-S5300G シリーズ Ethernet スイッチ

オペレーションマニュアル

4. 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-Proxy ARP

04-ARP スヌーピング

05-IP アドレス

06-DHCP の概要

07-DHCP サーバ

08-DHCP リレー

09-DHCP クライアント

10-DHCP スヌーピング

11-BOOTP クライアント

12-DNS

13-IP フォワーディングの基本

14-IP パフォーマンスの最適化

15-UDP ヘルパー

16-IPv6 の基本

17-DHCPv6 の概要

18-HTTP リダイレクト

目次

このセクションのページは **4-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 エントリタイプ 1-3
1.2. ARP 設定作業リスト 1-4
1.3. スタティック ARP エントリの設定 1-4
1.3.1. ショートスタティック ARP エントリの設定 1-4
1.3.2. ロングスタティック ARP エントリの設定 1-5
1.3.3. マルチポート ARP エントリの設定 1-5
1.4. ダイナミック ARP エントリの設定 1-6
1.4.1. 装置で学習できるダイナミック ARP エントリの最大数の設定 1-6
1.4.2. 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 1-7
1.4.3. ダイナミック ARP エントリのエージングタイマの設定 1-7
1.4.4. ダイナミック ARP エントリチェックの有効化 1-8
1.5. ARP と MAC アドレスのコンシステンシーチェック機能の有効化 1-8
1.6. ARP ロギング機能の有効化 1-9
1.7. ARP の表示と維持 1-9
1.8. ARP 設定例 1-10
1.8.1. ロングスタティック ARP の設定例 1-10
1.8.2. ショートスタティック ARP エントリの設定例 1-11
1.8.3. マルチポート ARP エントリの設定例 1-12

1章 ARP

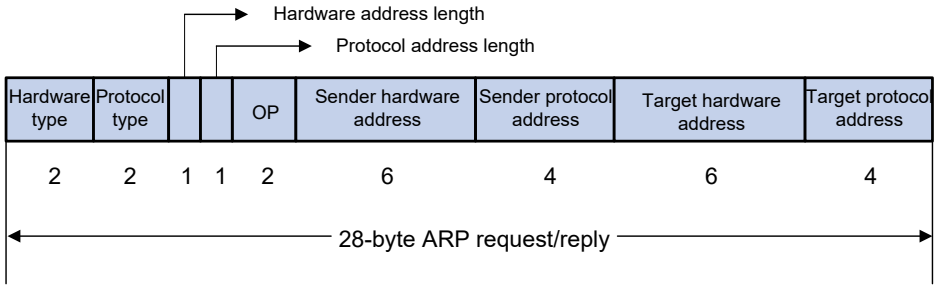
1.1. 概要

ARP（Address Resolution Protocol）とは、IP アドレスをもとに MAC アドレス(物理アドレス)情報を得ることができます。

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ます。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 and 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、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。

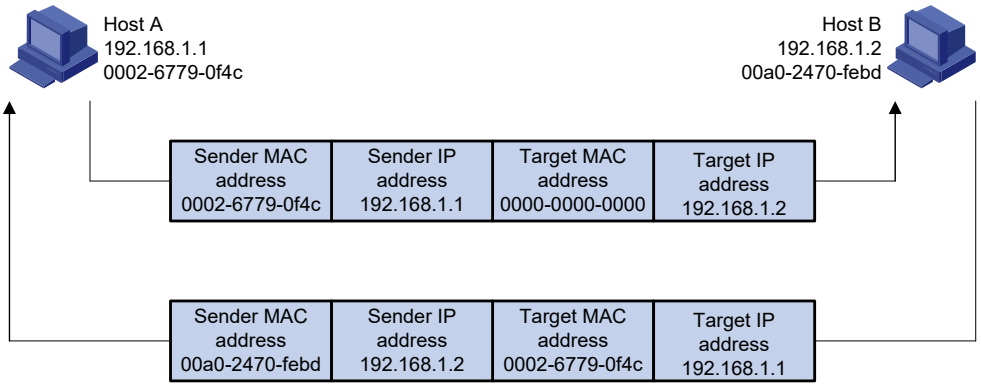
1.1.2. ARP 動作メカニズム

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。もし 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. もし 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。もし 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 エントリタイプ

ARP テーブルには、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、アップデートされます。エージングタイマが終了したとき、あるいは出力インタフェースがダウンしたとき、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、維持します。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 エントリによって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、スタティック ARP エントリで指定された 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 アドレスおよび以下の組み合わせから構成され、パケットを転送するのに直接使用されます。
  - VLAN と出力インタフェース
  - 入力インタフェースと出力インタフェース
- **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。

  出力インタフェースが VLAN インタフェースである場合、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。
- **マルチポート ARP エントリ**：IP アドレス、MAC アドレス、VLAN から構成されます。

  装置はパケット転送を行うマルチキャストあるいはマルチポートユニキャスト MAC アドレスエントリとして、同一の MAC アドレス、同一の VLAN ID を持つマルチポート ARP エントリを使用することができます。マルチポート ARP エントリは手動で設定します。マルチポート ARP エントリはエージアウトせず、ダイナミック ARP エントリによって上書きすることはできません。マルチキャスト MAC アドレスの詳細はセクション 6 *マルチキャスト オペレーションマニュアル*の”*マルチキャストの概要*”を参照してください。

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。

III. OpenFlow ARP エントリ

ARP は OpenFlow モジュールから学習することで OpenFlow ARP エントリを作成します。OpenFlow ARP エントリはエージアウトしません。またアップデートすることができません。OpenFlow ARP エントリはパケットを直接転送するためにしようされます。

IV. ルール ARP エントリ

ルール ARP エントリはパケットを直接転送するために使用することができます。ルール ARP エントリはエージアウトしません。またアップデートすることができません。スタティック ARP エントリによって上書きできます。

ARP は Portal モジュールによって学習したルール ARP エントリを作成します。

1.2. ARP設定作業リスト

作業リスト
（オプション設定項目）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 エントリの設定 • ロングスタティック ARP エントリの設定 • マルチポートスタティック ARP エントリの設定
（オプション設定項目）ダイナミックARPエントリの設定 • 装置で学習できるダイナミック ARP エントリの最大数の設定 • 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 • ダイナミック ARP エントリのエージングタイマの設定 • ダイナミック ARP チェックの有効化
（オプション設定項目）ARPロギング機能の有効化

1.3. 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ときに、適用されます。

1.3.1. ショートスタティック ARP エントリの設定

I. 制限とガイドライン

解決済みのショートスタティック ARP エントリは、特定のイベントで未解決になります。例えば解決済みの出力インタフェースがダウンしたあるいは、対応する VLAN、VLAN インタフェースが削除されたとき、未解決となります。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. 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*	—

1.3.2. ロングスタティック ARP エントリの設定

I. 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 エントリは以下のいずれかの状況で無効となります。

ロングスタティック ARP エントリは有効あるいは無効とすることができます。無効なロングスタティック ARP エントリはパケットの転送に使用することができません。ロングスタティック ARP エントリは以下の状態のとき、無効となります。

- 対応する VLAN インタフェースあるいは出力インタフェースがダウンしています。
- エントリの IP アドレスがローカル IP アドレスと衝突しています。
- インタフェースが同一サブネットの ARP エントリの IP アドレスを持っていません。

VLAN あるいは VLAN インタフェースが削除されたとき、VLAN のロングスタティック ARP エントリが削除されます。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. 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*]	—

1.3.3. マルチポート ARP エントリの設定

I. マルチポート ARP エントリ

マルチポート ARP エントリは IP アドレス、MAC アドレス、VLAN ID が含まれます。VLAN と出力インタフェースはマルチポートユニキャスト MAC アドレスエントリあるいはマルチキャスト MAC アドレスエントリによって指定されます。

マルチポート ARP エントリはダイナミック ARP エントリ、ショートスタティック ARP エントリ、あるいはロングスタティック ARP エントリに上書きすることができます。逆にショートスタティック ARP エントリ、あるいはロングスタティック ARP エントリはマルチポート ARP エントリに上書きすることができます。

II. 制限とガイドライン

パケット転送でマルチポート ARP エントリを適用させるためには、以下の対応を行う必要があります。

- マルチポートユニキャスト MAC アドレスエントリあるいはマルチキャスト MAC アドレスエントリが存在します。
- マルチポート ARP エントリの IP アドレスと VLAN インタフェースの IP アドレスは同一サブネット上に存在する必要があります。

III. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. マルチポートユニキャスト MAC アドレスエントリあるいはマルチキャスト MAC アドレスエントリを設定する	• マルチポートユニキャスト MAC アドレスエントリを設定する: **mac-address multiport** *mac-address* **interface** *interface-list* **vlan** *vlan-id* • 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*	**mac-address**コマンドの詳細はChapter 3 *Layer 2 - LAN Switching Command References*の” *MAC address table commands*”を参照してください。
3. マルチポート ARP エントリを設定する	**arp multiport** *ip-address mac-address vlan-id*	マルチポートARPエントリは同一のMACアドレス、同一のVLAN IDにする必要があります。

1.4. ダイナミックARPエントリの設定

1.4.1. 装置で学習できるダイナミック ARP エントリの最大数の設定

I. 装置で学習できるダイナミック ARP エントリの最大数

装置はダイナミックに ARP エントリを学習できます。多すぎる ARP エントリを保持しないように、装置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、装置は ARP エントリの学習を停止します。

既存のダイナミック ARP エントリ数が設定した値よりも少ない場合、装置はエージアウトしない限り、既存のダイナミックエントリを削除しません。**reset arp dynamic** コマンドでダイナミック ARP エントリを削除することができます。

II. 設定手順

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

操作	コマンド	補足
2. ダイナミック ARP エントリの最大数を設定する	**arp max-learning-number** *max-number* **slot** *slot-number*	デフォルト：7680 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。

1.4.2. 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

I. インタフェースで学習できる ARP エントリの最大数

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、インタフェースは 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ときのみ ARP エントリを学習します。

すべてのインタフェースのダイナミック ARP エントリの最大数は装置のダイナミック ARP エントリの最大数よりも少ない値にしてください。

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. 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：7680 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。

1.4.3. ダイナミック ARP エントリのエージングタイマの設定

I. ダイナミック ARP エントリのエージングタイマ

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。

II. 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. 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*	デフォルト：20分

1.4.4. ダイナミック ARP エントリチェックの有効化

I. ダイナミック ARP エントリチェック

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。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
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とMACアドレスのコンシステンシーチェック機能の有効化

I. ARP と MAC アドレスのコンシステンシーチェック機能について

パケットを受信するインタフェースが安定しないネットワークにおいて、ARP エントリの更新が即座に行われず、ARP と MAC アドレスの不一致が発生して正しいインタフェースに転送できなくなる可能性があります。この問題を回避するため、コンシステンシーチェック機能を有効にすることができます。ARP と MAC アドレスのインタフェースが異なる場合、ARP は ARP エントリが存在する VLAN に ARP リクエストを送信して、応答した ARP リプライを基に ARP エントリを更新します。通信パケットの受信ポートが頻繁に移動する環境では、コンシステンシーチェック機能を有効にすることを推奨します。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. コンシステンシーチェック機能を有効にする	**arp mac-interface-consistency check enable**	デフォルト：有効

1.6. ARPロギング機能の有効化

I. ARP ロギング機能

ARP が IP アドレスを正常に解決できないとき、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。ログ情報は管理者の問題個所の特定や解決の手助けとなります。装置は以下の ARP イベントのログを作成することができます。

- 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 アドレスは以下の IP アドレスのいずれでもありません。
  - 受信インタフェースの IP アドレス
  - VRRP グループの仮想 IP アドレス
- 受信した ARP エントリの送信元 IP アドレスが以下の IP アドレスの 1 つと重複しています。
  - 受信インタフェースの IP アドレス
  - VRRP グループの仮想 IP アドレス

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 の詳細はセクション 11 *システム管理 オペレーションマニュアル*の“*Information Center*”を参照してください。

II. 設定手順

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

1.7. 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、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** | **multiport** | **static**] [**slot** *slot-number*] | **vlan** *vlan-id* | **interface** *interface-type interface-number*] [**count** | **verbose**]
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マを表示する	**display arp timer aging**

操作	コマンド
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* | **multiport** | **slot** *slot-number* | **static** }

1.8. ARP設定例

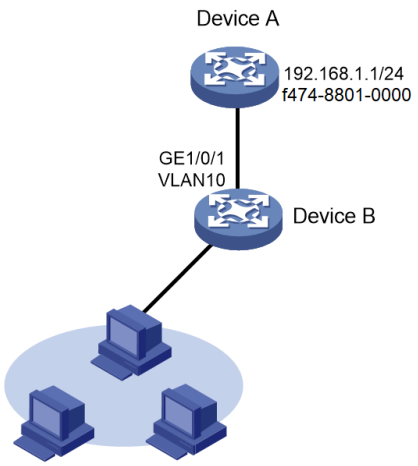
1.8.1. ロングスタティック ARP の設定例

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 8

[DeviceB-vlan-interface10] quit

IP アドレス 192.168.1.1 と MAC アドレス f474-8801-0000 のロングスタティック 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 のロングスタティック ARP エントリがあることを確認します。

[DeviceB] display arp static

```
  Type: S-Static    D-Dynamic    O-Openflow    R-Rule    M-Multiport  I-Invalid
IP address        MAC address     VID     Interface/Link ID      Aging Type
192.168.1.1       f474-8801-0000  10      GE1/0/1                N/A   S
```

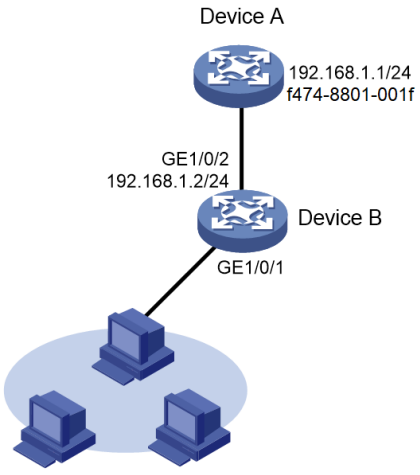
1.8.2. ショートスタティック ARP エントリの設定例

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、MAC アドレス f474-8801-001f のショートスタティック ARP エントリを設定します。

[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 エントリがあることを確認します。

[DeviceB] display arp static

```
  Type: S-Static   D-Dynamic   O-Openflow   R-Rule   M-Multiport  I-Invalid
IP address       MAC address     VID     Interface/Link ID      Aging Type
192.168.1.1      f474-8801-001f  N/A     N/A                    N/A   S
```

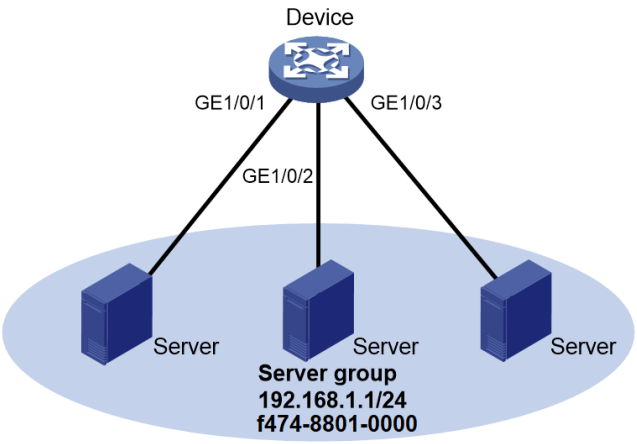
1.8.3. マルチポート ARP エントリの設定例

I. ネットワーク要件

図 1-5 に示すように Device は VLAN10 の GigabitEthernet 1/0/1～GigabitEthernet 1/0/3 を通して 3 つのサーバに接続します。サーバは IP アドレス 192.168.1.1/24、MAC アドレス f474-8801-0000 を共有します。

Device が 3 つのサーバに宛先 IP アドレス 192.168.1.1 に IP パケットを送信できるようにマルチポート ARP エントリを設定します。

図 1-5 ネットワーク図



II. 設定手順

VLAN 10 を作成します。

<Device> system-view

[Device] vlan 10

[Device-vlan10] quit

VLAN 10 に GigabitEthernet 1/0/1～GigabitEthernet 1/0/3 を割り当てます。

[Device] interface gigabitethernet 1/0/1

[Device-GigabitEthernet1/0/1] port access vlan 10

[Device-GigabitEthernet1/0/1] quit

[Device] interface gigabitethernet 1/0/2

[Device-GigabitEthernet1/0/2] port access vlan 10

[Device-GigabitEthernet1/0/2] quit

[Device] interface gigabitethernet 1/0/3

[Device-GigabitEthernet1/0/3] port access vlan 10

[Device-GigabitEthernet1/0/3] quit

VLAN インタフェース 10 を作成し、IP アドレスを指定します。

[Device] interface vlan-interface 10

[Device-vlan-interface10] ip address 192.168.1.2 24

[Device-vlan-interface10] quit

MAC アドレスが f474-8801-0000、出力インタフェースが VLAN10 の GigabitEthernet 1/0/1、GigabitEthernet 1/0/2、GigabitEthernet 1/0/3 のマルチポートユニキャスト MAC アドレスエントリを設定します。

[Device] mac-address multiport f474-8801-0000 interface gigabitethernet 1/0/1 to gigabitethernet 1/0/3 vlan 10

IP アドレス 192.168.1.1、MAC アドレス f474-8801-0000 のマルチポート ARP エントリを設定します。

[Device] arp multiport 192.168.1.1 f474-8801-0000 10

III. 設定の確認

Device が IP アドレス 192.168.1.1、MAC アドレス f474-8801-0000 のマルチポート ARP エントリがあることを確認します。

[Device] display arp

```
  Type: S-Static   D-Dynamic   O-Openflow   R-Rule   M-Multiport  I-Invalid
IP address       MAC address     VID     Interface/Link ID      Aging Type
192.168.1.1      f474-8801-0000  10      N/A                    N/A   M
```

目次

このセクションのページは **4-x-x** です。

2 章 Gratuitous ARP 2-1
2.1. 概要 2-1
2.1.1. IP アドレス重複 2-1
2.1.2. Gratuitous ARP パケットの学習 2-1
2.1.3. Gratuitous ARP パケットの送信間隔の設定 2-1
2.2. 設定作業リスト 2-2
2.3. IP アドレス重複通知の有効化 2-2
2.4. Gratuitous ARP パケットの学習機能の有効化 2-2
2.5. 定期的な Gratuitous ARP パケットの送信の有効化 2-3
2.6. 異なるサブネットからの ARP 要求に対する Gratuitous ARP パケットの送信の有効化 2-3
2.7. デバイスの MAC アドレス変更に対する gratuitous ARP パケット再送信の設定 2-4

2章 Gratuitous ARP

2.1. 概要

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。

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。もし 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。

2.1.1. IP アドレス重複

インタフェースで IP アドレスを取得するとき、装置はインタフェースが存在する VLAN に gratuitous ARP パケットをブロードキャストします。装置が ARP エントリを受信した場合、VLAN 内に別の装置の IP アドレスと重複しています。装置は重複していることをログメッセージとして表示し、IP アドレスを変更するように管理者に通知します。装置は重複している IP アドレスを使用しません。ARP エントリを受信しない場合、装置は IP アドレスを使用します。

2.1.2. 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。

2.1.3. 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とき、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。
- あいまいな dot1q あるいは QinQ termination が設定されている VLAN では装置の MAC アドレスをアップデートしてください。

2.2. 設定作業リスト

以下のすべての機能が無効であったとしても、Gratuitous ARP は IP アドレス重複検出機能を提供します。

作業リスト
（オプション設定項目）IPアドレス重複通知の有効化
（オプション設定項目）Gratuitous ARPパケットの学習機能の有効化
（オプション設定項目）定期的なGratuitous ARPパケットの送信の有効化
（オプション設定項目）異なるサブネットからのARP要求に対するGratuitous ARPパケットの送信の有効化

2.3. IPアドレス重複通知の有効化

I. IP アドレス重複通知の有効化

IP アドレスの重複を検出する際、装置は gratuitous ARP 要求を送信します。ARP 応答を受信したのち、装置はデフォルトでエラーメッセージの表示のみを行います。この機能を設定することで重複に関する ARP 応答を受信したのち、すぐにエラーメッセージを表示します。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. IP 重複通知を有効にする	**arp ip-conflict log prompt**	デフォルト：無効

2.4. Gratuitous ARPパケットの学習機能の有効化

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. 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

2.5. 定期的なGratuitous ARPパケットの送信の有効化

I. 制限とガイドライン

- 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、以下の条件に合っているときのみインタフェースで適用されます。
  - インタフェースのリンク状態がアップです。
  - インタフェースに 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。

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. 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** *milliseconds*]	デフォルト：無効

2.6. 異なるサブネットからのARP要求に対するGratuitous ARPパケットの送信の有効化

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

操作	コマンド	補足
2. 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

2.7. デバイスのMACアドレス変更に対するgratuitous ARPパケット再送信の設定

I. 制限とガイドライン

装置は、MAC アドレスの変更を他のデバイスに通知するために、Gratuitous ARP パケットを送信します。ただし、装置はデフォルトで 1 回だけ Gratuitous ARP パケットを送信するため、他の装置はパケットの受信に失敗する可能性があります。Gratuitous ARP パケットの再送信機能を設定して、他の装置がパケットを受信できるようにします。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. 装置の MAC アドレス変更のために、Gratuitous ARP パケットを再送信する時間と間隔を設定する。	**gratuitous-arp mac-change retransmit** *times* **interval** *seconds*	デフォルト：装置は1回だけMACアドレスの変更を通知するためにGratuitous ARP パケットを送信します。

目次

このセクションのページは **4-x-x** です。

3 章 Proxy ARP 3-1
3.1. 概要 3-1
3.2. 一般的な Proxy ARP の有効化 3-1
3.3. ローカル Proxy ARP の有効化 3-1
3.4. Proxy ARP の表示と維持 3-1
3.5. Proxy ARP 設定例 3-2
3.5.1. ARP 一般的な Proxy ARP の設定例 3-2

3章 Proxy ARP

3.1. 概要

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。

3.2. 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-type interface-number*	－
3. 一般的な Proxy ARP を有効にする	**proxy-arp enable**	デフォルト：無効

3.3. 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-type interface-number*	－
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

3.4. 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	**display proxy-arp** [**interface** *interface-type*

操作	コマンド
表示する	*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*]

3.5. Proxy ARP設定例

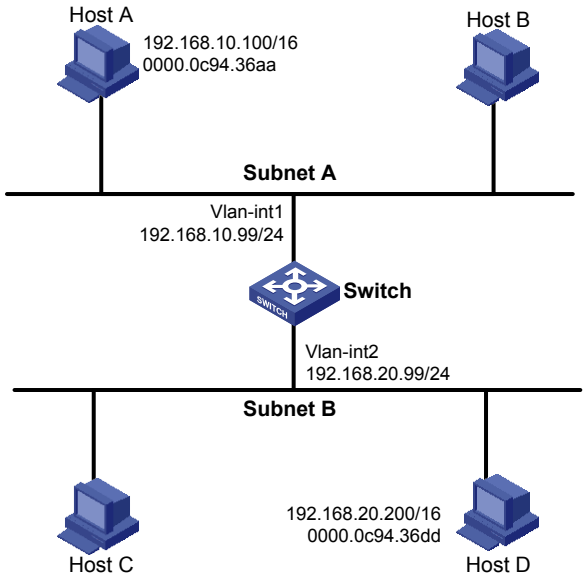
3.5.1. ARP 一般的な Proxy ARP の設定例

I. ネットワーク要件

図 3-1 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 VLAN 1、Host D は VLAN 2 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 3-1 ネットワーク図



II. 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.

III. 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 **4-x-x** です。

4 章 ARP スヌーピング 4-1
4.1. 概要 4-1
4.1.1. ARP snooping エントリの作成 4-1
4.1.2. ARP snooping エントリのエージング 4-1
4.1.3. ARP snooping の保護 4-1
4.2. ARP snooping の有効化 4-1
4.3. ARP snooping の表示と維持 4-1

4章 ARP スヌーピング

4.1. 概要

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。

4.1.1. ARP snooping エントリの作成

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。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。

4.1.2. ARP snooping エントリのエージング

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。

4.1.3. ARP snooping の保護

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、1 分後に削除されます。

4.2. ARP snoopingの有効化

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. ARP snooping を有効にする	**arp snooping enable**	デフォルト：無効

4.3. 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 ip** *ip-address* [**slot** *slot-number*]
ARP snoopingエントリを削除する	**reset arp snooping** [**ip** *ip-address* | **vlan** *vlan-id*]

目次

このセクションのページは **4-x-x** です。

5 章 IP アドレス 5-1
5.1. 概要 5-1
5.1.1. IP アドレスの説明とクラス 5-1
5.1.2. 特別な IP アドレス 5-2
5.1.3. サブネットとマスク 5-2
5.1.4. IP アドレスの割り当て 5-3
5.2. インタフェースへの IP アドレスの割り当て 5-3
5.3. IP アドレスの表示と維持 5-4
5.4. IP アドレスの設定例 5-4
5.4.1. 手動での IP アドレスの割り当て 5-4

5章 IP アドレス

5.1. 概要

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。

5.1.1. IP アドレスの説明とクラス

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。32 ビットの IP アドレスをわかりやすくするために、それぞれの長さを 4 オクテットのドット付きの 10 進数にします。先ほどの 32 ビットの 2 進数は、10.1.1.1 となります。

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 5-1 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 5-1 IP アドレスクラス

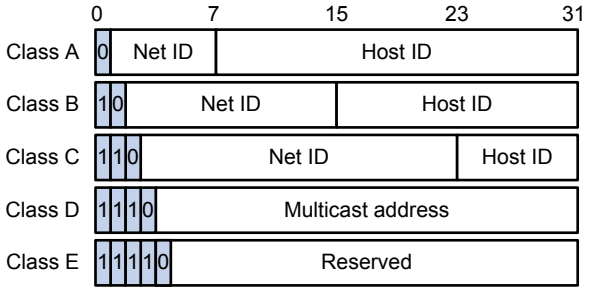


表 5-1 IP アドレスクラスと範囲

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	―
C	192.0.0.0 ～223.255.255.255	―

クラス	アドレス範囲	補足
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。

5.1.2. 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** ― 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** ― 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** ― 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。

5.1.3. サブネットとマスク

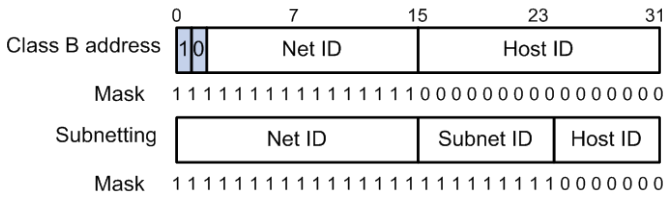
サブネットは、Host ID のいくつかのビットを使用して Subnet ID を作成し、ネットワークをサブネットと呼ばれるより小さいネットワークに分割します。

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 5-2 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。

5.1.4. IP アドレスの割り当て

インタフェースに IP アドレスを割り当てる方法はいかがあります。

- **手動での割り当て**－この章ではインタフェースに手動での IP アドレスの割り当てのみ記載します。
- **BOOTP**－BOOTP についての情報はセクション 4 *IP サービス オペレーションマニュアル*の“*BOOTP*”を参照してください。
- **DHCP**－DHCP についての情報はセクション 4 *IP サービス オペレーションマニュアル*の“*DHCP*”を参照してください。

IP アドレスの割り当ては上記のいずれか 1 つのみを行うことができます。IP アドレスの割り当て方法を変更した場合、新しく設定した方法が適用されます。

5.2. インタフェースへのIPアドレスの割り当て

I. インタフェースへの IP アドレスの手動割り当て

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。もし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。

II. 制限とガイドライン

- 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。新しく IP アドレスを設定した場合、古いアドレスが上書きされます。
- 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。
- IP アドレスがもっとも短いネットワークマスクで AND（論理積）されている場合、同一ネットワークアドレスで異なるマスクを持つ IP アドレスをインタフェースに割り当てることができます。たとえば、1.1.1.1/16 と 1.1.2.1/24 は同一ネットワークアドレス 1.1.0.0 にあります。このときネットワークマスクは 255.255.0.0 です。装置の 2 つのインタフェースに IP アドレスを割り当てることができます。デフォルトで 2 つのインタフェースに接続されているユーザは互いに通信できません。ユーザが通信できるようにするには、装置で一般的な Proxy ARP の設定を行う必要があります。詳細はセクション 4 *IP サービス オペレーションマニュアル*の“*Proxy ARP*”を参照してください。

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*	—
3. インタフェースに IP アドレスを設定する	**ip address** *ip-address* { *mask* | *mask-length* } [**sub**]	デフォルト：設定なし

5.3. 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
指定した、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*]
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** [**description**]

5.4. IPアドレスの設定例

5.4.1. 手動での IP アドレスの割り当て

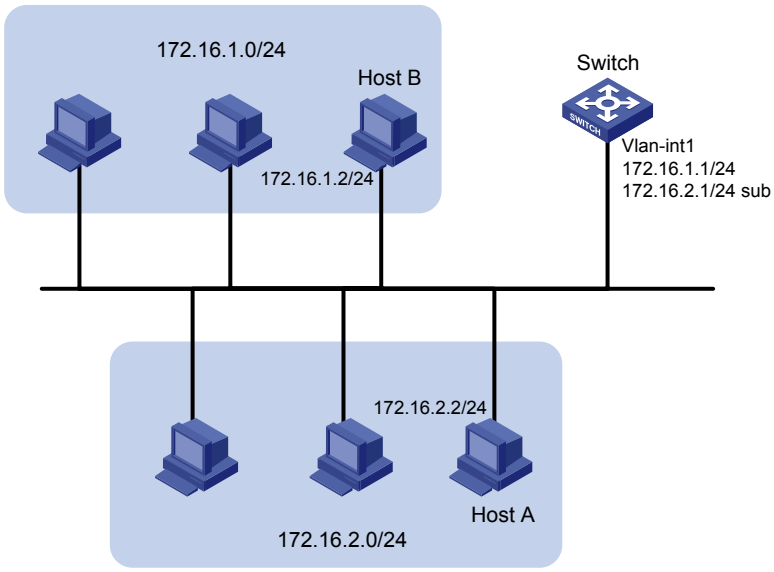
I. ネットワーク要件

図 5-3 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 5-3 ネットワーク図



II. 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。

III. 設定の確認

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
```

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
```

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 **4-x-x** です。

6 章 DHCP の概要 6-1
6.1. DHCP ネットワークモデル 6-1
6.2. DHCP アドレスの割り当て 6-1
6.2.1. 割り当てメカニズム 6-1
6.2.2. IP アドレスの割り当てプロセス 6-2
6.2.3. IP アドレスのリース延長 6-3
6.3. DHCP メッセージフォーマット 6-3
6.4. DHCP オプション 6-4
6.5. 一般的な DHCP オプション 6-4
6.6. 自己定義 DHCP オプション 6-5
6.6.1. ベンダ指定オプション (Option 43) 6-5
6.6.2. リレーエージェントオプション（オプション 82） 6-7
6.6.3. オプション 184 6-7
6.7. プロトコルと標準 6-8

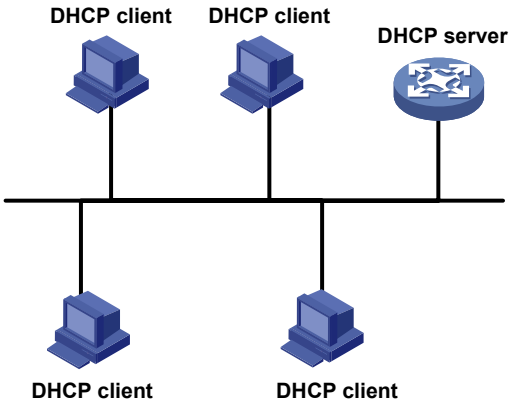
6章 DHCP の概要

6.1. DHCPネットワークモデル

DHCP(Dynamic Host Configuration Protocol)は、ネットワークの装置に設定情報を割り当てる機能を提供します。

図 6-1 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。DHCP クライアントは DHCP リレーエージェントによって別のサブネットの DHCP サーバから設定情報を取得することができます。DHCP リレーエージェントの詳細は、セクション 4 *IP サービス オペレーションマニュアル*の"*DHCP リレー*"を参照してください。

図 6-1 一般的な DHCP の構成



6.2. DHCPアドレスの割り当て

6.2.1. 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 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。

6.2.2. IP アドレスの割り当てプロセス

図 6-2 IP アドレスの割り当てプロセス

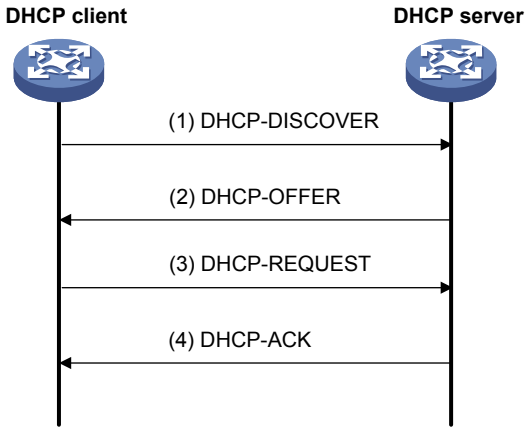


図 6-2 に示すように、DHCP サーバは以下のプロセスで DHCP クライアントに IP アドレスを割り当てます。

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、セクション 4 *IP サービス オペレーションマニュアル*の"*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. いくつかの DHCP サーバがクライアントに DHCP-OFFER を送信した場合、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。

そうでない場合、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。

6.2.3. 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 1 つを返します。

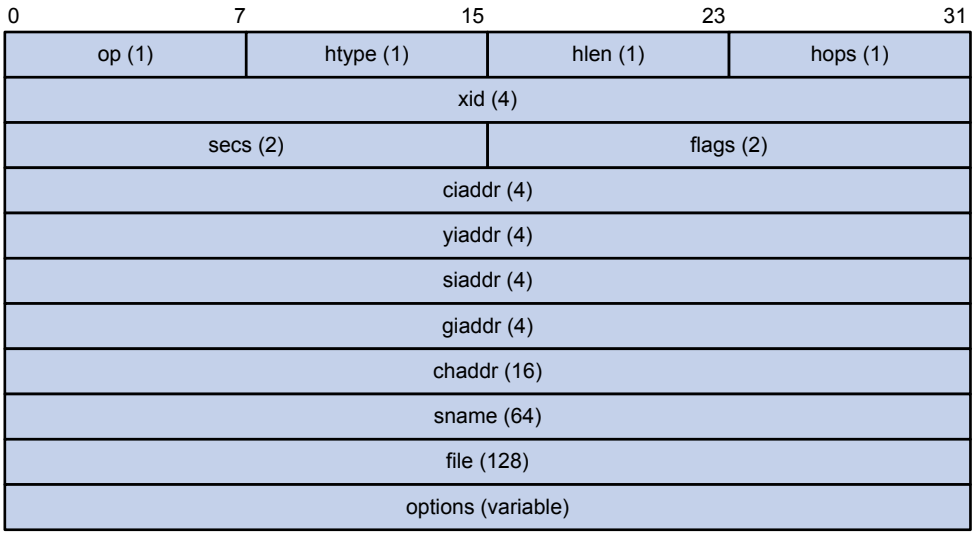
- クライアントのリース期間が延長されていることを確認する DHCP-ACK ユニキャストを返します。
- 要求を拒否する DHCP-NAK ユニキャストメッセージを返します。

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。

6.3. DHCPメッセージフォーマット

図 6-3 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 6-3 DHCP メッセージフォーマット



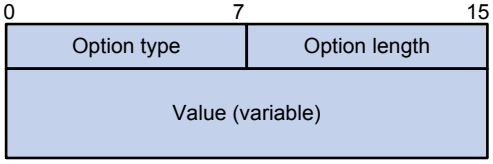
- **op**–オプションフィールドに定義されているメッセージタイプです。1 = REQUEST,2 = REPLY
- **htype, hlen**–DHCP クライアントのハードウェアアドレスのタイプと長さです。
- **hops**–要求メッセージが伝送される(経由する)リレーエージェントの数です。
- **xid**–トランザクション ID で、IP アドレスの割り当てを特定するために、クライアントがランダムに選択した数です。

- **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 のときは、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。そうでなければ 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いません。)
- **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。

6.4. 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 6-4 DHCP オプションフォーマット



6.5. 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。

6.6. 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。

6.6.1. ベンダ指定オプション (Option 43)

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。

II. オプション 43 のフォーマット

図 6-5 オプション 43 のフォーマット

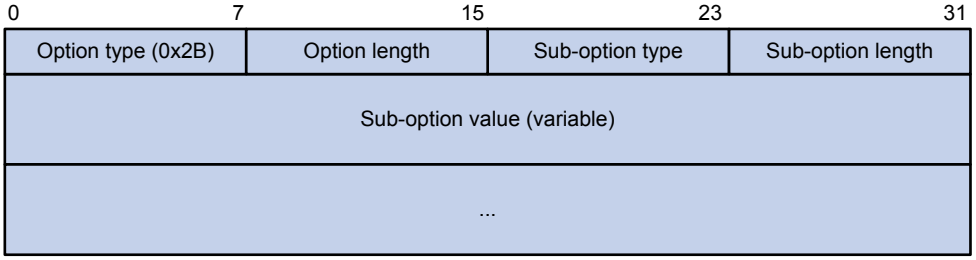


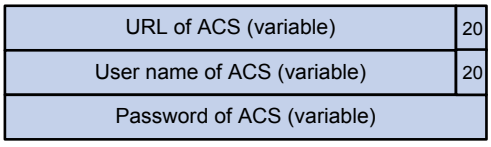
図 6-5 に示すように、ネットワーク設定パラメータは、異なるオプション 43 のサブオプションで送信されます。

- **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。

III. サブオプションフィールドのフォーマット

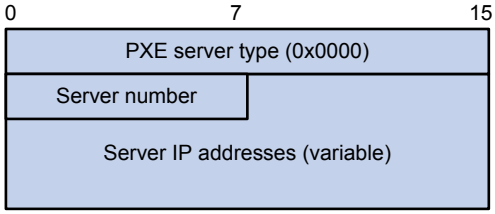
- **ACS パラメータのサブオプションフィールド**–図 6-6 に示すように、ACS パラメータのサブオプションのフィールドは、ACS の URL、ユーザ名、パスワードです。それぞれの間はスペース（0x20）で分離されます。

図 6-6 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 6-7 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 6-7 PXE サーバアドレスのサブオプションフィールド



6.6.2. 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 サブオプションは giaddr フィールドあるいはリレーインタフェースの IP アドレスを持ちます。**dhcp relay source-address** { *ip-address* | **interface** *interface-type interface-number* }コマンドを使用した場合、オプション 82 をサポートするため DHCP リレーエージェントを有効にする必要があります。サブオプションはオプション 82 に含まれます。

6.6.3. 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 を音声ス 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。

6.7. 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 **4-x-x** です。

7 章 DHCP サーバ 7-1
7.1. 概要 7-1
7.1.1. DHCP アドレス割り当てメカニズム 7-1
7.1.2. アドレスプール選択の原則 7-1
7.1.3. IP アドレス割り当て順序 7-2
7.2. DHCP 設定作業リスト 7-3
7.3. DHCP サーバのアドレスプールの設定 7-3
7.3.1. DHCP アドレスプールの設定作業リスト 7-3
7.3.2. DHCP アドレスプールの作成 7-4
7.3.3. 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指定 7-4
7.3.4. DHCP アドレスプールのスタティック割り当ての設定 7-6
7.3.5. DHCP クライアントのゲートウェイの設定 7-6
7.3.6. DHCP クライアントへのドメイン名サフィックスの指定 7-7
7.3.7. DHCP クライアントの DNS サーバの指定 7-8
7.3.8. DHCP クライアントの WINS サーバと NetBIOS ノードタイプの指定 7-8
7.3.9. DHCP クライアントの BIMS サーバ情報の指定 7-9
7.3.10. 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 7-9
7.3.11. DHCP クライアントのサーバの指定 7-10
7.3.12. DHCP クライアントのオプション 184 パラメータの設定 7-10
7.3.13. 自己定義 DHCP オプションの設定 7-11
7.4. インタフェースへのアドレスプールの適用 7-12
7.5. DHCP の有効化 7-13
7.6. インタフェースでの DHCP サーバの有効化 7-13
7.7. IP アドレス競合検出の設定 7-13
7.8. オプション 82 の処理モードの有効化 7-14
7.9. DHCP サーバが送信した DHCP パケットの DHCP 値の設定 7-14
7.10. DHCP サーバの表示と維持 7-15
7.11. DHCP サーバ設定例 7-16
7.11.1. スタティック IP アドレスの割り当て設定例 7-16
7.11.2. ダイナミック IP アドレスの割り当て設定例 7-17
7.11.3. プライマリ、セカンダリサブネット設定例 7-19
7.11.4. 自己定義オプション設定例 7-21
7.12. DHCP サーバ設定のトラブルシューティング 7-22
7.12.1. 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る 7-22

7章 DHCP サーバ

7.1. 概要

DHCP サーバは IP アドレスやクライアントの設定パラメータのプールを管理します。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。

7.1.1. DHCP 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とき、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 アドレス範囲を指定します。DHCP クライアントからの要求を受信したとき、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。

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。もし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。

7.1.2. 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、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位置に依存し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。それは最長一致(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 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)、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。
  - 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。それは最長一致(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。

正しいアドレスの割り当てを保証するため、サブネットの 1 つのダイナミック割り当てに使用する IP アドレスを保存します。

- **サーバと同一サブネット上のクライアント**－DHCP サーバの受信インタフェースが存在するサブネット
- **サーバと異なるサブネット上のクライアント**－クライアントに向かう最初の DHCP リレーのインタフェースが存在するサブネット

メモ:

IP アドレスの不正な割り当てを防ぐため、DHCP サーバまたは DHCP リレーエージェントの接続されるインタフェースがあるサブネットの IP アドレスは、できるだけダイナミック割り当てとしてください。

7.1.3. 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 フィールドに指定されている 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 アドレスを指定するために、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. DHCP アドレス割り当てメカニズム、アドレスプール選択の原則で検出された、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。
- アドレス重複があった IP アドレスは、1 時間後にほかの DHCP クライアントに割り当てることができます。

7.2. DHCP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
(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
(必須設定項目) DHCPの有効化
(必須設定項目) インタフェースへのDHCPサーバの有効化
(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) 拡張DHCP機能の設定 • オプション 82 の処理モードの有効化 • DHCP サーバの互換性の設定 • DHCP サーバが送信した DHCP パケットの DHCP 値の設定

7.3. DHCPサーバのアドレスプールの設定

7.3.1. DHCP アドレスプールの設定作業リスト

作業リスト
(必須設定項目) DHCPアドレスプールの作成
DHCPアドレスプールのIPアドレス範囲の指定 • 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指定 • DHCP アドレスプールのスタティック割り当ての設定

作業リスト
DHCPクライアントに割り当てられるほかの設定パラメータの指定 • 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指定 • DHCP クライアントの DNS サーバの指定 • DHCP クライアントの WINS サーバと NetBIOS ノードタイプの指定 • DHCP クライアントの BIMS サーバ情報の指定 • 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指定 • DHCP クライアントのサーバの指定 • クライアントのオプション 184 パラメータの設定 • 自己定義 DHCP オプションの設定

7.3.2. 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*	—

7.3.3. 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指定

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

プライマリサブネットで割り当て可能な IP アドレスがないとき、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。

II. 制限とガイドライン

forbidden-ip コマンドで指定された 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** コマンドで指定した 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。

III. 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指定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. address pool view に移行する	**dhcp server ip-pool** *pool-name*	—

操作	コマンド	補足
3. プライマリサブネットを指定する	**network** *network-address* [*mask-length* | **mask** *mask*]	デフォルト：設定なし 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指定することができます。 **network**コマンドを使用して複数指定した場合、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) プライマリサブネットを指定する	**network** *network-address* [*mask-length* | **mask** *mask*] **secondary**	デフォルト：設定なし 各アドレスプールで最大32のセカンダリサブネットを指定することができます。
5. (オプション設定項目) system view に戻る	**quit**	—

IV. ダイナミック割り当ての IP アドレスのリース期間の指定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. address pool view に移行する	**dhcp server ip-pool** *pool-name*	—
3. (オプション設定項目) アドレスのリース期間を指定する	**expired** { **day** *day* [**hour** *hour* [**minute** *minute* [**second** *second*]]] | **unlimited** }	デフォルト：1日

V. ダイナミック割り当てから除外する IP アドレスの指定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. address pool view に移行する	**dhcp server ip-pool** *pool-name*	—
3. (オプション設定項目) ダイナミック割り当てから指定された 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。
4. (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指定された IP アドレスを除外する	1. system view に戻る **quit** 2. グローバルにダイナミック割り当てから指定された 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。

7.3.4. DHCP アドレスプールのスタティック割り当ての設定

I. DHCP アドレスプールのスタティック割り当て

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。

II. 制限とガイドライン

- 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。そうでない場合、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。
- 同一装置に存在し、同じ MAC アドレスを使用する DHCP クライアントのスタティックバインディングを設定する場合、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 を指定する必要があります。

III. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. address pool view に移行する	**dhcp server ip-pool** *pool-name*	—
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。 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。
4. (オプション設定項目) アドレスのリース期間を指定する	**expired** { **day** *day* [**hour** *hour* [**minute** *minute* [**second** *second*]]] | **unlimited** }	デフォルト：1日

7.3.5. DHCP クライアントのゲートウェイの設定

I. DHCP クライアントのゲートウェイ

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。

II. 制限とガイドライン

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指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 で指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指定する場合、DHCP address pool view のゲートウェイアドレスをセカンダリサブネットのクライアントに割り当てます。
- address pool view のゲートウェイアドレスを指定するが、secondary subnet view にない場合、DHCP はセカンダリサブネットのクライアントに address pool view のゲートウェイアドレスを割り当てます。

III. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. DHCP address pool view に移行する	**dhcp server ip-pool** *pool-name*	—
3. ゲートウェイを指定する	**gateway-list** *ip-address*&<1-64>	デフォルト：指定なし
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) ゲートウェイを指定する	**gateway-list** *ip-address*&<1-64>	デフォルト：指定なし

7.3.6. DHCP クライアントへのドメイン名サフィックスの指定

I. DHCP クライアントのドメイン名サフィックス

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指定することで、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、セクション 4 *IP サービス オペレーションマニュアル*の"*DNS*"を参照してください。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. DHCP address pool view に移行する	**dhcp server ip-pool** *pool-name*	—
3. ドメイン名サフィックスを指定する	**domain-name** *domain-name*	デフォルト：指定なし

7.3.7. DHCP クライアントの DNS サーバの指定

I. DHCP クライアントの DNS サーバ

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 サーバを指定することができます。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. DHCP address pool view に移行する	**dhcp server ip-pool** *pool-name*	—
3. DNS サーバを指定する	**dns-list** *ip-address*&<1-8>	デフォルト：指定なし

7.3.8. DHCP クライアントの WINS サーバと NetBIOS ノードタイプの指定

I. DHCP クライアントの WINS サーバと NetBIOS ノードタイプ

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 サーバを指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 ノードタイプを指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。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. DHCP address pool view に移行する	**dhcp server ip-pool** *pool-name*	—
3. WINS サーバを指定する	**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：指定なし

操作	コマンド	補足
4. NetBIOS ノードタイプを指定する	**netbios-type** { **b-node** | **h-node** | **m-node** | **p-node** }	デフォルト：指定なし

7.3.9. DHCP クライアントの BIMS サーバ情報の指定

I. DHCP クライアントの BIMS サーバ情報

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。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. DHCP address pool view に移行する	**dhcp server ip-pool** *pool-name*	—
3. BIMS サーバの IP アドレス、ポート番号、共有キーを指定する	**bims-server ip** *ip-address* [**port** *port-number*] **sharekey** { **cipher** | **simple** } *key*	デフォルト：指定なし

7.3.10. 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

I. 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

オートコンフィグレーション（Auto Config）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とき、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、TFTP サーバが必要です。装置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。オートコンフィグレーション（Auto Config）の詳細はセクション 1 *はじめに オペレーションマニュアル*の“*Auto Config*“を参照してください。

II. TFTP サーバでのコンフィグレーションファイルの指定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. DHCP address pool view に移行する	**dhcp server ip-pool** *pool-name*	—

操作	コマンド	補足
3. TFTP サーバの IP アドレスあるいは名前を指定する	• TFTP サーバの IP アドレスを指定する: **tftp-server ip-address** *ip-address* • TFTP サーバの名前を指定する: **tftp-server domain-name** *domain-name*	どちらか1つのコマンドを使用します。 デフォルト：指定なし
4. ブートファイル名を指定する	**bootfile-name** *bootfile-name*	デフォルト：指定なし

7.3.11. DHCP クライアントのサーバの指定

I. DHCP クライアントのサーバ

特定の DHCP クライアントは TFTP サーバのような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 アドレスを指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。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. DHCP address pool view に移行する	**dhcp server ip-pool** *pool-name*	—
3. サーバの IP アドレスを指定する	**next-server** *ip-address*	デフォルト：指定なし

7.3.12. DHCP クライアントのオプション 184 パラメータの設定

I. 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 の詳細はセクション 4 *IP サービス オペレーションマニュアル*の”*DHCP の概要*”を参照してください。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. DHCP address pool view に移行する	**dhcp server ip-pool** *pool-name*	—

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 アドレスを指定する	**voice-config ncp-ip** *ip-address*	デフォルト：指定なし 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 アドレスを指定する	**voice-config as-ip** *ip-address*	デフォルト：指定なし
5. (オプション設定項目) Voice 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、ダイヤル番号を指定する	**voice-config fail-over** *ip-address dialer-string*	デフォルト：指定なし

7.3.13. 自己定義 DHCP オプションの設定

I. 自己定義 DHCP オプション

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 サーバを指定する場合、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。

II. 共通 DHCP オプション

表 7-1 に DHCP オプションとパラメータを示します。

表 7-1 共通 DHCP オプション

オプション	オプション名	対応コマンド	option コマンドの関連パラメータ
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**

オプション	オプション名	対応コマンド	option コマンドの関連パラメータ
67	Boot file name	**bootfile-name**	**ascii**
43	Vendor Specific Information	—	**hex**

III. 制限とガイドライン

自己定義 DHCP オプションを設定するとき、DHCP 運用プロセスに影響する可能性があるため注意してください。

DHCP アドレスプールの DHCP オプションをカスタマイズすることができます。

IV. DHCP アドレスプールの自己定義 DHCP オプションの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. DHCP address pool view に移行する	**dhcp server ip-pool** *pool-name*	—
3. 自己定義 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

7.4. インタフェースへのアドレスプールの適用

I. インタフェースへ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の割り当てを行います。

- クライアントのスタティックバインディングが含まれる場合、DHCP サーバは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。
- クライアントの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。

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*	—

操作	コマンド	補足
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。

7.5. DHCPの有効化

I. 制限とガイドライン

ほかの DHCP 設定を有効にする前に DHCP を有効に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. DHCP を有効にする	**dhcp enable**	デフォルト：無効

7.6. インタフェースでのDHCPサーバの有効化

I. 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。

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. 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

7.7. IPアドレス競合検出の設定

I. IP アドレス競合検出

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 サーバが指定した期間内に 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。

II. 設定手順

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指定する	**dhcp server ping packets** *number*	デフォルト：1 0は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はIPアドレスの競合検出を行いません。

7.8. オプション82の処理モードの有効化

I. オプション 82 の処理モード

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。DHCP リレーエージェントでの有効にする設定については、セクション 4 *IP サービス オペレーションマニュアル*の”*DHCP リレー*”を参照してください。

II. 設定手順

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 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

7.9. DHCPサーバが送信したDHCPパケットのDHCP値の設定

I. DHCP パケットの DHCP 値

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。

II. 設定手順

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

7.10. 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アドレスプールの情報を表示する	**display dhcp server pool** [*pool-name*]
DHCPサーバの統計情報を表示する	**display dhcp server statistics** [**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*]
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**

7.11. DHCPサーバ設定例

7.11.1. 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

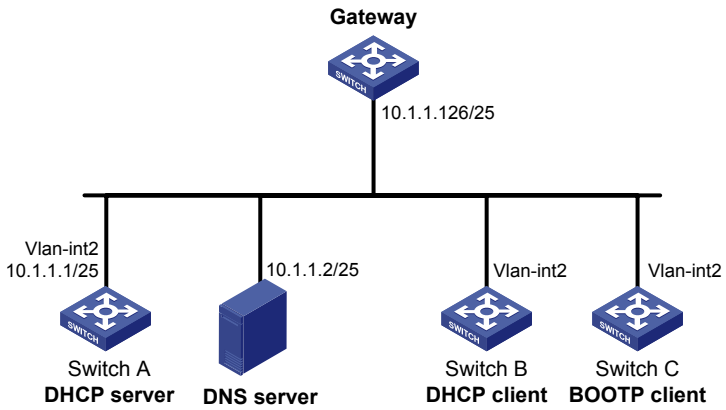
図 7-1 に示すように、Switch B(DHCP クライアント)、Switch C(BOOTP クライアント)は Switch A(DHCP サーバ)からスタティック IP アドレス、DNS サーバアドレス、ゲートウェイアドレスを取得します。

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 7-1 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 アドレスを指定します。

   <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を設定します。

[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を設定します。

[SwitchA-dhcp-pool-0] static-bind ip-address 10.1.1.6 25 hardware-address 000f-e200-01c0

DNS サーバ、ゲートウェイを指定します。

[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

[SwitchA]

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)
```

7.11.2. 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

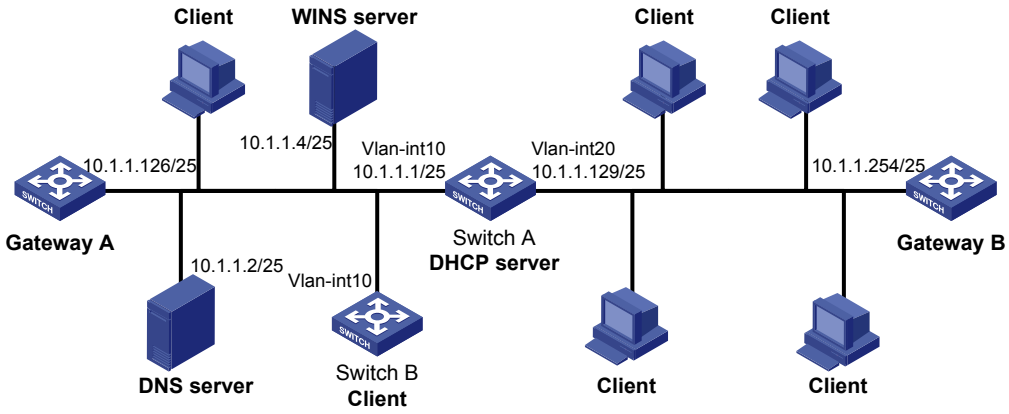
図 7-2 に示すように、DHCP サーバ(Switch A)はサブネット 10.1.1.0/24 のクライアントに IP アドレスを割り当てます。10.1.1.0/24 はさらに 10.1.1.0/25 と 10.1.1.128/25 にサブネット化されます。

Switch A の DHCP サーバの割り当てスキームを表 7-2 に示します。

表 7-2 割り当てスキーム

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	サブネット10.1.1.0/25のIPアドレス	10日12時間	• ゲートウェイ: 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	サブネット10.1.1.128/25のIPアドレス	5日	• ゲートウェイ: 10.1.1.254/25 • DNS サーバ: 10.1.1.2/25 • ドメイン名: aabbcc.com

図 7-2 ネットワーク図



II. 設定手順

1. VLAN インタフェースに IP アドレスを指定します。(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] 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

   # IP アドレス(DNS サーバ、WINS サーバ、ゲートウェイのアドレス)を除外します。

   <SwitchA> system-view

   [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
```

7.11.3. 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

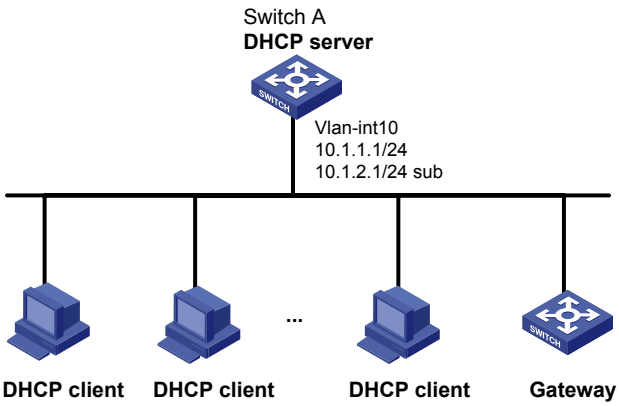
図 7-3 に示すように、DHCP サーバ(Switch A)は LAN 上のクライアントにダイナミックに IP アドレスを割り当てます。

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とき、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 7-3 ネットワーク図



II. 設定手順

DHCP を有効にします。

[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> system-view

[SwitchA] dhcp server ip-pool aa

プライマリアドレス範囲、ゲートウェイアドレスを指定します。

[SwitchA-dhcp-pool-aa] network 10.1.1.0 mask 255.255.255.0

[SwitchA-dhcp-pool-aa] gateway-list 10.1.1.254

セカンダリサブネット範囲、ゲートウェイアドレスを指定します。

[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
```

7.11.4. 自己定義オプション設定例

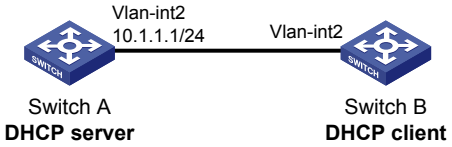
I. ネットワーク要件

図 7-4 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。アドレス割り当てのサブネットは 10.1.1.0/24 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セクション 4 *IP サービス オペレーションマニュアル*の"*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 7-4 ネットワーク図



II. 設定手順

1. インタフェースに IP アドレスを指定します。(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] 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-pool-0] network 10.1.1.0 mask 255.255.255.0

[SwitchA-dhcp-pool-0] option 43 hex 800B000002020304050303030303

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)
```

7.12. DHCPサーバ設定のトラブルシューティング

7.12.1. 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る

I. 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。

II. 解決策

サブネット上の別のホストが同一の IP アドレスを使用している可能性があります。

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調べます。
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 7 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 **4-x-x** です。

8 章 DHCP リレー……8-1
8.1. 概要……8-1
8.1.1. DHCP リレーエージェントの動作……8-1
8.1.2. DHCP リレーエージェントのオプション 82 のサポート……8-2
8.2. DHCP リレーエージェントの設定作業リスト……8-3
8.3. DHCP の有効化……8-3
8.4. インタフェースでの DHCP リレーエージェントの有効化……8-3
8.5. リレーエージェントの DHCP サーバの指定……8-4
8.6. DHCP リレーエージェントセキュリティ機能の設定……8-4
8.6.1. DHCP リレーエージェントのリレーエントリの記録の有効化……8-4
8.7. DHCP リレーエージェントでの IP アドレスのリリース設定……8-5
8.8. DHCP リレーエージェントのオプション 82 の設定……8-5
8.9. DHCP リレーエージェントが送信した DHCP パケットの DSCP の設定……8-6
8.10. DHCP リレーエージェントの表示と維持……8-7
8.11. DHCP リレーの設定例……8-7
8.11.1. DHCP リレーエージェントの基本設定例……8-7
8.11.2. オプション 82 設定例……8-8
8.12. DHCP リレーエージェントのトラブルシューティング……8-9
8.12.1. DHCP クライアントが、DHCP リレーエージェントを通して設定パラメータを取得することができない……8-9

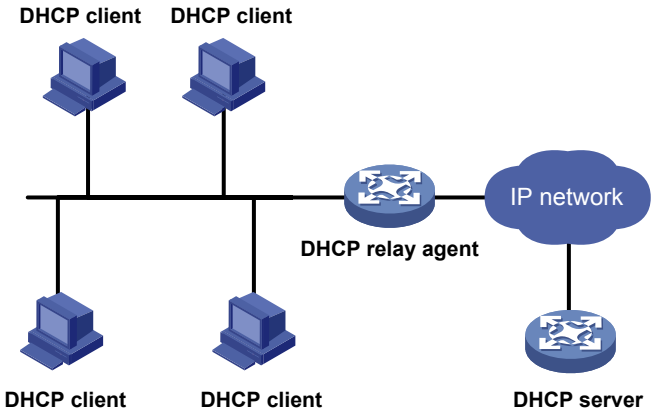
8章 DHCP リレー

8.1. 概要

DHCP リレー機能は、DHCP リレーエージェントを使用して、DHCP クライアントが別のサブネット上にある DHCP サーバから IP アドレスと設定パラメータを取得できるようにします。

図 8-1 に DHCP リレーエージェントの一般的な図を示します。

図 8-1 DHCP リレーエージェント

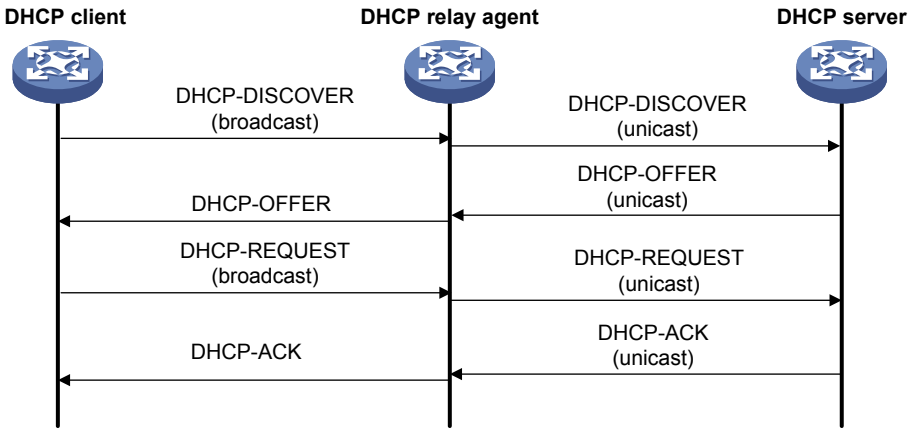


8.1.1. DHCP リレーエージェントの動作

DHCP サーバと DHCP クライアントは、DHCP リレーエージェントの有無に関わらず、同様の方法で互いに相互に通信します。相互接続の詳細は、セクション 4 *IP サービス オペレーションマニュアル*の"*DHCP の概要*"を参照してください。以下に、DHCP リレーエージェントに関連した手順を示します。

1. DHCP クライアントから DHCP-DISCOVER または DHCP-REQUEST ブロードキャストメッセージを受信すると、DHCP リレーエージェントは以下の処理を行います。
   a. DHCP リレーエージェントはメッセージの giaddr フィールドに IP アドレスを入力します。
   b. メッセージを指定した DHCP サーバにユニキャストで転送します。
2. giaddr フィールドにもとづいて、DHCP サーバは IP アドレスおよびその他の設定パラメータをリレーエージェントに返信します。
3. リレーエージェントはそれらの情報をクライアントへ転送します。

図 8-2 DHCP リレーエージェントの動作



8.1.2. DHCP リレーエージェントのオプション 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。オプション 82 は以下の作業を行います。

- セキュリティとアカウンティングのため、DHCP クライアントの位置を示します。
- DHCP クライアントに指定した範囲の IP アドレスを割り当てます。

詳細は、セクション 4 *IP サービス オペレーションマニュアル*の"*DHCP の概要*"を参照してください。

DHCP リレーエージェントがオプション 82 をサポートしている場合、表 8-1 に示されている処理方法に従って、DHCP 要求を処理します。

DHCP サーバからの返答にオプション 82 が含まれている場合は、DHCP リレーエージェントがクライアントに応答を転送する前にオプション 82 を取り除きます。

表 8-1 DHCP リレーエージェントのオプション 82 の処理方法

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 リレーエージェントの動作
Option 82	Drop	メッセージを廃棄します。
	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	元のオプション82を設定されたパディング形式、パディングの内容、パディングタイプに従って、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	N/A	設定されたパディング形式、パディングの内容、パディングタイプに従って、元のオプション82に追加し、メッセージを転送します。

8.2. DHCPリレーエージェントの設定作業リスト

作業リスト
(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リレーエージェントの有効化
(必須設定項目) リレーエージェントのDHCPサーバの指定
(オプション設定項目) DHCPリレーエージェントセキュリティ機能の設定
(オプション設定項目) DHCPリレーエージェントでのIPアドレスのリリース設定
(オプション設定項目) オプション82の設定
(オプション設定項目) DHCPリレーエージェントが送信したDHCPパケットのDHCP値の設定

8.3. DHCPの有効化

I. 制限とガイドライン

他の DHCP リレーエージェントの設定を有効にするために、DHCP を有効にしてください。

II. 設定手順

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

8.4. インタフェースでのDHCPリレーエージェントの有効化

I. インタフェースでの DHCP リレーエージェントの有効化

DHCP リレーエージェントが有効なとき、インタフェースは DHCP サーバに受信した DHCP 要求を転送します。

DHCP リレーエージェントのインタフェースの IP アドレスが含まれる IP アドレスプールは DHCP サーバに設定する必要があります。そうでない場合、DHCP リレーエージェントに接続される DHCP クライアントは IP アドレスを取得できません。

II. 設定手順

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

操作	コマンド	補足
3. DHCP リレーエージェントを有効にする	**dhcp select relay**	デフォルト：DHCPが有効にされたとき、インタフェースはDHCPサーバモードで動作します。

8.5. リレーエージェントのDHCPサーバの指定

I. リレーエージェントの DHCP サーバの指定

可用性を向上するため、DHCP リレーエージェントでいくつかの DHCP サーバを指定することができます。インタフェースがクライアントから要求メッセージを受信したとき、リレーエージェントはすべての DHCP サーバに要求メッセージを転送します。

II. 制限とガイドライン

指定された DHCP サーバアドレスは、リレーエージェントインタフェースの IP アドレスと異なるサブネットにする必要があります。そうでなければクライアントは IP アドレスの取得に失敗します。

III. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. interface view に移行する	**interface** *interface-type interface-number*	—
3. リレーエージェントに DHCP サーバアドレスを指定する	**dhcp relay server-address** *ip-address*	デフォルト：指定なし 最大8つのDHCPサーバを指定することができます。

8.6. DHCPリレーエージェントセキュリティ機能の設定

8.6.1. DHCP リレーエージェントのリレーエントリの記録の有効化

I. DHCP リレーエージェントのリレーエントリの記録の有効化

DHCP から IP アドレスを取得した後、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情報(リレーエントリ)を自動的に記録することができます。

ARP アドレスチェック、IP ソースガードのようないくつかのセキュリティ機能は、入力パケットを確認するため、記録されたリレーエントリを使用し、エントリにマッチしないパケットをブロック

します。ブロックすることで、不正なホストがリレーエージェントを通して外部ネットワークにアクセスできないようにします。

II. 制限とガイドライン

DHCP リレーエージェントは同期/非同期シリアルインタフェースで動作する 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情報は記録しません。

III. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. DHCP リレーエージェントのリレーエントリの記録を有効にする	**dhcp relay client-information record**	デフォルト：無効

8.7. DHCPリレーエージェントでのIPアドレスのリリース設定

I. DHCP リレーエージェントでの IP アドレスのリリース設定

クライアントの IP アドレスをリリースするためにリレーエージェントを設定します。リレーエージェントは DHCP-RELEASE メッセージをサーバに送信し、リレーエントリを削除します。DHCP-RELEASE メッセージを受信した DHCP サーバは IP アドレスをリリースします。

このコマンドでは、DHCP リレーエージェントでリレーエントリが記録された IP アドレスのみリリースすることができます。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. IP アドレスをリリースするために DHCP リレーエージェントを設定する	**dhcp relay release ip** *client-ip*	—

8.8. DHCPリレーエージェントのオプション82の設定

オプション 82 をサポートするため、関連する DHCP サーバと DHCP リレーエージェントの設定を実行してください。DHCP サーバのオプション 82 の設定についてはセクション 4 *IP サービス オペレーションマニュアル*の"*DHCP サーバ*"を参照してください。

I. 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. オプション 82 を動作できるようにリレーエージェントで有効にする	**dhcp relay 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 が含まれる要求メッセージの処理方法を設定する	**dhcp relay information strategy** { **drop** | **keep** | **replace** }	デフォルト：**replace** **replace**パラメータを指定した場合、パディングモードとパディングタイプを設定してください。 **drop**あるいは**keep**パラメータを指定した場合、パディングモードとパディングタイプを設定する必要はありません。
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モードとパディングタイプを設定する	**dhcp relay information circuit-id** { **string** *circuit-id* | { **normal** | **verbose** [**node-identifier** { **mac** | **sysname** | **user-defined** *node-identifier* }] } [**format** { **ascii** | **hex** }] }	デフォルト：サーキットIDサブオプションのパディングモードは**normal**で、パディングタイプは**hex**です。 オプション82のサブオプション1が設定されている場合、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リレーエージェントはオプション82の追加、更新に失敗します。
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モードとパディングタイプを設定する	**dhcp relay information remote-id** { **normal** [**format** { **ascii** | **hex** }] | **string** *remote-id* | **sysname** }	デフォルト：リモートIDサブオプションのパディングモードは**normal**で、パディングタイプは**hex**です。

8.9. DHCPリレーエージェントが送信したDHCPパケットのDSCPの設定

I. DHCP リレーエージェントが送信した DHCP パケットの DSCP

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。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. DHCP リレーエージェントが送信した DHCP パケットの DHCP を設定する	**dhcp dscp** *dscp-value*	デフォルト：56

8.10. DHCPリレーエージェントの表示と維持

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リレーエージェントのリレーエントリを表示する	**display dhcp relay client-information** [**interface** *interface-type interface-number* | **ip** *ip-address*]
DHCPリレーエージェントのオプション82の設定情報を表示する	**display dhcp relay information** [**interface** *interface-type interface-number*]
インタフェース上のDHCPリレーエージェントのDHCPサーバ情報を表示する	**display dhcp relay server-address** [**interface** *interface-type interface-number*]
DHCPリレーエージェントのパケット統計情報を表示する	**display dhcp relay statistics** [**interface** *interface-type interface-number*]
DHCPリレーエージェントのリレーエントリを削除する	**reset dhcp relay client-information** [**interface** *interface-type interface-number* | **ip** *ip-address*]
DHCPリレーエージェントのパケット統計情報を削除する	**reset dhcp relay statistics** [**interface** *interface-type interface-number*]

8.11. DHCPリレーの設定例

8.11.1. DHCP リレーエージェントの基本設定例

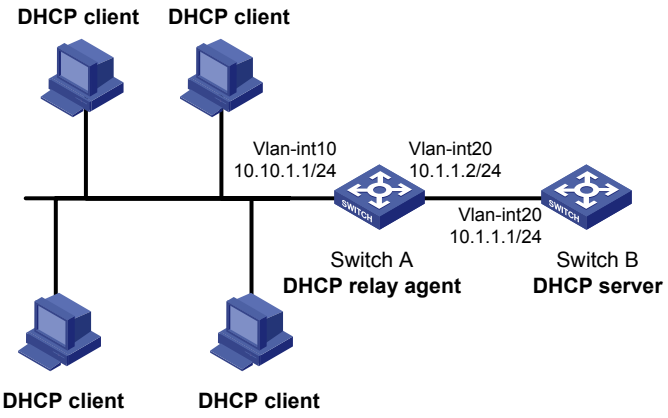
I. ネットワーク要件

図 8-3 に示すように、DHCP クライアントが別のサブネット上にある DHCP サーバから IP アドレスと設定パラメータを取得するため、Switch A に DHCP リレーエージェントを設定します。

DHCP リレーエージェントとサーバは異なるサブネットにあり、互いに通信できるようにするため、スタティックあるいはダイナミックルーティングを設定します。

クライアントとサーバ間の通信を行うため、DHCP サーバで設定を行います。DHCP サーバの設定については、セクション 4 *IP サービス オペレーションマニュアル*の"*DHCP サーバ*"を参照してください。

図 8-3 ネットワーク図



II. 設定手順

インタフェースの IP アドレスを指定します。(詳細は省略します)

DHCP を有効にします。

<SwitchA> system-view

[SwitchA] dhcp enable

VLAN インタフェース 10 で DHCP リレーエージェントを有効にします。

[SwitchA] interface vlan-interface 10

[SwitchA-Vlan-interface10] dhcp select relay

リレーエージェントで DHCP サーバの IP アドレスを指定します。

[SwitchA-Vlan-interface10] dhcp relay server-address 10.1.1.1

III. 設定の確認

DHCP クライアントが DHCP リレーエージェントを通して DHCP サーバから IP アドレスと他のネットワーク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）

DHCP リレーエージェントによって転送された DHCP パケットの統計情報を表示します。

[SwitchA] display dhcp relay statistics

DHCP リレーエージェントの記録を有効にしている場合、リレーエントリを表示します。

[SwitchA] display dhcp relay client-information

8.11.2. オプション 82 設定例

I. ネットワーク要件

図 8-3 に示すように、DHCP リレーエージェント(Switch A)は、DHCP サーバ(Switch B)に DHCP 要求を転送する前に、DHCP 要求のオプション 82 を置き換えます。

- サーキット ID サブオプションは **company001** です。
- リモート ID サブオプションは **device001** です。

オプション 82 を使用するため、オプション 82 を処理する DHCP サーバを有効にする必要があります。

II. 設定手順

インタフェースの IP アドレスを指定します。(詳細は省略します)

DHCP を有効にします。

<SwitchA> system-view

[SwitchA] dhcp enable

VLAN インタフェース 10 で DHCP リレーエージェントを有効にします。

[SwitchA] interface vlan-interface 10

[SwitchA-Vlan-interface10] dhcp select relay

DHCP サーバの IP アドレスを指定します。

[SwitchA-Vlan-interface10] dhcp relay server-address 10.1.1.1

オプション 82 の処理方法とパディングモードを設定します。

[SwitchA-Vlan-interface10] dhcp relay information enable

[SwitchA-Vlan-interface10] dhcp relay information strategy replace

[SwitchA-Vlan-interface10] dhcp relay information circuit-id string company001

[SwitchA-Vlan-interface10] dhcp relay information remote-id string device001

8.12. DHCPリレーエージェントのトラブルシューティング

8.12.1. DHCP クライアントが、DHCP リレーエージェントを通して設定パラメータを取得することができない

I. 症状

DHCP クライアントが、DHCP リレーエージェントを通して設定パラメータを取得することができません。

II. 解決策

DHCP リレーエージェントあるいは DHCP サーバの設定に問題が発生している可能性があります。

問題を切り分けるため、デバッグを有効にし、DHCP リレーエージェントで **display** コマンドを実行します。デバッグ情報とインタフェース状態の情報を確認してください。

以下の項目を確認してください。

- DHCP サーバと DHCP リレーエージェントで DHCP が有効になっているかどうか確認してください。
- DHCP サーバが DHCP クライアントと同じサブネットでアドレスプールを持っているかどうか確認してください。

- DHCP サーバと DHCP リレーエージェントが互いに通信可能であることを確認してください。
- DHCP クライアントに接続される DHCP リレーエージェントのインタフェースで、DHCP サーバのアドレスが正しく設定されてい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 **4-x-x** です。

9 章 DHCP クライアント 9-1
9.1. 概要 9-1
9.2. 制限とガイドライン 9-1
9.3. DHCP クライアント設定作業リスト 9-1
9.4. インタフェースでの DHCP クライアントの有効化 9-1
9.5. アドレス重複検出の有効化 9-2
9.6. DHCP クライアントが送信する DHCP パケットの DSCP の設定 9-2
9.7. DHCP クライアントの表示と維持 9-2
9.8. DHCP クライアント設定例 9-3

9章 DHCP クライアント

9.1. 概要

DHCP クライアントが有効である場合、インタフェースは、DHCP を使用して DHCP サーバから IP アドレスなどの設定パラメータを取得します。

9.2. 制限とガイドライン

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。

9.3. DHCPクライアント設定作業リスト

作業リスト
(必須設定項目) インタフェースでのDHCPクライアントの有効化
(オプション設定項目) アドレス重複検出の有効化
(オプション設定項目) DHCPクライアントが送信したDHCPパケットのDSCP値の設定

9.4. インタフェースでのDHCPクライアントの有効化

I. 制限とガイドライン

- 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、古い設定は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同一サブネットの IP アドレス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。

II. 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. 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

9.5. アドレス重複検出の有効化

I. アドレス重複検出

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。

II. 設定手順

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

9.6. DHCPクライアントが送信するDHCPパケットのDSCPの設定

I. 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。

II. 設定手順

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

9.7. 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クライアントの情報を表示する	**display dhcp client** [**verbose**] [**interface**

操作	コマンド
	interface-type interface-number]

9.8. DHCPクライアント設定例

I. ネットワーク要件

図 9-2 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 9-1 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 9-1 オプション 121 フォーマット

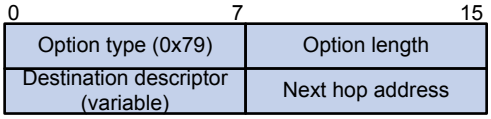
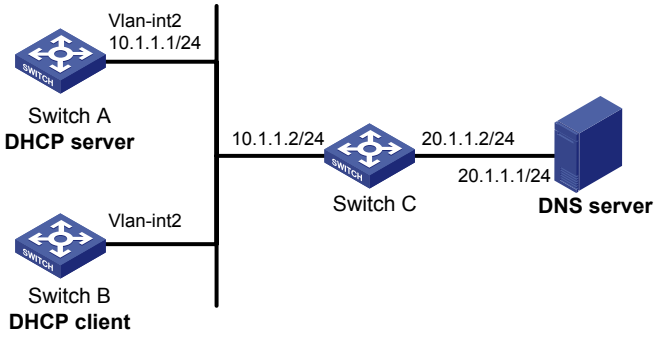


図 9-2 ネットワーク図



II. 設定手順

1. Switch A 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 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

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

[SwitchA-dhcp-pool-0] quit

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

III. 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 **4-x-x** です。

10 章 DHCP スヌーピング 10-1
10.1. 概要 10-1
10.1.1. 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 10-1
10.1.2. DHCP snooping でのオプション 82 のサポート 10-2
10.2. 制限とガイドライン 10-3
10.3. DHCP snooping 設定作業リスト 10-3
10.4. DHCP snooping の基本機能の設定 10-4
10.4.1. 一般的なネットワークにおける DHCP snooping の基本機能の設定 10-4
10.5. オプション 82 の設定 10-4
10.6. DHCP snooping の表示と維持 10-6
10.7. DHCP snooping 設定例 10-6
10.7.1. DHCP snooping の基本機能の設定例 10-6
10.7.2. オプション 82 設定例 10-7

10章 DHCP スヌーピング

10.1. 概要

DHCP snooping は DHCP のセキュリティを行います。

DHCP snooping は DHCP クライアントとサーバ、あるいは DHCP クライアントとリレーエージェント間で動作し、許可された DHCP サーバから IP アドレスを取得できるようにします。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** – 許可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。詳細は、セクション 8 *セキュリティ オペレーションマニュアル*の"*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、セクション 8 *セキュリティ オペレーションマニュアル*の"*IP ソースガード*"を参照してください。
- **VLAN マッピング** – DHCP snooping エントリはパケットをクライアントに送信する前にパケットのサービスプロバイダ VLAN をカスタマ VLAN に置き換えます。詳細はセクション 3 *アクセス オペレーションマニュアル*の”*VLAN マッピング*”を参照してください。

10.1.1. 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信頼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 10-1 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 10-1 トラステッドポートと非トラステッドポート

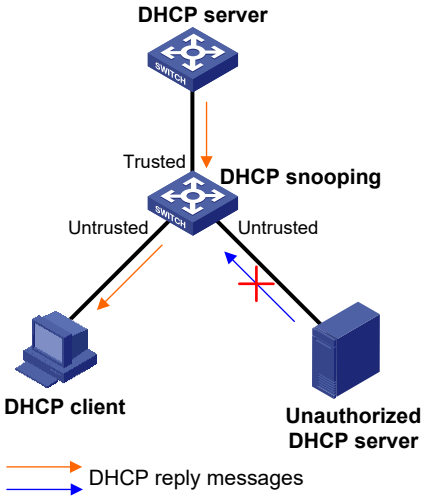
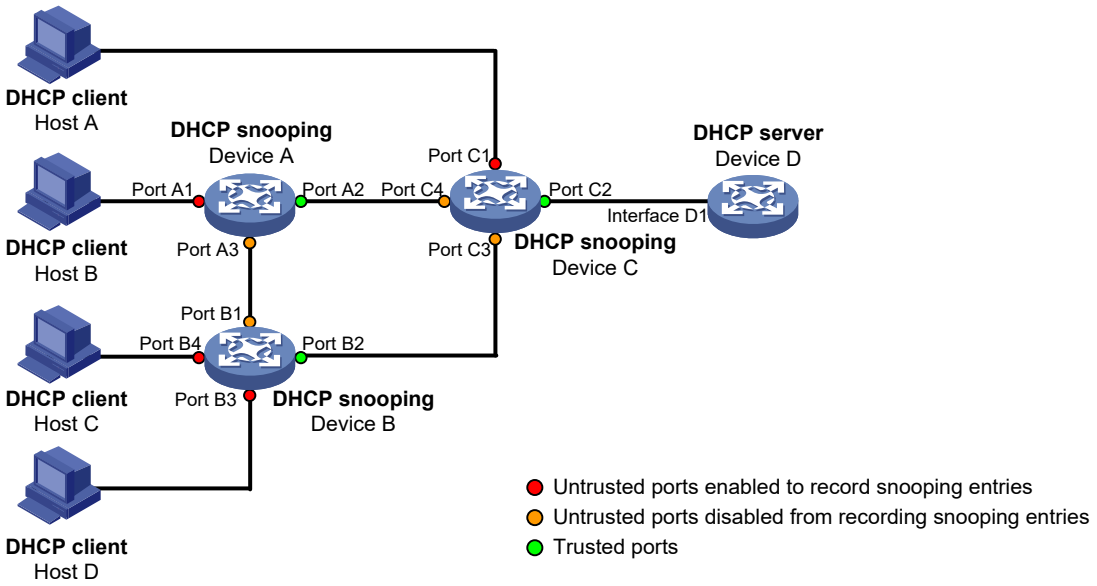


図 10-2 に示すようなカスケードネットワーク構成では、システムリソースを節約するため、DHCP Snooping エントリを記録する DHCP クライアントに接続されている非トラステッドポートのみ有効にすることができます。

図 10-2 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



10.1.2. 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、セクション 4 *IP サービス オペレーションマニュアル*の"*DHCP の概要*"を参照してください。

DHCP snooping は表 10-1 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 10-1 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	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	元のオプション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、元のオプション82に追加し、メッセージを転送します。

10.2. 制限とガイドライン

- 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。
- 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、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、セクション 3 *アクセス オペレーションマニュアル*の”*リンクアグリゲーション*”を参照してください。
- VLAN マッピングとの併用はできません。

10.3. DHCP snooping設定作業リスト

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

10.4. DHCP snoopingの基本機能の設定

10.4.1. 一般的なネットワークにおける DHCP snooping の基本機能の設定

I. 一般的なネットワークにおける DHCP snooping の基本機能

DHCP snooping の基本機能は以下のことについて記載します。

- DHCP snooping の有効化
- DHCP snooping のトラステッドポートの設定
- DHCP snooping エントリのクライアント情報の記録の有効化

DHCP snooping をグローバルで有効にした場合、装置のすべてのインタフェースで有効になります。

II. グローバルでの DHCP snooping の基本機能の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. 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. (オプション設定項目) DHCP snooping エントリの記録を有効にする	1. system view に戻る **quit** 2. interface view に移行する **interface** *interface-type interface-number* 3. 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。 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。

10.5. オプション82の設定

I. 制限とガイドライン

- 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 の設定の詳細はセクション 4 *IP サービス オペレーションマニュアル*の"*DHCP サーバ*"を参照してください。
- 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、Chapter 1 *Fundamentals Command References* の”*Device management commands*”を参照してください。
- DHCP snooping が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 と QinQ を同時動作します。
  - DHCP snooping が 2 つの VLAN タグの DHCP パケットを受信します。

  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。外部 VLAN タグを 16 進数で表記すると 10、内部 VLAN タグ 20 を 16 進数で表記すると 14 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. 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** { **drop** | **keep** | **replace** }	デフォルト：**replace** **replace**と設定されている場合、オプション82のパディングモードとコードタイプ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、パディングモードとコードタイプを設定する必要はありません。
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モード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：パディングモードは**normal**、コードタイプは**hex**です。 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。

操作	コマンド	補足
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モード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 : パディングモードは**normal**、コードタイプは**hex**です。

10.6. 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*]] [**verbose**]
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*]
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*]

10.7. DHCP snooping設定例

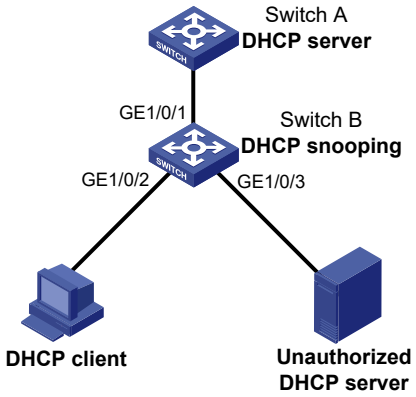
10.7.1. DHCP snooping の基本機能の設定例

I. ネットワーク要件

図 10-3 に示すように設定します。Switch B は許可された DHCP サーバに GigabitEthernet 1/0/1 を通して接続されています。許可されていない DHCP サーバに GigabitEthernet 1/0/3 を通して接続されています。DHCP クライアントに GigabitEthernet 1/0/2 を通して接続されています。

DHCP サーバからの応答を転送するため、許可されている DHCP サーバに接続されているポートのみ設定します。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 10-3 ネットワーク図



II. 設定手順

グローバルで 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

10.7.2. オプション 82 設定例

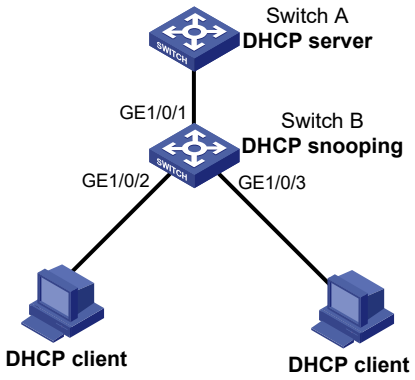
I. ネットワーク要件

図 10-4 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 10-4 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 **4-x-x** です。

11 章 BOOTP クライアント 11-1
11.1. 概要 11-1
11.1.1. BOOTP クライアントアプリケーション 11-1
11.1.2. 動的 IP アドレスの取得 11-1
11.1.3. プロトコルと標準 11-1
11.2. インタフェースの BOOTP を使用した IP アドレス取得の設定 11-2
11.3. BOOTP クライアントの表示と維持 11-2
11.4. BOOTP クライアントの設定例 11-2
11.4.1. BOOTP クライアントの設定例 11-2

11章 BOOTP クライアント

11.1. 概要

11.1.1. BOOTP クライアントアプリケーション

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。

11.1.2. 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。

11.1.3. 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*

11.2. インタフェースのBOOTPを使用したIP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**	ー
2. interface view に移行する	**interface** *interface-type interface-number*	BOOTPクライアントはVLANインタフェースでのみ適用します。
3. インタフェース BOOTP を使用した IP アドレス取得設定をする	**ip address bootp-alloc**	デフォルト：設定なし

11.3. 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*]

11.4. BOOTPクライアントの設定例

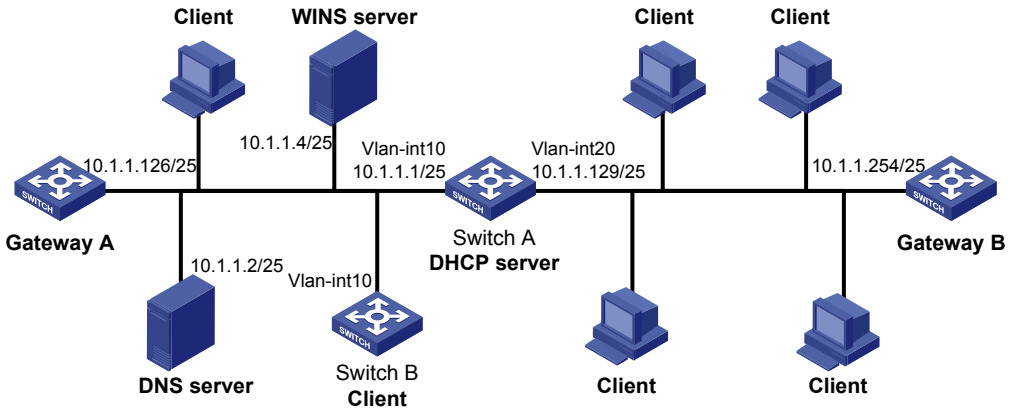
11.4.1. BOOTP クライアントの設定例

I. ネットワーク要件

図 11-1 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。詳細はセクション 4 *IP サービス オペレーションマニュアル*の”*DHCP サーバ*”を参照してください。

図 11-1 ネットワーク図



II. 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ことについて記載しています。

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

III. 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 **4-x-x** です。

12 章 DNS 12-1
12.1. 概要 12-1
12.1.1. DNS サービスタイプ 12-1
12.1.2. スタティックドメイン名解決 12-1
12.1.3. ダイナミックドメイン名解決 12-1
12.1.4. DNS プロキシ 12-3
12.2. DNS 設定作業リスト 12-4
12.3. DNS クライアントの設定 12-4
12.3.1. スタティックドメイン名解決の設定 12-4
12.3.2. ダイナミックドメイン名解決の設定 12-4
12.4. DNS プロキシの設定 12-5
12.5. 送信される DNS パケットの DSCP 値の設定 12-6
12.6. DNS の表示と維持 12-6
12.7. IPv4 DNS 設定例 12-6
12.7.1. スタティックドメイン名解決の設定例 12-6
12.7.2. ダイナミックドメイン名解決の設定例 12-7
12.7.3. DNS プロキシの設定例 12-10
12.8. DNS 設定のトラブルシューティング 12-11
12.8.1. IP アドレスの名前解決に失敗する 12-11

12章 DNS

12.1. 概要

DNS(Domain Name System)は TCP/IP アプリケーションで使用する分散データベースで、ドメイン名を対応する IP アドレスに変換します。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。

12.1.1. DNS サービスタイプ

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)な名前解決のとき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。

12.1.2. スタティックドメイン名解決

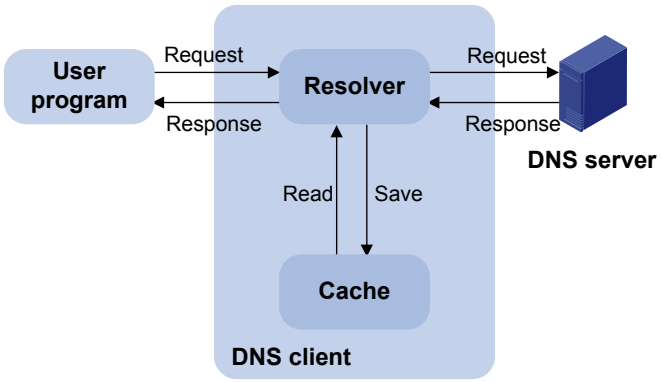
スタティックドメイン名解決は、ドメイン名と IP アドレスの間にマッピングを手動でマッピングを作成します。たとえば、Telnet などのアプリケーションを使用する際に、装置のスタティックドメイン名解決のマッピングを作成することができます。

12.1.3. ダイナミックドメイン名解決

I. アーキテクチャ

図 12-1 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 12-1 ダイナミックドメイン名解決



装置は DNS クライアントとして動作し、DNS サーバとして動作しません。

エイリアスが DNS サーバのドメイン名に設定されている場合、装置はホストの IP アドレスにエイリアスを使用することができます。

II. 解決手段

ダイナミックドメイン名の解決手段を以下に示します。

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。

III. キャッシュ

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とき、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。

IV. 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ときに使用します。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 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、ユーザが入力したドメイン名（たとえば aabbcc）がクエリとして IP アドレスを使用します。
- 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。

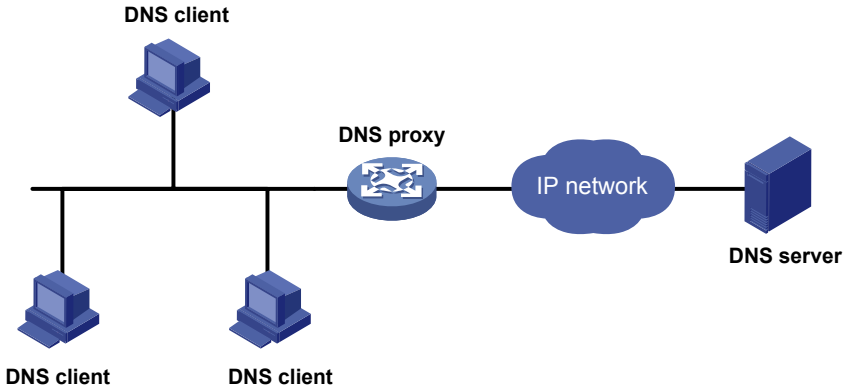
12.1.4. DNS プロキシ

図 12-2 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 12-2 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。

12.2. DNS設定作業リスト

作業リスト
DNSクライアントの設定 必要とされる作業を選択してください。 • スタティ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

12.3. DNSクライアントの設定

12.3.1. スタティックドメイン名解決の設定

I. 制限とガイドライン

パブリックネットワークでは、各ホスト名は 1 つの IPv4 アドレスのみ割り当てられます。

パブリックネットワークの DNS エントリは最大 2048 まで設定することができます。パブリックネットワークで DNS エントリを設定することができます。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. スタティック名前解決テーブルでホスト名と IP 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

12.3.2. ダイナミックドメイン名解決の設定

I. 制限とガイドライン

- 装置の DNS サーバの最大数を以下に示します。
- system view で、パブリックネットワークの DNS サーバの IP アドレスは最大で 6 つまで指定することができます。パブリックネットワークで DNS サーバの IP アドレスを設定することができます。
- interface view で、パブリックネットワークの DNS サーバの IP アドレスは最大で 6 つまで指定することができます。パブリックネットワークで DNS サーバの IP アドレスを設定することができます。

- system view で設定した DNS サーバのアドレスは interface view で設定した DNS サーバのアドレスより優先されます。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 サーバのアドレスは DHCP など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。装置は最初に最も高い優先度の DNS サーバのアドレスに DNS クエリを送信します。DNS クエリがドメイン名の解決に失敗した場合、2 番目以降の優先度の DNS サーバのアドレスを使用します。
- システムはユーザが入力した不完全なドメイン名に自動的に追加する DNS サフィックスを設定することができます。
  - パブリックネットワークの DNS サフィックスは最大 16 まで設定できます。パブリックネットワークで 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、手動で設定した DNS サフィックスが優先されます。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。装置は最初に最も高い優先度の DNS サフィックスを使用します。DNS クエリがドメイン名の解決に失敗した場合、2 番目以降の優先度の DNS サーバのアドレスを使用します。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. 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
3. (オプション設定項目) 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

12.4. DNSプロキシの設定

I. 制限とガイドライン

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。もし 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。

II. 設定手順

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

12.5. 送信されるDNSパケットのDSCP値の設定

I. 送信される DNS パケットの DSCP 値

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。

II. 設定手順

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

12.6. 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
DNSサフィックスを表示する	**display dns domain** [**dynamic**]
ドメイン名解決テーブルを表示する	**display dns host** [**ip**]
DNSサーバ情報を表示する	**display dns server** [**dynamic**]
ダイナミックドメイン名エントリの情報を削除する	**reset dns host** [**ip**]

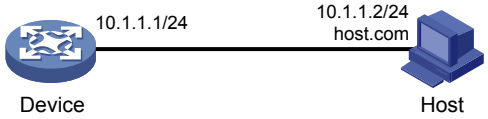
12.7. IPv4 DNS設定例

12.7.1. 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 12-3 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 12-3 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。

<Device> system-view

[Device] ip host host.com 10.1.1.2

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。

[Device] ping host.com

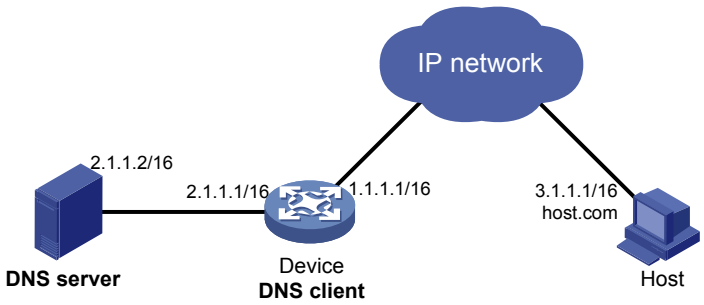
```
Ping host.com (10.1.1.2): 56 data bytes, press CTRL_C to break
56 bytes from 10.1.1.2: icmp_seq=0 ttl=255 time=1.000 ms
56 bytes from 10.1.1.2: icmp_seq=1 ttl=255 time=1.000 ms
56 bytes from 10.1.1.2: icmp_seq=2 ttl=255 time=1.000 ms
56 bytes from 10.1.1.2: icmp_seq=3 ttl=255 time=1.000 ms
56 bytes 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
```

12.7.2. 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 12-4 に示すように DNS サーバを設定します。ホストのドメイン名 host、com ドメインの IP アドレス 3.1.1.1/16 間のマッピングを DNS サーバに記録するように設定します。ドメイン名 host がホストにアクセスできるように装置の DNS と DNS サフィックス com を設定します。

図 12-4 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 12-4 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 サーバを設定します。

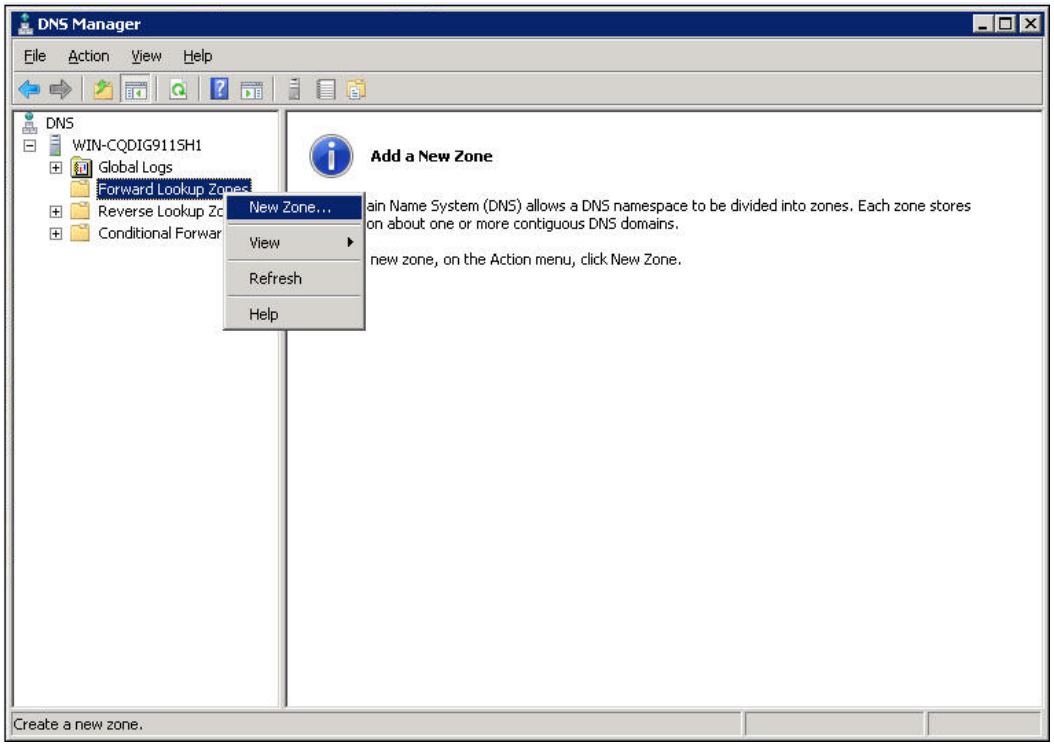
   OS が異なると、設定も方法変わる可能性があります。以下の設定例は、Windows 2008 R2 が動作する PC での設定方法です。

a. Select Start > Programs > Administrative Tools > DNS を選択します。

図 12-5 に示すように DNS server の設定ページが表示されます。

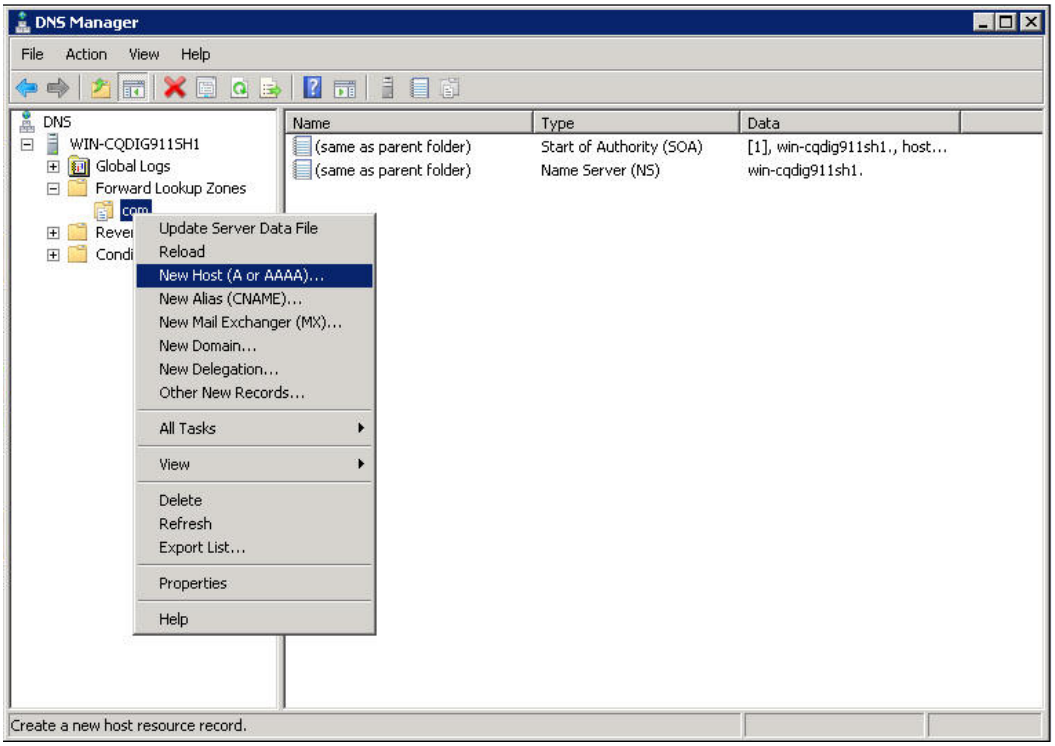
b. [Forward Lookup Zones]を右クリックし、[New zone]を選択します。指示に従って、新しいゾーン com を作成します。

図 12-5 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 12-6 ホストの追加

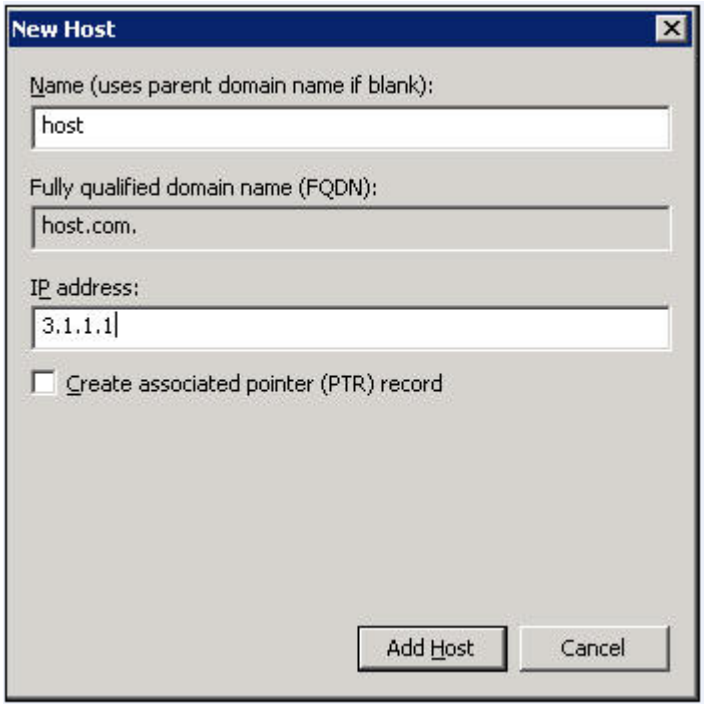


d. ダイアログボックスで、ホスト名 host、IP アドレス 3.1.1.1 を入力します。

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 12-7 ドメイン名と IP アドレス間のマッピングの作成 s



2. DNS クライアントを設定します。

IP アドレスとして 2.1.1.2 を指定します。

<Device> system-view

[Device] 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。

[Device] dns domain com

III. 設定の確認

装置でドメイン名 host.com の名前解決が行われ、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。

[Device] ping host

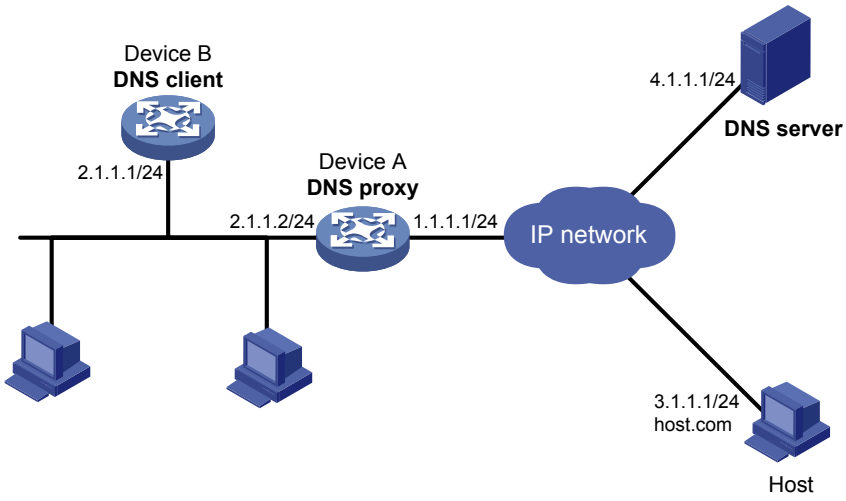
```
Ping host.com (3.1.1.1): 56 data bytes, press CTRL_C to break
56 bytes from 3.1.1.1: icmp_seq=0 ttl=255 time=1.000 ms
56 bytes from 3.1.1.1: icmp_seq=1 ttl=255 time=1.000 ms
56 bytes from 3.1.1.1: icmp_seq=2 ttl=255 time=1.000 ms
56 bytes from 3.1.1.1: icmp_seq=3 ttl=255 time=1.000 ms
56 bytes from 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
```

12.7.3. DNS プロキシの設定例

I. ネットワーク要件

図 12-8 に示すように、DNS クライアント（Device B）と DNS サーバ 4.1.1.1 間の DNS パケットを転送するため、DNS プロキシとして Device A を設定します。

図 12-8 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 12-8 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 サーバを設定します。

   この設定は DNS サーバによって異なります。Windows2008 RS が動作する PC を DNS サーバとして使用する場合、セクション 4 *IP サービス オペレーションマニュアル*の”*DNS*”の”*IPv4 DNS 設定例*”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 プロキシが動作してい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
```

12.8. DNS設定のトラブルシューティング

12.8.1. IP アドレスの名前解決に失敗する

I. 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。

II. 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 **4-x-x** です。

13 章 IP フォワーディングの基本 13-1
13.1. FIB テーブル 13-1
13.2. FIB テーブルエントリの表示と維持 13-2

13章 IP フォワーディングの基本

13.1. FIBテーブル

装置はパケットの転送先を決定するため、FIB(forwarding information base)テーブルを使用します。

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、セクション 5 *ルーティングプロトコル オペレーションマニュアル*の”*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: 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
10.2.0.0/16         10.2.1.1        U        GE1/0/1                  Null
10.2.1.1/32         127.0.0.1       UH       InLoop0                  Null
127.0.0.0/8         127.0.0.1       U        InLoop0                  Null
127.0.0.1/32        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 であるとき、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 進数で表現されることもあります。
- **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。

13.2. 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 **4-x-x** です。

14 章 IP パフォーマンスの最適化 14-1
14.1. IP パフォーマンスの最適化設定作業リスト 14-1
14.2. ダイレクトブロードキャストの送受信の有効化 14-1
14.2.1. ダイレクトブロードキャストの送受信の有効化 14-1
14.2.2. 設定手順 14-2
14.2.3. ダイレクトブロードキャストの送受信の有効化の設定例 14-2
14.3. インタフェースで送信する IPv4 パケットの MTU サイズの設定 14-3
14.4. ICMP エラーメッセージの送信の有効化 14-4
14.4.1. ICMP エラーメッセージ 14-4
14.4.2. ICMP リダイレクトメッセージの送信の有効化 14-4
14.4.3. ICMP タイムアウトメッセージの送信の有効化 14-4
14.4.4. ICMP 宛先到達不能メッセージの送信の有効化 14-5
14.5. ICMP エラーメッセージのレートリミットの設定 14-6
14.6. TCP path MTU discovery の設定 14-6
14.7. TCP バッファサイズの設定 14-8
14.8. TCP タイマの設定 14-8
14.9. IP パフォーマンスの最適化の表示と維持 14-8

14章 IP パフォーマンスの最適化

14.1. IPパフォーマンスの最適化設定作業リスト

作業リスト
(オプション設定項目) IPパケット機能の設定 • ダイレクトブロードキャストの送受信の有効化 • インタフェースで送信する IPv4 パケットの MTU サイズの設定 インタフェースのMTUサイズの設定はIRFスタックで設定可能です。
(オプション設定項目) ICMPパケット機能の設定 • ICMP エラーメッセージの送信の有効化 • ICMP エラーメッセージのレートリミットの設定
(オプション設定項目) TCPパケット機能の設定 • TCP path MTU discovery の設定 • TCP バッファサイズの設定 • TCP タイマの設定

14.2. ダイレクトブロードキャストの送受信の有効化

14.2.1. 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**－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。
- **Wake on LAN**－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。

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でこれらの機能を設定することができます。

14.2.2. 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. 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

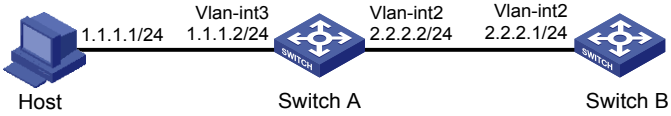
14.2.3. ダイレクトブロードキャストの送受信の有効化の設定例

I. ネットワーク要件

図 14-1 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 14-1 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 3、VLAN インタフェース 2 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 IP アドレスを指定し、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。

ホストに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

III. 設定の確認

設定を完了したのち、ホストから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 を受信することができます。すべての Switch で **ip forward-broadcast** コマンドを削除した場合、インタフェースは ping を受信することができません。

14.3. インタフェースで送信するIPv4パケットのMTUサイズの設定

I. インタフェースで送信する IPv4 パケットの MTU サイズの設定

パケットが出力インタフェースの MTU サイズを超えたとき、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で送信する IPv4 パケットの MTU サイズを設定します。

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	**interface** *interface-type interface-number*	—
3. インタフェースで送信する IPv4 パケットの MTU サイズを設定する	**ip mtu** *mtu-size*	デフォルト：設定なし

14.4. ICMPエラーメッセージの送信の有効化

14.4.1. ICMP エラーメッセージ

ICMP エラーメッセージはネットワークの管理を容易にし、ネットワークレイヤプロトコル、トランスポートレイヤプロトコルで、ほかの装置からのアップデートおよびエラーを送信するために使用します。

ICMP エラーメッセージを送ることはネットワークの管理を簡略化しますが、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。この問題を防ぐため、ICMP エラーメッセージの送信はデフォルトで無効となっています。必要に応じて異なるタイプの ICMP エラーメッセージの送信を有効にすることができます。

ICMP エラーメッセージには ICMP リダイレクトメッセージ、ICMP タイムアウトメッセージ、ICMP 宛先到達不能メッセージがあります。

14.4.2. ICMP リダイレクトメッセージの送信の有効化

I. 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。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. ICMP リダイレクトパケットの送信を有効にする	**ip redirects enable**	デフォルト：無効

14.4.3. ICMP タイムアウトメッセージの送信の有効化

I. ICMP タイムアウトメッセージ

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。

- 装置は以下の場合、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ありません。

- 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、装置が受信したとき、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。

II. 制限とガイドライン

ICMP タイムアウトメッセージが無効である場合、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。Fragment Reassembly Timeout の ICMP エラーパケットは正常に送信します。

III. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. ICMP タイムアウトパケットの送信を有効にする	**ip ttl-expires enable**	デフォルト：無効

14.4.4. ICMP 宛先到達不能メッセージの送信の有効化

I. ICMP 宛先到達不能メッセージ

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。

- 装置は以下の場合、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。
  - デフォルトルートが存在しません。
- 装置は以下の場合、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ローカル装置でサポートしていません。
- 装置は以下の場合、Port Unreachable の ICMP エラーパケットを送信元に送信します。
  - 宛先が装置でトランスポート層プロトコルが UDP のパケットを受信しました。
  - 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。
- 装置は以下の場合、Source Routing Failure の ICMP エラーパケットを送信元に送信します。
  - パケットを送信するため送信元が、Strict Source Routing を使用します。
  - 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中間装置が検出しました。
- 装置は以下の場合、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。
  - 送信するパケットに DF セット(フラグメント禁止)が付与されています。

II. 制限とガイドライン

DHCP が有効な装置が ICMP エコーリクエストを送信しないで ICMP エコーリプライを受信した場合、装置は送信元に ICMP 宛先不能パケットを送信しません。DHCP の詳細はセクション 4 *IP サービス オペレーションマニュアル*の“*DHCP の概要*”を参照してください。

III. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. 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

14.5. ICMPエラーメッセージのレートリミットの設定

I. トークンバケットアルゴリズム

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表す 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ときに、トークンはバケットから取り除かれます。バケットが空のときに、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。

II. 設定手順

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** *milliseconds* [*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。

14.6. TCP path MTU discoveryの設定

I. TCP path MTU discovery

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。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。path MTU は経路の最小リンクの MTU が増大するとき、送信元の装置がパス MTU をできるようにするため、エージングメカニズムを使用します。

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、パケットの転送を行いません。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 32byte よりも小さい状態で、もし 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、出力インタフェースの 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、65535byte の MTU 値を含んでいます。最小 TCP MSS の値はシステムで 32byte と決められているため、実際の最小 MTU は 72byte です。

経路上で最小リンク MTU が増加したとき、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とき、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。

II. 設定要件

TCP 通信を行うすべての装置で **ip unreachables enable** コマンドを使用して ICMP エラーメッセージを送信するようにしていることを確認してください。

III. 設定手順

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

14.7. 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

14.8. TCPタイマの設定

I. TCP タイマ

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 状態に変更されるとき、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。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. TCP SYN wait タイマを設定する	**tcp timer syn-timeout** *time-value*	デフォルト：75秒
3. TCP FIN wait タイマを設定する	**tcp timer fin-timeout** *time-value*	デフォルト：675秒

14.9. IP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
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表示する	**display ip statistics** [**slot** *slot-number*]
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	**display tcp** [**slot** *slot-number*]

操作	コマンド
示する	
TCPトラフィックの統計情報を表示する	**display tcp statistics** [**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*]]
UDP接続の概要情報を表示する	**display udp** [**slot** *slot-number*]
UDPトラフィックの統計情報を表示する	**display udp statistics** [**slot** *slot-number*]
UDP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**
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 **4-x-x** です。

15 章 UDP ヘルパー 15-1
15.1. UDP ヘルパー 15-1
15.2. UDP ヘルパーを使用したブロードキャストをユニキャストに変換する設定 15-1
15.3. UDP ヘルパーの表示と維持 15-2
15.4. UDP ヘルパー設定例 15-2
15.4.1. UDP を使用したブロードキャストをユニキャストに変換する設定例 15-2

15章 UDP ヘルパー

15.1. UDPヘルパー

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。

15.2. UDPヘルパーを使用したブロードキャストをユニキャストに変換する設定

I. ブロードキャストからユニキャストへの変換

ブロードキャストパケットを指定した UDP ポートのユニキャストパケットに変換するように設定ができます。

UDP ブロードキャストパケットを受け取ると、UDP 宛先ポート番号を設定された UDP ポート番号に変換します。

- マッチが見つかるならば、UDP ヘルパーはパケットを複写し、設定されたユニキャストアドレスにコピーの宛先 IP アドレスを修正します。そして、UDP ヘルパーはユニキャストパケットをユニキャストアドレスに転送します。
- マッチが見つからないならば、UDP ヘルパーはパケットを処理しません。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. 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 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。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。
4. interface view に移行する	**interface** *interface-type interface-number*	—

操作	コマンド	補足
5. 宛先サーバの IP アドレスを指定する	**udp-helper server** *ip-address* [**global**]	デフォルト：指定なし 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設定してください。 UDPパケットを転送する宛先IPアドレスとして、最大20の設定が可能です。

15.3. 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**

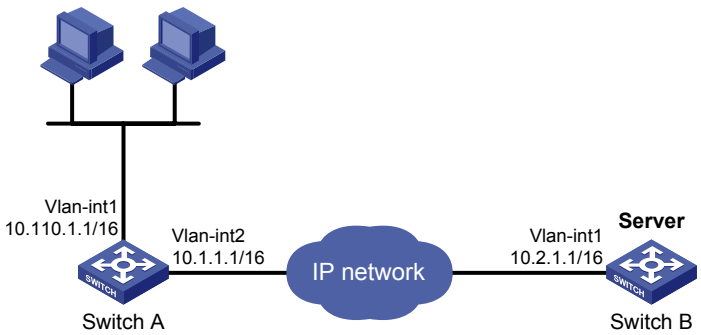
15.4. UDPヘルパー設定例

15.4.1. UDP を使用したブロードキャストをユニキャストに変換する設定例

I. ネットワーク要件

図 15-1 に示すように、ブロードキャストパケットを宛先サーバ(Switch B)の IP アドレス 10.2.1.1/16 に転送するように、UDP ヘルパーを設定します。Switch A はブロードキャストパケットを UDP 宛先ポート番号 55 のユニキャストパケットに変換し、宛先 IP アドレス 10.2.1.1/16 のサーバに転送します。

図 15-1 ネットワーク図



II. 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 で宛先サーバ 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

III. 設定の確認

VLAN インタフェース 1 で UDP ヘルパーによってブロードキャストパケットからユニキャストパケットに変換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 **4-x-x** です。

16 章 IPv6 の基本 16-1
16.1. 概要 16-1
16.1.1. IPv6 の機能 16-1
16.1.2. IPv6 アドレス 16-2
16.1.3. IPv6 path MTU discovery(IPv6 PMTU 探索) 16-5
16.1.4. IPv6 変換技術 16-6
16.1.5. プロトコルと標準 16-6
16.2. IPv6 の基本設定の作業リスト 16-7
16.3. IPv6 グローバルユニキャストアドレスの設定 16-7
16.3.1. IPv6 グローバルユニキャストアドレス 16-7
16.3.2. EUI-64 フォーマット IPv6 アドレスの作成 16-8
16.3.3. IPv6 グローバルユニキャストアドレスの手動設定 16-8
16.3.4. ステートレスアドレス自動設定 16-8
16.4. IPv6 リンクローカルアドレスの設定 16-9
16.4.1. IPv6 リンクローカルアドレス 16-9
16.4.2. 制限とガイドライン 16-9
16.4.3. インタフェースの IPv6 リンクローカルアドレスの自動生成の設定 16-10
16.4.4. IPv6 リンクローカルアドレスの手動割り当ての設定 16-10
16.5. IPv6 エニーキャストアドレスの設定 16-10
16.6. path MTU 探索(ディスカバリ)の設定 16-11
16.6.1. インタフェースの MTU の設定 16-11
16.6.2. IPv6 アドレスのスタティック path MTU の設定 16-11
16.6.3. path MTU のエージングタイマの設定 16-11
16.7. ICMPv6 メッセージ送信の管理 16-12
16.7.1. ICMPv6 エラーメッセージのレートリミットの設定 16-12
16.7.2. マルチキャストエコー要求への応答の有効化 16-13
16.7.3. ICMPv6s 宛先到達不能メッセージの有効化 16-13
16.7.4. ICMPv6 時間超過メッセージの送信の有効化 16-14
16.8. IPv6 の基本設定の表示と維持 16-14
16.9. IPv6 の基本設定例 16-15

16章 IPv6 の基本

16.1. 概要

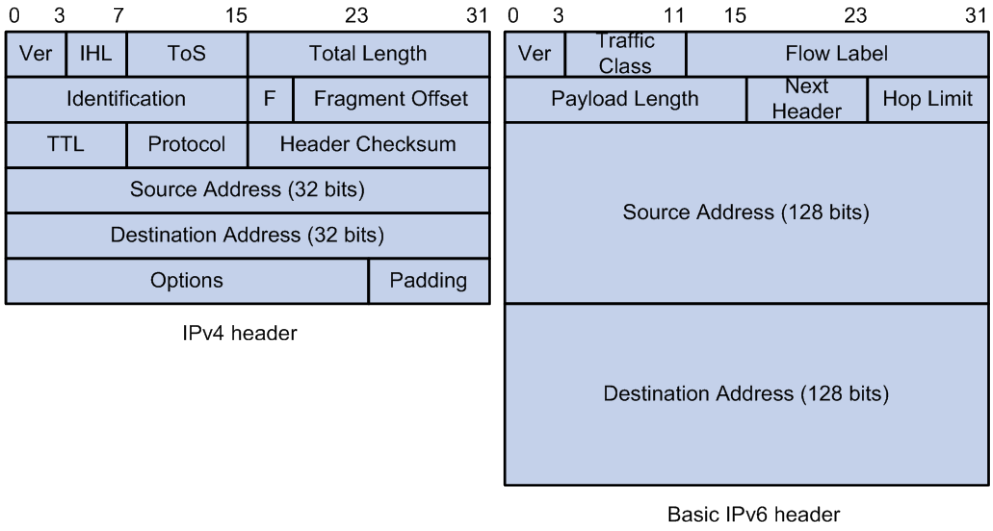
IPv6(Internet Protocol Version 6)は、IPv4(Internet Protocol Version 4)の後継として IETF(Internet Engineering Task Force)によって設計されました。IPv6 と IPv4 の大きな相違は、IP アドレスのサイズが 32 ビットから 128 ビットに増大している点です。

16.1.1. IPv6 の機能

I. ヘッダフォーマットの簡易化

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 16-1 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. ビルトインセキュリティ

IPv6 は IPsec を標準の拡張ヘッダとして使用し、エンドツーエンドのセキュリティを提供します。この機能はさまざまな IPv6 アプリケーション間の相互運用性を向上させます。

VI. 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。

VII. 拡張ネイバ検索(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。

VIII. 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。

16.1.2. 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とき、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。

  IPv6 にブロードキャストアドレスはありません。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、最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 16-1 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 16-1 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	ほかのフォーマット	－
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	

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
	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(最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(最も短縮した形式で表すと:)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 16-2 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 16-2 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
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ときに使用します。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

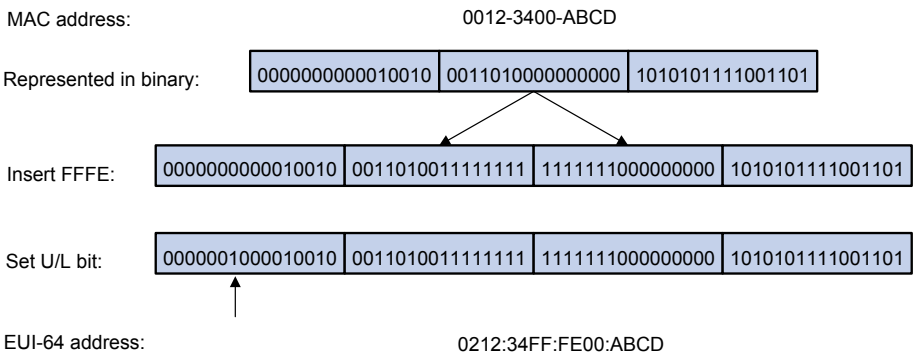
IPv6 ユニキャストアドレスのインタフェース識別子は、リンク上のインタフェースを識別するために使用され、リンク上で固有のものでなければなりません。インタフェース識別子は 64 ビット長です。

IEEE802 インタフェース(Ethernet インタフェース、VLAN インタフェースなど)ではインタフェースフォーマットのインタフェース識別子（ID）は、そのインタフェースのリンクレイヤアドレスから派生したものです。IPv6 アドレスのインタフェース識別子は 64 ビット長ですが、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。

1. 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。
2. 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 16-2 MAC アドレスから EUI-64 インタフェース識別子への変換



IEEE EUI-64 アドレスフォーマットのインタフェース識別子の低位 32 ビットはトンネルインタフェースの送信元 IPv4 アドレスです。ISATAP トンネルインタフェースの IEEE EUI-64 アドレスのインタフェース識別子の高位 32 ビットは 0000:5EFE です。ここでは他のインタフェースはすべて 0 です。

他のタイプのインタフェース(シリアルインタフェースなど)では、IEEE EUI-64 アドレスフォーマットのインタフェース識別子は、装置によってランダムに作成されます。

16.1.3. 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。

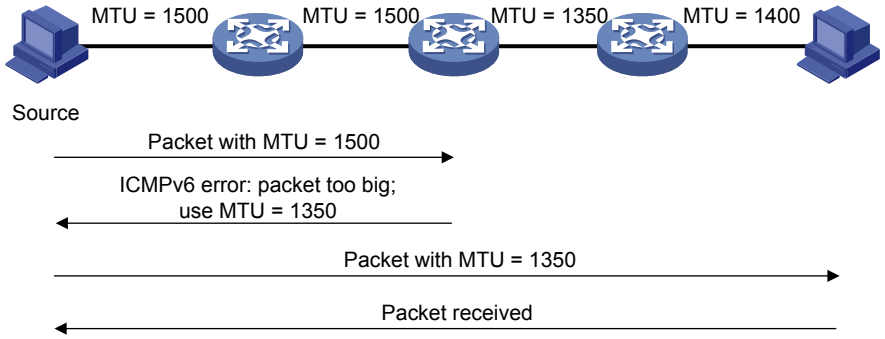
図 16-3 に PMTU ディスカバリの動作手順を示します。

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、以下の処理を行います。

- 装置は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。

図 16-3 Path MTU 探索(ディスカバリ)の処理



16.1.4. IPv6 変換技術

IPv6 変換技術を使用することで IPv4 と IPv6 間で通信を行うことができます。

I. Dual stack

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最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一意な 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。

II. トンネリング

トンネリングはあるネットワークプロトコルを他のネットワークプロトコルのパケットにカプセル化し、ネットワークを転送する技術です。

16.1.5. プロトコルと標準

- 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*

16.2. IPv6の基本設定の作業リスト

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 必要に応じて以下の作業を選択してください。 • 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) 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

16.3. IPv6グローバルユニキャストアドレスの設定

16.3.1. IPv6 グローバルユニキャストアドレス

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とき、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。

16.3.2. EUI-64 フォーマット IPv6 アドレスの作成

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

16.3.3. IPv6 グローバルユニキャストアドレスの手動設定

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. 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

16.3.4. ステートレスアドレス自動設定

I. ステートレスアドレス自動設定

ステートレスアドレス自動の設定は、受信した RA メッセージのアドレスプリフィックスとインタフェース ID を使用して IPv6 グローバルユニキャストアドレスを自動で生成するようにインタフェースを有効にします。Ethernet インタフェースあるいは VLAN インタフェースのような IEEE802 インタフェースでは、インタフェース ID はインタフェースの MAC アドレスをもとに作成され、グローバルで固有です。

II. 制限とガイドライン

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。

III. ステートレスアドレス自動設定の有効化

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. 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

16.4. IPv6リンクローカルアドレスの設定

16.4.1. IPv6 リンクローカルアドレス

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。

16.4.2. 制限とガイドライン

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。

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。
  - 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。
  - 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われます。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。

16.4.3. インタフェースの 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。

16.4.4. 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 link-local**	デフォルト：設定なし

16.5. 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

16.6. path MTU探索(ディスカバリ)の設定

16.6.1. インタフェースの MTU の設定

I. インタフェースの MTU

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。

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. インタフェースの MTU を設定する	**ipv6 mtu** *mtu-size*	デフォルト：設定なし

16.6.2. IPv6 アドレスのスタティック path MTU の設定

I. IPv6 アドレスのスタティック path MTU

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。(セクション 4 *IP サービス オペレーションマニュアル*の”*IPv6 の基本*”の”*path MTU discovery(IPv6 PMTU 探索)*”を参照してください。)

II. 設定手順

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

16.6.3. path MTU のエージングタイマの設定

I. ダイナミック path MTU のエージングタイマ

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(セクション 4 *IP サービス オペレーションマニュアル*の"*IPv6 の基本*"の"*IPv6 path MTU discovery*"を参照してください)、以下の処理を行います。

- path MTU にもとづいて送信元ホストはパケットを宛先ホストに送信します。

- path 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。

II. 制限とガイドライン

スタティック PMTU へのエージングタイマは無効です。

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. 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

16.7. ICMPv6メッセージ送信の管理

16.7.1. ICMPv6 エラーメッセージのレートリミットの設定

I. ICMPv6 エラーメッセージのレートリミット

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表す 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ときに、トークンはバケットから取り除かれます。バケットが空のとき、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。

II. 設定手順

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** *milliseconds* [*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。

16.7.2. マルチキャストエコー要求への応答の有効化

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

16.7.3. ICMPv6s 宛先到達不能メッセージの有効化

I. ICMPv6 宛先到達不能メッセージ

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**ーもしすべてのルートにパケットが一致しない場合、装置は、送信元にルートがないこと示す ICMPv6 エラーメッセージを送信します。
- **ICMPv6 Communication with Destination Administratively Prohibited メッセージ**ー装置がパケットの転送を禁止している場合（Firewall フィルタや ACL など）、装置は送信元に ICMPv6 Communication with Destination Network Administratively Prohibited ICMPv6 エラーメッセージを送信します。
- **ICMPv6 Beyond Scope of Source Address メッセージ**ー宛先が送信元 IPv6 アドレスの境界を超えている（たとえば、宛先 IPv6 アドレスがグローバルなユニキャストアドレスであるのに対して送信元 IPv6 アドレスがリンクローカルアドレスであるとき）場合、装置は、送信元に Beyond Scope of Source Address ICMPv6 エラーメッセージを送信します。
- **ICMPv6 Address Unreachable メッセージ**ーもし装置が宛先 IPv6 アドレスのリンクレイヤアドレスの解決ができない場合、装置は送信元に Address Unreachable ICMPv6 エラーメッセージを送信します。
- **ICMPv6 Port Unreachable メッセージ**ー装置向けの UDP パケットを受信したが UDP 宛先ポート番号がマッチしない場合、装置は送信元に Port Unreachable ICMPv6 エラーメッセージを送信します。

II. 制限とガイドライン

ICMPv6 宛先到達不能メッセージは、宛先が送信元装置から到達できないことを示します。攻撃者はネットワークの機能に影響する不正な ICMPv6 宛先到達不能メッセージを装置で作成するように偽の攻撃を行います。偽の攻撃からネットワークを防ぎ、不要なネットワークのトラフィックを減少させるため、ICMPv6 宛先到達不能メッセージの送信を無効にすることができます。

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. 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

16.7.4. ICMPv6 時間超過メッセージの送信の有効化

I. ICMPv6 時間超過メッセージの送信

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 のとき、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とき、ICMPv6 Fragment Reassembly Timeout メッセージを送信元に送信します。

II. 制限とガイドライン

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。

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. 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：無効

16.8. 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。

display tcp statistics コマンド、**display udp statistics** コマンド、**reset tcp statistics** コマンド、**reset udp statistics** コマンドの詳細は Chapter 4 *Layer 3 - IP Services Command References* の“*IP performance optimization commands*”を参照してください。

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**]
IPv6アドレスのPMTU情報を表示する	**display ipv6 pathmtu** { *ipv6-address* | { **all** | **dynamic** | **static** } [**count**] }
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*]

操作	コマンド
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アドレスのPMTU情報を削除する	**reset ipv6 pathmtu** { **all** | **dynamic** | **static** }
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**

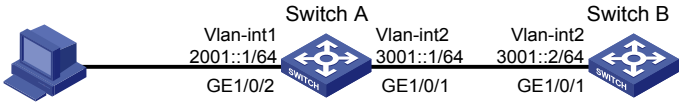
16.9. IPv6の基本設定例

I. ネットワーク要件

図 16-4 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 16-4 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指定します。

   <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指定します。

<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、ネクストホップアドレス 3001::1 の IPv6 スタティックルートを設定します。

[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    I-Invalid
IPv6 address                Link Layer      VID  Interface/Link ID      State T Age
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
```

Switch A、Switch B、Host 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
```

出力は、Switch B から Switch A、Host から Switch B、Switch A に ping が実行できることを示しています。

目次

このセクションのページは **4-x-x** です。

17 章 DHCPv6 の概要 17-1
17.1. DHCPv6 アドレス/プレフィックス割り当て 17-1
17.1.1. 2 つのメッセージによる高速割り当て 17-1
17.1.2. 4 つのメッセージによる割り当て 17-1
17.2. アドレス/プレフィックスのリース更新 17-2
17.3. ステートレス DHCPv6 17-3
17.4. DHCPv6 オプション 17-4
17.4.1. オプション 18 17-4
17.4.2. オプション 37 17-4
17.5. プロトコルと標準 17-5

17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。

17.1. DHCPv6アドレス/プレフィックス割り当て

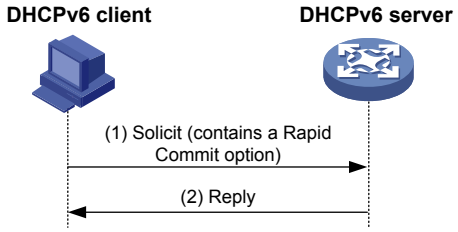
DHCPv6 アドレス/プレフィックスの割り当てのプロセスは 2 つあるいは 4 つのメッセージがあります。

17.1.1. 2 つのメッセージによる高速割り当て

図 17-1 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. もし 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。もし 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 17-1 2 つのメッセージによる高速割り当て



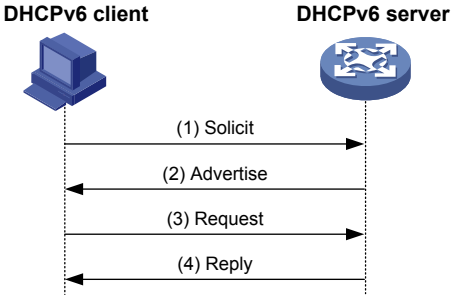
17.1.2. 4 つのメッセージによる割り当て

図 17-2 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 17-2 4 つのメッセージによる割り当て



17.2. 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 17-3 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

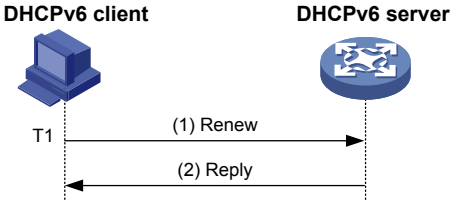


図 17-4 に示すように、T1 で DHCPv6 クライアントは DHCPv6 サーバに Renew メッセージを送信します。T1 で推奨する値は、preferred 期限の半分の値です。DHCPv6 サーバは、クライアントに、リースが更新されるかどうかを通知するため、Reply メッセージで応答します。

図 17-4 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

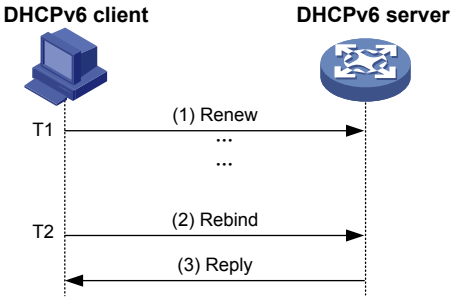


図 17-4 に示すように、処理します。

- 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、セクション 4 *IP サービス オペレーションマニュアル* の"*IPv6 の基本*"を参照してください。

17.3. 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 17-5 ステートレス DHCPv6 の動作

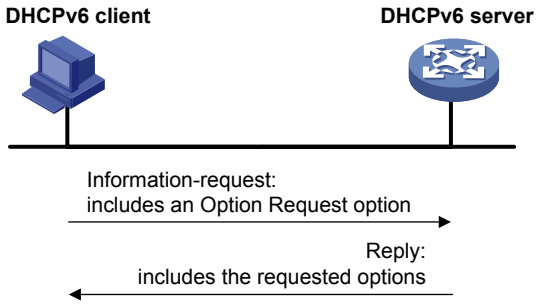


図 17-5 におけるステートレス DHCPv6 の動作を以下に示します。

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。もし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。もし一致しない場合、クライアントは設定パラメータを無視します。もし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。

17.4. DHCPv6オプション

17.4.1. 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 17-6 オプション 18 フォーマット

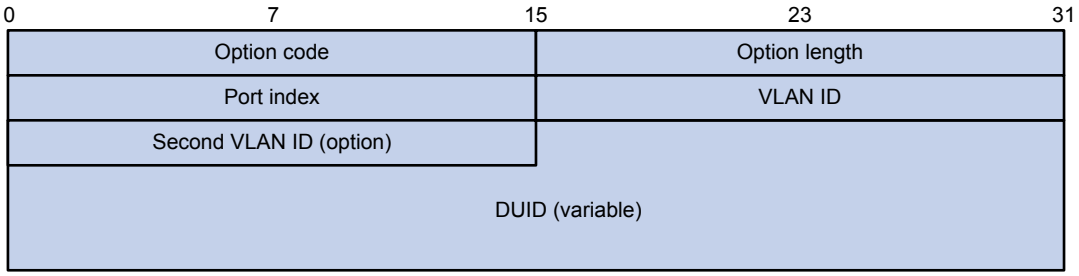


図 17-6 にオプション 18 のフォーマットを示します。以下のフィールドを示します。

- 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。

17.4.2. 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 17-7 オプション 37 フォーマット

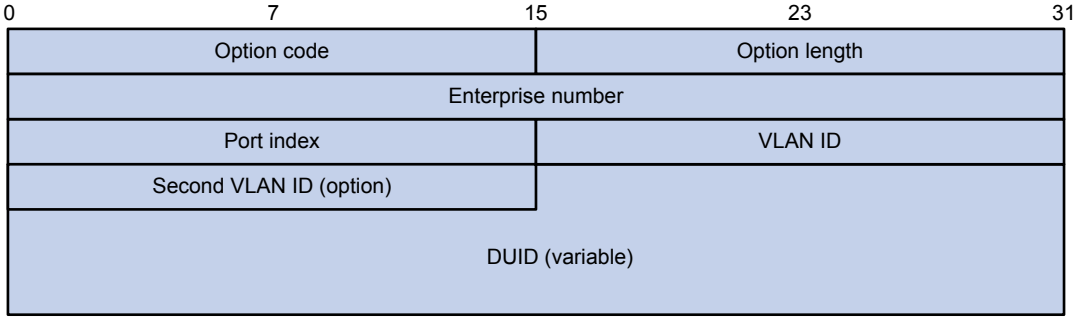


図 17-7 にオプション 37 のフォーマットを示します。以下のフィールドを示します。

- 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。

17.5. 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*

目次

このセクションのページは **4-x-x** です。

18 章 HTTP リダイレクト 18-1
18.1. 概要 18-1
18.2. HTTP リダイレクト設定作業リスト 18-1
18.3. HTTPS リダイレクトリスニングポート番号の指定 18-1
18.4. HTTPS リダイレクトサービスと SSL サーバポリシーの関連付け 18-2

18章 HTTP リダイレクト

18.1. 概要

HTTP リダイレクトはユーザの HTTP あるいは HTTPS 要求を指定した URL にリダイレクトします。以下の機能で使用されます。

- 802.1X 認証、MAC アドレス認証、ポートセキュリティのリダイレクト URL の割り当て
- 802.1X 認証の EAD アシスタント URL リダイレクト
- ポータルの URL リダイレクトサービス

18.2. HTTPリダイレクト設定作業リスト

作業リスト
HTTP要求をリダイレクトするために必要な設定はありません。 HTTPS要求をリダイレクトする場合、以下の処理を行います。 • HTTPS リダイレクトリスニングポート番号の指定 • (オプション設定項目) HTTPS リダイレクトサービスと SSL サーバポリシーの関連付け

18.3. HTTPSリダイレクトリスニングポート番号の指定

I. HTTPS リダイレクトリスニングポート番号

HTTPS 要求の HTTPS リダイレクトサービスが HTTPS 要求をリスニングする TCP ポート番号を指定すると、装置は HTTPS 要求をリダイレクトすることができます。

II. 制限とガイドライン

ポート番号の競合によるサービス使用不可を回避するために、既知のプロトコルで使用される TCP ポート番号を指定しないでください。また他の TCP ベースのサービスで使用される TCP ポート番号を指定しないでください。サービスで使用される TCP ポート番号を表示する場合、**display tcp** コマンドを使用してください。詳細は Chapter 4 *Layer 3–IP Services Command Reference* の“*IP performance optimization commands*”を参照してください。

複数設定を行った場合、最後に行った設定が適用されます。

III. 設定手順

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

操作	コマンド	補足
2. HTTPS リスニングポート番号を指定する	**http-redirect https-port** *port-number*	デフォルト：8443

メモ:

undo http-redirect https-port コマンドを実行すると、ポート番号指定なしに設定されます。デフォルト値に戻す場合は、**http-redirect https-port 8443** コマンドを実行してください。

18.4. HTTPSリダイレクトサービスとSSLサーバポリシーの関連付け

I. HTTPS リダイレクトサービスと SSL サーバポリシーの関連付け

HTTPS リダイレクトのセキュリティを向上させるために、SSL サーバポリシーを HTTPS リダイレクトサービスに関連付けることができます。詳細は、セクション 8 *セキュリティ オペレーション マニュアル*の“*SSL*”を参照してください。

II. 制限とガイドライン

関連する SSL サーバポリシーが存在しない場合、HTTPS リダイレクトは使用できません。最初に、存在しない SSL サーバポリシーを HTTPS リダイレクトサービスに関連付け、その後、SSL サーバポリシーを設定することができます。

HTTPS リダイレクトサービスに関連付けられた SSL サーバポリシーを変更する場合、新しいポリシーが即座に適用されます。

複数設定を行った場合、最後に行った設定が適用されます。

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. HTTPS リダイレクトサービスを SSL サーバポリシーに関連付ける	**http-redirect ssl-server-policy** *policy-name*	デフォルト：設定なし HTTPリダイレクトサービスはSelf割り当て証明書とデフォルトのSSLパラメータを使用します。

QX-S5300G シリーズ Ethernet スイッチ

オペレーションマニュアル

5. 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-スタティックルーティング
03-デフォルトルート
04-IPv6 スタティックルーティング
05-IPv6 デフォルトルート

目次

このセクションのページは **5-x-x** です。

1 章 IP ルーティングの基本 1-1
1.1. 概要 1-1
1.1.1. ルーティングテーブル 1-1
1.1.2. ルートのカテゴリ 1-1
1.1.3. ダイナミックルーティングプロトコル 1-2
1.1.4. ルートの優先順位 1-2
1.1.5. ロードバランス（負荷分散） 1-3
1.1.6. ルートバックアップ 1-3
1.1.7. ルート再帰 1-3
1.1.8. ルート再配信 1-3
1.2. RIB ルートの生存時間とラベルの設定 1-3
1.3. FIB ルートの最大生存時間の設定 1-4
1.4. ルート高速切り替えの有効化 1-5
1.5. 装置でサポートされるアクティブルートの最大数の設定 1-6
1.6. ルーティングテーブルの表示と維持 1-6

1章 IP ルーティングの基本

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。マルチキャストルーティングプロトコルの情報についてはセクション 6 *マルチキャスト オペレーションマニュアル*を参照してください。

1.1. 概要

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。パケットの宛先 IP アドレスをもとにして、ルータはルーティングテーブルからパケットのルートを検索し、ネクストホップにパケットを転送します。ルートは IP パケットの宛先を指示するために使用するパス情報です。

1.1.1. ルーティングテーブル

RIB (routing information base)はルート再帰、ルート再配信、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 テーブルの詳細はセクション 4 *IP サービス オペレーションマニュアル*の”*IP フォワーディングの基本*”を参照してください。

1.1.2. ルートのカテゴリ

表 1-1 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
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。
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。

1.1.3. ダイナミックルーティングプロトコル

スタティックルートは小規模で安定したネットワークで使われます。必要な設定とシステムリソースを少なくすることができます。構成が頻繁に変更するネットワークにおいては、ダイナミックルーティングプロトコルを設定することが一般的です。スタティックルーティングと比較して、ダイナミックルーティングは設定が複雑で、多くのルータとネットワークのリソースが必要となります。

ダイナミックルーティングは、構成の変更に適応した到達可能性の情報を、ダイナミックに収集し、報告します。ダイナミックルーティングは大規模のネットワークに適しています。

表 1-2 にダイナミックルーティングプロトコルのカテゴリを示します。

表 1-2 ダイナミックルーティングプロトコルのカテゴリ

基準	カテゴリ
動作の範囲	• **IGP**–AS 内で動作します。RIP、OSPF があります。 • **EGP**–AS 間で動作します。もっとも一般的な EGP は BGP です。
ルーティングアルゴリズム	• **ディスタンスベクタプロトコル**－RIP や BGP があります。BGP はパスベクタプロトコルにも該当します。 • **リンクステートプロトコル**－OSPF が含まれます。
宛先アドレスタイプ	• **ユニキャストルーティングプロトコル**–RIP、OSPF、BGP があります。 • マルチキャストルーティングプロトコル－PIM-SM があります。
IPバージョン	• **IPv4 ルーティングプロトコル**－RIP、OSPF、BGP があります。 • **IPv6 ルーティングプロトコル**－RIPng、OSPFv3、IPv6 BGP があります。

AS は同じルーティングポリシーを使用するルータのグループを示します。AS は同一管理者のもとで動作します。

1.1.4. ルートの優先順位

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、デフォルトで優先順位を持ちます。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もっとも高い優先順位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 1-3 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順位が高くなります。

表 1-3 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
Multicast static route	1
Unicast static route	60
Unknown (信用されていない送信元からのルート)	256

1.1.5. ロードバランス（負荷分散）

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。

1.1.6. 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、もっとも優先順位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とき、セカンダリルートの中でもっとも優先順位が高いルートでパケットが転送されます。障害が復旧したとき、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。

1.1.7. ルート再帰

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。

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。

1.1.8. ルート再配信

ルート再配信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配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配信の情報を記録します。

1.2. RIBルートの生存時間とラベルの設定

I. RIB ルートの生存時間とラベルの設定

この機能は、非常に多くのルートエントリあるいは長い GR 間隔によって、プロトコルの収束が非常に遅くなるために、特定のプロトコルのルートがエージアウトしてしまうことを防止します。

II. 制限とガイドライン

設定は次のプロトコルへの変更、あるいは RIB の処理の切り替わりで適用されます。

III. 設定手順(IPv4)

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. RIB view に移行する	**rib**	—
3. RIB IPv4 アドレスファミリーを作成し、RIB IPv4 address family view に移行する	**address-family ipv4**	—
4. RIB の IPv4 ルートとラベルの最大生存時間を設定する	**protocol** *protocol* **lifetime** *seconds*	デフォルト：480秒

IV. 設定手順(IPv6)

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. RIB view に移行する	**rib**	—
3. RIB IPv6 アドレスファミリーを作成し、RIB IPv6 address family view に移行する	**address-family ipv6**	—
4. RIB の IPv6 ルートとラベルの最大生存時間を設定する	**protocol** *protocol* **lifetime** *seconds*	デフォルト：480秒

1.3. FIBルートの最大生存時間の設定

I. FIB ルートの最大生存時間

GR が無効であるとき、プロトコルのプロセスの切り替えあるいは RIB のプロセスの切り替え後、FIB エントリは一定の間保持する必要があります。GR が有効であるとき、プロトコルのプロセスの切り替えあるいは RIB のプロセスの切り替え後､FIB エントリはすぐさま削除する必要があります。この機能はこの要件を満たすために設定します。

II. 設定手順(IPv4)

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. RIB view に移行する	**rib**	—
3. RIB IPv4 アドレスファミリーを作成し、RIB IPv4 address family view に移行する	**address-family ipv4**	—
4. FIB の IPv4 ルートの最大生存時間を設定する	**fib lifetime** *seconds*	デフォルト：600秒

III. 設定手順(IPv6)

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. RIB view に移行する	**rib**	—
3. RIB IPv6 アドレスファミリーを作成し、RIB IPv6 address family view に移行する	**address-family ipv6**	—
4. FIB の IPv6 ルートの最大生存時間を設定する	**fib lifetime** *seconds*	デフォルト：600秒

1.4. ルート高速切り替えの有効化

I. ルート高速切り替えの有効化

このコマンドは、ECMP ルート、プライマリ/セカンダリルートを含む多くのルートのために装置で同一の物理出力インタフェースを提供します。

インタフェースでリンク障害が発生したとき、装置は別のルートに切り替える前に以下の処理を実行する必要があります。

1. リンクのすべての ARP エントリを削除します。
2. 関連した FIB エントリを削除するため、FIB に指示します。

この手順は長い時間がかかり、トラフィックの中断が行われます。この問題を解決するため、ルートの高速切り替えを有効にすることができます。この機能はルートの切り替えを行うため、無効な FIB エントリを削除するため、装置が早急に FIB を指示するようにします。

II. 設定手順(IPv4)

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. ルート高速切り替えを有効にする	**ip route fast-switchover enable**	デフォルト：無効

III. 設定手順(IPv6)

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. ルート高速切り替えを有効にする	**ipv6 route fast-switchover enable**	デフォルト：無効

1.5. 装置でサポートされるアクティブルートの最大数の設定

I. 装置でサポートされるアクティブルートの最大数の設定

この機能により、装置がサポートするアクティブな IPv4/IPv6 ルートの最大数を設定できます。アクティブな IPv4/IPv6 ルートの最大数を超えると、装置はまだ新しいアクティブルートを受け入れますが、システムログメッセージを生成します。メッセージにもとづいて関連するアクションを実行して、システムリソースを節約できます。

II. 設定手順(IPv4)

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. RIB view に移行する	**rib**	—
3. RIB IPv4 アドレスファミリーを作成し、RIB IPv4 address family view に移行する	**address-family ipv4**	—
4. 装置でサポートされるアクティブルートの最大数を設定する	**routing-table limit** *number* **simply-alert**	デフォルト：設定なし RIB IPv4 address family view での設定は、パブリックネットワークのアクティブIPv4 ルートの数を制限します。

III. 設定手順(IPv6)

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. RIB view に移行する	**rib**	—
3. RIB IPv6 アドレスファミリーを作成し、RIB IPv6 address family view に移行する	**address-family ipv6**	—
4. 装置でサポートされるアクティブルートの最大数を設定する	**routing-table limit** *number* **simply-alert**	デフォルト：設定なし RIB IPv6 address family view での設定は、パブリックネットワークのアクティブIPv6 ルートの数を制限します。

1.6. 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**] **display ip routing-table** [**all-routes**]
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** [**all-routes**] **statistics**
IPv6 RIB GRの状態情報を表示する	**display ipv6 rib graceful-restart**
IPv6ルーティングテーブルの情報を表示する	**display ipv6 routing-table** [**verbose**] **display ipv6 routing-table** [**all-routes**]
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**]
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**]
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** [**all-routes**] **statistics**
RIB GRの状態情報を表示する	**display rib graceful-restart**
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 **5-x-x** です。

2 章 スタティックルーティング 2-1
2.1. 概要 2-1
2.2. スタティックルートの設定 2-1
2.3. スタティックルートの削除 2-1
2.4. スタティックルートでの BFD の設定 2-2
2.4.1. 概要 2-2
2.4.2. 双方向コントロールモードの設定 2-2
2.4.3. Single ホップエコーパケットモード 2-3
2.5. スタティックルートの表示と維持 2-3
2.6. スタティックルートの設定例 2-4
2.6.1. 基本的なスタティックルートの設定例 2-4
2.6.2. BFD スタティックルートの設定例(ダイレクトネクストホップ) 2-6
2.6.3. BFD スタティックルートの設定例(インダイレクトネクストホップ) 2-8

2章 スタティックルーティング

2.1. 概要

スタティックルートは手動で設定します。ネットワークの構成が簡単であれば、スタティックルートの設定だけで問題なく運用することができます。

ただし、ネットワーク障害やトポロジーの変化が起きた場合、ネットワーク管理者がスタティックルートを修正する必要があります。

2.2. スタティックルートの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. スタティックルートを設定する	**ip route-static** *dest-address* { *mask-length* | *mask* } { *interface-type interface-number* [*next-hop-address*] | *next-hop-address* } [**permanent** | **track** *track-entry-number*] [**preference** *preference*] [**tag** *tag-value*] [**description** *text*]	デフォルト：設定なし ネクストホップへの到達可能性をモニタするため、スタティックルートとTrackを関連づけることができます。Trackの詳細はセクション 9 *高可用性 オペレーションマニュアル* の”*Track*”を参照してください。
3. (オプション設定項目) スタティックルートのデフォルトプリファレンスを設定する	**ip route-static default-preference** *default-preference-value*	デフォルト：60

2.3. スタティックルートの削除

I. スタティックルートの削除

1 つのスタティックルートを削除するには、**undo route-static** コマンドを使用します。

デフォルトルートを含むすべてのスタティックルートを削除するには、**delete static-routes all** コマンドを使用します。

II. 設定手順

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

操作	コマンド	補足
2. すべてのスタティックルートを削除する	**delete static-routes all**	—

2.4. スタティックルートでのBFDの設定

⚠ 重要:

BFD が有効になっていると、ルートフラップを悪化させる可能性があります。

2.4.1. 概要

BFD(Bidirectional forwarding detection)は、一般的な用途、標準な用途、および手段、プロトコルから独立して、素早い障害検知メカニズムを提供します。BFD は、ルーティングプロトコルのような上位層のプロトコルの 2 台のルータ間の双方向の転送経路の障害を、一様で早急に検出することができます。

BFD に関する詳細は、セクション 9 *高可用性 オペレーションマニュアル*の"*BFD*"を参照してください。

2.4.2. 双方向コントロールモードの設定

I. 双方向コントロールモード

2 つの装置間で双方向検知を行うため、BFD コントロールパケットを使用する場合、各装置のピア宛のスタティックルートで BFD コントロールパケットモードを有効にする必要があります。

スタティックルートを設定し、BFD コントロールパケットモードを有効にするために、以下の 1 つを使用します。

- 出力インタフェースと直接接続されたネクストホップを指定します。
- 直接接続されていないネクストホップと指定された BFD パケットの送信元アドレスを指定します。

II. スタティックルート(ダイレクトネクストホップ)での BFD コントロールモードの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. スタティックルートで BFD コントロールパケットモードを有効にする	**ip route-static** *dest-address* { *mask-length* | *mask* } *interface-type interface-number next-hop-address* **bfd control-packet** [**preference** *preference*] [**tag** *tag-value*] [**description** *text*]	デフォルト：設定なし

III. スタティックルート(インダイレクトネクストホップ)での BFD コントロールモードの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. スタティックルートで BFD コントロールパケットモードを有効にする	**ip route-static** *dest-address* { *mask-length* | *mask* } { *next-hop-address* **bfd control-packet bfd-source** *ip-address* } [**preference** *preference*] [**tag tag-value**] [**description** *text*]	デフォルト：設定なし

2.4.3. Single ホップエコーパケットモード

I. Single ホップエコーパケットモード

スタティックルートで BFD エコーパケットモードを有効にすると、ローカル装置は BFD エコーパケットをピアへ送信します。ピアからの応答によって装置間のリンクのテストを行います。

⚠ 重要:

BFD はスプーフィング属性の出力インタフェースでスタティックルートを設定することはできません。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. エコーパケットの送信元アドレスを設定する	**bfd echo-source-ip** *ip-address*	デフォルト：設定なし 詳細はChapter 9 *High Availability Command Referencesの”BFD commands”*を参照してください。
3. スタティックルートで BFD エコーパケットモードを有効にする	**ip route-static** *dest-address* { *mask-length* | *mask* } *interface-type interface-number next-hop-address* **bfd echo-packet** [**preference** *preference*] [**tag** *tag-value*] [**description** *text*]	デフォルト：設定なし

2.5. スタティックルートの表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
スタティックルート情報を表示する	**display ip routing-table protocol static** [**inactive** | **verbose**]

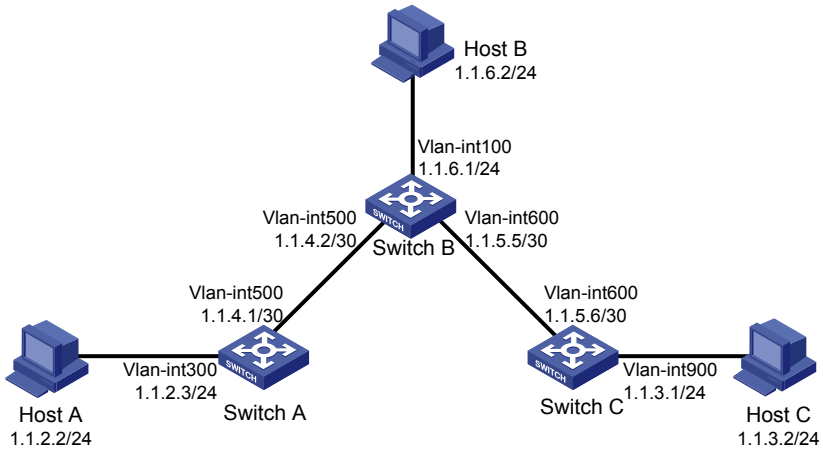
2.6. スタティックルートの設定例

2.6.1. 基本的なスタティックルートの設定例

I. ネットワーク要件

図 2-1 に示すように、2 つのホスト間で相互接続できるように、スイッチでスタティックルートを設定します。

図 2-1 ネットワーク図



II. 設定手順

1. 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. スタティックルートを設定します。

   # Switch A にデフォルトルートを設定します。

   ```
   <SwitchA> system-view
   [SwitchA] ip route-static 0.0.0.0 0.0.0.0 1.1.4.2
   ```

   # Switch B に 2 つのスタティックルートを設定します。

   ```
   <SwitchB> system-view
   [SwitchB] ip route-static 1.1.2.0 255.255.255.0 1.1.4.1
   [SwitchB] ip route-static 1.1.3.0 255.255.255.0 1.1.5.6
   ```

   # Switch C にデフォルトルートを設定します。

   ```
   <SwitchC> system-view
   [SwitchC] ip route-static 0.0.0.0 0.0.0.0 1.1.5.5
   ```

3. Host A、Host B、Host C にそれぞれ 1.1.2.3、1.1.6.1、1.1.3.1 のデフォルトゲートウェイアドレスを設定します。(詳細は省略します)

III. 設定の確認

Switch A のスタティックルートを表示します。

```
[SwitchA] display ip routing-table protocol static

Summary Count : 1

Static Routing table Status : <Active>
Summary Count : 1

Destination/Mask    Proto   Pre  Cost         NextHop         Interface
0.0.0.0/0           Static 60   0            1.1.4.2         Vlan500

Static Routing table Status : <Inactive>
Summary Count : 0
```

Switch B のスタティックルートを表示します。

```
[SwitchB] display ip routing-table protocol static

Summary Count : 2

Static Routing table Status : <Active>
Summary Count : 2

Destination/Mask    Proto   Pre  Cost         NextHop         Interface
1.1.2.0/24          Static 60   0            1.1.4.1         Vlan500

Static Routing table Status : <Inactive>
Summary Count : 0
```

Host B で **ping** コマンドを使用し、ホスト A への接続を確認します。(2 つのホストは Windows XP で動作していると仮定します。)

```
C:\Documents and Settings\Administrator>ping 1.1.2.2

Pinging 1.1.2.2 with 32 bytes of data:

Reply from 1.1.2.2: bytes=32 time=1ms TTL=126
Reply from 1.1.2.2: bytes=32 time=1ms TTL=126
Reply from 1.1.2.2: bytes=32 time=1ms TTL=126
Reply from 1.1.2.2: bytes=32 time=1ms TTL=126

Ping statistics for 1.1.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

Host B で **tracert** コマンドを使用し、Host A への接続を確認します。

```
C:\Documents and Settings\Administrator>tracert 1.1.2.2
```

```
Tracing route to 1.1.2.2 over a maximum of 30 hops

  1    <1 ms    <1 ms    <1 ms  1.1.6.1
  2    <1 ms    <1 ms    <1 ms  1.1.4.1
  3     1 ms    <1 ms    <1 ms  1.1.2.2

Trace complete.
```

2.6.2. BFD スタティックルートの設定例(ダイレクトネクストホップ)

I. ネットワーク要件

図 2-2 に示すように設定します。

- Switch A のサブネット 120.1.1.0/24 にスタティックルートを設定します。
- Switch B のサブネット 121.1.1.0/24 にスタティックルートを設定します。
- 両方のルートに BFD を有効にします。
- Switch C のサブネット 120.1.1.0/24、121.1.1.0/24 にスタティックルートを設定します。

レイヤ 2 スイッチを経由した Switch A と Switch B 間のリンクが故障したとき、すぐに故障を検出し、Switch C を使用して Switch A と Switch B 間で通信ができるように BFD を有効にします。

図 2-2 ネットワーク図

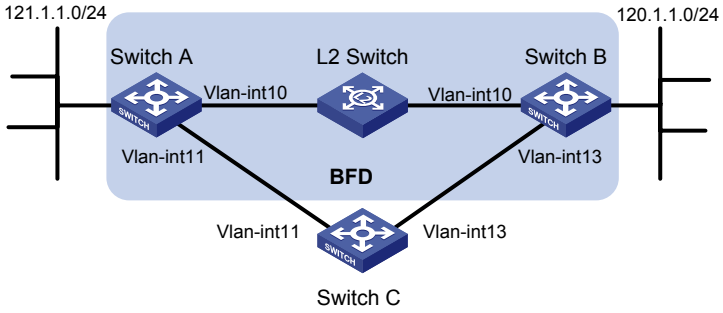


表 2-1 インタフェースと IP アドレスの割り当て

装置	インタフェース	IP アドレス
Switch A	VLAN-interface 10	12.1.1.1/24
Switch A	VLAN-interface 11	10.1.1.102/24
Switch B	VLAN-interface 10	12.1.1.2/24
Switch B	VLAN-interface 13	13.1.1.1/24
Switch C	VLAN-interface 11	10.1.1.100/24
Switch C	VLAN-interface 13	13.1.1.2/24

II. 設定手順

1. 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. スタティックルートと BFD を設定します。

Switch A にスタティックルートを設定し、レイヤ 2 スイッチを通してスタティックルートを行うため BFD コントロールパケットモードを有効にします。

```
<SwitchA> system-view
[SwitchA] interface vlan-interface 10
[SwitchA-vlan-interface10] bfd min-transmit-interval 500
[SwitchA-vlan-interface10] bfd min-receive-interval 500
[SwitchA-vlan-interface10] bfd detect-multiplier 9
[SwitchA-vlan-interface10] quit
[SwitchA] ip route-static 120.1.1.0 24 vlan-interface 10 12.1.1.2 bfd control-packet
[SwitchA] ip route-static 120.1.1.0 24 vlan-interface 11 10.1.1.100 preference 65
[SwitchA] quit
```

Switch B にスタティックルートを設定し、レイヤ 2 スイッチを通してスタティックルートを行うため BFD コントロールパケットモードを有効にします。

```
<SwitchB> system-view
[SwitchB] interface vlan-interface 10
[SwitchB-vlan-interface10] bfd min-transmit-interval 500
[SwitchB-vlan-interface10] bfd min-receive-interval 500
[SwitchB-vlan-interface10] bfd detect-multiplier 9
[SwitchB-vlan-interface10] quit
[SwitchB] ip route-static 121.1.1.0 24 vlan-interface 10 12.1.1.1 bfd control-packet
[SwitchB] ip route-static 121.1.1.0 24 vlan-interface 13 13.1.1.2 preference 65
[SwitchB] quit
```

Switch C でスタティックルートを設定します。

```
<SwitchC> system-view
[SwitchC] ip route-static 120.1.1.0 24 13.1.1.1
[SwitchC] ip route-static 121.1.1.0 24 10.1.1.102
```

III. 設定の確認

Switch A の BFD セッションを表示します。

```
<SwitchA> display bfd session

 Total Session Num: 1     Up Session Num: 1     Init Mode: Active

 IPv4 Session Working Under Ctrl Mode:

 LD/RD          SourceAddr      DestAddr        State    Holdtime     Interface
 4/7            12.1.1.1        12.1.1.2        Up       2000ms       Vlan10
```

出力は、BFD セッションが作成されたことを示しています。

Switch A のスタティックルート情報を表示します。

```
<SwitchA> display ip routing-table protocol static

Summary Count : 1
```

```
Static Routing table Status : <Active>
Summary Count : 1

Destination/Mask    Proto   Pre  Cost          NextHop         Interface
120.1.1.0/24        Static 60   0             12.1.1.2        Vlan10

Static Routing table Status : <Inactive>
Summary Count : 0
```

出力では、Switch A は VLAN インタフェース 10 を経由して Switch B と通信していることを示しています。

そして VLAN インタフェース 10 を経由したリンクが故障します。

Switch A のスタティックルート情報を表示します。

```
<SwitchA> display ip routing-table protocol static

Summary Count : 1

Static Routing table Status : <Active>
Summary Count : 1

Destination/Mask    Proto   Pre  Cost          NextHop         Interface
120.1.1.0/24        Static 65   0             10.1.1.100      Vlan11

Static Routing table Status : <Inactive>
Summary Count : 0
```

出力では、Switch A は VLAN インタフェース 11 を経由して Switch B と通信していることを示しています。

2.6.3. BFD スタティックルートの設定例(インダイレクトネクストホップ)

I. ネットワーク要件

図 2-3 に示すように設定します。

- Switch A は、VLAN インタフェース 10 の出力インタフェースで Switch B のループバック 1(2.2.2.9/32)へのルートを持っています。
- Switch B は、VLAN インタフェース 12 の出力インタフェースで Switch B のループバック 1(1.1.1.9/32)へのルートを持っています。
- Switch D は、VLAN インタフェース 10 の出力インタフェースで 1.1.1.9/32、VLAN インタフェース 12 の出力インタフェースにて 2.2.2.9/32 へのルートを持っています。

以下のようにスタティックルートを設定します。

- Switch A にサブネット 120.1.1.0/24 のスタティックルートを設定します。
- Switch B にサブネット 121.1.1.0/24 のスタティックルートを設定します。
- 両方のルートで BFD を有効にします。

- Switch C と Switch D の両方でサブネット 120.1.1.0/24 とサブネット 121.1.1.0/24 へのスタティックルートを設定します。

Switch A と Switch B 間の Switch D が故障したとき、すぐさま Switch C で検出し、通信できるように BFD を有効にします。

図 2-3 ネットワーク図

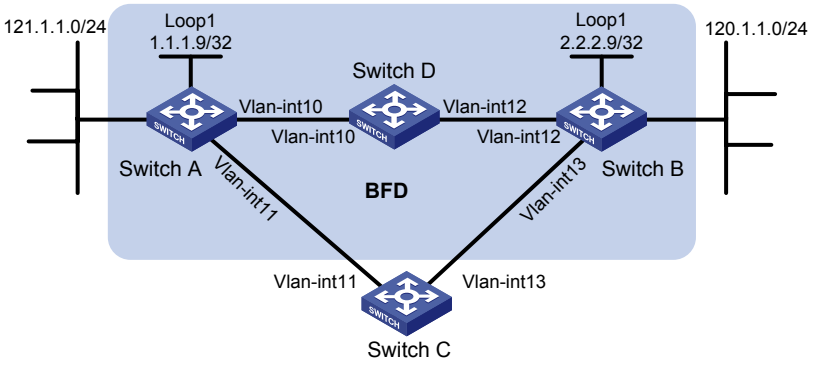


表 2-2 インタフェースと IP アドレスの割り当て

装置	インタフェース	IP アドレス
Switch A	VLAN-interface 10	12.1.1.1/24
Switch A	VLAN-interface 11	10.1.1.102/24
Switch A	Loopback 1	1.1.1.9/32
Switch B	VLAN-interface 12	11.1.1.1/24
Switch B	VLAN-interface 13	13.1.1.1/24
Switch B	Loopback 1	2.2.2.9/32
Switch C	VLAN-interface 11	10.1.1.100/24
Switch C	VLAN-interface 13	13.1.1.2/24
Switch D	VLAN-interface 10	12.1.1.2/24
Switch D	VLAN-interface 12	11.1.1.2/24

II. 設定手順

1. 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. スタティックルートと BFD を設定します。

   # Switch A にスタティックルートを設定し、Switch D を通してスタティックルートを行うため BFD コントロールパケットモードを有効にします。

```
<SwitchA> system-view
[SwitchA] bfd multi-hop min-transmit-interval 500
[SwitchA] bfd multi-hop min-receive-interval 500
[SwitchA] bfd multi-hop detect-multiplier 9
[SwitchA] ip route-static 120.1.1.0 24 2.2.2.9 bfd control-packet bfd-source 1.1.1.9
[SwitchA] ip route-static 120.1.1.0 24 vlan-interface 11 10.1.1.100 preference 65
```

```
[SwitchA] quit
```

Switch B にスタティックルートを設定し、Switch D を通してスタティックルートを行うため BFD コントロールパケットモードを有効にします。

```
<SwitchB> system-view
[SwitchB] bfd multi-hop min-transmit-interval 500
[SwitchB] bfd multi-hop min-receive-interval 500
[SwitchB] bfd multi-hop detect-multiplier 9
[SwitchB] ip route-static 121.1.1.0 24 1.1.1.9 bfd control-packet bfd-source 2.2.2.9
[SwitchB] ip route-static 121.1.1.0 24 vlan-interface 13 13.1.1.2 preference 65
[SwitchB] quit
```

Switch C でスタティックルートを設定します。

```
<SwitchC> system-view
[SwitchC] ip route-static 120.1.1.0 24 13.1.1.1
[SwitchC] ip route-static 121.1.1.0 24 10.1.1.102
```

Switch D でスタティックルートを設定します。

```
<SwitchD> system-view
[SwitchD] ip route-static 120.1.1.0 24 11.1.1.1
[SwitchD] ip route-static 121.1.1.0 24 12.1.1.1
```

III. 設定の確認

Switch A の BFD セッションを表示します。

```
<SwitchA> display bfd session

 Total Session Num: 1     Up Session Num: 1     Init Mode: Active

 IPv4 Session Working Under Ctrl Mode:

 LD/RD          SourceAddr      DestAddr        State    Holdtime    Interface
 4/7            1.1.1.9         2.2.2.9         Up       2000ms      N/A
```

出力では BFD セッションが作成されたことを示しています。

Switch A のスタティックルートを表示します。

```
<SwitchA> display ip routing-table protocol static

Summary Count : 1

Static Routing table Status : <Active>
Summary Count : 1

Destination/Mask    Proto   Pre  Cost         NextHop         Interface
120.1.1.0/24        Static 60   0            12.1.1.2        Vlan10

Static Routing table Status : <Inactive>
Summary Count : 0
```

出力では、Switch A は VLAN インタフェース 10 を経由して Switch B と通信していることを示しています。

そして VLAN インタフェース 10 を経由したリンクが故障します。

Switch A のスタティックルートを表示します。

```
<SwitchA> display ip routing-table protocol static

Summary Count : 1

Static Routing table Status : <Active>
Summary Count : 1

Destination/Mask    Proto   Pre  Cost          NextHop         Interface
120.1.1.0/24        Static 65    0             10.1.1.100      Vlan11

Static Routing table Status : <Inactive>
Summary Count : 0
```

出力では、Switch A は VLAN インタフェース 11 を経由して Switch B と通信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 **5-x-x** です。

3 章 デフォルトルート 3-1

3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、ICMP 到達不能パケットが送信元に送信されます。

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。詳細はセクション 5 *ルーティングプロトコル オペレーションマニュアル*の"*スタティックルーティング*"を参照してください。

目次

このセクションのページは **5-x-x** です。

4 章 IPv6 スタティックルーティング 4-1
4.1. 概要 4-1
4.2. IPv6 スタティックルートの設定 4-1
4.3. IPv6 スタティックルートの削除 4-1
4.4. IPv6 スタティックルートでの BFD の設定 4-2
4.4.1. 概要 4-2
4.4.2. 制限とガイドライン 4-2
4.4.3. 双方向コントロールモードの設定 4-2
4.5. IPv6 スタティックルートの表示と維持 4-3
4.6. IPv6 スタティックルートの設定例 4-3
4.6.1. 基本的な IPv6 スタティックルートの設定例 4-3
4.6.2. BFD の IPv6 スタティックルートの設定例(ダイレクトネクストホップ) 4-5
4.6.3. BFD の IPv6 スタティックルートの設定例(インダイレクトネクストホップ) 4-8

4章 IPv6 スタティックルーティング

4.1. 概要

スタティックルートは手動で設定されます。ネットワークのトポロジの変化に対応できません。ネットワークが故障、あるいはトポロジの変更が行われた場合、ネットワーク管理者は手動でスタティックルートを修正する必要があります。IPv6 スタティックルーティングも同様に簡単な IPv6 ネットワークで動作します。

4.2. IPv6スタティックルートの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. IPv6 スタティックルートを設定する	**ipv6 route-static** *ipv6-address prefix-length* { *interface-type interface-number* [*next-hop-address*] | *next-hop-address* } [**permanent**] [**preference** *preference*] [**tag** *tag-value*] [**description** *text*]	デフォルト：設定なし
3. (オプション設定項目)IPv6 スタティックルートのデフォルトプリファレンスを設定する	**ipv6 route-static default-preference** *default-preference-value*	デフォルト：60

4.3. IPv6スタティックルートの削除

I. IPv6 スタティックルートの削除

1 つのスタティックルートを削除するには、**undo route-static** コマンドを使用します。

デフォルトルートを含むすべてのスタティックルートを削除するには、**delete static-routes all** コマンドを使用します。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. すべてのスタティックルートを削除する	**delete ipv6 static-routes all**	—

4.4. IPv6スタティックルートでのBFDの設定

4.4.1. 概要

BFD(Bidirectional forwarding detection)は、一般的な用途、標準な用途、および手段、プロトコルから独立して、素早い障害検知メカニズムを提供します。BFD は、IPv6 ルーティングプロトコルのような上位層のプロトコルの 2 台のルータ間の双方向の転送経路の障害を、一様で早急に検出することができます。

BFD に関する詳細は、セクション 9 *高可用性 オペレーションマニュアル*の"*BFD*"を参照してください。

4.4.2. 制限とガイドライン

BFD が有効になっていると、ルートフラップを悪化させる可能性があります。

4.4.3. 双方向コントロールモードの設定

I. 双方向コントロールモード

2 つの装置間で双方向検知を行うため、BFD コントロールパケットを使用する場合、各装置のピア宛のスタティックルートで BFD コントロールパケットモードを有効にする必要があります。

スタティックルートを設定し、BFD コントロールパケットモードを有効にするために、以下の 1 つを使用します。

- 出力インタフェースと直接接続されたネクストホップを指定します。
- 直接接続されていないネクストホップと指定された BFD パケットの送信元アドレスを指定します。

II. IPv6 スタティックルート(ダイレクトネクストホップ)での BFD コントロールモードの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. スタティックルートで BFD コントロールパケットモードを有効にする	**ipv6 route-static** *ipv6-address prefix-length interface-type interface-number next-hop-address* **bfd control-packet** [**bfd-source** *ipv6-address*] [**preference** *preference*] [**tag** *tag-value*] [**description** *text*]	デフォルト：設定なし

III. IPv6 スタティックルート(インダイレクトネクストホップ)での BFD コントロールモードの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. スタティックルートで BFD コントロールパケットモードを有効にする	**ipv6 route-static** *ipv6-address prefix-length* { *next-hop-address* **bfd control-packet bfd-source** *ipv6-address* } [**preference** *preference*] [**tag** *tag-value*] [**description** *text*]	デフォルト：設定なし

4.5. IPv6 スタティックルートの表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
IPv6スタティックルート情報を表示する	**display ipv6 routing-table protocol static** [**inactive** | **verbose**]

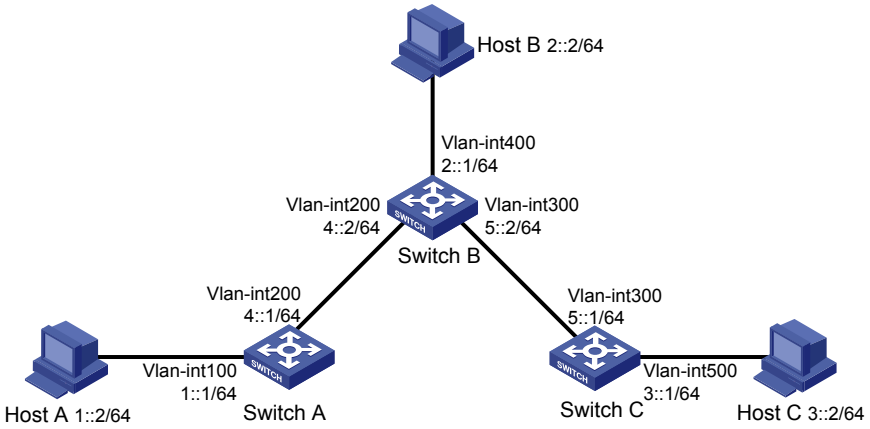
4.6. IPv6スタティックルートの設定例

4.6.1. 基本的な IPv6 スタティックルートの設定例

I. ネットワーク要件

図 4-1 に示すように、2 つのホスト間で相互接続できるように、スイッチで IPv6 スタティックルートを設定します。

図 4-1 ネットワーク図



II. 設定手順

1. すべての VLAN インタフェースの IPv6 アドレスを設定します。(詳細は省略します)
2. IPv6 スタティックルートを設定します。

   # Switch A にデフォルトの IPv6 スタティックルートを設定します。

   ```
   <SwitchA> system-view
   [SwitchA] ipv6 route-static :: 0 4::2
   ```

   # Switch B に 2 つの IPv6 スタティックルートを設定します。

   ```
   <SwitchB> system-view
   [SwitchB] ipv6 route-static 1:: 64 4::1
   [SwitchB] ipv6 route-static 3:: 64 5::1
   ```

   # Switch C にデフォルトの IPv6 スタティックルートを設定します。

   ```
   <SwitchC> system-view
   [SwitchC] ipv6 route-static :: 0 5::2
   ```

3. すべてのホストの IPv6 アドレスを設定し、Host A、Host B、Host C にそれぞれ 1::1、2::1、3::1 のデフォルトゲートウェイアドレスを設定します。(詳細は省略します)

III. 設定の確認

Switch A の IPv6 スタティックルートを表示します。

```
[SwitchA] display ipv6 routing-table protocol static

Summary Count : 1

Static Routing table Status : <Active>
Summary Count : 1

Destination: ::                                     Protocol   : Static
NextHop    : 4::2                                   Preference: 60
Interface  : Vlan-interface200                      Cost       : 0

Static Routing table Status : <Inactive>
Summary Count : 0
```

Switch B の IPv6 スタティックルートを表示します。

```
[SwitchB] display ipv6 routing-table protocol static

Summary Count : 2

Static Routing table Status : <Active>
Summary Count : 2

Destination: 1::/64                                 Protocol   : Static
NextHop    : 4::1                                   Preference: 60
Interface  : Vlan-interface200                      Cost       : 0

Destination: 3::/64                                 Protocol   : Static
NextHop    : 5::1                                   Preference: 60
```

```
Interface   : Vlan-interface300                    Cost       : 0

Static Routing table Status : <Inactive>
Summary Count : 0
```

 # ping コマンドを使用して接続を確認します。

```
[SwitchA] ping ipv6 3::1
Ping6(56 data bytes) 4::1 --> 3::1, press CTRL_C to break
56 bytes from 3::1, icmp_seq=0 hlim=62 time=0.700 ms
56 bytes from 3::1, icmp_seq=1 hlim=62 time=0.351 ms
56 bytes from 3::1, icmp_seq=2 hlim=62 time=0.338 ms
56 bytes from 3::1, icmp_seq=3 hlim=62 time=0.373 ms
56 bytes from 3::1, icmp_seq=4 hlim=62 time=0.316 ms

--- Ping6 statistics for 3::1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.316/0.416/0.700/0.143 ms
```

4.6.2. BFD の IPv6 スタティックルートの設定例(ダイレクトネクストホップ)

I. ネットワーク要件

図 4-2 に示すように設定します。

- Switch A のサブネット 120::/64 に IPv6 スタティックルートを設定します。
- Switch B のサブネット 121::/64 に IPv6 スタティックルートを設定します。
- 両方のルートに BFD を有効にします。
- Switch C のサブネット 120::/64、121::/64 にスタティックルートを設定します。

レイヤ 2 スイッチを経由した Switch A と Switch B 間のリンクが故障したとき、すぐに故障を検出し、Switch C を使用して Switch A と Switch B 間で通信ができるように BFD を有効にします。

図 4-2 ネットワーク図

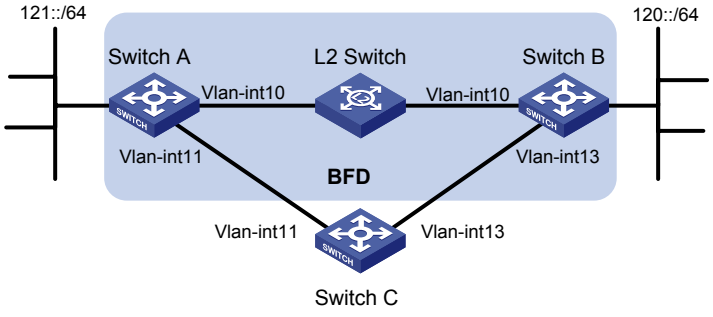


表 4-1 インタフェースと IPv6 アドレスの割り当て

装置	インタフェース	IPv6 アドレス
Switch A	Vlan-int10	12::1/64

装置	インタフェース	IPv6 アドレス
Switch A	Vlan-int11	10::102/64
Switch B	Vlan-int10	12::2/64
Switch B	Vlan-int13	13::1/64
Switch C	Vlan-int11	10::100/64
Switch C	Vlan-int13	13::2/64

II. 設定手順

1. インタフェースの IPv6 アドレスを設定します。(詳細は省略します)
2. IPv6 スタティックルートと BFD を設定します。

Switch A に IPv6 スタティックルートを設定し、レイヤ 2 スイッチを通してスタティックルートを行うため BFD コントロールパケットモードを有効にします。

```
<SwitchA> system-view
[SwitchA] interface vlan-interface 10
[SwitchA-vlan-interface10] bfd min-transmit-interval 500
[SwitchA-vlan-interface10] bfd min-receive-interval 500
[SwitchA-vlan-interface10] bfd detect-multiplier 9
[SwitchA-vlan-interface10] quit
[SwitchA] ipv6 route-static 120:: 64 vlan-interface 10 12::2 bfd control-packet
[SwitchA] ipv6 route-static 120:: 64 10::100 preference 65
[SwitchA] quit
```

Switch B に IPv6 スタティックルートを設定し、レイヤ 2 スイッチを通してスタティックルートを行うため BFD コントロールパケットモードを有効にします。

```
<SwitchB> system-view
[SwitchB] interface vlan-interface 10
[SwitchB-vlan-interface10] bfd min-transmit-interval 500
[SwitchB-vlan-interface10] bfd min-receive-interval 500
[SwitchB-vlan-interface10] bfd detect-multiplier 9
[SwitchB-vlan-interface10] quit
[SwitchB] ipv6 route-static 121:: 64 vlan-interface 10 12::1 bfd control-packet
[SwitchB] ipv6 route-static 121:: 64 vlan-interface 13 13::2 preference 65
[SwitchB] quit
```

Switch C に IPv6 スタティックルートを設定します。

```
<SwitchC> system-view
[SwitchC] ipv6 route-static 120:: 64 13::1
[SwitchC] ipv6 route-static 121:: 64 10::102
```

III. 設定の確認

Switch A の BFD セッションを表示します。

```
<SwitchA> display bfd session

 Total Session Num: 1     Up Session Num: 1     Init Mode: Active

 IPv6 Session Working Under Ctrl Mode:
```

```
       Local Discr: 513                  Remote Discr: 33
         Source IP: 12::1
    Destination IP: 12::2
     Session State: Up                          Interface: Vlan10
         Hold Time: 2012ms
```

出力は、BFD セッションが作成されたことを示しています。

Switch A の IPv6 スタティックルート情報を表示します。

```
<SwitchA> display ipv6 routing-table protocol static

Summary Count : 1

Static Routing table Status : <Active>
Summary Count : 1

Destination: 120::/64                                   Protocol  : Static
NextHop    : 12::2                                      Preference: 60
Interface  : Vlan10                                     Cost      : 0

Direct Routing table Status : <Inactive>
Summary Count : 0
```

出力では、Switch A は VLAN インタフェース 10 を経由して Switch B と通信していることを示しています。

そして VLAN インタフェース 10 を経由したリンクが故障します。

Switch A の IPv6 スタティックルート情報を表示します。

```
<SwitchA> display ipv6 routing-table protocol static

Summary Count : 1

Static Routing table Status : <Active>
Summary Count : 1

Destination: 120::/64                                   Protocol  : Static
NextHop    : 10::100                                    Preference: 65
Interface  : Vlan11                                     Cost      : 0

Static Routing table Status : < Inactive>
Summary Count : 0
```

出力では、Switch A は VLAN インタフェース 11 を経由して Switch B と通信していることを示しています。

4.6.3. BFD の IPv6 スタティックルートの設定例(インダイレクトネクストホップ)

I. ネットワーク要件

図 4-3 に示すように設定します。

- Switch A は、VLAN インタフェース 10 の出力インタフェースにて Switch B のループバック 1(2::9/128)へのルートを持っています。
- Switch B は、VLAN インタフェース 12 の出力インタフェースにて Switch B のループバック 1(1::9/128)へのルートを持っています。
- Switch D は、VLAN インタフェース 10 の出力インタフェースにて 1.1.1.9/32、VLAN インタフェース 12 の出力インタフェースにて 2::9/128 へのルートを持っています。

以下のように IPv6 スタティックルートを設定します。

- Switch A にサブネット 120::/64 の IPv6 スタティックルートを設定します。
- Switch B にサブネット 121::/64 の IPv6 スタティックルートを設定します。
- 両方のルートで BFD を有効にします。
- Switch C と Switch D の両方でサブネット 120::/64 とサブネット 121::/64 への IPv6 スタティックルートを設定します。

Switch A と Switch B 間の Switch D が故障したとき、すぐさま Switch C で検出し、通信できるように BFD を有効にします。

図 4-3 ネットワーク図

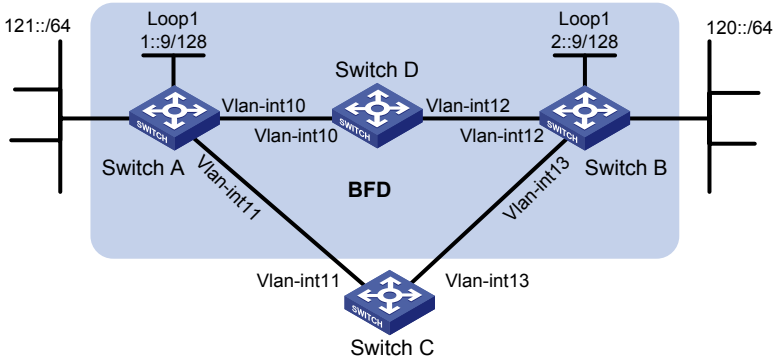


表 4-2 インタフェースと IPv6 アドレスの割り当て

装置	インタフェース	IPv6 アドレス
Switch A	Vlan-int10	12::1/64
Switch A	Vlan-int11	10::102/64
Switch A	Loop1	1::9/128
Switch B	Vlan-int12	11::2/64
Switch B	Vlan-int13	13::1/64
Switch B	Loop1	2::9/128
Switch C	Vlan-int11	10::100/64

装置	インタフェース	IPv6 アドレス
Switch C	Vlan-int13	13::2/64
Switch D	Vlan-int10	12::2/64
Switch D	Vlan-int12	11::1/64

II. 設定手順

1. インタフェースの IPv6 アドレスを設定します。(詳細は省略します)
2. IPv6 スタティックルートと BFD を設定します。

Switch A に IPv6 スタティックルートを設定し、Switch D を通して IPv6 スタティックルートを行うため BFD コントロールパケットモードを有効にします。

```
<SwitchA> system-view
[SwitchA] bfd multi-hop min-transmit-interval 500
[SwitchA] bfd multi-hop min-receive-interval 500
[SwitchA] bfd multi-hop detect-multiplier 9
[SwitchA] ipv6 route-static 120:: 64 2::9 bfd control-packet bfd-source 1::9
[SwitchA] ipv6 route-static 120:: 64 10::100 preference 65
[SwitchA] ipv6 route-static 2::9 128 12::2
[SwitchA] quit
```

Switch B に IPv6 スタティックルートを設定し、Switch D を通して IPv6 スタティックルートを行うため BFD コントロールパケットモードを有効にします。

```
<SwitchB> system-view
[SwitchB] bfd multi-hop min-transmit-interval 500
[SwitchB] bfd multi-hop min-receive-interval 500
[SwitchB] bfd multi-hop detect-multiplier 9
[SwitchB] ipv6 route-static 121:: 64 1::9 bfd control-packet bfd-source 2::9
[SwitchB] ipv6 route-static 121:: 64 13::2 preference 65
[SwitchB] ipv6 route-static 1::9 128 11::1
[SwitchB] quit
```

Switch C に IPv6 スタティックルートを設定します。

```
<SwitchC> system-view
[SwitchC] ipv6 route-static 120:: 64 13::1
[SwitchC] ipv6 route-static 121:: 64 10::102
```

Switch D に IPv6 スタティックルートを設定します。

```
<SwitchD> system-view
[SwitchD] ipv6 route-static 120:: 64 11::2
[SwitchD] ipv6 route-static 121:: 64 12::1
[SwitchD] ipv6 route-static 2::9 128 11::2
[SwitchD] ipv6 route-static 1::9 128 12::1
```

III. 設定の確認

Switch A の BFD セッションを表示します。

```
<SwitchA> display bfd session

 Total Session Num: 1     Up Session Num: 1     Init Mode: Active
```

```
 IPv6 Session Working Under Ctrl Mode:

       Local Discr: 513                 Remote Discr: 33
         Source IP: 1::9
    Destination IP: 2::9
     Session State: Up                        Interface: N/A
         Hold Time: 2012ms
```

出力では BFD セッションが作成されたことを示しています。

Switch A の IPv6 スタティックルートを表示します。

```
<SwitchA> display ipv6 routing-table protocol static

Summary Count : 1

Static Routing table Status : <Active>
Summary Count : 1

Destination: 120::/64                                  Protocol  : Static
NextHop    : 2::9                                      Preference: 60
Interface  : Vlan10                                    Cost      : 0

Static Routing table Status : <Inactive>
Summary Count : 0
```

出力では、Switch A は VLAN インタフェース 10 を経由して Switch B と通信していることを示しています。

そして VLAN インタフェース 10 を経由したリンクが故障します。

Switch A の IPv6 スタティックルートを表示します。

```
<SwitchA> display ipv6 routing-table protocol static

Summary Count : 1

Static Routing table Status : <Active>
Summary Count : 1

Destination: 120::/64                                  Protocol  : Static
NextHop    : 10::100                                   Preference: 65
Interface  : Vlan11                                    Cost      : 0

Static Routing table Status : <Inactive>
Summary Count : 0
```

出力では、Switch A は VLAN インタフェース 11 を経由して Switch B と通信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 **5-x-x** です。

5 章 IPv6 デフォルトルート 5-1

5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。詳細はセクション 5 *ルーティングプロトコル オペレーションマニュアル*の”*IPv6 スタティックルーティング*”を参照してください。

QX-S5300G シリーズ Ethernet スイッチ

オペレーションマニュアル

6. 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-マルチキャスト VLAN
04-MLD スヌーピング
05-IPv6 マルチキャスト VLAN

目次

このセクションのページは **6-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 1-3
1.1.3. マルチキャストの利点とアプリケーション 1-4
1.2. マルチキャストモデル 1-4
1.2.1. ASM モデル 1-4
1.2.2. SFM モデル 1-5
1.2.3. SSM モデル 1-5
1.3. マルチキャストアドレス 1-5
1.3.1. IP マルチキャストアドレス 1-5
1.3.2. イーサネットマルチキャスト MAC アドレス 1-8
1.4. マルチキャストプロトコル 1-9
1.4.1. レイヤ 3 マルチキャストプロトコル 1-9
1.4.2. レイヤ 2 マルチキャストプロトコル 1-11
1.5. マルチキャストパケットの転送メカニズム 1-12
1.6. マルチキャストアーキテクチャ 1-12
1.7. マルチキャストの一般的な表記方法 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 ユニキャストの通信

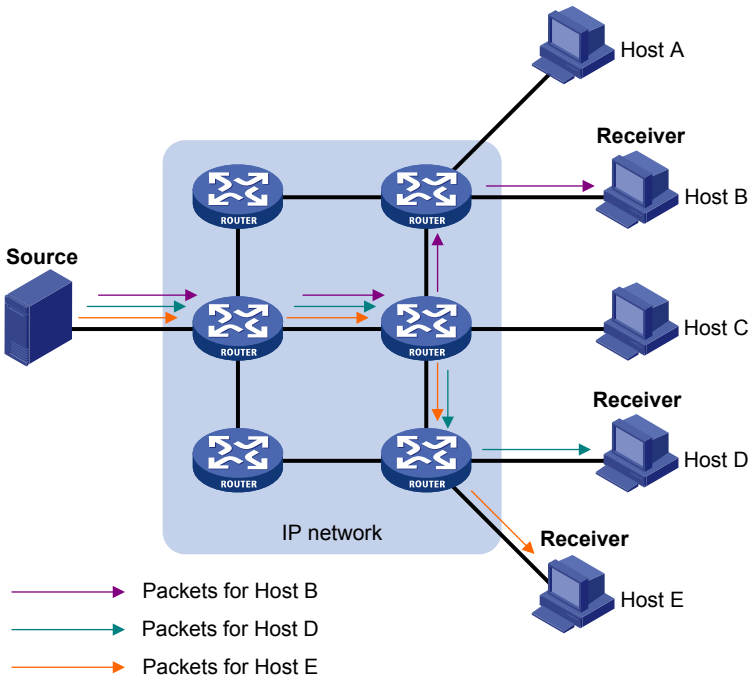


図 1-1 において、Host B と Host D と Host E は情報を必要とします。個別の通信チャネルは情報送信元から各ホストに対して確立する必要があります。

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

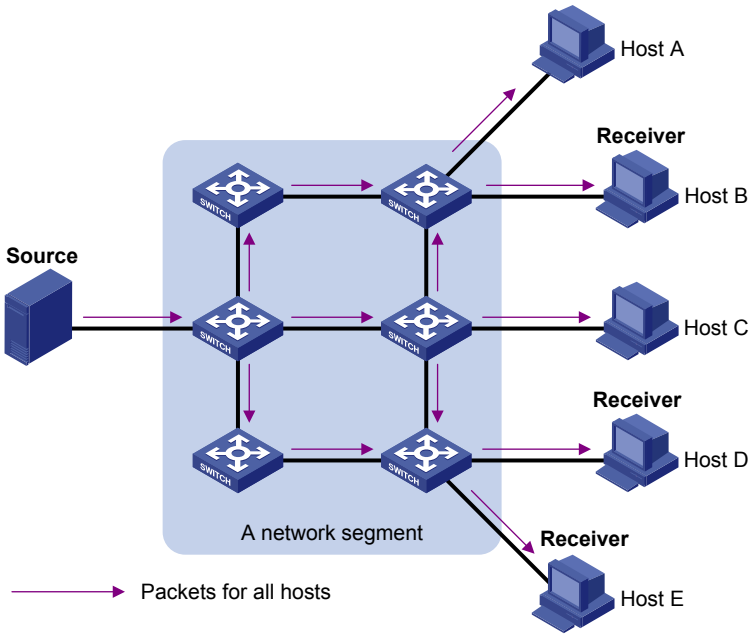


図 1-2 に示すように、Host B と Host D と Host E は情報を必要とします。情報が同一ネットワーク上にブロードキャストされた場合、Host A と Host C も情報を受信してしまいます。これにより、情報セキュリティの問題に加えて、同一ネットワーク上でトラフィックフラッディングも発生してしまいます。

ブロードキャストはホストのグループにデータを送信するマルチキャストほど効率的ではありません。

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

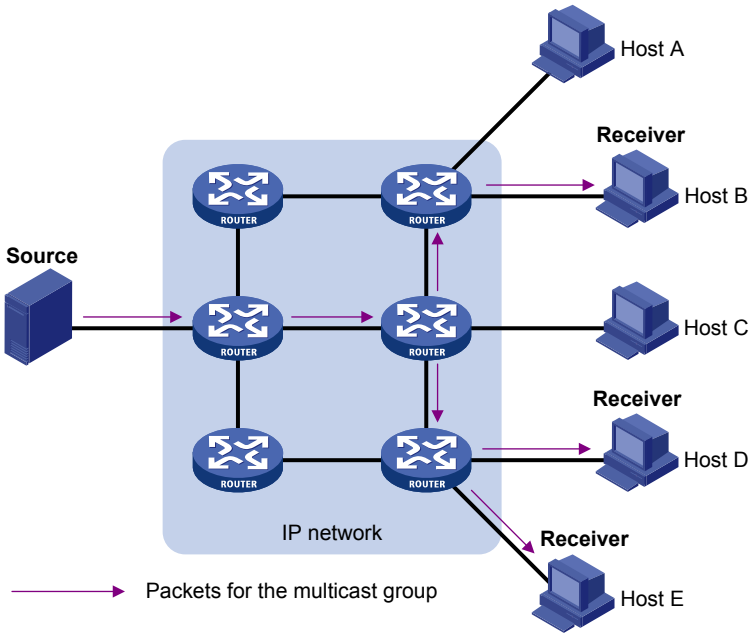


図 1-3 に示すようにマルチキャスト送信元（Source）は情報のコピーを 1 つだけマルチキャストグループへ送信します。情報の受信者である Host B、Host D、Host E は、マルチキャストグループに参加する必要があります。ネットワーク上のルータはグループメンバの配置にもとづいて情報を複製して転送します。最終的に、情報は Host B と Host D と Host E に正確に送信されます。

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、マルチキャスト送信元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。
- マルチキャスト送信元は情報の送信者です。マルチキャスト送信元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送信元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。	マルチキャスト送信元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. マルチキャストのアプリケーション

- 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）がマルチキャスト送信元（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。

1.2.1. ASM モデル

ASM モデルでは、すべてのマルチキャスト送信元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送信元の位置を認識していません。

1.2.2. SFM モデル

SFM モデルは ASM モデルから派生しています。マルチキャスト送信元（ソース）にとっては、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送信元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、マルチキャスト送信元（ソース）がすべて有効というわけではありません。マルチキャスト送信元はフィルタされます。

1.2.3. 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送信元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送信元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送信元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. マルチキャストアドレス

1.3.1. IP マルチキャストアドレス

I. 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	予約されている恒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を表 1-3 に示します。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

アドレスブロック	説明
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:

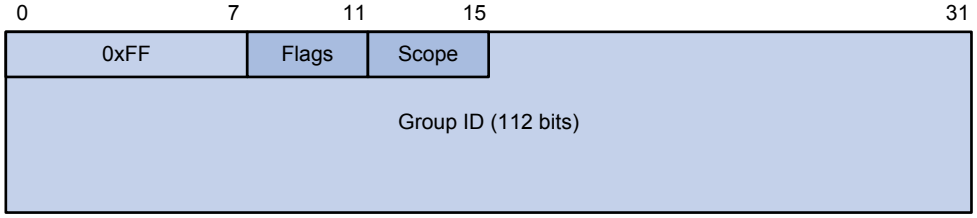
“Glop”は、異なる自律システム (AS) 間でマルチキャストアドレスを割り当てるメカニズムです。233.0.0.0 の中間の 2 バイトに AS の数字を入力することで、その AS に 255 のマルチキャストアドレスが得られます。詳細は、RFC2770 を参照してください。

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です。
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です。
224.0.0.3	未割り当てです。
224.0.0.4	DVMRP（Distance Vector Multicast Routing Protocol）ルータです。
224.0.0.5	OSPF（Open Shortest Path First）ルータです。
224.0.0.6	OSPFのDRまたはバックアップDRです。
224.0.0.7	ST（Shared Tree）ルータです。
224.0.0.8	STホストです。
224.0.0.9	RIPv2（Routing Information Protocol version 2）ルータです。
224.0.0.11	モバイルエージェントです。
224.0.0.12	DHCP（Dynamic Host Configuration Protocol）サーバまたはリレーエージェントです。
224.0.0.13	すべてのPIM（Protocol Independent Multicast）ルータです。
224.0.0.14	RSVP（Resource Reservation Protocol）のカプセル化です。
224.0.0.15	すべてのCBT（Core-Based Tree）ルータです。
224.0.0.16	指定されたSBM（Subnetwork Bandwidth Management）です。
224.0.0.17	すべてのSBMです。
224.0.0.18	VRRP（Virtual Router Redundancy Protocol）です。

II. 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** ー 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** ー 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 Flags 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** ー 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	予約済みです。
1	インタフェースノードローカルです。
2	リンクローカルです。
3	サブネットローカルです。
4	アドミンローカルです。
5	サイトローカルです。

値	意味
6, 7, 9 ～ D	未割り当てです。
8	組織ローカルです。
E	グローバルです。

- **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。

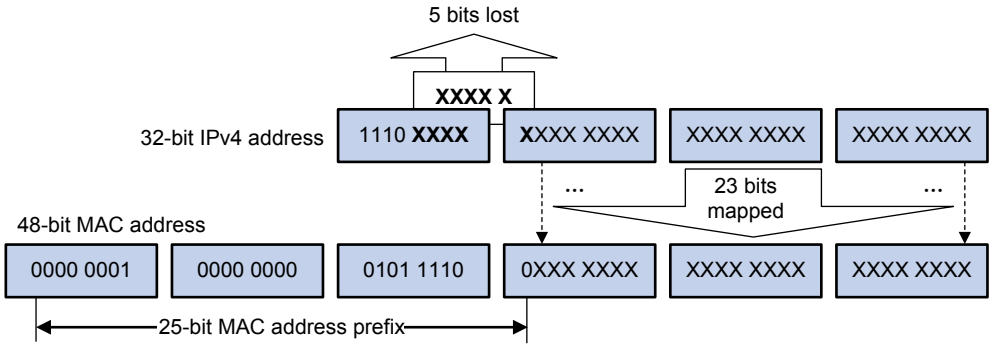
1.3.2. イーサネットマルチキャスト MAC アドレス

イーサネットマルチキャスト MAC アドレスはデータリンクレイヤで同一のマルチキャストグループに属しているレシーバを識別するために使用します。

I. 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

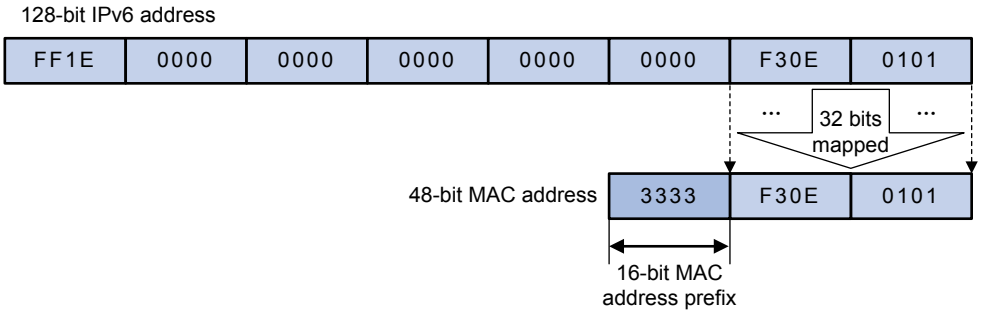


IPv4 マルチキャストアドレスの上位 4 ビットは 1110 で固定です。IPv4 アドレスと MAC アドレスのマッピングで使用され、IPv4 マルチキャストアドレスの 5 ビットは失われます。その結果、32 個のマルチキャスト IPv4 アドレスは同じ MAC アドレスにマッピングされます。そのため、レイヤ 2 マルチキャスト転送においては、他の IPv4 マルチキャストグループに宛てたマルチキャストデータを受け取る場合があります。そのような冗長データは上位層によってフィルタする必要があります。

II. 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



1.4. 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

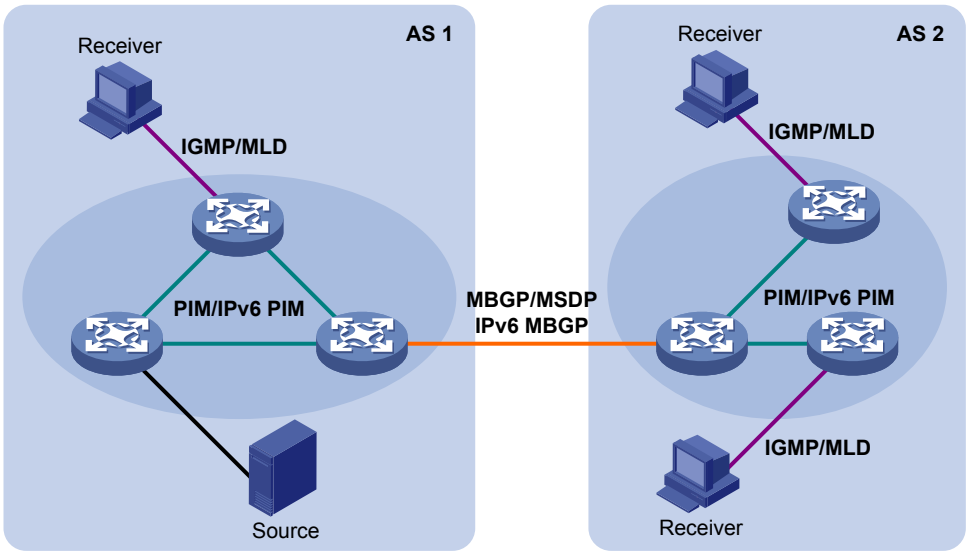
    レイヤ 2 マルチキャストプロトコル ― IGMP snooping、MLD snooping、PIM snooping、IPv6 PIM snooping、マルチキャスト VLAN、IPv6 マルチキャスト VLAN
- IPv4、IPv6 マルチキャストプロトコル
  - **IPv4 ネットワーク** ― IGMP snooping、PIM snooping、マルチキャスト VLAN、IGMP、PIM、MSDP、MBGP
  - **IPv6 ネットワーク** ― MLD snooping、IPv6 PIM snooping、IPv6 マルチキャスト VLAN、MLD、IPv6 PIM、IPv6 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。レイヤ 2 マルチキャストプロトコルに関する詳細は、関連する章を参照してください。

1.4.1. レイヤ 3 マルチキャストプロトコル

図 1-8 に示すようにレイヤ 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で、グループメンバシップを確立して維持するため直接接続を行います。

- 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。

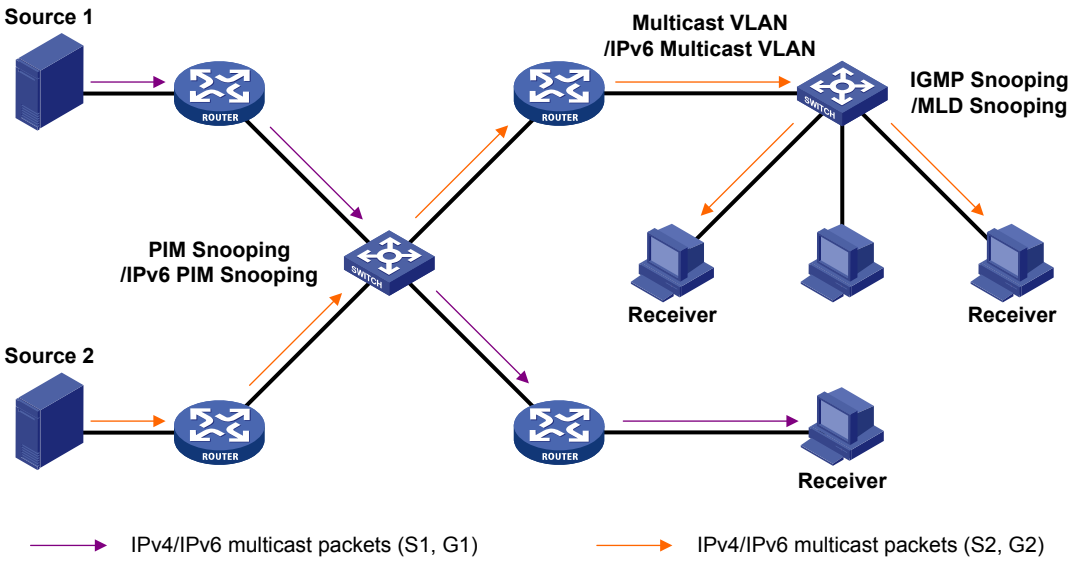
  - マルチキャストデータをレシーバに配信するために、ドメイン内マルチキャストルーティングプロトコルを使用してマルチキャスト送信元の発見、AS 内マルチキャスト配信ツリーの構築を行います。さまざまな成熟したドメイン内マルチキャストルーティングプロトコルの中でも、PIM (protocol independent multicast) はよく使用されています。PIM にはスパースモード (PIM-SM) があります。
  - ドメイン間マルチキャストルーティングプロトコルは 2 つの AS 間でマルチキャストの情報を発見するのに使われます。このプロトコルには、MSDP(Multicast Source 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送信元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。

1.4.2. レイヤ 2 マルチキャストプロトコル

図 1-9 に示すようにレイヤ 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 メッセージを確認することによって、レイヤ 2 マルチキャスト転送テーブルを作成します。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。

1.5. 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。

1.6. 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。

1.7. 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。

目次

このセクションのページは **6-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 の基本コンセプト 2-1
2.1.2. IGMP snooping 関連ポート 2-1
2.1.3. IGMP snooping の動作 2-3
2.1.4. IGMP snooping プロキシー機能 2-5
2.1.5. プロトコルと標準 2-6
2.2. 制限とガイドライン 2-6
2.3. VLAN ベース IGMP snooping の設定作業リスト 2-6
2.4. IGMP snooping 機能の有効化 2-7
2.5. IGMP snooping の有効化 2-8
2.5.1. VLAN での IGMP snooping の有効化 2-8
2.6. IGMP snooping の基本機能の設定 2-8
2.6.1. IGMP snooping のバージョンの設定 2-8
2.6.2. IGMP snooping 転送エントリの最大数の設定 2-9
2.6.3. 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
2.6.4. last member クエリ間隔の設定 2-10
2.7. IGMP snooping ポート機能の設定 2-11
2.7.1. ダイナミックポートのエージングタイマの設定 2-11
2.7.2. スタティックメンバポートの設定 2-12
2.7.3. スタティックルータポートの設定 2-13
2.7.4. シミュレーティッドメンバホストの設定 2-13
2.7.5. fast-leave 処理の有効化 2-14
2.8. IGMP snooping クエリアの設定 2-15
2.8.1. IGMP snooping クエリアの有効化 2-15
2.8.2. IGMP general query と response のパラメータの設定 2-15
2.9. IGMP snooping プロキシー機能の有効化 2-16
2.10. IGMP メッセージのパラメータの設定 2-17
2.10.1. IGMP メッセージの送信元 IP アドレスの設定 2-17
2.10.2. IGMP メッセージの 802.1p 優先度の設定 2-18
2.11. IGMP snooping ポリシーの設定 2-19
2.11.1. マルチキャストグループポリシーの設定 2-19
2.11.2. マルチキャストソースポートフィルタの有効化 2-20
2.11.3. 未知のマルチキャストデータ廃棄機能の設定 2-20
2.11.4. IGMP report 抑制の有効化 2-21
2.11.5. 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
2.11.6. マルチキャストグループ置き換え機能の有効化 2-22
2.12. 送信する IGMP snooping プロトコルパケットの DSCP の設定 2-23
2.13. IGMP snooping の表示と維持 2-23
2.14. IGMP snooping 設定例 2-24
2.14.1. VLAN ベース IGMP snooping 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加入の設定例 2-24
2.14.2. VLAN ベース IGMP snooping スタティックポートの設定例 2-27

2.14.3. VLAN ベース IGMP snooping クエリアの設定例 2-30
2.14.4. VLAN ベース IGMP snooping プロキシー機能の設定例 2-33
2.15. IGMP snooping のトラブルシューティング 2-36
2.15.1. レイヤ 2 マルチキャスト転送ができない 2-36
2.15.2. マルチキャストグループポリシーが動作しない 2-36

2章 IGMP スヌーピング

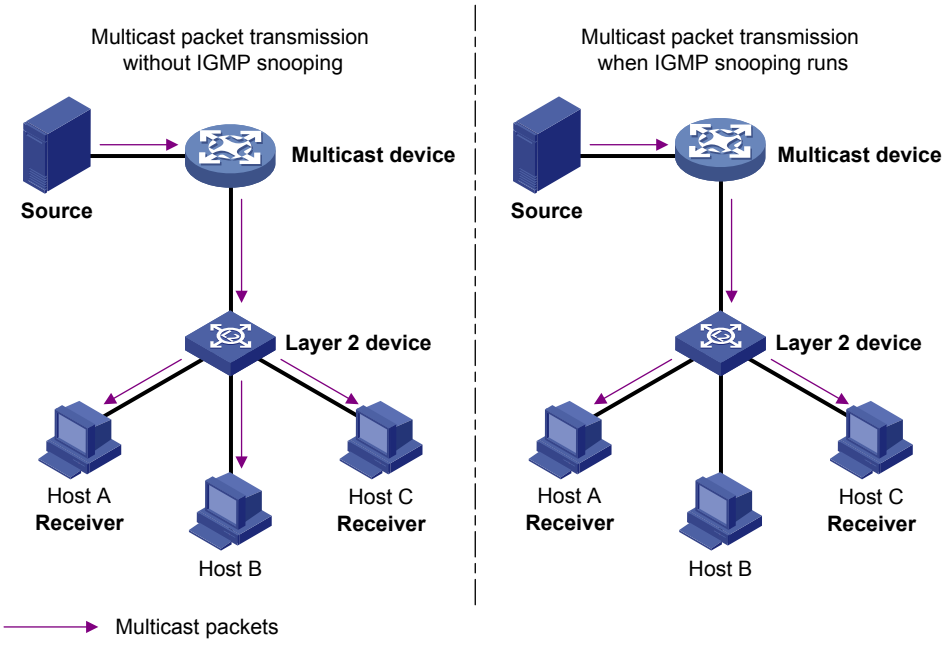
2.1. 概要

IGMP snooping はマルチキャスト転送の効率を改良するために、マルチキャストを行うメカニズムとして、レイヤ 2 装置で動作します。IGMP snooping はレイヤ 3 マルチキャスト装置とホスト間で交換された IGMP メッセージからレイヤ 2 マルチキャスト転送エントリを作成します。

2.1.1. IGMP snooping の基本コンセプト

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ブロードキャストされます。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、レシーバへのみ転送されます。

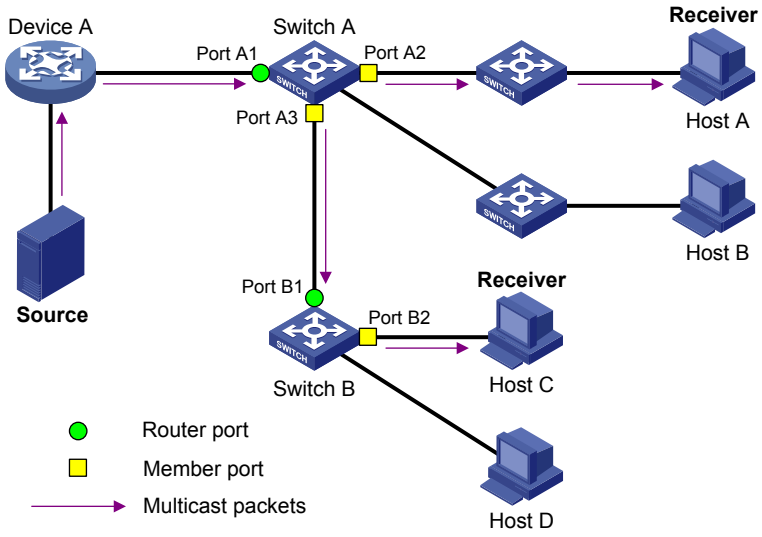
図 2-1 IGMP snooping を有効にする前と有効にした後のマルチキャストパケットの転送



2.1.2. IGMP snooping 関連ポート

図 2-2 に示すように、IGMP snooping は Switch A と Switch B で動作しています。Host A と Host C はマルチキャストグループのレシーバです。

図 2-2 IGMP snooping 関連ポート



I. ルータポート

IGMP snooping が有効なレイヤ 2 装置では、ポートはレイヤ 3 マルチキャスト方向へのポートはルータポートと呼ばれます。図 2-1 では、Switch A の Port A1、Switch B の Port B1 はルータポートです。

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**－ポートで送信元アドレスが 0.0.0.0 でない IGMP general query あるいは PIM hello メッセージを受信した場合、ポートはダイナミックルータポートリストに追加されます。同時にポートのエージング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た場合、タイマは再起動します。タイマが満了する前にメッセージを受信しない場合、装置は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**－ルータポートとしてスタティックに設定した場合、ポートはスタティックルータポートに追加されます。スタティックルータポートはエージアウトしません。手動でスタティックルータポートから削除しない限り、削除されません。

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 が有効なレイヤ 2 装置では、ポートは受信ホスト方向へのポートはメンバポートと呼ばれます。図 2-1 では、Switch A の Port A2、Port A3、Switch B の Port B2 はメンバポートです。

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**－ポートで IGMP report を受信した場合、ポートは出力インタフェースとして、ダイナミック IGMP snooping 転送テーブルのエントリに追加されます。同時にポートのエージングタイマが開始します。タイマが満了する前に IGMP report を受信した場合、タイマは再起動します。タイマが満了する前に IGMP report を受信しない場合、装置はダイナミック IGMP snooping 転送エントリからポートを削除します。
- **スタティックメンバポート**－メンバポートとしてスタティックに設定した場合、ポートは出力インタフェースとしてスタティック 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。手動でスタティックメンバポートから削除しない限り、削除されません。

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。

2.1.3. 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、セクション 6 *マルチキャスト オペレーションマニュアル*の”*IGMP snooping*”の”*スタティックメンバポートの設定*”、”*スタティックルータポートの設定*”を参照してください。

IGMP メッセージのタイプは、general query、IGMP report、leave message 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 query

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 query を定期的に送信します。

IGMP クエリアから IGMP general query を受信すると、レイヤ 2 装置は、メッセージを受信したポートと同じ VLAN に属するすべてのポート（受信ポート以外）へ IGMP general query 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、レイヤ 2 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は、レイヤ 2 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 query に応答します。
- マルチキャストグループ membership を適用します。

ホストからの IGMP report を受信すると、レイヤ 2 装置は VLAN 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再スタートします。

メモ:

レイヤ 2 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 レポートの転送を行いません。非ルータポートがメンバホストに接続された場合、メンバホストは非ルータポートによって転送された IGMP report を受信した際に IGMP report を抑制します。レイヤ 2 装置は非ルータポートに接続されたメンバホストの存在を知ることはできません。

III. Leave message

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、レイヤ 2 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。

レイヤ 2 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、レイヤ 2 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、レイヤ 2 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、レイヤ 2 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、レイヤ 2 装置は以下のアクションを実行します。
  - IGMP leave メッセージを廃棄します。
  - グループが受信ポートに接続されているアクティブレシーバが存在するか確認するため、IGMP group-specific query を送信します。
  - 受信ポートのエージングタイマを、IGMP last-member query の送信間隔の 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、レイヤ 2 装置は以下のアクションを実行します。
  - 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。
  - グループが受信ポートに接続されているアクティブレシーバが存在するか確認するため、IGMP group-specific query を送信します。
  - 受信ポートのエージングタイマを、IGMP last-member query の送信間隔の 2 倍に設定します。

ポートで IGMP leave メッセージを受信すると、IGMP クエリアはメッセージのマルチキャストグループを解決します。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 query を送信します。

IGMP group-specific query を受信したのち、レイヤ 2 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、query を転送します。

直接に接続されているホストから IGMP report に対する応答を待ちます。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、レイヤ 2 装置は以下のアクションの 1 つを実行します。

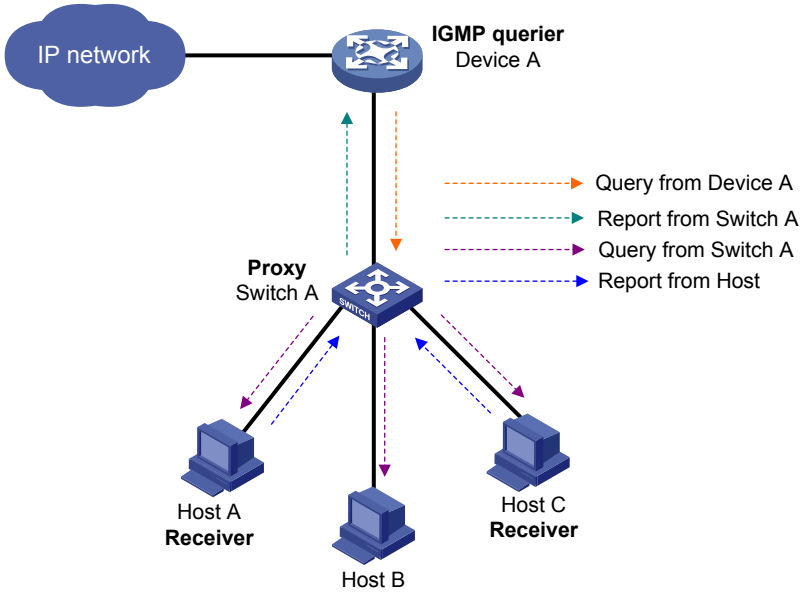
- エージングタイマが満了する前にポートが IGMP report を受信した場合、レイヤ 2 装置はエージングタイマを再起動します。
- エージングタイマが満了する前にポートが IGMP report を受信しない場合、レイヤ 2 装置はマルチキャストグループの転送エントリからポートを削除します。

2.1.4. 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 Device 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ます。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ます。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とき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。

2.1.5. プロトコルと標準

RFC 4541, *Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches*

2.2. 制限とガイドライン

セカンダリ VLAN から受信した IGMP report のため、関連する IGMP snooping 転送エントリはプライマリ VLAN によって管理されます。そのため、プライマリ VLAN で IGMP snooping を有効にする必要があります。セカンダリ VLAN で設定された IGMP snooping の設定は適用されません。プライマリ VLAN とセカンダリ VLAN の詳細はセクション 3 *アクセス オペレーションマニュアル* の“*VLAN*”を参照してください。

アグリゲートインタフェースで設定された IGMP snooping の設定は、メンバポートの設定に影響しません。さらに、アグリゲートインタフェースの設定はアグリゲーションの計算に追加されません。ポートがアグリゲーショングループから取り外されたのち、アグリゲーショングループのメンバポートの設定が適用されます。

VLAN view の VLAN、あるいは IGMP-snooping view の複数の VLAN で設定することができます。IGMP view の設定と IGMP-snooping view の設定の優先度は同一ですが、最後に行われた設定が適用されます。

VLAN view の VLAN、あるいは IGMP-snooping view のすべての VLAN でグローバルに設定することができます。VLAN で行われた設定はグローバルで行われた設定よりも優先されます。

interface view の VLAN、あるいは IGMP-snooping view の指定した VLAN のすべてのインタフェースで設定することができます。インタフェースで行われた設定は IGMP-snooping view で行われた設定よりも優先されます。

2.3. VLANベースIGMP snoopingの設定作業リスト

作業リスト
1. IGMP snooping 機能の有効化

作業リスト
2.　IGMP snooping の有効化 必要に応じて以下の機能を選択してください。 • VLAN での IGMP snooping の有効化 • (オプション設定項目) IGMP snooping の基本機能の設定 　○ IGMP snooping のバージョンの設定 　○ IGMP snooping 転送エントリの最大数の設定 　○ 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 　○ IGMP last-member query の間隔の設定
3.　(オプション設定項目)IGMP snooping ポート機能の設定 • ダイナミックポートのエージングタイマの設定 • スタティックメンバポートの設定 • スタティックルータポートの設定 • シミュレーティッドメンバホストの設定 • fast-leave 処理の有効化
4.　(オプション設定項目)IGMP snooping クエリアの設定 • IGMP snooping クエリアの有効化 • IGMP query と response のパラメータの設定
5.　(オプション設定項目) IGMP snooping プロキシー機能の有効化
6.　(オプション設定項目)IGMP メッセージパラメータの設定 • IGMP メッセージの送信元 IP アドレスの設定 • IGMP メッセージの 802.1p 優先度の設定
7.　(オプション設定項目) IGMP snooping ポリシーの設定 • マルチキャストグループポリシーの設定 • マルチキャストソースポートフィルタの設定 • 未知のマルチキャストデータ廃棄機能の設定 • IGMP report 抑制機能の設定 • 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 • マルチキャストグループ置き換え機能の設定
8.　(オプション設定項目) 送信する IGMP snooping プロトコルパケットの DSCP の設定

2.4. IGMP snooping機能の有効化

I. IGMP snooping 機能の有効化の条件

IGMP snooping 機能を有効化する前に、他の IGMP snooping 機能の設定を完了させてください。

II. 設定手順

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. 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

2.5. IGMP snoopingの有効化

2.5.1. VLAN での IGMP snooping の有効化

I. 制限とガイドライン

VLAN の IGMP snooping の設定は VLAN のメンバポートでのみ適用されます。

II. VLAN の IGMP の有効化の設定手順

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. VLAN で IGMP snooping を有効にする	**igmp-snooping enable**	デフォルト：無効

2.6. IGMP snoopingの基本機能の設定

2.6.1. IGMP snooping のバージョンの設定

I. IGMP snooping のバージョンの設定

IGMP snooping のバージョン異なると、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 の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。

II. 制限とガイドライン

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 に切り替わったとき復元されます。

スタティック IGMP snooping 転送エントリの詳細については、セクション 6 *マルチキャスト オペレーションマニュアルの”IGMP snooping”の”スタティックメンバポートの設定”*を参照してください

III. VLAN での IGMP snooping のバージョンの設定

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 snooping のバージョンを指定する	**igmp-snooping version** *version-number*	デフォルト：2

2.6.2. IGMP snooping 転送エントリの最大数の設定

I. 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。

II. 設定手順

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

2.6.3. 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

I. 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 マルチキャストでは、マルチキャスト MAC アドレスエントリは IGMP snooping のようなレイヤ 2 マルチキャストプロトコルを通してダイナミックに作成することができます。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付けることで、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。

II. 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とき、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。

III. 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*	—

IV. 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	• 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*	—
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*	—

2.6.4. last member クエリ間隔の設定

I. 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 になったときに、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ときに同時に送信する 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。

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

2.7. IGMP snoopingポート機能の設定

2.7.1. ダイナミックポートのエージングタイマの設定

I. ダイナミックポートのエージングタイマの設定

エージングタイマが満了するときまでに IGMP general query あるいは PIM Hello メッセージを受信しない場合、ダイナミックルータ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。

エージングタイマが満了するときまでに IGMP Report を受信しない場合、ダイナミックメンバポートはダイナミックメンバポートリストからポートを削除します。

II. 制限とガイドライン

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。もし 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。

レイヤ 2 装置が開始した IGMP group-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が行われます。

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 IGMP last member クエリ間隔の 2 倍に設定します。IGMP last member クエリ間隔の詳細は “*last member クエリ間隔の設定*” を参照してください。

III. 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**	—

操作	コマンド	補足
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** *interval*	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** *interval*	デフォルト：260秒

IV. 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** *interval*	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** *interval*	デフォルト：260秒

2.7.2. スタティックメンバポートの設定

I. スタティックメンバポートの設定

ホストに接続されたポートが常にグループのマルチキャストを受信できるように、ポートをマルチキャストグループのスタティックメンバポートに設定することができます。スタティックメンバポートは IGMP クエリに応答しません。ポートの設定を完了あるいは設定を取り消したとき、ポートは不要な IGMP report や leave メッセージを送信しません。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. Layer 2 Ethernet interface view あるいは aggregate 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*	—

操作	コマンド	補足
3. 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*	デフォルト：設定なし

2.7.3. スタティックルータポートの設定

I. スタティックルータポートの設定

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とき、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。

II. 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 view あるいは aggregate 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*	—
3. ポートをスタティックポートに設定する	**igmp-snooping static-router-port vlan** *vlan-id*	デフォルト：設定なし

2.7.4. シミュレーティッドメンバホストの設定

I. 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とき、以下の方法により独立したホストと同等になります。

- 設定が完了したとき、unsolicited IGMP report を送信します。
- IGMP report として IGMP general query に応答します。
- 設定を削除したとき、IGMP leave メッセージを送信します。

この操作を行うとき、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。

II. 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 view あるいは aggregate 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*	—
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

2.7.5. fast-leave 処理の有効化

I. fast-leave 処理

この機能を有効にすることで、ポートが leave メッセージを受信したときに、装置は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。

レイヤ 2 装置はグループの IGMP group-specific クエリをポートに送信あるいは転送しません。

II. 制限とガイドライン

VLAN の複数のホストが接続しているポートに fast-leave 処理機能を有効にしないでください。そうでない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。

III. 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. 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

IV. ポートでのでの 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**	—

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	• 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*	—
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

2.8. IGMP snoopingクエリアの設定

2.8.1. IGMP snooping クエリアの有効化

I. IGMP snooping クエリア

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 query 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。

II. 制限とガイドライン

IGMP snooping クエリアを有効にするとき､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 query 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。

III. VLAN での IGMP snooping クエリアの有効化

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

2.8.2. IGMP general query と response のパラメータの設定

I. IGMP general query と response のパラメータ

ネットワークの実際の状況にもとづいて､IGMP general query の送信間隔を調整することができます。

IGMP general query 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 になったときに、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 query の最大応答時間を適切に設定すると、ホストは速やかに query 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ときに同時に送信する 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。

II. 制限とガイドライン

IGMP general query 間隔は IGMP general query の最大応答時間よりも大きいことを確認してください。そうしないと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。

III. グローバルでの IGMP query 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 query の最大応答時間を設定する	**max-response-time** *seconds*	デフォルト：10秒

IV. VLAN での IGMP query 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 query 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 query 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

2.9. IGMP snoopingプロキシー機能の有効化

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. 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

2.10. IGMPメッセージのパラメータの設定

2.10.1. IGMP メッセージの送信元 IP アドレスの設定

I. 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 query をポートで受信すると、レイヤ 2 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の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 クエリアとして動作するレイヤ 2 装置によって送信された IGMP query 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 query 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。

またシミュレーティッドメンバホストによって送信されたIGMP reportの送信元IPアドレスを変更することができます。

II. VLAN での IGMP メッセージの送信元 IP 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**	ー
2. VLAN view に移行する	**vlan** *vlan-id*	ー
3. IGMP general query 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。
4. IGMP group-specific query 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：IGMP snoopingクエリアがIGMP queryを受信した場合、IGMP queryの送信元IPアドレスです。 そうでなければ現在の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。
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。

操作	コマンド	補足
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。

2.10.2. IGMP メッセージの 802.1p 優先度の設定

I. IGMP メッセージの 802.1p 優先度

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。

II. 制限とガイドライン

IGMP-snooping view の設定はすべての VLAN でのみ適用されます。

III. 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**	—
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*	—

IV. 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*	—

2.11. IGMP snoopingポリシーの設定

2.11.1. マルチキャストグループポリシーの設定

I. マルチキャストグループポリシー

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。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。

マルチキャストアプリケーションにおいて、ユーザがマルチキャストプログラムを要求したとき、ホストが不要な IGMP report を送信します。レイヤ 2 装置は IGMP report をフィルタするため、マルチキャストグループポリシーを使用します。IGMP report がマルチキャストポリシーで許可されているときのみホストがマルチキャストグループに加入することができます。

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	• 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*	—
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

2.11.2. マルチキャストソースポートフィルタの有効化

I. マルチキャストソースポートフィルタ

この機能はレイヤ 2 装置が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。

II. 制限とガイドライン

マルチキャストソースポートフィルタが有効である場合、システムは自動でマルチキャストソースフィルタリングを有効にします。

IGMP-snooping view の複数の VLAN で設定することができます。interface view の設定と IGMP-snooping view の設定の優先度は同一ですが、最後に行われた設定が適用されます。

III. 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

IV. 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*	—
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

2.11.3. 未知のマルチキャストデータ廃棄機能の設定

I. 未知のマルチキャストデータ廃棄機能

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。

この機能は未知のマルチキャストデータをルータポートにのみ転送します。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。

II. 制限とガイドライン

未知の IPv4 マルチキャストデータの廃棄機能が有効であるとき、IPv6 マルチキャストデータも廃棄します。

未知のマルチキャストデータの廃棄機能が有効であるとき、装置はルータポートでの受信を除き、ルータポートから未知のマルチキャストデータを転送します。

III. VLAN での未知のマルチキャストデータ廃棄機能の有効化

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. 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。

2.11.4. IGMP report 抑制の有効化

I. IGMP report 抑制

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。この機能によってマルチキャストトラフィックを削減できます。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. IGMP-snooping view に移行する	**igmp-snooping**	—
3. IGMP report 抑制を有効にする	**report-aggregation**	デフォルト：有効

2.11.5. 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

I. 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。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ときは、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

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	• 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*	—
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の設定をする	**igmp-snooping group-limit** *limit* [**vlan** *vlan-list*]	デフォルト：4294967295

2.11.6. マルチキャストグループ置き換え機能の有効化

I. マルチキャストグループ置き換え機能

この機能は、グループのメンバ数が上限を超えたとき、レイヤ 2 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装置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。

II. 制限とガイドライン

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。

III. 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

IV. 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**	—

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	• 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*	—
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

2.12. 送信するIGMP snoopingプロトコルパケットのDSCPの設定

I. 送信する IGMP snooping プロトコルパケットの DSCP

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。

II. 設定手順

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. 送信する IGMP snooping プロトコルパケットの DSCP を設定する	**dscp** *dscp-value*	デフォルト：48

2.13. 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*]
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*]

操作	コマンド
スタティックIGMP snoopingグループ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*]
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の情報を表示する	**display l2-multicast ip** [**group** *group-address* | **source** *source-address*] * [**vlan** *vlan-id*] [**slot** *slot-number*]
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の情報を表示する	**display l2-multicast mac** [*mac-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アドレスエントリの情報を表示する	**display mac-address** [*mac-address* [**vlan** *vlan-id*] [**multicast**] [**vlan** *vlan-id*] [**count**]]
ダイナミックIGMP snoopingグループ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* }
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**

2.14. IGMP snooping設定例

2.14.1. VLAN ベース IGMP snooping 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加入の設定例

I. ネットワーク要件

図 2-4 に示すように、Router A は IGMPv2 で動作させ、IGMP クエリアとして機能し、Switch A は IGMPv2 snooping を動作させます。

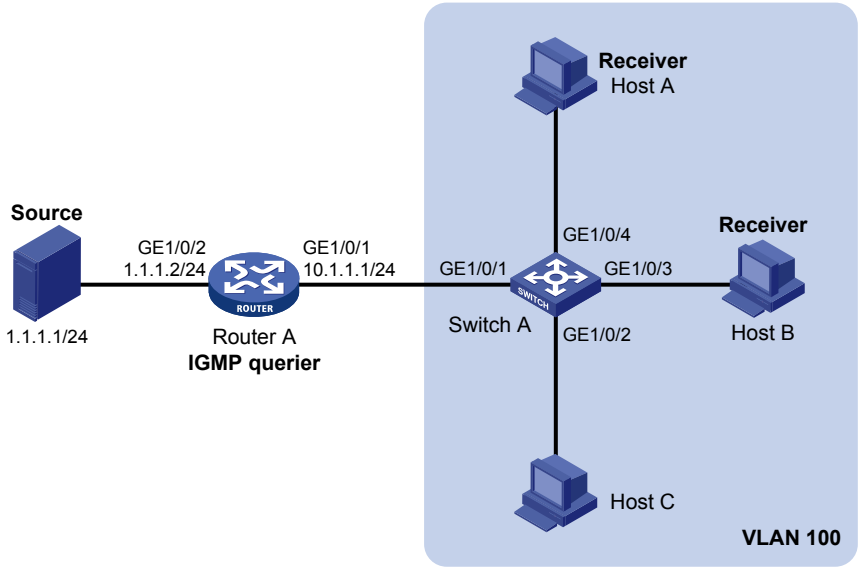
以下の要件に従うようにマルチキャストグループポリシーを設定し、シミュレーティッドメンバホストの加入の設定を行います。

- Host A、Host B はマルチキャストグループ 224.1.1.1 にアドレスされたマルチキャストデータのみ受信します。マルチキャストデータは Switch A の GigabitEthernet 1/0/3、GigabitEthernet

1/0/4 を通して連続して転送されます。たとえ Host A、Host B でマルチキャストデータを受信するのに失敗したとしても、絶え間なく転送されます。

- Switch A はVLAN 100 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 と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 のホストはマルチキャストグループ 224.1.1.1 のみに参加できるように、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。

2.14.2. VLAN ベース IGMP snooping スタティックポートの設定例

I. ネットワーク要件

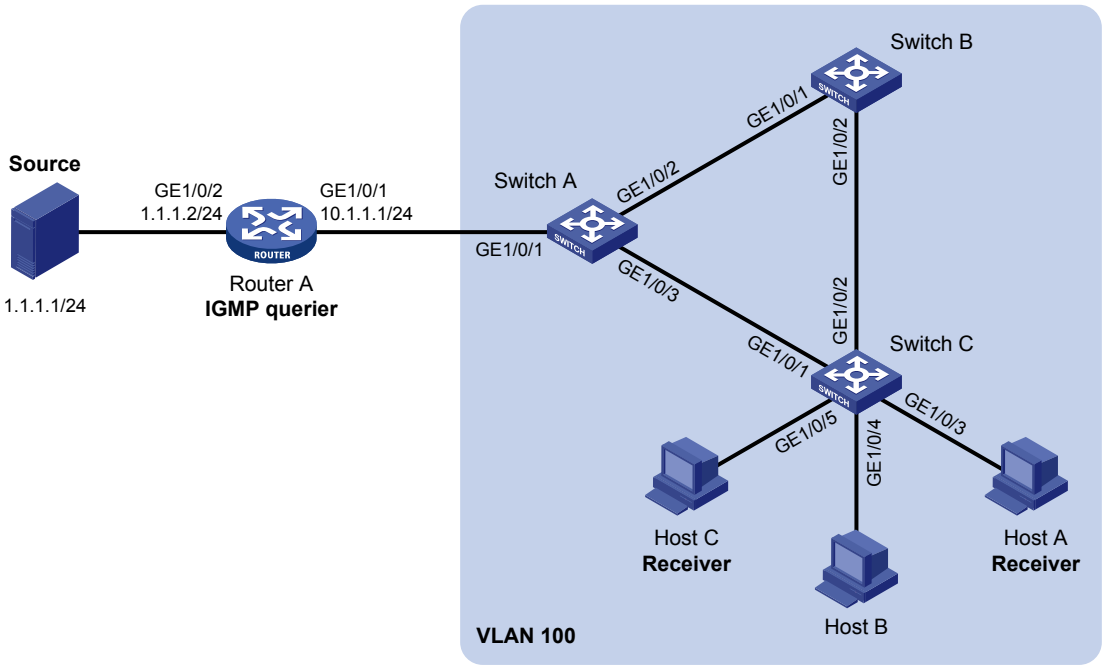
図 2-5 に示すようなネットワークを設定します。

- 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 の恒久的なレシーバです。

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 に接続されているレシーバに転送されます。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レシーバ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 の詳細はセクション 3 *アクセス オペレーションマニュアル*の“*STP*”を参照してください。

図 2-5 ネットワーク図



II. 設定手順

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)

1. 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

2. 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 1/0/3 を割り当てます。

[SwitchA] vlan 100

[SwitchA-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/3

VLAN100 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

3. 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

VLAN100 で IGMP snooping を有効にします。

[SwitchB-vlan100] igmp-snooping enable

[SwitchB-vlan100] quit

4. Switch C を設定します。

グローバルで 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 VLAN100 のスタティック IGMP snooping グループ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。

2.14.3. VLAN ベース IGMP snooping クエリアの設定例

I. ネットワーク要件

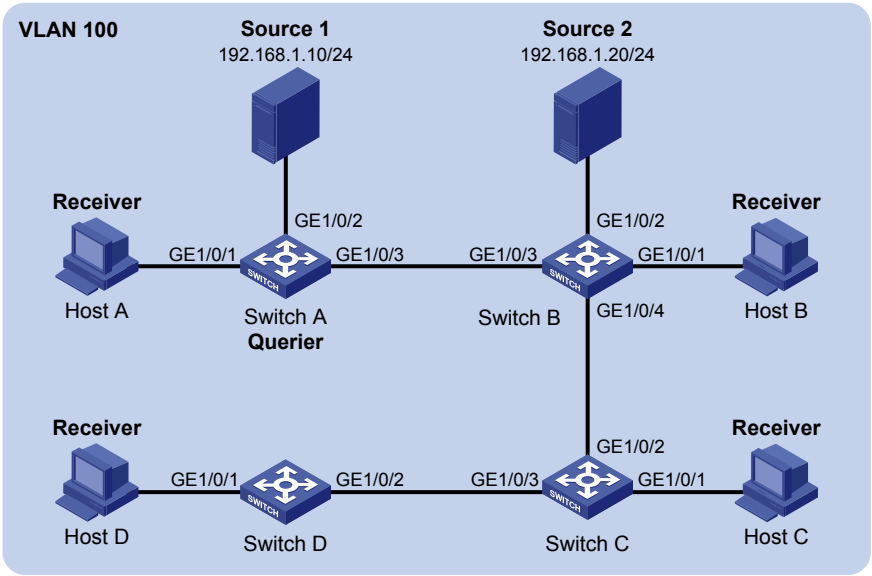
図 2-6 に示すようなネットワークを設定します。

- 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 のレシーバで、Host B、Host D はマルチキャストグループ 225.1.1.1 のレシーバです。
- すべてのレシーバホストは 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 query 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 と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 query 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 query 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 と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 と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 と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、PIMv2 hello メッセージを通して学習した IGMP 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 query を受信することができます。

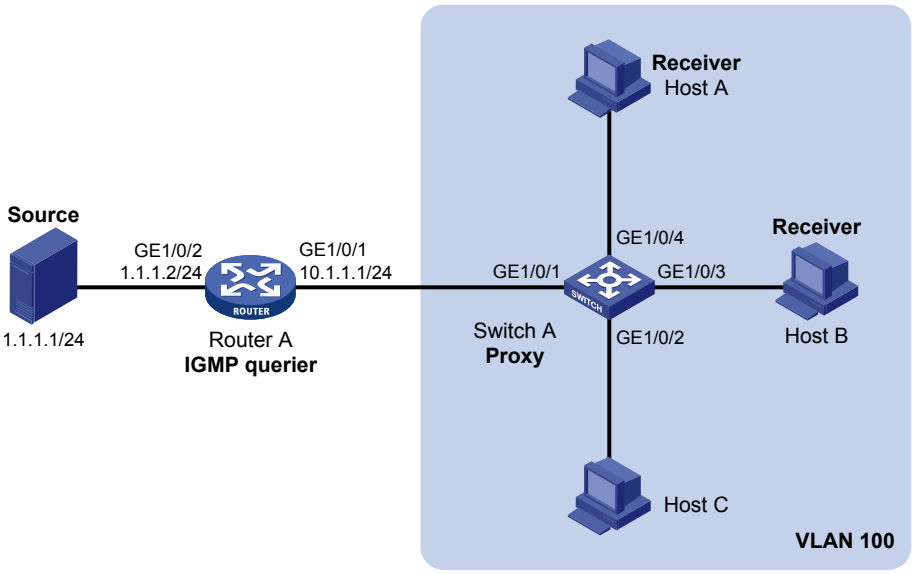
2.14.4. VLAN ベース IGMP snooping プロキシー機能の設定例

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 IGMP を有効にし、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。

2.15. IGMP snoopingのトラブルシューティング

2.15.1. レイヤ 2 マルチキャスト転送ができない

I. 症状

IGMP snooping を使用したレイヤ 2 装置でレイヤ 2 マルチキャスト転送ができません。

II. 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。

2.15.2. 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. 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 **6-x-x** です。

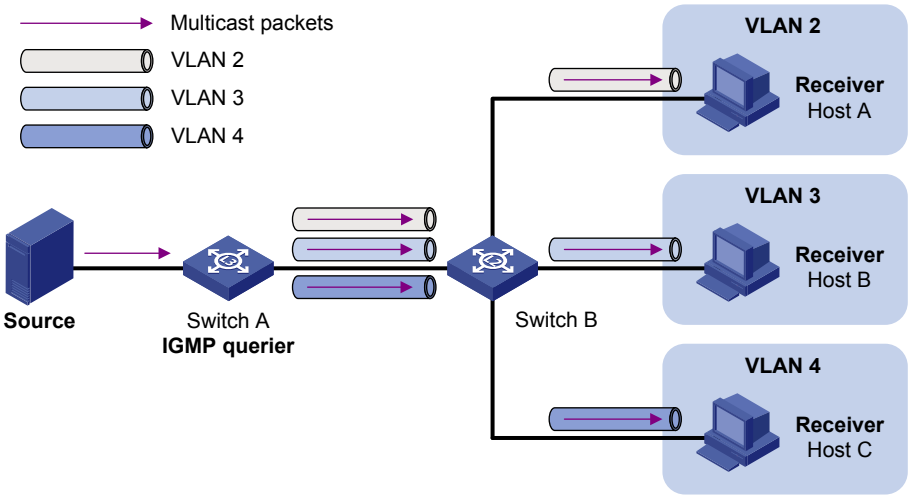
3 章 マルチキャスト VLAN……3-1
3.1. 概要……3-1
3.2. マルチキャスト VLAN 方法……3-1
3.2.1. サブ VLAN ベースマルチキャスト VLAN……3-1
3.2.2. ポートベースマルチキャスト VLAN……3-2
3.3. 制限とガイドライン……3-3
3.4. サブ VLAN ベースマルチキャスト VLAN……3-3
3.5. ポートベースマルチキャスト VLAN の設定……3-4
3.6. マルチキャスト VLAN の転送エントリの最大数の設定……3-5
3.7. マルチキャスト VLAN の表示と維持……3-5
3.8. マルチキャスト VLAN の設定例……3-6
3.8.1. サブ VLAN ベースマルチキャスト VLAN の設定例……3-6
3.8.2. ポートベースマルチキャスト VLAN の設定例……3-9

3章 マルチキャスト VLAN

3.1. 概要

図 3-1 に示すように、異なる VLAN のホスト A、ホスト B、ホスト C は同じマルチキャストグループに所属しています。Switch A（レイヤ 3 装置）がグループのマルチキャストデータを受信するとき、Switch B（レイヤ 2 装置）のユーザ VLAN 毎にマルチキャストトラフィックをコピーします。この結果、ネットワークの帯域を浪費するだけでなく、レイヤ 3 装置にも負荷をかけてしまいます。

図 3-1 マルチキャスト VLAN を使用しないマルチキャストの転送



Switch B でマルチキャスト VLAN を設定した後、Switch A は Switch B のマルチキャスト VLAN にマルチキャストデータを 1 つのコピーのみを送信します。この方法はネットワークの帯域を節約し、レイヤ 3 装置の負荷を軽減します。

3.2. マルチキャストVLAN方法

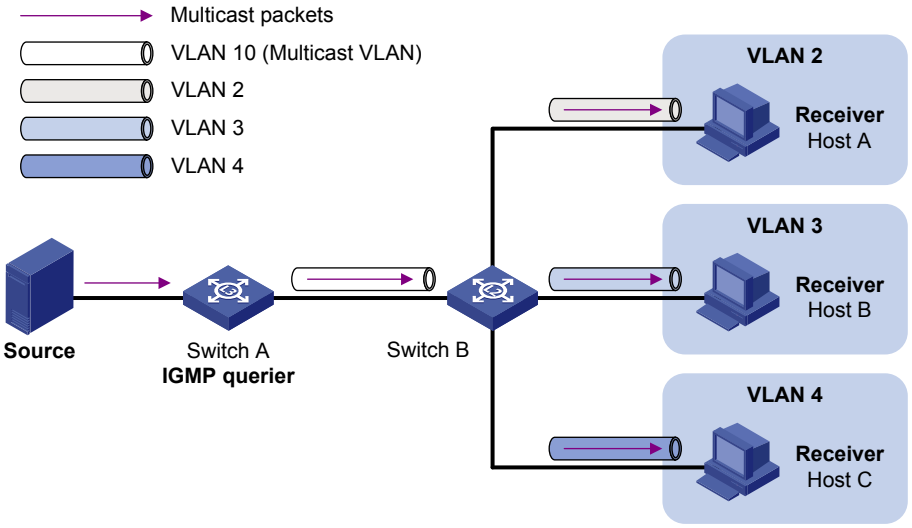
マルチキャスト VLAN はサブ VLAN ベースマルチキャストとポートベースマルチキャスト VLAN があります。

3.2.1. サブ VLAN ベースマルチキャスト VLAN

図 3-2 にサブ VLAN ベースマルチキャスト VLAN を示します。

- ホスト A、ホスト B、ホスト C はそれぞれ VLAN 2、VLAN 3、VLAN 4 に属します。
- Switch B において、VLAN10 をマルチキャスト VLAN に設定します。VLAN 2、VLAN 3、VLAN 4 は VLAN 10 のサブ VLAN です。
- マルチキャスト VLAN とマルチキャスト VLAN のサブ VLAN 上で IGMP Snooping を有効にします。

図 3-2 サブ VLAN ベースマルチキャスト VLAN



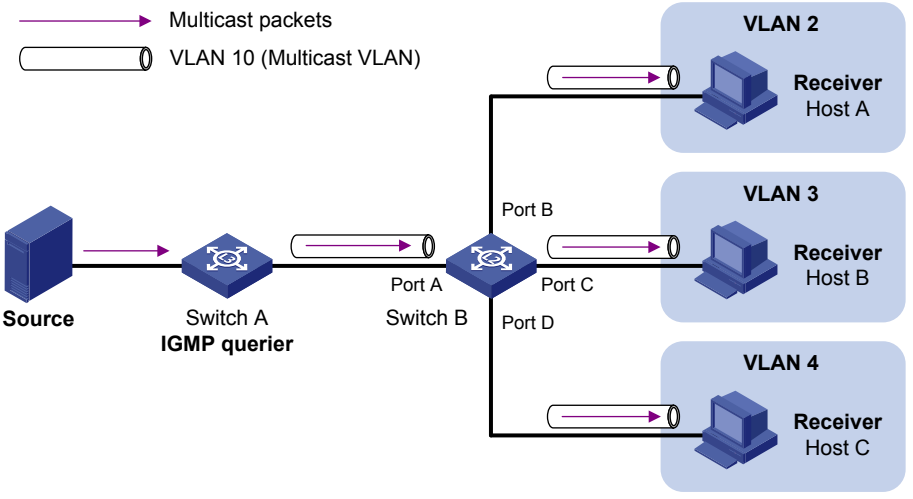
設定後､IGMP Snooping はマルチキャスト VLAN のルータポートとサブ VLAN のメンバポートを管理します。Switch A がマルチキャストソースからマルチキャストデータを受信するとき、Switch B のマルチキャスト VLAN に 1 つのマルチキャストデータのみを送信します。そして、Switch B はマルチキャスト VLAN のサブ VLAN へ分けられたコピーを送信します。

3.2.2. ポートベースマルチキャスト VLAN

図 3-3 にポートベースベースマルチキャスト VLAN を示します。

- ホスト A、ホスト B、ホスト C はそれぞれ VLAN 2、VLAN 3、VLAN 4 に属します。
- Switch B において、VLAN10 はマルチキャスト VLAN です。
- ホストが接続されているすべてのユーザポートはハイブリッドポートです。VLAN 10 が割り当てられています。
- マルチキャスト VLAN とすべてのユーザ VLAN 上で IGMP Snooping を有効にします。

図 3-3 ポートベースマルチキャスト VLAN



IGMP Snooping はマルチキャスト VLAN のルータポートとメンバポートを管理します。Switch B がユーザポートで IGMP メッセージを受信すると、メッセージにマルチキャスト VLAN のタグをつけて IGMP クエリアへ送信します。Switch B でマルチキャストデータの 1 つコピーのみをマルチキャスト VLAN に送信します。そして、Switch B はマルチキャスト VLAN の各ユーザポートに分けられたコピーを送信します。

3.3. 制限とガイドライン

マルチキャスト VLAN に指定される VLAN が事前に作成されている必要があります。

サブ VLAN ベースマルチキャスト VLAN とポートベースマルチキャスト VLAN の両方を装置に設定する場合、ポートベースマルチキャスト VLAN が優先されます。

IP マルチキャストルーティングが有効な装置でマルチキャスト VLAN を設定しないでください。設定した場合、エラーメッセージを表示します。またマルチキャスト VLAN が設定されている装置で IP マルチキャストルーティングを有効にしないでください。マルチキャストの転送にエラーが発生します。

VLAN インタフェースで PIM あるいは IGMP が有効の場合、マルチキャスト VLAN あるいはマルチキャストサブ VLAN として設定しないでください。設定した場合、エラーメッセージを表示します。また VLAN インタフェースがマルチキャスト VLAN あるいはマルチキャストサブ VLAN に属している場合、VLAN インタフェースで PIM あるいは IGMP を有効にしないでください。マルチキャストの転送にエラーが発生します。

マルチキャスト VLAN 機能はセカンダリ VLAN で適用されません。セカンダリ VLAN にマルチキャスト VLAN の設定を行わないことを推奨します。セカンダリ VLAN の詳細はセクション 3 *アクセスオペレーションマニュアル*の“*VLAN*”を参照してください。

3.4. サブVLANベースマルチキャストVLAN

I. 制限とガイドライン

マルチキャスト VLAN のサブ VLAN として設定されている VLAN は事前に作成されている必要があります。他のマルチキャスト VLAN あるいはサブ VLAN であってはいけません。

II. 設定要件

サブ VLAN ベースマルチキャスト VLAN を設定する前に、以下の作業を完了させてください。

- 必要な VLAN を作成します。
- マルチキャスト VLAN に設定する VLAN とサブ VLAN で IGMP Snooping を有効にします。

III. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. VLAN をマルチキャスト VLAN に設定し、multicast VLAN view へ移行する	**multicast-vlan** *vlan-id*	デフォルト：設定なし

操作	コマンド	補足
3. サブ VLAN をマルチキャスト VLAN に割り当てる	**subvlan** *vlan-list*	—

3.5. ポートベースマルチキャストVLANの設定

I. 制限とガイドライン

multicast VLAN view あるいは interface view のマルチキャスト VLAN にユーザポートを割り当てることができます。設定の優先度は同一です。

ユーザポートは 1 つのマルチキャスト VLAN にのみ所属することができます。

II. 設定要件

ポートベースマルチキャスト VLAN の設定をする前に、以下の作業を完了させてください。

- 必要な VLAN を作成します。
- マルチキャスト VLAN に設定する VLAN で IGMP snooping を有効にします。
- 受信ホストを含むすべての VLAN で IGMP Snooping を有効にします。
- ユーザのポートの属性を設定してください。転送されたパケットがマルチキャスト VLAN として設定された VLAN から転送され、VLAN のタグ付けが行われていることを確認してください。ポートの属性の詳細はセクション 3 *アクセス オペレーションマニュアル*の“*VLAN*”を参照してください。

III. multicast VLAN view でのマルチキャスト VLAN へのポートの割り当て

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. VLAN をマルチキャスト VLAN に設定し、multicast VLAN view へ移行する	**multicast-vlan** *vlan-id*	デフォルト：設定なし
3. ポートをマルチキャスト VLAN に割り当てる	**port** *interface-list*	—

IV. interface view でのマルチキャスト VLAN へのポートの割り当て

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. VLAN をマルチキャスト VLAN に設定し、multicast VLAN view へ移行する	**multicast-vlan** *vlan-id*	デフォルト：設定なし
3. system view に戻る	**quit**	—

操作	コマンド	補足
4. Layer 2 Ethernet interface view あるいは aggregate 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*	—
5. 現在のポートをマルチキャスト VLAN ポートに設定する	**port multicast-vlan** *vlan-id*	—

3.6. マルチキャストVLANの転送エントリの最大数の設定

I. マルチキャスト VLAN の転送エントリの最大数の設定

装置でマルチキャスト VLAN の IGMP Snooping 転送テーブルのエントリの最大数を設定できます。マルチキャスト VLAN の転送エントリ数が上限に達すると、いくつかのエントリがタイムアウトするか、手動で削除するまで、装置はマルチキャスト VLAN の転送エントリを作成しません。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. マルチキャスト VLAN の転送エントリの最大数を設定する	**multicast-vlan entry-limit** *limit*	デフォルト：4000

3.7. マルチキャスト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
マルチキャストVLANの情報を表示する	**display multicast-vlan** [*vlan-id*]
マルチキャスト転送テーブルの情報を表示する	**display multicast-vlan forwarding-table** [*group-address* [**mask** { *mask-length* | *mask* }] | *source-address* [**mask** { *mask-length* | *mask* }] | **slot** *slot-number* | **subvlan** *vlan-id* | **vlan** *vlan-id*] *
マルチキャストVLANのマルチキャストグループの情報を表示する	**display multicast-vlan group** [*source-address* | *group-address* | **slot** *slot-number* | **verbose** | **vlan** *vlan-id*] *

操作	コマンド
マルチキャストVLANのマルチキャストグループを削除する	**reset multicast-vlan group** [**source-address** [**mask** { *mask-length* | *mask* }] | *group-address* [**mask** { *mask-length* | *mask* }] | **vlan** *vlan-id*] *

3.8. マルチキャストVLANの設定例

3.8.1. サブ VLAN ベースマルチキャスト VLAN の設定例

I. ネットワーク要件

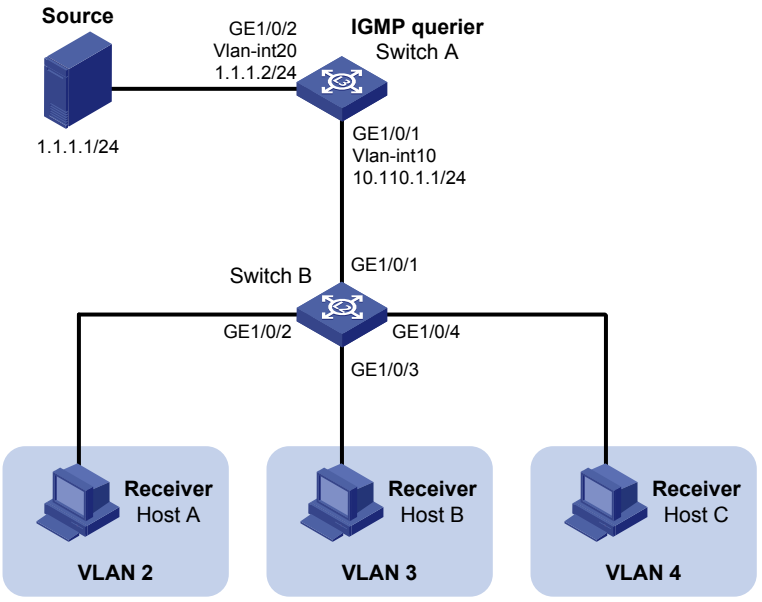
図 3-4 に示すように設定します。

- レイヤ 3 装置の Switch A で IGMPv2 が動作します。レイヤ 2 装置の Switch B で IGMPv2 Snooping が動作します。Switch A は IGMP クエリアです。
- マルチキャストソースはマルチキャストデータをマルチキャストグループ 224.1.1.1 へ送信します。Host A、Host B、Host C はマルチキャストグループのレシーバです。ホストはそれぞれ VLAN2 から VLAN4 に属しています。

Switch B でサブ VLAN ベースマルチキャスト VLAN を以下の要件に適用するように設定します。

- Switch A がマルチキャスト VLAN を通じてマルチキャストデータを Switch B へ送信します。
- Switch B が異なるユーザ VLAN に属するレシーバへマルチキャストデータを転送します。

図 3-4 ネットワーク図



II. 設定手順

1. Switch A の設定

   # IP マルチキャストルーティングを有効にします。

   <SwitchA> system-view

[SwitchA] multicast routing

[SwitchA-mrib] quit

VLAN20 を作成し、GigabitEthernet 1/0/2 を VLAN に割り当てます。

[SwitchA] vlan 20

[SwitchA-vlan20] port gigabitethernet 1/0/2

[SwitchA-vlan20] quit

VLAN インタフェース 20 に IP アドレスを設定し、PIM-SM を有効にします。

[SwitchA] interface vlan-interface 20

[SwitchA-Vlan-interface20] ip address 1.1.1.2 24

[SwitchA-Vlan-interface20] pim sm

[SwitchA-Vlan-interface20] quit

VLAN10 を作成します。

[SwitchA] vlan 10

[SwitchA-vlan10] quit

ハイブリッドポートとして GigabitEthernet 1/0/1 を設定し、タグ付きメンバとして VLAN 10 からのパケットにタグをつけます。

[SwitchA] interface gigabitethernet 1/0/1

[SwitchA-GigabitEthernet1/0/1] port link-type hybrid

[SwitchA-GigabitEthernet1/0/1] port hybrid vlan 10 tagged

[SwitchA-GigabitEthernet1/0/1] quit

VLAN インタフェース 10 に IP アドレスを設定し、IGMP を有効にします。

[SwitchA] interface vlan-interface 10

[SwitchA-Vlan-interface10] ip address 10.110.1.1 24

[SwitchA-Vlan-interface10] igmp enable

[SwitchA-Vlan-interface10] quit

2. Switch B の設定

IGMP Snooping を有効にします。

<SwitchB> system-view

[SwitchB] igmp-snooping

[SwitchB-igmp-snooping] quit

VLAN 2 を作成し、GigabitEthernet 1/0/2 を割り当て、VLAN で IGMP Snooping を有効にします。

[SwitchB] vlan 2

[SwitchB-vlan2] port gigabitethernet 1/0/2

[SwitchB-vlan2] igmp-snooping enable

[SwitchB-vlan2] quit

VLAN 3 を作成し、GigabitEthernet 1/0/3 を割り当て、VLAN で IGMP Snooping を有効にします。

[SwitchB] vlan 3

[SwitchB-vlan3] port gigabitethernet 1/0/3

[SwitchB-vlan3] igmp-snooping enable

[SwitchB-vlan3] quit

VLAN 4 を作成し、GigabitEthernet 1/0/4 を割り当て、VLAN で IGMP Snooping を有効にします。

[SwitchB] vlan 4

[SwitchB-vlan4] port gigabitethernet 1/0/4

[SwitchB-vlan4] igmp-snooping enable

[SwitchB-vlan4] quit

VLAN10 を作成し、IGMP Snooping を有効にします。

[SwitchB] vlan 10

[SwitchB-vlan10] igmp-snooping enable

[SwitchB-vlan10] quit

ハイブリッドポートとして GigabitEthernet 1/0/1 を設定し、タグ付きメンバとして VLAN 10 からのパケットにタグをつけます。

[SwitchB] interface gigabitethernet 1/0/1

[SwitchB-GigabitEthernet1/0/1] port link-type hybrid

[SwitchB-GigabitEthernet1/0/1] port hybrid vlan 10 tagged

[SwitchB-GigabitEthernet1/0/1] quit

マルチキャスト VLAN として VLAN 10 を設定し、サブ VLAN として VLAN 2～VLAN 4 を設定します。

[SwitchB] multicast-vlan 10

[SwitchB-mvlan-10] subvlan 2 to 4

[SwitchB-mvlan-10] quit

III. 設定の確認

Switch B ですべてのマルチキャスト VLAN の情報を表示します。

[SwitchB] display multicast-vlan

```
Total 1 multicast VLANs.

Multicast VLAN 10:
  Sub-VLAN list(3 in total):
     2-4
  Port list(0 in total):
```

Switch B でマルチキャスト VLAN の転送エントリの情報を表示します。

[SwitchB] display multicast-vlan group

```
Total 1 entries.

Multicast VLAN 10: Total 1 entries.
  (0.0.0.0, 224.1.1.1)
    Sub-VLANs (3 in total):
```

```
VLAN 2
VLAN 3
VLAN 4
```

出力では次のことを示します。マルチキャスト VLAN（VLAN 10）はサブ VLAN 2～VLAN 4 が含まれます。Switch B は VLAN 10 のマルチキャストデータを VLAN 2～VLAN 4 にコピーしています。

3.8.2. ポートベースマルチキャスト VLAN の設定例

I. ネットワーク要件

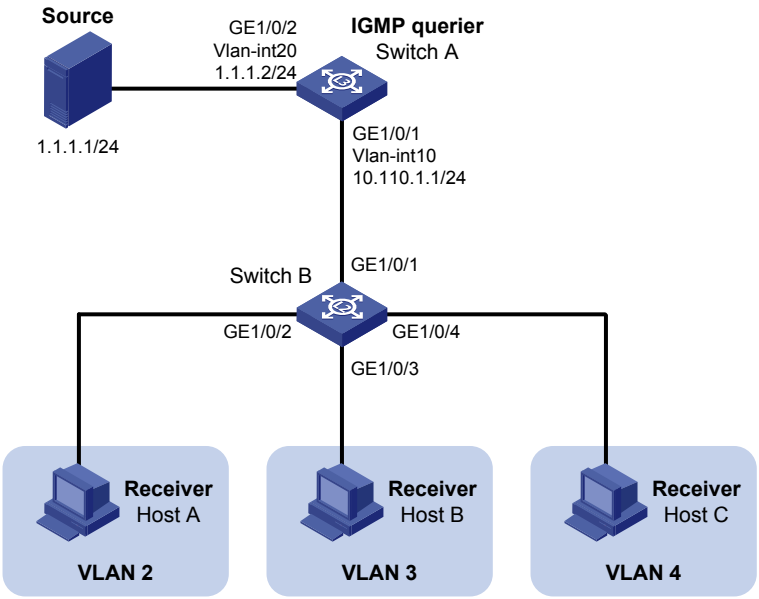
図 3-5 に示すように設定します。

- Switch A で IGMPv2 が動作します。Switch B で IGMPv2 Snooping が動作します。
- Switch A は IGMP クエリアです。
- マルチキャストソースはマルチキャストデータをマルチキャストグループ 224.1.1.1 に送信します。Host A、Host B、Host C はマルチキャストグループのレシーバです。ホストはそれぞれ VLAN 2～VLAN 4 に属しています。

Switch B でポートベースマルチキャスト VLAN を以下の要件に適用するように設定します。

- Switch A はマルチキャスト VLAN を通じてマルチキャストデータを Switch B へ送信します。
- Switch B が異なるユーザ VLAN に属するレシーバへマルチキャストデータを転送します。

図 3-5 ネットワーク図



II. 設定手順

1. Switch A の設定

   # IP マルチキャストルーティングを有効にします。

   <SwitchA> system-view

   [SwitchA] multicast routing

   [SwitchA-mrib] quit

VLAN20 を作成し、GigabitEthernet 1/0/2 を VLAN に割り当てます。

[SwitchA] vlan 20

[SwitchA-vlan20] port gigabitethernet 1/0/2

[SwitchA-vlan20] quit

VLAN インタフェース 20 に IP アドレスを設定し、PIM-SM を有効にします。

[SwitchA] interface vlan-interface 20

[SwitchA-Vlan-interface20] ip address 1.1.1.2 24

[SwitchA-Vlan-interface20] pim sm

[SwitchA-Vlan-interface20] quit

VLAN10 を作成し、GigabitEthernet 1/0/1 を VLAN に割り当てます。

[SwitchA] vlan 10

[SwitchA-vlan10] port gigabitethernet 1/0/1

[SwitchA-vlan10] quit

VLAN インタフェース 10 に IP アドレスを設定し、インタフェースで IGMP を有効にします。

[SwitchA] interface vlan-interface 10

[SwitchA-Vlan-interface10] ip address 10.110.1.1 24

[SwitchA-Vlan-interface10] igmp enable

[SwitchA-Vlan-interface10] quit

2. Switch B の設定

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

VLAN10 を作成し、GigabitEthernet 1/0/1 を割り当て、IGMP Snooping を有効にします。

[SwitchB] vlan 10

[SwitchB-vlan10] port gigabitethernet 1/0/1

[SwitchB-vlan10] igmp-snooping enable

[SwitchB-vlan10] quit

VLAN 2 を作成し、IGMP Snooping を有効にします。

[SwitchB] vlan 2

[SwitchB-vlan2] igmp-snooping enable

[SwitchB-vlan2] quit

VLAN 3 を作成し、IGMP Snooping を有効にします。

[SwitchB] vlan 3

[SwitchB-vlan3] igmp-snooping enable

[SwitchB-vlan3] quit

VLAN 4 を作成し、IGMP Snooping を有効にします。

[SwitchB] vlan 4

[SwitchB-vlan4] igmp-snooping enable

[SwitchB-vlan4] quit

ハイブリッドポートとして GigabitEthernet 1/0/2 を設定し、ハイブリッドポートの PVID を 2 に設定します。

[SwitchB] interface gigabitethernet 1/0/2

[SwitchB-GigabitEthernet1/0/2] port link-type hybrid

[SwitchB-GigabitEthernet1/0/2] port hybrid pvid vlan 2

VLAN2、VLAN10 に GigabitEthernet 1/0/2 を割り当て、タグなしメンバとして VLAN2、VLAN10 からのパケットからタグを外します。

[SwitchB-GigabitEthernet1/0/2] port hybrid vlan 2 untagged

[SwitchB-GigabitEthernet1/0/2] port hybrid vlan 10 untagged

[SwitchB-GigabitEthernet1/0/2] quit

ハイブリッドポートとして GigabitEthernet 1/0/3 を設定し、ハイブリッドポートの PVID を 3 に設定します。

[SwitchB] interface gigabitethernet 1/0/3

[SwitchB-GigabitEthernet1/0/3] port link-type hybrid

[SwitchB-GigabitEthernet1/0/3] port hybrid pvid vlan 3

VLAN 3、VLAN 10 に GigabitEthernet 1/0/3 を割り当て、タグなしメンバとして VLAN 3、VLAN 10 からのパケットからタグを外します。

[SwitchB-GigabitEthernet1/0/3] port hybrid vlan 3 untagged

[SwitchB-GigabitEthernet1/0/3] port hybrid vlan 10 untagged

[SwitchB-GigabitEthernet1/0/3] quit

ハイブリッドポートとして GigabitEthernet 1/0/4 を設定し、ハイブリッドポートの PVID を 4 に設定します。

[SwitchB] interface gigabitethernet 1/0/4

[SwitchB-GigabitEthernet1/0/4] port link-type hybrid

[SwitchB-GigabitEthernet1/0/4] port hybrid pvid vlan 4

VLAN 4、VLAN 10 に GigabitEthernet 1/0/4 を割り当て、タグなしメンバとして VLAN 4、VLAN 10 からのパケットからタグを外します。

[SwitchB-GigabitEthernet1/0/4] port hybrid vlan 4 untagged

[SwitchB-GigabitEthernet1/0/4] port hybrid vlan 10 untagged

[SwitchB-GigabitEthernet1/0/4] quit

マルチキャスト VLAN として VLAN10 を設定します。

[SwitchB] multicast-vlan 10

GigabitEthernet 1/0/2 と GigabitEthernet 1/0/3 に VLAN10 を割り当てます。

[SwitchB-mvlan-10] port gigabitethernet 1/0/2 to gigabitethernet 1/0/3

[SwitchB-mvlan-10] quit

GigabitEthernet 1/0/4 に VLAN10 を割り当てます。

[SwitchB] interface gigabitethernet 1/0/4

[SwitchB-GigabitEthernet1/0/4] port multicast-vlan 10

[SwitchB-GigabitEthernet1/0/4] quit

III. 設定の確認

Switch B のマルチキャスト VLAN の情報を表示します。

[SwitchB] display multicast-vlan

```
Total 1 multicast VLANs.

Multicast VLAN 10:
  Sub-VLAN list(0 in total):
  Port list(3 in total):
    GE1/0/2
    GE1/0/3
    GE1/0/4
```

Switch B でダイナミックマルチキャストグループの IGMP Snooping 転送エントリを表示します。

[SwitchB] display igmp-snooping group

```
Total 1 entries.

VLAN 10: Total 1 entries.
  (0.0.0.0, 224.1.1.1)
    Host slots (0 in total):
    Host ports (3 in total):
      GE1/0/2         (00:03:23)
      GE1/0/3         (00:04:07)
      GE1/0/4         (00:04:16)
```

出力では、IGMP Snooping が VLAN10 のユーザポートを維持していることを示します。Switch B はユーザポートを通して VLAN 10 のマルチキャストデータを転送します。

目次

このセクションのページは **6-x-x** です。

4 章 MLD スヌーピング ····· 4-1
4.1. 概要 ····· 4-1
4.1.1. MLD snooping の基本コンセプト ····· 4-1
4.1.2. MLD snooping 関連ポート ····· 4-1
4.1.3. MLD snooping の動作 ····· 4-3
4.1.4. プロトコルと標準 ····· 4-4
4.2. 制限とガイドライン ····· 4-5
4.3. VLAN ベース MLD snooping の設定作業リスト ····· 4-5
4.4. MLD snooping 機能の有効化 ····· 4-6
4.5. MLD snooping の有効化 ····· 4-6
4.5.1. VLAN での MLD snooping の有効化 ····· 4-6
4.6. MLD snooping の基本機能の設定 ····· 4-7
4.6.1. MLD snooping のバージョンの設定 ····· 4-7
4.6.2. MLD snooping 転送エントリの最大数の設定 ····· 4-8
4.6.3. スタティック IPv6 マルチキャスト MAC アドレスエントリの設定 ····· 4-8
4.6.4. MLD last listener クエリ間隔の設定 ····· 4-9
4.7. MLD snooping ポート機能の設定 ····· 4-10
4.7.1. ダイナミックポートのエージングタイマの設定 ····· 4-10
4.7.2. スタティックメンバポートの設定 ····· 4-11
4.7.3. スタティックルータポートの設定 ····· 4-12
4.7.4. シミュレーティッドメンバホストの設定 ····· 4-12
4.7.5. fast-leave 処理の有効化 ····· 4-13
4.8. MLD snooping クエリアの設定 ····· 4-14
4.8.1. MLD snooping クエリアの有効化 ····· 4-14
4.8.2. MLD general query と response のパラメータの設定 ····· 4-14
4.9. MLD メッセージのパラメータの設定 ····· 4-15
4.9.1. MLD メッセージの送信元 IPv6 アドレスの設定 ····· 4-15
4.9.2. MLD メッセージの 802.1p 優先度の設定 ····· 4-17
4.10. MLD snooping ポリシーの設定 ····· 4-17
4.10.1. IPv6 マルチキャストグループポリシーの設定 ····· 4-17
4.10.2. IPv6 マルチキャストソースポートフィルタの有効化 ····· 4-18
4.10.3. 未知の IPv6 マルチキャストデータ廃棄機能の設定 ····· 4-19
4.10.4. MLD report 抑制の有効化 ····· 4-20
4.10.5. ポートで参加可能な IPv6 マルチキャストグループの最大数の設定 ····· 4-20
4.10.6. IPv6 マルチキャストグループ置き換え機能の有効化 ····· 4-21
4.11. 送信する MLD snooping プロトコルパケットの DSCP の設定 ····· 4-22
4.12. MLD snooping の表示と維持 ····· 4-22
4.13. MLD snooping 設定例 ····· 4-23
4.13.1. VLAN ベース 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の加入の設定例 ····· 4-23
4.13.2. VLAN ベース MLD snooping スタティックポートの設定例 ····· 4-26
4.13.3. VLAN ベース MLD snooping クエリアの設定例 ····· 4-29
4.14. MLD snooping のトラブルシューティング ····· 4-31
4.14.1. レイヤ 2 マルチキャスト転送ができない ····· 4-31

4.14.2. IPv6 マルチキャストグループポリシーが動作しない 4-32

4章 MLD スヌーピング

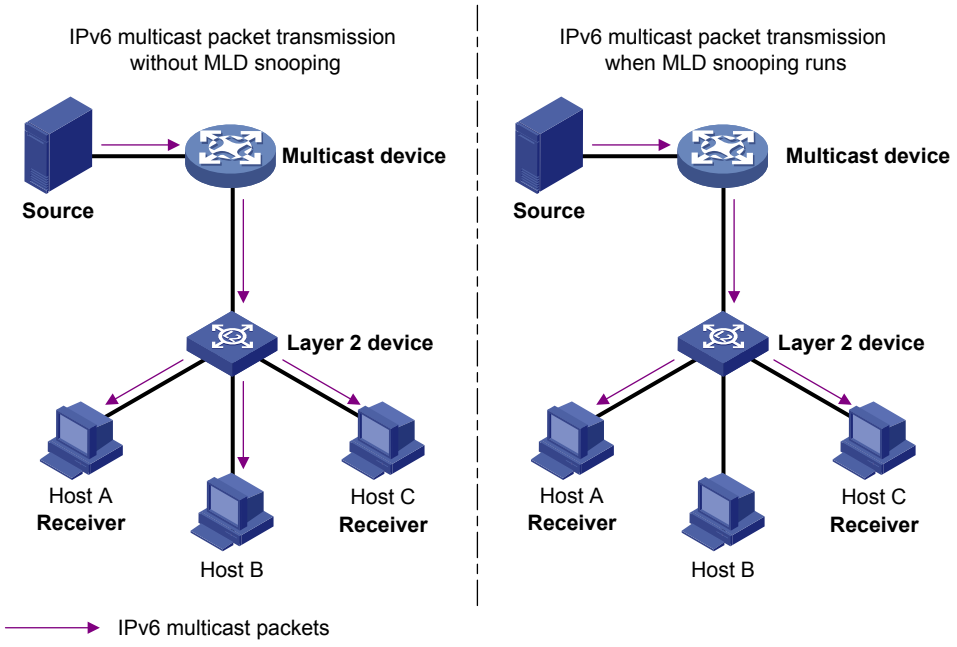
4.1. 概要

MLD snooping はマルチキャスト転送の効率を改良するために、IPv6 マルチキャストを行うメカニズムとして、レイヤ 2 装置で動作します。MLD snooping はレイヤ 3 マルチキャスト装置とホストと装置間で交換された MLD メッセージからレイヤ 2 マルチキャスト転送エントリを作成します。

4.1.1. MLD snooping の基本コンセプト

図 4-1 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 VLAN のすべてのポートにブロードキャストされます。レイヤ 2 装置で MLD snooping を有効にすると、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は、レシーバへのみ転送されます。

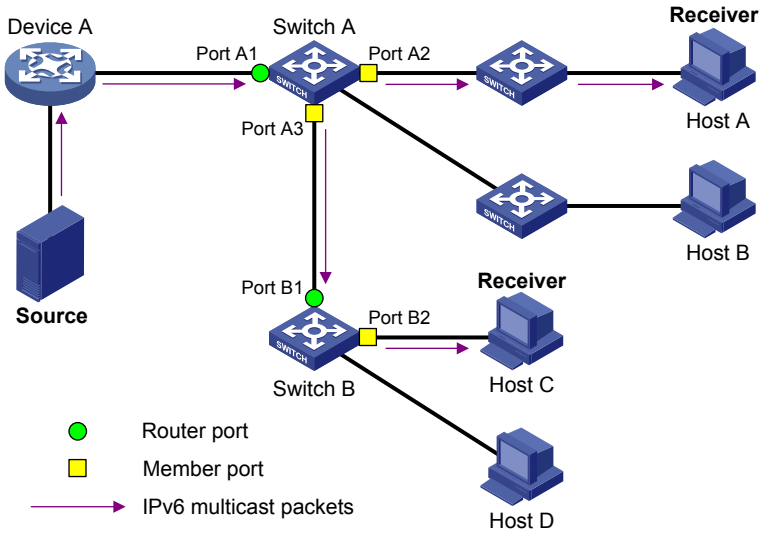
図 4-1 MLD snooping を有効にする前と有効にした後のマルチキャストパケットの転送



4.1.2. MLD snooping 関連ポート

図 4-2 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。

図 4-2 MLD snooping 関連ポート



I. ルータポート

MLD snooping が有効なレイヤ 2 装置では、ポートはレイヤ 3 マルチキャスト方向へのポートはルータポートと呼ばれます。図 4-2 では、Switch A の Port A1、Switch B の Port B1 はルータポートです。

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**－ポートで送信元アドレスが 0::0 でない MLD general query あるいは IPv6 PIM hello メッセージを受信した場合、ポートはダイナミックルータポートリストに追加されます。同時にポートのエージング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た場合、タイマは再起動します。タイマが満了する前にメッセージを受信しない場合、装置は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**－ルータポートとしてスタティックに設定した場合、ポートはスタティックルータポートに追加されます。スタティックルータポートはエージアウトしません。手動でスタティックルータポートから削除しない限り、削除されません。

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 が有効なレイヤ 2 装置では、ポートは受信ホスト方向へのポートはメンバポートと呼ばれます。図 4-2 では、Switch A の Port A2、Port A3、Switch B の Port B2 はメンバポートです。

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**－ポートで MLD report を受信した場合、ポートは出力インタフェースとして、ダイナミック MLD snooping 転送テーブルのエントリに追加されます。同時にポートのエージングタイマが開始します。タイマが満了する前に MLD report を受信した場合、タイマは再起動します。タイマが満了する前に MLD report を受信しない場合、装置はダイナミック MLD snooping 転送エントリからポートを削除します。
- **スタティックメンバポート**－メンバポートとしてスタティックに設定した場合、ポートは出力インタフェースとしてスタティック 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。手動でスタティックメンバポートから削除しない限り、削除されません。

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。

4.1.3. 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、セクション 6 *マルチキャスト オペレーションマニュアル*の”*MLD snooping*”の”*スタティックメンバポートの設定*”、”*スタティックルータポートの設定*”を参照してください。

MLD メッセージのタイプは、general query、MLD report、done message 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 query

MLD クエリアは、アクティブな 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 query を定期的に送信します。

MLD クエリアから MLD general query を受信すると、レイヤ 2 装置は、メッセージを受信したポートと同じ VLAN に属するすべてのポート（受信ポート以外）へ MLD general query 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、レイヤ 2 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は、レイヤ 2 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、MLD query に応答します。
- IPv6 マルチキャストグループ membership を適用します。

ホストからの MLD report を受信すると、レイヤ 2 装置は VLAN のすべてのルータポートからそれを転送し、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、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再スタートします。

メモ:

レイヤ 2 装置は MLD report の抑制を行わないため、非ルータポートを通して MLD レポートの転送を行いません。非ルータポートがメンバホストに接続された場合、メンバホストは非ルータポートによって転送された MLD report を受信した際に MLD report を抑制します。レイヤ 2 装置は非ルータポートに接続されたメンバホストの存在を知ることはできません。

III. Done message

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とき、レイヤ 2 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、レイヤ 2 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マッチするが、受信ポートが転送エントリに含まれていない場合、レイヤ 2 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、レイヤ 2 装置は以下のアクションを実行します。
  - MLD done メッセージを廃棄します。
  - グループが受信ポートに接続されているアクティブレシーバが存在するか確認するため、MLD multicast-address-specific query を送信します。
  - 受信ポートのエージングタイマを、MLD last listener query の送信間隔の 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、レイヤ 2 装置は以下のアクションを実行します。
  - 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。
  - グループが受信ポートに接続されているアクティブレシーバが存在するか確認するため、MLD multicast-address-specific query を送信します。
  - 受信ポートのエージングタイマを、MLD last listener query の送信間隔の 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 query を送信します。

MLD multicast-address-specific query を受信したのち、レイヤ 2 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、query を転送します。

直接に接続されているホストから MLD report に対する応答を待ちます。done メッセージを受信したダイナミックメンバポートのため、レイヤ 2 装置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、レイヤ 2 装置はエージングタイマを再起動します。
- エージングタイマが満了する前にポートが MLD report を受信しない場合、レイヤ 2 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。

4.1.4. プロトコルと標準

RFC 4541, *Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches*

4.2. 制限とガイドライン

セカンダリ VLAN から受信した MLD report のため、関連する MLD snooping 転送エントリはプライマリ VLAN によって管理されます。そのため、プライマリ VLAN で MLD snooping を有効にする必要があります。セカンダリ VLAN で設定された MLD snooping の設定は適用されません。プライマリ VLAN とセカンダリ VLAN の詳細はセクション 3 *アクセス オペレーションマニュアル*の“*VLAN*”を参照してください。

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。さらに、アグリゲートインタフェースの設定はアグリゲーションの計算に追加されません。ポートがアグリゲーショングループから取り外されたのち、アグリゲーショングループのメンバポートの設定が適用されます。

VLAN view の VLAN、あるいは MLD-snooping view の複数の VLAN で設定することができます。MLD view の設定と MLD-snooping view の設定の優先度は同一ですが、最後に行われた設定が適用されます。

VLAN view の VLAN、あるいは MLD-snooping view のすべての VLAN でグローバルに設定することができます。VLAN で行われた設定はグローバルで行われた設定よりも優先されます。

interface view の VLAN、あるいは MLD-snooping view の指定した VLAN のすべてのインタフェースで設定することができます。インタフェースで行われた設定は MLD-snooping view で行われた設定よりも優先されます。

4.3. VLANベースMLD snoopingの設定作業リスト

作業リスト
1. MLD snooping 機能の有効化
2. MLD snooping の有効化 必要に応じて以下の機能を選択してください。 • VLAN での MLD snooping の有効化 3. (オプション設定項目) MLD snooping の基本機能の設定 • MLD snooping のバージョンの設定 • MLD snooping 転送エントリの最大数の設定 • スタティック IPv6 マルチキャスト MAC アドレスエントリの設定 • MLD last listener query の間隔の設定
4. (オプション設定項目) MLD snooping ポート機能の設定 • ダイナミックポートのエージングタイマの設定 • スタティックメンバポートの設定 • スタティックルータポートの設定 • シミュレーティッドメンバホストの設定 • fast-leave 処理の有効化

作業リスト
5.　(オプション設定項目) MLD snooping クエリアの設定 • MLD snooping クエリアの有効化 • MLD general query と response のパラメータの設定
6.　(オプション設定項目) MLD メッセージパラメータの設定 • MLD メッセージの送信元 IPv6 アドレスの設定 • MLD メッセージの 802.1p 優先度の設定
7.　(オプション設定項目) MLD snooping ポリシーの設定 • IPv6 マルチキャストグループポリシーの設定 • IPv6 マルチキャストソースポートフィルタの設定 • 未知の IPv6 マルチキャストデータ廃棄機能の設定 • MLD report 抑制機能の設定 • ポートで参加可能な IPv6 マルチキャストグループの最大数の設定 • マルチキャストグループ置き換え機能の設定
8.　(オプション設定項目) 送信する MLD snooping プロトコルパケットの DSCP の設定

4.4.　MLD snooping機能の有効化

I.　MLD snooping 機能の有効化の条件

MLD snooping 機能を有効化する前に、他の MLD snooping 機能の設定を完了させてください。

II.　設定手順

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

4.5.　MLD snoopingの有効化

4.5.1.　VLAN での MLD snooping の有効化

I.　制限とガイドライン

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。

VLAN 用の MLD snooping は、VLAN のメンバポートでのみ動作します。

II.　複数の VLAN での MLD snooping の有効化

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**	デフォルト：無効
3. 複数の VLAN で MLD snooping を有効にする	**enable vlan** *vlan-list*	デフォルト：無効

III. VLAN での MLD snooping の有効化

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. VLAN で MLD snooping を有効にする	**mld-snooping enable**	デフォルト：無効

4.6. MLD snoopingの基本機能の設定

4.6.1. MLD snooping のバージョンの設定

I. MLD snooping のバージョンの設定

MLD snooping のバージョン異なると、MLD 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。

- MLDv1 snooping は MLDPv1 と MLDv2 のメッセージを処理することができますが、MLDv2 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。
- MLDv2 snooping は MLDv1、MLDv2 メッセージを処理することができます。

II. 制限とガイドライン

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 に切り替わったとき復元されます。

スタティック MLD snooping 転送エントリの詳細については、セクション 6 *マルチキャスト オペレーションマニュアル*の”*MLD snooping*”の”*スタティックポートの設定*”を参照してください。

III. 複数の VLAN での MLD snooping のバージョンの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. MLD-snooping view に移行する	**mld-snooping**	デフォルト：無効
3. 複数での 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

IV. VLAN での MLD snooping のバージョンの設定

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 snooping のバージョンを指定する	**mld-snooping version** *version-number*	デフォルト：1

4.6.2. MLD snooping 転送エントリの最大数の設定

I. MLD snooping 転送エントリの最大数の設定

MLD 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。

II. 設定手順

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

4.6.3. スタティック IPv6 マルチキャスト MAC アドレスエントリの設定

I. スタティック IPv6 マルチキャスト MAC アドレスエントリ

レイヤ 2 IPv6 マルチキャストでは、IPv6 マルチキャスト MAC アドレスエントリは MLD snooping のようなレイヤ 2 マルチキャストプロトコルを通してダイナミックに作成することができます。IPv6 マルチキャスト MAC アドレスと、IPv6 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付けることで、スタティック IPv6 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。

II. 制限とガイドライン

スタティック IPv6 マルチキャスト MAC アドレスエントリを設定するとき、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。

III. system view でのスタティック IPv6 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**	—

操作	コマンド	補足
2. スタティック IPv6 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*	—

IV. interface view でのスタティック IPv6 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	• 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*	—
3. スタティック IPv6 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*	—

4.6.4. MLD last listener クエリ間隔の設定

I. MLD last listener クエリ間隔

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（ホストは、受信したクエリの 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 になったときに、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 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ときに同時に送信する 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。

II. グローバルでの MLD last listener 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. MLD-snooping view に移行する	**mld-snooping**	—
3. MLD last listener クエリの送信間隔を設定する	**last-listener-query-interval** *interval*	デフォルト：1秒

III. VLAN での MLD last listener 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. MLD last listener クエリの送信間隔を設定する	**mld-snooping last-listener-query-interval** *interval*	デフォルト：1秒

4.7. MLD snoopingポート機能の設定

4.7.1. ダイナミックポートのエージングタイマの設定

I. ダイナミックポートのエージングタイマ

エージングタイマが満了するときまでに MLD general query あるいは IPv6 PIM Hello メッセージを受信しない場合、ダイナミックルータ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。

エージングタイマが満了するときまでに MLD Report を受信しない場合、ダイナミックメンバポートはダイナミックメンバポートリストからポートを削除します。

II. 制限とガイドライン

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。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 メッセージの時間で指定されません。この場合、**mld-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 MLD-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。もし 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。

レイヤ 2 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が行われます。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 member クエリ間隔の 2 倍に設定します。MLD last listener クエリ間隔の詳細は“*MLD last listener クエリ間隔の設定*”を参照してください。

III. 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**	—

操作	コマンド	補足
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

IV. 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

4.7.2. スタティックメンバポートの設定

I. スタティックメンバポートの設定

ホストに接続されたポートが常にグループの IPv6 マルチキャストを受信できるように、ポートを 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に設定することができます。スタティックメンバポートは MLD クエリに応答しません。ポートの設定を完了あるいは設定を取り消したとき、ポートは不要な unsolicited report や done メッセージを送信しません。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. Layer 2 Ethernet interface view あるいは aggregate 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*	—

操作	コマンド	補足
3. 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** *group-address* [**source-ip** *source-address*] **vlan** *vlan-id*	デフォルト：設定なし

4.7.3. スタティックルータポートの設定

I. スタティックルータポートの設定

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を設定するとき、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。

II. 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 view あるいは aggregate 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*	—
3. ポートをスタティックポートに設定する	**mld-snooping static-router-port vlan** *vlan-id*	デフォルト：設定なし

4.7.4. シミュレーティッドメンバホストの設定

I. 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とき、以下の方法により独立したホストと同等になります。

- 設定が完了したとき、unsolicited MLD report を送信します。
- MLD report として MLD general query に応答します。
- 設定を削除したとき、MLD done メッセージを送信します。

この操作を行うとき、シミュレーティッドホストの MLD のバージョンと 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。

II. 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 view あるいは aggregate 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*	—
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	**mld-snooping host-join** *ipv6-group-address* [**source-ip** *source-address*] **vlan** *vlan-id*	デフォルト：設定なし

4.7.5. fast-leave 処理の有効化

I. fast-leave 処理

この機能を有効にすることで、ポートが done メッセージを受信したときに、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すぐに削除することができます。

レイヤ 2 装置はグループの MLD multicast-address-specific クエリをポートに送信あるいは転送しません。

II. 制限とガイドライン

VLAN の複数のホストが接続しているポートに fast-leave 処理機能を有効にしないでください。そうでないと同じ 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。

III. 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 MLD snooping fast-leave 処理機能を設定する	**fast-leave** [**vlan** *vlan-list*]	デフォルト：無効

IV. ポートでのでの 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. Layer 2 Ethernet interface view あるいは aggregate 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*	—
3. ポートで MLD snooping fast-leave 処理機能を設定する	**mld-snooping fast-leave** [**vlan** *vlan-list*]	デフォルト：無効

4.8. MLD snoopingクエリアの設定

4.8.1. MLD snooping クエリアの有効化

I. MLD snooping クエリア

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 MLD general query 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。

II. 制限とガイドライン

MLD snooping クエリアを有効にするとき、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 query を送信するので MLD クエリアの選択に影響を与える可能性があります。

III. VLAN での MLD snooping クエリアの有効化

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

4.8.2. MLD general query と response のパラメータの設定

I. MLD general query と response のパラメータ

ネットワークの実際の状況にもとづいて、MLD general query の送信間隔を調整することができます。

MLD general query 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 になったときに、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 query の最大応答時間を適切に設定すると、ホストは速やかに query 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ときに同時に送信する 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。

II. 制限とガイドライン

MLD general query 間隔は MLD general query の最大応答時間よりも大きいことを確認してください。そうしないと IPv6 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。

III. グローバルでの MLD query 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 query の最大応答時間を設定する	**max-response-time** *seconds*	デフォルト：10秒

IV. VLAN での MLD query 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 query 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 query 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

4.9. MLDメッセージのパラメータの設定

4.9.1. MLD メッセージの送信元 IPv6 アドレスの設定

I. MLD メッセージの送信元 IPv6 アドレスの設定

MLD snooping クエリアが送信した 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 クエリア選定に影響する可能性があります。

またシミュレーティッドメンバホストによって送信された MLD report の送信元 IPv6 アドレスを変更することができます。

II. VLAN での MLD メッセージの送信元 IPv6 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**	ー
2. VLAN view に移行する	**vlan** *vlan-id*	ー
3. MLD general query 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 group-specific query 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： MLD snoopingクエリアがMLD general queryを受信していた場合、MLD multicast-address-specific queriesの送信元IPv6アドレスはMLD general queryの送信元IPv6アドレスです。 MLD snoopingクエリアがMLD general queryを受信していない場合、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。
5. MLD reports 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 leave メッセージの送信元 IPv6 アドレスを設定する	**mld-snooping leave source-ip** *ipv6-address*	デフォルト： 現在のVLANインタフェースのIPv6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。

4.9.2. MLD メッセージの 802.1p 優先度の設定

I. MLD メッセージの 802.1p 優先度

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 MLD 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 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。

II. 制限とガイドライン

MLD-snooping view の設定はすべての VLAN でのみ適用されます。

III. 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*	—

IV. 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*	—
3. MLD メッセージの 802.1p 優先度を設定する	**mld-snooping** **dot1p-priority** *priority*	—

4.10. MLD snoopingポリシーの設定

4.10.1. IPv6 マルチキャストグループポリシーの設定

I. IPv6 マルチキャストグループポリシー

IPv6 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 MLD report をフィルタします。受信ホストが加入する IPv6 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。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。

IPv6 マルチキャストアプリケーションにおいて、ユーザがマルチキャストプログラムを要求したとき、ホストが不要な MLD report を送信します。レイヤ 2 装置は MLD report をフィルタするため、IPv6 マルチキャストグループポリシーを使用します。MLD report がマルチキャストポリシーで許可されているときのみホストが IPv6 マルチキャストグループに加入することができます。

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. 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**	—
2. Layer 2 Ethernet interface view あるいは aggregate 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*	—
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

4.10.2. IPv6 マルチキャストソースポートフィルタの有効化

I. IPv6 マルチキャストソースポートフィルタ

この機能はレイヤ 2 装置がすべての IPv6 マルチキャストデータパケットを廃棄し、IPv6 マルチキャストプロトコルパケットを許可します。IPv6 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。

II. 制限とガイドライン

IPv6 マルチキャストソースポートフィルタが有効である場合、システムは自動で IPv6 マルチキャストソースフィルタリングを有効にします。

MLD-snooping view の複数の VLAN で設定することができます。interface view の設定と MLD-snooping view の設定の優先度は同一ですが、最後に行われた設定が適用されます。

III. 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**	—

操作	コマンド	補足
2. MLD-snooping view に移行する	**mldsnooping**	—
3. IPv6 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

IV. ポートでの IPv6 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*	—
3. IPv6 マルチキャストソースポートフィルタを有効にする	**mld-snooping source-deny**	デフォルト：無効

4.10.3. 未知の IPv6 マルチキャストデータ廃棄機能の設定

I. 未知の IPv6 マルチキャストデータ廃棄機能

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。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。

この機能は未知の IPv6 マルチキャストデータをルータポートにのみ転送します。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。この機能を無効にした場合、装置は未知の IPv6 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。

II. 制限とガイドライン

未知の IPv6 マルチキャストデータの廃棄機能が有効であるとき、IPv4 マルチキャストデータも廃棄します。

未知の IPv6 マルチキャストデータの廃棄機能が有効であるとき、装置はルータポートでの受信を除き、ルータポートから未知の IPv6 マルチキャストデータを転送します。

III. VLAN での未知の IPv6 マルチキャストデータ廃棄機能の有効化

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. VLAN view に移行する	**vlan** *vlan-id*	—
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。

4.10.4. MLD report 抑制の有効化

I. MLD report 抑制の有効化

この機能は IPv6 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 MLD report のみを転送します。以降の同じ IPv6 マルチキャストグループからの MLD report を廃棄します。この機能によってマルチキャストトラフィックを削減できます。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. MLD-snooping view に移行する	**mld-snooping**	—
3. MLD report 抑制を有効にする	**report-aggregation**	デフォルト：有効

4.10.5. ポートで参加可能な IPv6 マルチキャストグループの最大数の設定

I. ポートで参加可能な 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、ポートで参加可能な 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。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最大数に達したときは、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ホストは、最大数になる前に、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

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	• 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*	—

操作	コマンド	補足
3. ポートで参加可能な IPv6 マルチキャストグループの最大数の設定をする	**mld-snooping group-limit** *limit* [**vlan** *vlan-list*]	デフォルト：4294967295

4.10.6. IPv6 マルチキャストグループ置き換え機能の有効化

I. IPv6 マルチキャストグループ置き換え機能

この機能は、グループのメンバ数が上限を超えたとき、レイヤ 2 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 IPv6 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装置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 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。

II. 制限とガイドライン

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。

III. 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

IV. ポートでの IPv6 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	• 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*	—
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

4.11. 送信するMLD snoopingプロトコルパケットのDSCPの設定

I. 送信する MLD snooping プロトコルパケットの DSCP

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。

II. 設定手順

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. 送信する MLD snooping プロトコルパケットの DSCP を設定する	**dscp** *dscp-value*	デフォルト：48

4.12. 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の情報を表示する	**display ipv6 l2-multicast ip** [**group** *ipv6-group-address* | **source** *ipv6-source-address*] * [**vlan** *vlan-id*] [**slot** *slot-number*]
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の情報を表示する	**display ipv6 l2-multicast mac** [*mac-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*]
スタティックIPv6マルチキャストMACアドレスエントリの情報を表示する	**display mac-address** [*mac-address* [**vlan** *vlan-id*] | [**multicast**] [**vlan** *vlan-id*] [**count**]]
MLD snooping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グループ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*] [**interface** *interface-type interface-number* | [**verbose**] [**slot** *slot-number*]]

操作	コマンド
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*] [**verbose**] [**slot** *slot-number*]
スタティックMLD snoopingグループ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*]
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*] [**verbose**] [**slot** *slot-number*]
MLD snoopingによって学習されたMLDメッセージとIPv6 PIM helloメッセージの統計情報を表示する	**display mld-snooping statistics**
ダイナミックMLD snoopingグループ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メッセージとIPv6 PIM helloメッセージの統計情報を削除する	**reset mld-snooping statistics**

4.13. MLD snooping設定例

4.13.1. VLAN ベース 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の加入の設定例

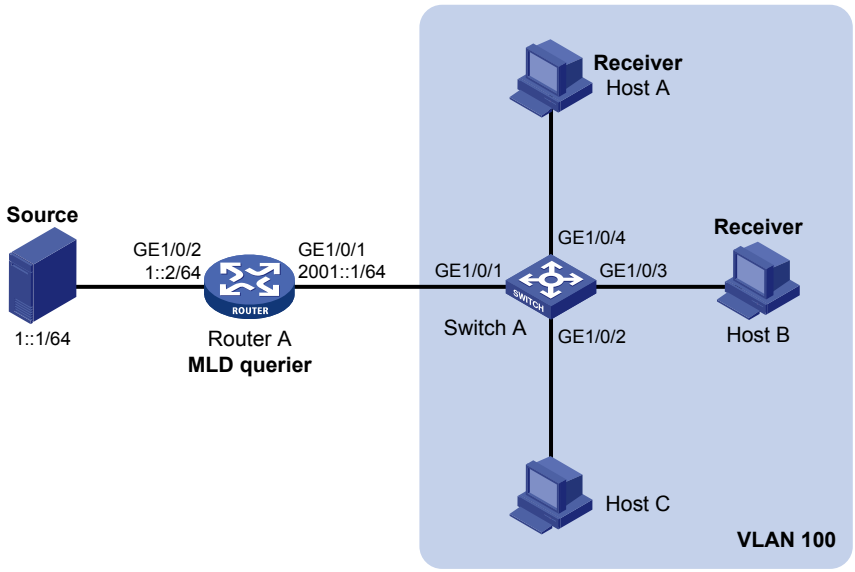
I. ネットワーク要件

図 4-3 に示すように、Router A は MLDv1 で動作させ、MLD クエリアとして機能し、Switch A は MLDv1 snooping を動作させます。

以下の要件に従うようにグループポリシーを設定し、シミュレーティッドメンバホストの加入の設定を行います。

- Host A、Host B は IPv6 マルチキャストグループ FF1E::101 にアドレスされた IPv6 マルチキャストデータのみ受信します。IPv6 マルチキャストデータは Switch A の GigabitEthernet 1/0/3、GigabitEthernet 1/0/4 を通して連続して転送されます。たとえ Host A、Host B でマルチキャストデータを受信するのに失敗したとしても、絶え間なく転送されます。
- Switch A は VLAN 100 でフラッディングしないように未知の IPv6 マルチキャストデータを廃棄します。

図 4-3 ネットワーク図



II. 設定手順

1. 図 4-3 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 MLD snooping と未知の 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 のホストは IPv6 マルチキャストグループ FF1E::101 のみに参加できるように、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

Host A と Host B が IPv6 マルチキャストグループ FF1E::101、FF1E::202 に加入するため MLD 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 MLD snooping グループ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 IPv6 マルチキャストグループ FF1E::101 に加入しています。
- Host A と Host B が IPv6 マルチキャストグループ FF1E::202 に加入できないことを示しています。IPv6 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。

4.13.2. VLAN ベース MLD snooping スタティックポートの設定例

I. ネットワーク要件

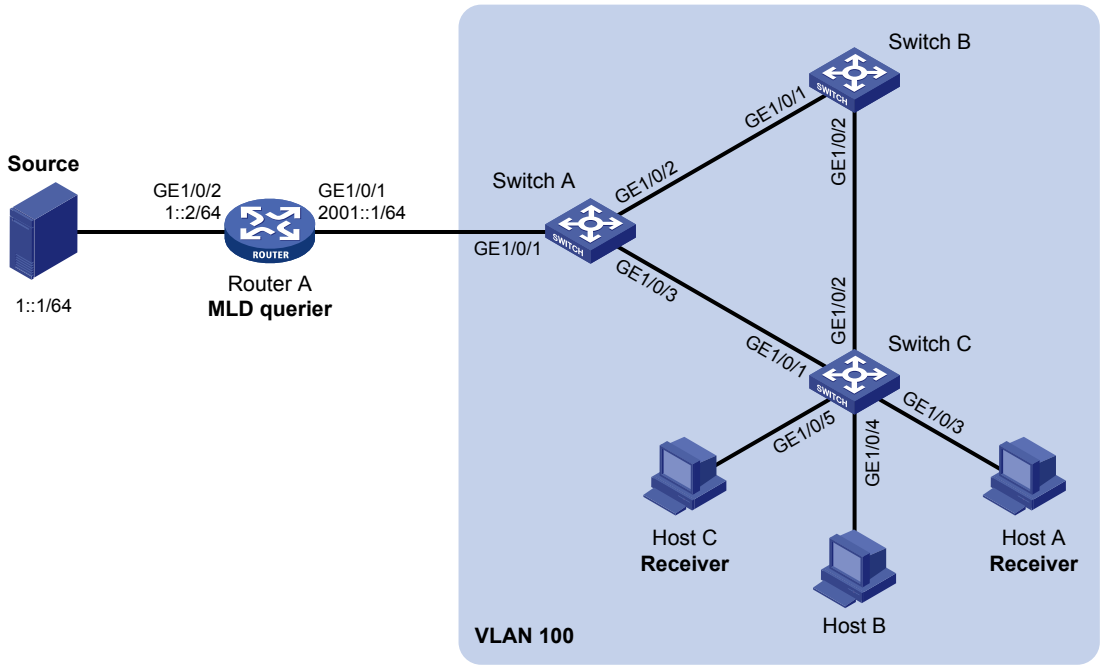
図 4-4 に示すようなネットワークを設定します。

- 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 はマルチキャストグループ FF1E::101 の恒久的なレシーバです。

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。

- 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 IPv6 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 に接続されているレシーバに転送されます。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レシーバ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 の詳細はセクション 3 *アクセス オペレーションマニュアル*の“*STP*”を参照してください。

図 4-4 ネットワーク図



II. 設定手順

1. 図 4-4 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 1/0/3 を割り当てます。

   [SwitchA] vlan 100

   [SwitchA-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/3

   # VLAN100 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。

   # グローバルに 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

VLAN100 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

VLAN100 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 VLAN100 のスタティック MLD snooping グループ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。

4.13.3. VLAN ベース MLD snooping クエリアの設定例

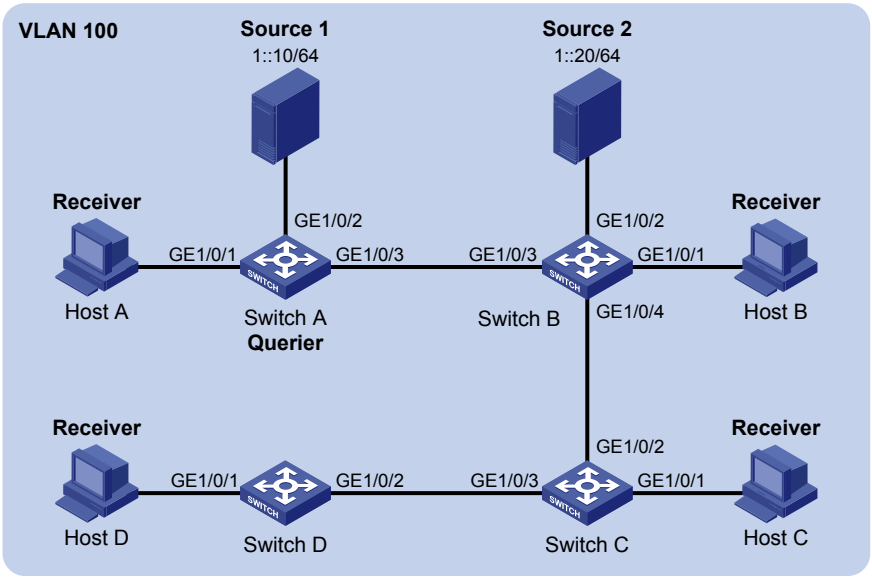
I. ネットワーク要件

図 4-5 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 IPv6 マルチキャストグループ FF1E::101、FF1E::102 に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 のレシーバで、Host B、Host D は IPv6 マルチキャストグループ FF1E::102 のレシーバです。
- すべてのレシーバホストは MLDv1 が動作し、すべての装置は MLDv1 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 MLD snooping クエリアとして動作します。

VLAN で未知の 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 マルチキャストパケットの廃棄機能を有効にします。

図 4-5 ネットワーク図



II. 設定手順

1. Switch A を設定します。

   # グローバルに 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 と未知の 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 クエリア機能を有効にします。

[SwitchA-vlan100] MLD-snooping querier

[SwitchA-vlan100] quit

2. Switch B を設定します。

グローバルに 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

VLAN 100 で MLD Snooping と未知の 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。

グローバルに 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 と未知の 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。

グローバルに 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 と未知の 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 で MLD snooping、IPv6 PIM hello メッセージを通して学習した MLD 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のち、Switch A を除くすべての Switch が MLD general query を受信することができます。

4.14. MLD snoopingのトラブルシューティング

4.14.1. レイヤ 2 マルチキャスト転送ができない

I. 症状

MLD snooping を使用したレイヤ 2 装置でレイヤ 2 マルチキャスト転送ができません。

II. 解決策

1. MLD snooping 情報を表示するため **display mld-snooping** コマンドを使用します。
2. MLD snooping が有効になっていない場合、グローバルで **mld-snooping** コマンドを使用して MLD snooping を有効にし、VLAN 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. グローバルで MLD snooping が有効で、対応する VLAN で MLD snooping が無効になっている場合、対応する VLAN の 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。

4.14.2. 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

IPv6 マルチキャストポリシーによって許可されていない IPv6 マルチキャストグループから、ホストが IPv6 マルチキャストデータを受信できません。

II. 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 または対応するポートの 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** 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。

目次

このセクションのページは **6-x-x** です。

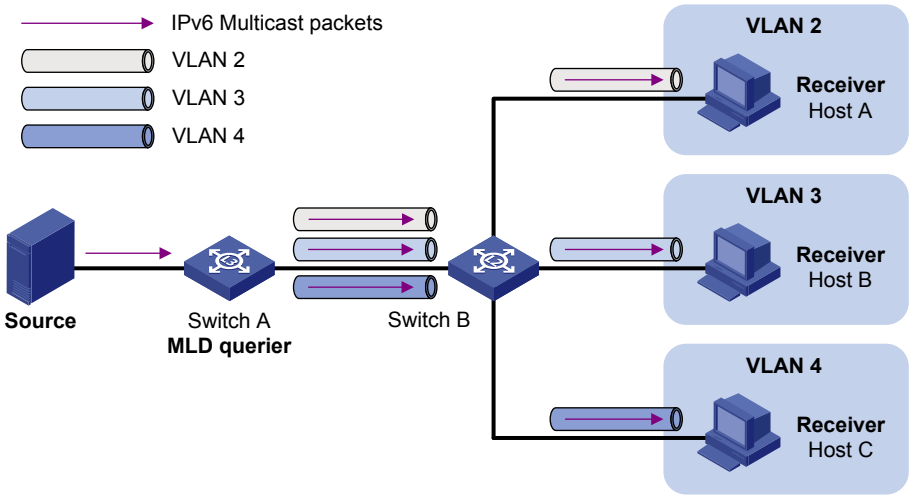
5 章 IPv6 マルチキャスト VLAN 5-1
5.1. 概要 5-1
5.2. IPv6 マルチキャスト VLAN 方法 5-1
5.2.1. サブ VLAN ベース IPv6 マルチキャスト VLAN 5-1
5.2.2. ポートベース IPv6 マルチキャスト VLAN 5-2
5.3. 制限とガイドライン 5-3
5.4. サブ VLAN ベース IPv6 マルチキャスト VLAN 5-3
5.5. ポートベース IPv6 マルチキャスト VLAN の設定 5-4
5.6. IPv6 マルチキャスト VLAN の転送エントリの最大数の設定 5-5
5.7. IPv6 マルチキャスト VLAN の表示と維持 5-5
5.8. IPv6 マルチキャスト VLAN の設定例 5-6
5.8.1. サブ VLAN ベース IPv6 マルチキャスト VLAN の設定例 5-6
5.8.2. ポートベース IPv6 マルチキャスト VLAN の設定例 5-9

5章 IPv6 マルチキャスト VLAN

5.1. 概要

図 5-1 示すとおり、ホスト A、ホスト B、ホスト C は異なる VLAN に属しており、同じ IPv6 マルチキャストグループに所属しています。Switch A（レイヤ 3 装置）がグループの IPv6 マルチキャストデータを受信するとき、Switch B（レイヤ 2 装置）にデータのコピーを 3 回送信します。この結果、ネットワークの帯域を浪費するだけでなく、レイヤ 3 装置にも負荷をかけてしまいます。

図 5-1 IPv6 マルチキャスト VLAN を使用しないマルチキャストの転送



Switch B で IPv6 マルチキャスト VLAN 機能を設定したのち、Switch A は Switch B の IPv6 マルチキャスト VLAN に IPv6 マルチキャストデータを 1 回コピーして送信します。これによりネットワークの帯域を節約し、レイヤ 3 装置の負荷を軽減します。

5.2. IPv6マルチキャストVLAN方法

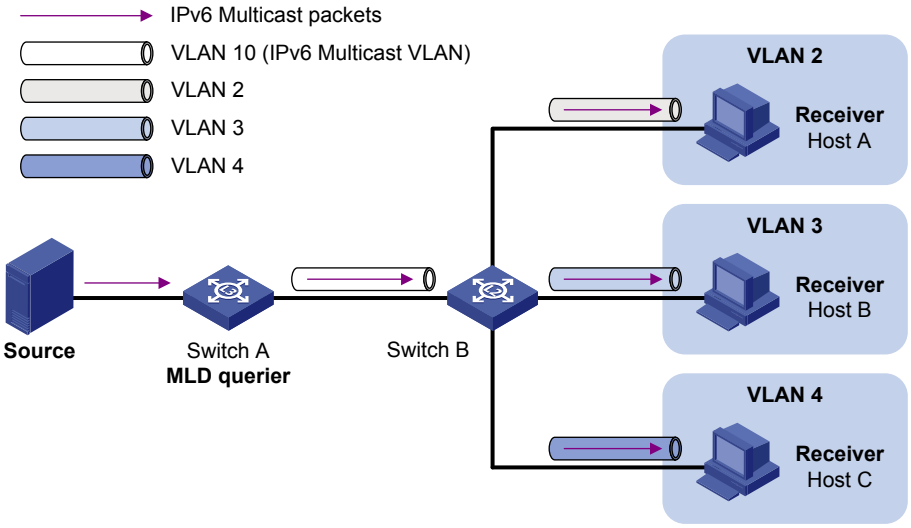
IPv6 マルチキャスト VLAN はサブ VLAN ベース IPv6 マルチキャスト VLAN とポートベース IPv6 マルチキャスト VLAN があります。

5.2.1. サブ VLAN ベース IPv6 マルチキャスト VLAN

図 5-2 にサブ VLAN ベースマルチキャスト VLAN を示します。

- ホスト A、ホスト B、ホスト C はそれぞれ VLAN 2、VLAN 3、VLAN 4 に属します。
- Switch B において、VLAN10 をマルチキャスト VLAN に設定します。VLAN 2、VLAN 3、VLAN 4 は VLAN 10 のサブ VLAN です。
- マルチキャスト VLAN とマルチキャスト VLAN のサブ VLAN 上で MLD Snooping を有効にします。

図 5-2 サブ VLAN ベース IPv6 マルチキャスト VLAN



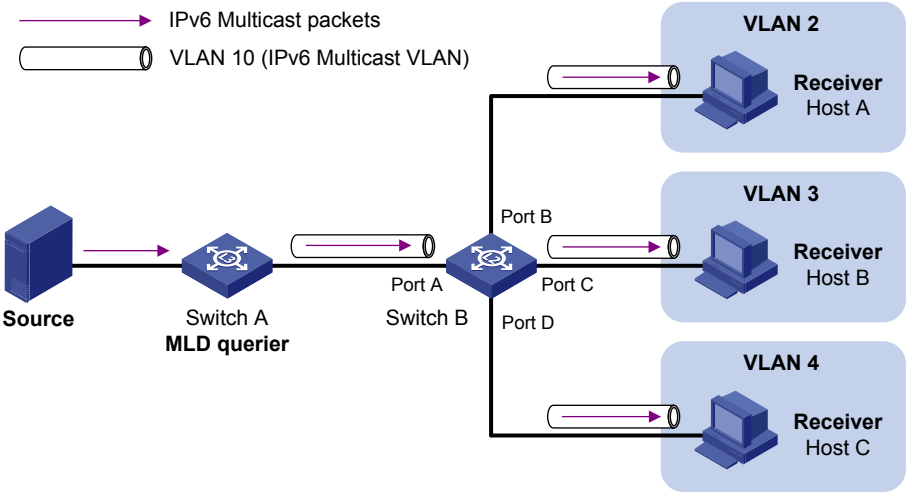
設定後、MLD Snooping は IPv6 マルチキャスト VLAN のルータポートとサブ VLAN のメンバポートを管理します。Switch A が IPv6 マルチキャストソースから IPv6 マルチキャストデータを受信するとき、Switch B の IPv6 マルチキャスト VLAN に 1 つの IPv6 マルチキャストデータのみを送信します。そして、Switch B は IPv6 マルチキャスト VLAN のサブ VLAN へ分けられたコピーを送信します。

5.2.2. ポートベース IPv6 マルチキャスト VLAN

図 5-3 にポートベースベース IPv6 マルチキャスト VLAN を示します。

- ホスト A、ホスト B、ホスト C はそれぞれ VLAN 2、VLAN 3、VLAN 4 に属します。
- Switch B において、VLAN10 は IPv6 マルチキャスト VLAN です。
- ホストが接続されているすべてのユーザポートはハイブリッドポートです。VLAN 10 が割り当てられています。
- マルチキャスト VLAN とすべてのユーザ VLAN 上で MLD Snooping を有効にします。

図 5-3 ポートベース IPv6 マルチキャスト VLAN



MLD Snooping は IPv6 マルチキャスト VLAN のルータポートとメンバポートを管理します。Switch B がユーザポートで MLD メッセージを受信すると、メッセージに IPv6 マルチキャスト VLAN のタグをつけて MLD クエリアへ送信します。Switch B で IPv6 マルチキャストデータの 1 つコピーのみを IPv6 マルチキャスト VLAN に送信します。そして、Switch B は IPv6 マルチキャスト VLAN の各ユーザポートに分けられたコピーを送信します。

5.3. 制限とガイドライン

IPv6 マルチキャスト VLAN に指定される VLAN が事前に作成されている必要があります。

サブ VLAN ベース IPv6 マルチキャスト VLAN とポートベース IPv6 マルチキャスト VLAN の両方を装置に設定する場合、ポートベース IPv6 マルチキャスト VLAN が優先されます。

IPv6 マルチキャストルーティングが有効な装置で IPv6 マルチキャスト VLAN を設定しないでください。設定した場合、エラーメッセージを表示します。また IPv6 マルチキャスト VLAN が設定されている装置で IPv6 マルチキャストルーティングを有効にしないでください。マルチキャストの転送にエラーが発生します。

VLAN インタフェースで IPv6 PIM あるいは MLD が有効の場合、IPv6 マルチキャスト VLAN あるいはマルチキャストサブ VLAN として設定しないでください。設定した場合、エラーメッセージを表示します。また VLAN インタフェースが IPv6 マルチキャスト VLAN あるいはマルチキャストサブ VLAN に属している場合、VLAN インタフェースで IPv6PIM あるいは MLD を有効にしないでください。マルチキャストの転送にエラーが発生します。

IPv6 マルチキャスト VLAN 機能はセカンダリ VLAN で適用されません。セカンダリ VLAN に IPv6 マルチキャスト VLAN の設定を行わないことを推奨します。セカンダリ VLAN の詳細はセクション 3 *アクセス オペレーションマニュアル*の“*VLAN*”を参照してください。

5.4. サブVLANベースIPv6マルチキャストVLAN

I. 制限とガイドライン

IPv6 マルチキャスト VLAN のサブ VLAN として設定されている VLAN は事前に作成されている必要があります。他の IPv6 マルチキャスト VLAN あるいはサブ VLAN であってはいけません。

II. 設定要件

サブ VLAN ベース IPv6 マルチキャスト VLAN を設定する前に、以下の作業を完了させてください。

- 必要な VLAN を作成します。
- IPv6 マルチキャスト VLAN に設定する VLAN とサブ VLAN で MLD Snooping を有効にします。

III. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. VLAN を IPv6 マルチキャスト VLAN に設定し、IPv6 multicast VLAN view へ移行する	**ipv6 multicast-vlan** *vlan-id*	デフォルト：設定なし

操作	コマンド	補足
3. サブ VLAN を IPv6 マルチキャスト VLAN に割り当てる	**subvlan** *vlan-list*	—

5.5. ポートベースIPv6マルチキャストVLANの設定

I. 制限とガイドライン

IPv6 multicast VLAN view あるいは interface view の IPv6 マルチキャスト VLAN にユーザポートを割り当てることができます。設定の優先度は同一です。

ユーザポートは 1 つの IPv6 マルチキャスト VLAN にのみ所属することができます。

II. 設定要件

ポートベース IPv6 マルチキャスト VLAN の設定をする前に、以下の作業を完了させてください。

- 必要な VLAN を作成します。
- IPv6 マルチキャスト VLAN に設定する VLAN で MLD snooping を有効にします。
- 受信ホストを含むすべての VLAN で MLD Snooping を有効にします。
- ユーザのポートの属性を設定してください。転送されたパケットが IPv6 マルチキャスト VLAN として設定された VLAN から転送され、VLAN のタグ付けが行われていることを確認してください。ポートの属性の詳細はセクション 3 *アクセス オペレーションマニュアル*の“*VLAN*”を参照してください。

III. IPv6 multicast VLAN view での IPv6 マルチキャスト VLAN へのポートの割り当て

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. VLAN を IPv6 マルチキャスト VLAN に設定し、IPv6 multicast VLAN view へ移行する	**ipv6 multicast-vlan** *vlan-id*	デフォルト：設定なし
3. ポートを IPv6 マルチキャスト VLAN に割り当てる	**port** *interface-list*	—

IV. interface view での IPv6 マルチキャスト VLAN へのポートの割り当て

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. VLAN を IPv6 マルチキャスト VLAN に設定し、IPv6 multicast VLAN view へ移行する	**ipv6 multicast-vlan** *vlan-id*	デフォルト：設定なし
3. system view に戻る	**quit**	—

操作	コマンド	補足
4. Layer 2 Ethernet interface view あるいは aggregate 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*	—
5. 現在のポートを IPv6 マルチキャスト VLAN ポートに設定する	**ipv6 port multicast-vlan** *vlan-id*	—

5.6. IPv6マルチキャストVLANの転送エントリの最大数の設定

I. IPv6 マルチキャスト VLAN の転送エントリの最大数の設定

装置で IPv6 マルチキャスト VLAN の MLD Snooping 転送テーブルのエントリの最大数を設定できます。IPv6 マルチキャスト VLAN の転送エントリ数が上限に達すると、いくつかのエントリがタイムアウトするか、手動で削除するまで、装置は IPv6 マルチキャスト VLAN の転送エントリを作成しません。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. IPv6 マルチキャスト VLAN の転送エントリの最大数を設定する	**ipv6 multicast-vlan entry-limit** *limit*	デフォルト：4000

5.7. IPv6マルチキャスト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
IPv6 マルチキャストVLANの情報を表示する	**display ipv6 multicast-vlan** [*vlan-id*]
IPv6マルチキャスト転送テーブルの情報を表示する	**display ipv6 multicast-vlan forwarding-table** [*ipv6-source-address* [*prefix-length*] | *ipv6-group-address* [*prefix-length*] | **slot** *slot-number* | **subvlan** *vlan-id* | **vlan** *vlan-id*] *

操作	コマンド
IPv6マルチキャストVLANのIPv6マルチキャストグループの情報を表示する	**display ipv6 multicast-vlan group** [*ipv6-source-address* | *ipv6-group-address* | **slot** *slot-number* | **verbose** | **vlan** *vlan-id*] *
IPv6マルチキャストVLANのIPv6マルチキャストグループを削除する	**reset ipv6 multicast-vlan group** [*ipv6-group-address* [*prefix-length*] | *ipv6-source-address* [*prefix-length*] | **vlan** *vlan-id*] *

5.8. IPv6マルチキャストVLANの設定例

5.8.1. サブ VLAN ベース IPv6 マルチキャスト VLAN の設定例

I. ネットワーク要件

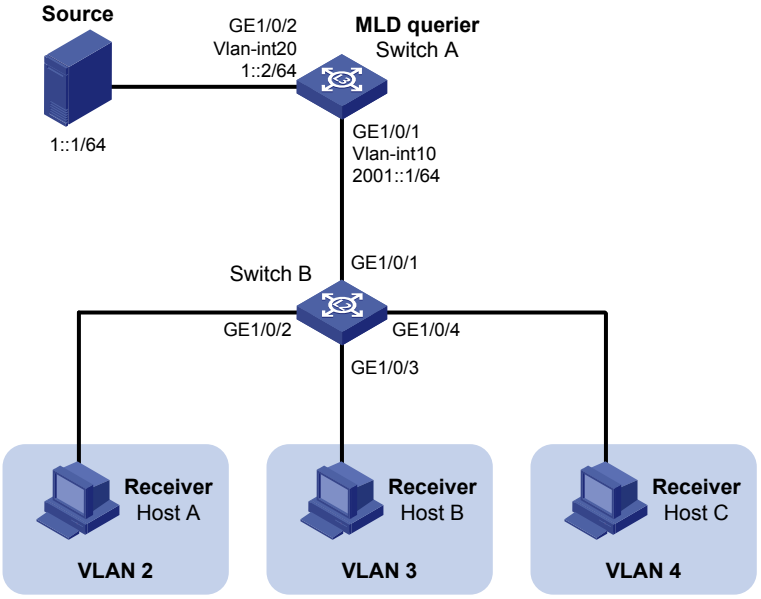
図 5-4 に示すように設定します。

- レイヤ 3 装置の Switch A で MLDv1 が動作します。レイヤ 2 装置の Switch B で MLDv1 Snooping が動作します。Switch A は MLD クエリアです。
- IPv6 マルチキャストソースは IPv6 マルチキャストデータをマルチキャストグループ FF1E::101 へ送信します。Host A、Host B、Host C は IPv6 マルチキャストグループのレシーバです。ホストはそれぞれ VLAN2 から VLAN4 に属しています。

Switch B でサブ VLAN ベース IPv6 マルチキャスト VLAN を以下の要件に適用するように設定します。

- Switch A が IPv6 マルチキャスト VLAN を通じて IPv6 マルチキャストデータを Switch B へ送信します。
- Switch B が異なるユーザ VLAN に属するレシーバへ IPv6 マルチキャストデータを転送します。

図 5-4 ネットワーク図



II. 設定手順

1. Switch A の設定

IPv6 マルチキャストルーティングを有効にします。

<SwitchA> system-view

[SwitchA] ipv6 multicast routing

[SwitchA-mrib6] quit

VLAN20 を作成し、GigabitEthernet 1/0/2 を VLAN に割り当てます。

[SwitchA] vlan 20

[SwitchA-vlan20] port gigabitethernet 1/0/2

[SwitchA-vlan20] quit

VLAN インタフェース 20 に IPv6 アドレスを設定し、IPv6 PIM-SM を有効にします。

[SwitchA] interface vlan-interface 20

[SwitchA-Vlan-interface20] ipv6 address 1::2 64

[SwitchA-Vlan-interface20] ipv6 pim sm

[SwitchA-Vlan-interface20] quit

VLAN10 を作成します。

[SwitchA] vlan 10

[SwitchA-vlan10] quit

ハイブリッドポートとして GigabitEthernet 1/0/1 を設定し、タグ付きメンバとして VLAN 10 からのパケットにタグをつけます。

[SwitchA] interface gigabitethernet 1/0/1

[SwitchA-GigabitEthernet1/0/1] port link-type hybrid

[SwitchA-GigabitEthernet1/0/1] port hybrid vlan 10 tagged

[SwitchA-GigabitEthernet1/0/1] quit

VLAN インタフェース 10 に IPv6 アドレスを設定し、MLD を有効にします。

[SwitchA] interface vlan-interface 10

[SwitchA-Vlan-interface10] ipv6 address 2001::1 64

[SwitchA-Vlan-interface10] mld enable

[SwitchA-Vlan-interface10] quit

2. Switch B の設定

MLD Snooping を有効にします。

<SwitchB> system-view

[SwitchB] mld-snooping

[SwitchB-mld-snooping] quit

VLAN 2 を作成し、GigabitEthernet 1/0/2 を割り当て、VLAN で MLD Snooping を有効にします。

[SwitchB] vlan 2

[SwitchB-vlan2] port gigabitethernet 1/0/2

[SwitchB-vlan2] mld-snooping enable

[SwitchB-vlan2] quit

VLAN 3 を作成し、GigabitEthernet 1/0/3 を割り当て、VLAN で MLD Snooping を有効にします。

[SwitchB] vlan 3

[SwitchB-vlan3] port gigabitethernet 1/0/3

[SwitchB-vlan3] mld-snooping enable

[SwitchB-vlan3] quit

VLAN 4 を作成し、GigabitEthernet 1/0/4 を割り当て、VLAN で MLD Snooping を有効にします。

[SwitchB] vlan 4

[SwitchB-vlan4] port gigabitethernet 1/0/4

[SwitchB-vlan4] mld-snooping enable

[SwitchB-vlan4] quit

VLAN10 を作成し、MLD Snooping を有効にします。

[SwitchB] vlan 10

[SwitchB-vlan10] mld-snooping enable

[SwitchB-vlan10] quit

ハイブリッドポートとして GigabitEthernet 1/0/1 を設定し、タグ付きメンバとして VLAN 10 からのパケットにタグをつけます。

[SwitchB] interface gigabitethernet 1/0/1

[SwitchB-GigabitEthernet1/0/1] port link-type hybrid

[SwitchB-GigabitEthernet1/0/1] port hybrid vlan 10 tagged

[SwitchB-GigabitEthernet1/0/1] quit

IPv6 マルチキャスト VLAN として VLAN 10 を設定し、サブ VLAN として VLAN 2～VLAN 4 を設定します。

[SwitchB] ipv6 multicast-vlan 10

[SwitchB-ipv6-mvlan-10] subvlan 2 to 4

[SwitchB-ipv6-mvlan-10] quit

III. 設定の確認

Switch B ですべての IPv6 マルチキャスト VLAN の情報を表示します。

[SwitchB] display ipv6 multicast-vlan

```
Total 1 IPv6 multicast VLANs.

IPv6 multicast VLAN 10:
  Sub-VLAN list(3 in total):
     2-4
  Port list(0 in total):
```

Switch B で IPv6 マルチキャスト VLAN の転送エントリの情報を表示します。

[SwitchB] display ipv6 multicast-vlan group

```
Total 1 entries.

IPv6 multicast VLAN 10: Total 1 entries.
  (::, FF1E::101)
    Sub-VLANs (3 in total):
      VLAN 2
      VLAN 3
      VLAN 4
```

出力では次のことを示します。IPv6 マルチキャストグループ FF1E::101 は IPv6 マルチキャスト VLAN 10 に所属しています。IPv6 マルチキャスト VLAN（VLAN 10）はサブ VLAN 2～VLAN 4 が含まれます。Switch B は VLAN 10 の IPv6 マルチキャストデータを VLAN 2～VLAN 4 にコピーしています。

5.8.2. ポートベース IPv6 マルチキャスト VLAN の設定例

I. ネットワーク要件

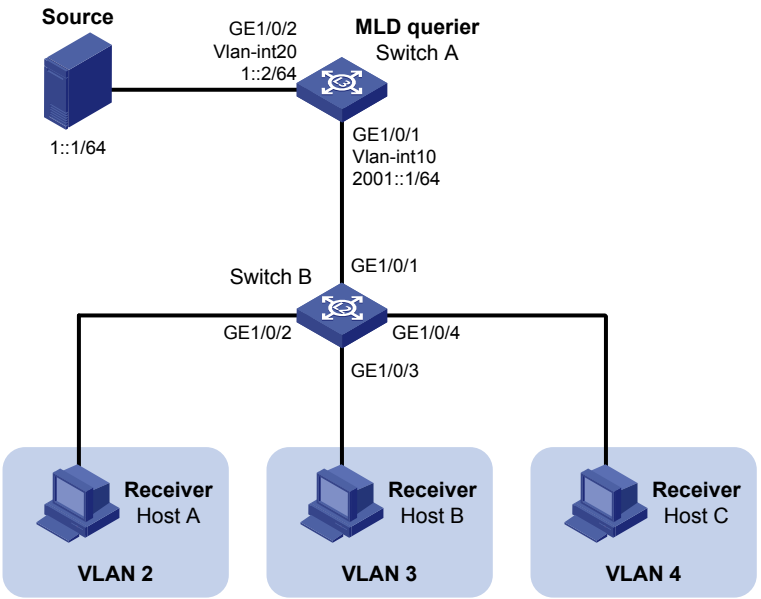
図 5-5 に示すように設定します。

- Switch A で MLDv1 が動作します。Switch B で MLDv1 Snooping が動作します。Switch A は MLD クエリアです。
- IPv6 マルチキャストソースは IPv6 マルチキャストデータを IPv6 マルチキャストグループ FF1E::101 に送信します。Host A、Host B、Host C は IPv6 マルチキャストグループのレシーバです。ホストはそれぞれ VLAN 2～VLAN 4 に属しています。

Switch B でポートベース IPv6 マルチキャスト VLAN を以下の要件に適用するように設定します。

- Switch A は IPv6 マルチキャスト VLAN を通じて IPv6 マルチキャストデータを Switch B へ送信します。
- Switch B が異なるユーザ VLAN に属するレシーバへ IPv6 マルチキャストデータを転送します。

図 5-5 ネットワーク図



II. 設定手順

1. Switch A の設定

IPv6 マルチキャストルーティングを有効にします。

<SwitchA> system-view

[SwitchA] ipv6 multicast routing

[SwitchA-mrib6] quit

VLAN20 を作成し、GigabitEthernet 1/0/2 を VLAN に割り当てます。

[SwitchA] vlan 20

[SwitchA-vlan20] port gigabitethernet 1/0/2

[SwitchA-vlan20] quit

VLAN インタフェース 20 に IPv6 アドレスを設定し、IPv6 PIM-SM を有効にします。

[SwitchA] interface vlan-interface 20

[SwitchA-Vlan-interface20] ipv6 address 1::2 64

[SwitchA-Vlan-interface20] ipv6 pim sm

[SwitchA-Vlan-interface20] quit

VLAN10 を作成し、GigabitEthernet 1/0/1 を VLAN に割り当てます。

[SwitchA] vlan 10

[SwitchA-vlan10] port gigabitethernet 1/0/1

[SwitchA-vlan10] quit

VLAN インタフェース 10 に IPv6 アドレスを設定し、インタフェースで MLD を有効にします。

[SwitchA] interface vlan-interface 10

[SwitchA-Vlan-interface10] ipv6 address 2001::1 64

[SwitchA-Vlan-interface10] mld enable

[SwitchA-Vlan-interface10] quit

2. Switch B の設定

グローバルに MLD Snooping を有効にします。

<SwitchB> system-view

[SwitchB] mld-snooping

[SwitchB-mld-snooping] quit

VLAN10 を作成し、GigabitEthernet 1/0/1 を割り当て、MLD Snooping を有効にします。

[SwitchB] vlan 10

[SwitchB-vlan10] port gigabitethernet 1/0/1

[SwitchB-vlan10] mld-snooping enable

[SwitchB-vlan10] quit

VLAN 2 を作成し、MLD Snooping を有効にします。

[SwitchB] vlan 2

[SwitchB-vlan2] mld-snooping enable

[SwitchB-vlan2] quit

VLAN 3 を作成し、MLD Snooping を有効にします。

[SwitchB] vlan 3

[SwitchB-vlan3] mld-snooping enable

[SwitchB-vlan3] quit

VLAN 4 を作成し、MLD Snooping を有効にします。

[SwitchB] vlan 4

[SwitchB-vlan4] mld-snooping enable

[SwitchB-vlan4] quit

ハイブリッドポートとして GigabitEthernet 1/0/2 を設定し、ハイブリッドポートの PVID を 2 に設定します。

[SwitchB] interface gigabitethernet 1/0/2

[SwitchB-GigabitEthernet1/0/2] port link-type hybrid

[SwitchB-GigabitEthernet1/0/2] port hybrid pvid vlan 2

VLAN2、VLAN10 に GigabitEthernet 1/0/2 を割り当て、タグなしメンバとして VLAN2、VLAN10 からのパケットからタグを外します。

[SwitchB-GigabitEthernet1/0/2] port hybrid vlan 2 untagged

[SwitchB-GigabitEthernet1/0/2] port hybrid vlan 10 untagged

[SwitchB-GigabitEthernet1/0/2] quit

ハイブリッドポートとして GigabitEthernet 1/0/3 を設定し、ハイブリッドポートの PVID を 3 に設定します。

[SwitchB] interface gigabitethernet 1/0/3

[SwitchB-GigabitEthernet1/0/3] port link-type hybrid

[SwitchB-GigabitEthernet1/0/3] port hybrid pvid vlan 3

VLAN 3、VLAN 10 に GigabitEthernet 1/0/3 を割り当て、タグなしメンバとして VLAN 3、VLAN 10 からのパケットからタグを外します。

[SwitchB-GigabitEthernet1/0/3] port hybrid vlan 3 untagged

[SwitchB-GigabitEthernet1/0/3] port hybrid vlan 10 untagged

[SwitchB-GigabitEthernet1/0/3] quit

ハイブリッドポートとして GigabitEthernet 1/0/4 を設定し、ハイブリッドポートの PVID を 4 に設定します。

[SwitchB] interface gigabitethernet 1/0/4

[SwitchB-GigabitEthernet1/0/4] port link-type hybrid

[SwitchB-GigabitEthernet1/0/4] port hybrid pvid vlan 4

VLAN 4、VLAN 10 に GigabitEthernet 1/0/4 を割り当て、タグなしメンバとして VLAN 4、VLAN 10 からのパケットからタグを外します。

[SwitchB-GigabitEthernet1/0/4] port hybrid vlan 4 untagged

[SwitchB-GigabitEthernet1/0/4] port hybrid vlan 10 untagged

[SwitchB-GigabitEthernet1/0/4] quit

IPv6 マルチキャスト VLAN として VLAN10 を設定します。

[SwitchB] ipv6 multicast-vlan 10

GigabitEthernet 1/0/2 と GigabitEthernet 1/0/3 に VLAN10 を割り当てます。

[SwitchB-ipv6-mvlan-10] port gigabitethernet 1/0/2 to gigabitethernet 1/0/3

[SwitchB-ipv6-mvlan-10] quit

GigabitEthernet 1/0/4 に VLAN10 を割り当てます。

[SwitchB] interface gigabitethernet 1/0/4

[SwitchB-GigabitEthernet1/0/4] ipv6 port multicast-vlan 10

[SwitchB-GigabitEthernet1/0/4] quit

III. 設定の確認

Switch B の IPv6 マルチキャスト VLAN の情報を表示します。

[SwitchB] display ipv6 multicast-vlan

```
Total 1 IPv6 multicast VLANs.

IPv6 multicast VLAN 10:
  Sub-VLAN list(0 in total):
  Port list(3 in total):
    GE1/0/2
    GE1/0/3
    GE1/0/4
```

Switch B でダイナミックマルチキャストグループの MLD Snooping 転送エントリを表示します。

[SwitchB] display mld-snooping group

```
Total 1 entries.

VLAN 10: Total 1 entries.
  (::, FF1E::101)
    Host slots (0 in total):
    Host ports (3 in total):
      GE1/0/2          (00:03:23)
      GE1/0/3          (00:04:07)
      GE1/0/4          (00:04:16)
```

出力では、MLD Snooping が VLAN10 のユーザポートを維持していることを示します。Switch B はユーザポートを通して VLAN 10 の IPv6 マルチキャストデータを転送します。

QX-S5300G シリーズ Ethernet スイッチ

オペレーションマニュアル

7.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-トラフィックポリシング、GTS、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-付録
13-データバッファ機能
14-タイムレンジ

目次

このセクションのページは **7-x-x** です。

1 章 ACL 1-1
1.1. 概要 1-1
1.1.1. ACL の番号づけと命名 1-1
1.1.2. ACL タイプ 1-1
1.1.3. Match order 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. 制限とガイドライン：ACL の設定 1-4
1.3. 設定作業リスト 1-5
1.4. 標準 ACL の設定 1-5
1.4.1. 標準 ACL 1-5
1.4.2. 標準 IPv4 ACL の設定 1-5
1.4.3. 標準 IPv6 ACL の設定 1-6
1.5. 拡張 ACL の設定 1-6
1.5.1. 拡張 ACL 1-6
1.5.2. 拡張 IPv4 ACL の設定 1-7
1.5.3. 拡張 IPv6 ACL の設定 1-8
1.6. Layer 2 ACL の設定 1-9
1.7. ACL のコピー 1-10
1.8. ACL へのパケットフィルタの設定 1-11
1.8.1. ACL へのパケットフィルタ 1-11
1.8.2. 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 1-11
1.8.3. パケットフィルタリングのログ作成の設定 1-11
1.8.4. VLAN インタフェースのパケットフィルタリング適用範囲の設定 1-12
1.9. ACL の表示と管理 1-12
1.10. ACL 設定例 1-13
1.10.1. パケットフィルタベースのインタフェースの設定 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。

1.1.1. ACL の番号づけと命名

各 ACL のカテゴリには、ACL 番号の固有な範囲があります。ACL を作成するとき、ACL 番号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。

標準 ACL と拡張 ACL を同一の ACL 番号で使用する場合、**ipv6** パラメータを使用して区別する必要があります。同一名の ACL を使用する場合、**ipv6** パラメータあるいは **mac** パラメータを使用して区別する必要があります。

1.1.2. ACL タイプ

カテゴリ	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

カテゴリ	ACL 番号	IP バージョン	マッチング基準
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

🕮 **メモ:**

ハードウェアベースの ACL(QoS, packet-filter など)は暗黙の permit となり、ソフトウェアベースの ACL(telnet, snmp など)は暗黙の deny になります。

1.1.3. Match order

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. ルールが作成された順
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

ACL 種別	走査順
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。

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。この章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。

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、8 となります。

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（デフォルト）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、20 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。

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. 制限とガイドライン：ACLの設定

- ACL 番号が付いた ACL を作成する場合、以下のコマンドを使用して ACL の view に移行することができます。
  - **acl** [**ipv6**] **number** *acl-number*
  - **acl** { [**ipv6**] { **advanced** | **basic** } | **mac** } *acl-number*
- **acl** [**ipv6**] **number** *acl-number* **name** *acl-name* コマンドを使用して ACL 番号が付いた ACL を作成する場合、以下のコマンドを使用して ACL の view に移行することができます。
  - **acl** [**ipv6**] **name** *acl-name* （標準 ACL、拡張 ACL のみ）
  - **acl** [**ipv6**] **number** *acl-number* [**name** *acl-name*]
  - **acl** { [**ipv6**] { **advanced** | **basic** } | **mac** } **name** *acl-name*
- **acl** { [**ipv6**] { **advanced** | **basic** } | **mac** } **name** *acl-name* コマンドを使用して ACL 名が付いた ACL を作成する場合、以下のコマンドを使用して ACL の view に移行することができます。
  - **acl** [**ipv6**] **name** *acl-name* （標準 ACL、拡張 ACL のみ）
  - **acl** { [**ipv6**] { **advanced** | **basic** } | **mac** } **name** *acl-name*
- ACL が ACL ルールの順番を含んでいる場合、あるいは以下の一致条件と機能に加えて有効な機能がある場合、一致するパケットはソフトウェアベースによるスロー転送が行われます。
  - 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
  - Transport レイヤプロトコル
  - ICMP/ICMPv6 メッセージタイプ、ICMP/ICMPv6 メッセージコード、ICMP/ICMPv6 メッセージ名
  - ロギング
  - タイムレンジ

スロー転送は、スロー転送エントリの計算を行うため、コントロールプレーンにパケットを送信する必要があります。この処理は装置の転送性能に影響を与えます。

1.3. 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 • 拡張 ACL の設定 • Layer2 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

1.4. 標準ACLの設定

1.4.1. 標準 ACL

標準 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。

1.4.2. 標準 IPv4 ACL の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
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** }] • **acl number** *acl-number* [**match-order** { **auto** | **config** }]	—
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. ルールの作成、または修正をする	**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

1.4.3. 標準 IPv6 ACL の設定

I. 制限とガイドライン

QoS の traffic classification あるいはパケットフィルタリングを使用する場合、**fragment** キーワードを指定しないでください。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
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** }] • **acl ipv6 number** *acl-number* [**match-order** { **auto** | **config** }]	—
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

1.5. 拡張ACLの設定

1.5.1. 拡張 ACL

拡張 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 ACL と比較すると、拡張 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。

1.5.2. 拡張 IPv4 ACL の設定

I. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
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** }] • **acl number** *acl-number* [**match-order** { **auto** | **config** }]	—
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

1.5.3. 拡張 IPv6 ACL の設定

I. 制限とガイドライン

QoS の traffic classification あるいは QoS のパケットフィルタリングを使用する場合：

- **fragment** キーワードを使用しないでください。
- 出力アプリケーションを使用する場合、**routing** キーワード、**flow-label** キーワードを使用しないでください。
- 出力アプリケーションを使用する場合、*protocol* キーワードで **ipv6-ah**、あるいは 0、43、44、51、60 を指定しないでください。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
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** }] • **acl ipv6 number** *acl-number* [**match-order** { **auto** | **config** }]	—
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

操作	コマンド	補足
5. ルールの作成、または修正する	**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

1.6. Layer 2 ACLの設定

I. Layer 2 ACL

Layer 2 は“Ethernet フレームヘッダ“と呼ばれます。Layer2 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

II. 設定手順

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. 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** }] • **acl number** *acl-number* [**match-order** { **auto** | **config** }]	—
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

1.7. ACLのコピー

I. 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。

II. 制限とガイドライン

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。

III. 設定手順

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

操作	コマンド
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* }

1.8. ACLへのパケットフィルタの設定

1.8.1. ACL へのパケットフィルタ

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。

1.8.2. 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

I. 制限とガイドライン

同一方向のインタフェースに ACL を設定する場合、最大で 3 つ（1 つの IPv4 ACL、1 つの IPv6 ACL、1 つの Layer 2 ACL）を適用することができます。

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。

この章のインタフェースはレイヤ 2 Ethernet インタフェース、レイヤ 3 Ethernet インタフェース、VLAN インタフェースを含むインタフェースを示します。レイヤ 2 インタフェースを指定する場合、**port link-mode** コマンドを使用することができます。詳細はセクション 3 *アクセス オペレーションマニュアル*を参照してください。

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. 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

1.8.3. パケットフィルタリングのログ作成の設定

I. パケット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 の詳細はセクション 10 *システム管理 オペレーションマニュアルの"Information Center"* を参照してください。

II. 設定手順

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

1.8.4. VLAN インタフェースのパケットフィルタリング適用範囲の設定

🕮 **メモ:**

packet-filter filter コマンドは、Ver7.2.17 以降でサポートしています。

I. VLAN インタフェースのパケットフィルタリング適用範囲の設定

VLAN インタフェースのパケットフィルタリングの適用範囲を設定できます。

- **route** : VLAN インタフェースを跨いで転送されるパケット
- **all** ：すべてのパケット

II. 設定手順

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. VLAN インタフェースのパケットフィルタリング適用範囲を設定する	**packet-filter filter** [**route** | **all**]	デフォルト：route

1.9. ACLの表示と管理

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
1つまたはすべてのACLの情報を表示する	**display acl** [**ipv6** | **mac**] { *acl-number* | **all** | **name** *acl-name* }

操作	コマンド
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**] [**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* }]

1.10. ACL設定例

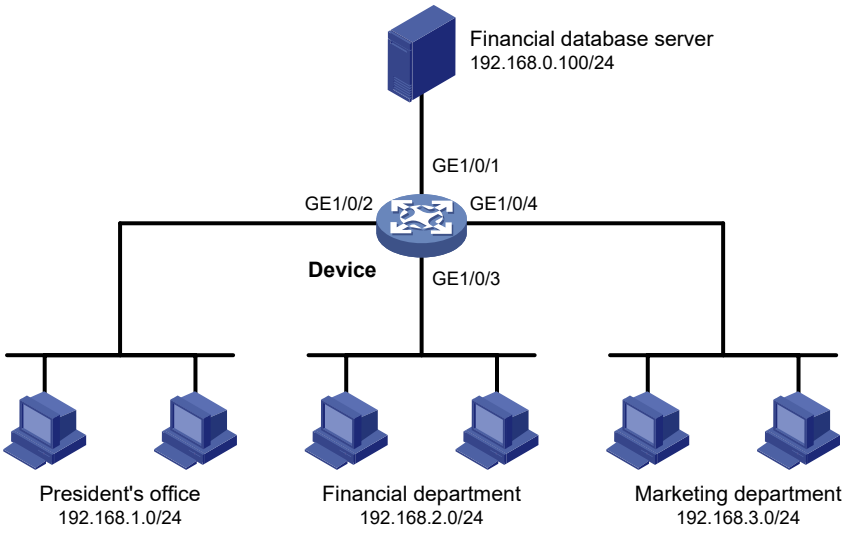
1.10.1. パケットフィルタベースのインタフェースの設定

I. ネットワーク要件

会社は Device A 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



II. 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 インタフェース上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

III. 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 XP 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
```

出力は、経理データベースサーバへ ping が通ることを示します。

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),
```

出力は、経理データベースサーバへの ping は通らないことを示します。

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 **7-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. ネットワークの QoS 技術 2-2
2.3. 装置における QoS プロセスフロー 2-3
2.4. QoS 設定アプローチ 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。

ネットワークのリソースは限られています。QoS を設定するとき、異なるアプリケーションの特性を考慮する必要があります。たとえば、あるトラフィックフローの帯域幅を固定にした場合、他のトラフィックの帯域幅が影響を受ける可能性があります。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あり、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レイヤの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. ネットワークのQoS技術

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

簡単に上記の QoS 技術を説明します。

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。

図 2-1 ネットワークの QoS 技術の位置

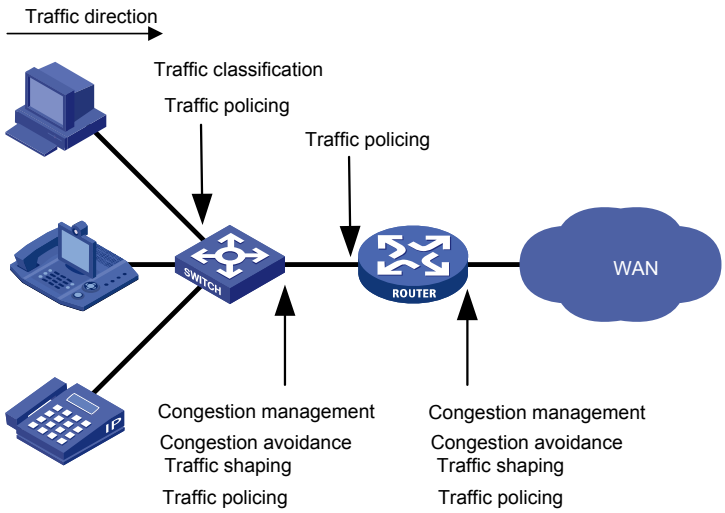


図 2-1 に示すように、以下にトラフィックの分類、トラフィックシェーピング、トラフィックポリシー、輻輳管理、輻輳回避の主要な機能を実装します。

- **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**ー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。

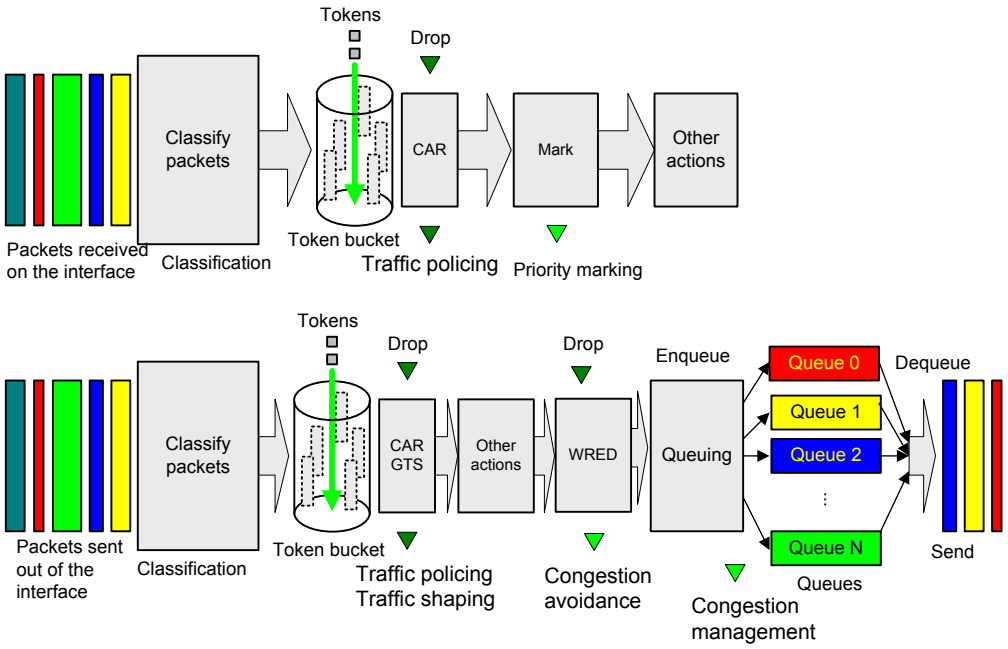
2.3. 装置におけるQoSプロセスフロー

図 2-2 に QoS モジュールのプロセストラフィックの動作についての概要を示します。

1. トラフィック分類を識別し、後続の QoS アクションを行うため、トラフィックのクラス分けを行います。
2. QoS モジュールは、設定されたクラスのトラフィックにおいて、トラフィックプロセスフェーズとネットワークの状態に依存してさまざまな QoS アクションを行います。たとえば、以下の処理を行うため、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
- 輻輳が発生した際の輻輳制御

図 2-2 QoS プロセスフロー



2.4. QoS設定アプローチ

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。

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、トラフィックシェーピングやトラフィックポリシーなどの目的で、クラスとトラフィックを使用して QoS のアクションを定義します。トラフィックを制御するため、インタフェースのようなオブジェクトに適用することができます。

非ポリシーベースでは QoS ポリシーを使用しないで QoS サービスパラメータを設定します。たとえば、QoS ポリシーを使用しないでインタフェースにレートリミット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 **7-x-x** です。

3 章 QoS ポリシー 3-1
3.1. 概要 3-1
3.2. QoS ポリシーの設定作業リスト 3-1
3.3. トラフィッククラスの定義 3-1
3.4. トラフィック動作の定義 3-2
3.5. QoS ポリシーの定義 3-2
3.6. QoS ポリシーの適用 3-2
3.6.1. アプリケーションの適用 3-2
3.6.2. QoS ポリシーの制限とガイドライン 3-3
3.6.3. インタフェースへの QoS ポリシーの適用 3-3
3.6.4. VLAN への QoS ポリシーの適用 3-3
3.6.5. グローバル QoS ポリシーの適用 3-4
3.7. QoS ポリシーの表示と管理 3-4

3章 QoS ポリシー

3.1. 概要

QoS ポリシーには以下があります。

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、AND または OR の演算子（オペレータ）を使用します。

- トラフィッククラスーラフィックを特定するための条件を定義します。
- トラフィック動作ーー致するパケットに行う 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ることで、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。

3.2. QoSポリシーの設定作業リスト

作業リスト
(必須設定項目) 少なくとも1つの作業を行ってください。 1. トラフィッククラスの定義 2. トラフィック動作の定義 3. QoS ポリシーの定義 4. 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 QoS ポリシーの適用

3.3. 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

操作	コマンド	補足
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 Chapter 7 *ACL and QoS Command Reference*の”*QoS policy commands*”を参照してください。

3.4. トラフィック動作の定義

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. トラフィック動作を作成し traffic behavior view に移行する	**traffic behavior** *behavior-name*	―
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、トラフィック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、セクション 7 *ACL and QoS オペレーションマニュアル*を参照してください。	デフォルト：設定なし

3.5. QoSポリシーの定義

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*	―
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。

3.6. QoSポリシーの適用

3.6.1. アプリケーションの適用

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。

3.6.2. QoS ポリシーの制限とガイドライン

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)

3.6.3. インタフェースへの QoS ポリシーの適用

I. 制限とガイドライン

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、RIP パケット、LDP パケット、SSH パケットがあります。

QoS ポリシーはレイヤ 2 Ethernet インタフェース、レイヤ 3 Ethernet インタフェースの両方に適用することができます。この章のインタフェースはレイヤ 2 Ethernet インタフェース、レイヤ 3 Ethernet インタフェースを含むインタフェースを示します。**port link-mode** コマンドを使用して Ethernet ポートをレイヤ 2 あるいはレイヤ 3 に設定することができます。(詳細はセクション 3 *アクセスオペレーションマニュアルの”Ethernet インタフェース*"を参照してください。)

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. 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

3.6.4. VLAN への QoS ポリシーの適用

I. VLAN への QoS ポリシーの適用

VLAN のすべてのポートのトラフィックに QoS ポリシーを適用することができます。

II. 制限とガイドライン

QoS ポリシーはダイナミック VLAN には適用できません。

VLAN に QoS ポリシーを適用する場合、すべての IRF スタックメンバ装置の VLAN に適用されます。

IRF スタックメンバ装置のハードウェアリソースが不足している場合、IRF スタックメンバ装置での VLAN への QoS ポリシーの適用に失敗する可能性があります。ほかの IRF スタックメンバ装置に適用された QoS ポリシーの設定は自動で戻りません。正確に行うため、QoS ポリシーの設定を削除する場合、**undo qos vlan-policy vlan** コマンドを使用してください。

III. 設定手順

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

3.6.5. グローバル QoS ポリシーの適用

I. グローバルでの 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。

II. 制限とガイドライン

VLAN に QoS ポリシーを適用する場合、すべての IRF スタックメンバ装置の VLAN に適用されます。

IRF スタックメンバ装置のハードウェアリソースが不足している場合、IRF スタックメンバ装置での VLAN への QoS ポリシーの適用に失敗する可能性があります。ほかの IRF スタックメンバ装置に適用された QoS ポリシーの設定は自動で戻りません。正確に行うため、QoS ポリシーの設定を削除する場合、**undo qos vlan-policy vlan** コマンドを使用してください。

III. 設定手順

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

3.7. QoSポリシーの表示と管理

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**]

操作	コマンド
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**]
QoSとACLのリソース使用状況を表示する	**display qos-acl resource** [**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*]
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*]
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*]
グローバルに適用されたQoSポリシーの統計情報を削除する	**reset qos policy global** [**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**]

目次

このセクションのページは **7-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 4-1
4.1.2. プライオリティマップ 4-2
4.1.3. プライオリティマッピングの設定方法 4-2
4.1.4. プライオリティのマッピング手順 4-2
4.2. プライオリティマッピングの設定作業リスト 4-3
4.3. プライオリティマッピングの設定 4-4
4.4. プライオリティトラステッドモードの設定 4-4
4.5. インタフェースのポートプライオリティの変更 4-5
4.6. プライオリティマッピングの表示と維持 4-5
4.7. プライオリティマッピングの設定例 4-6
4.7.1. トラステッドモードの設定例 4-6
4.7.2. プライオリティマッピングとプライオリティマーキングの設定例 4-7

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、装置は以下のいずれかの方法で 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

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 7 *ACL and QoS "付録"* を参照してください。

- **ユーザプライオリティー**装置が自動で転送するパスに従いパケットのプライオリティフィールドから優先度を決定します。パケットのスケジューリングプライオリティと転送プライオリティを決定します。ユーザプライオリティは以下のアイテムを示します。
  - レイヤ 2 パケットの 802.1p プライオリティ
  - レイヤ 3 パケットの IP プレシーデンス、DSCP

ローカルに割り当てられたプライオリティは装置内でのみ使用されます。プライオリティはローカルプレシーデンス、ドロッププライオリティがあります。

- **ローカルプレシーデンス**－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プ

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。

（セクション 7 *ACL and QoS オペレーションマニュアル*の”*付録*”のデフォルトプライオリティのマップに示すように）デフォルトのプライオリティマップ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。

4.1.3. プライオリティマッピングの設定方法

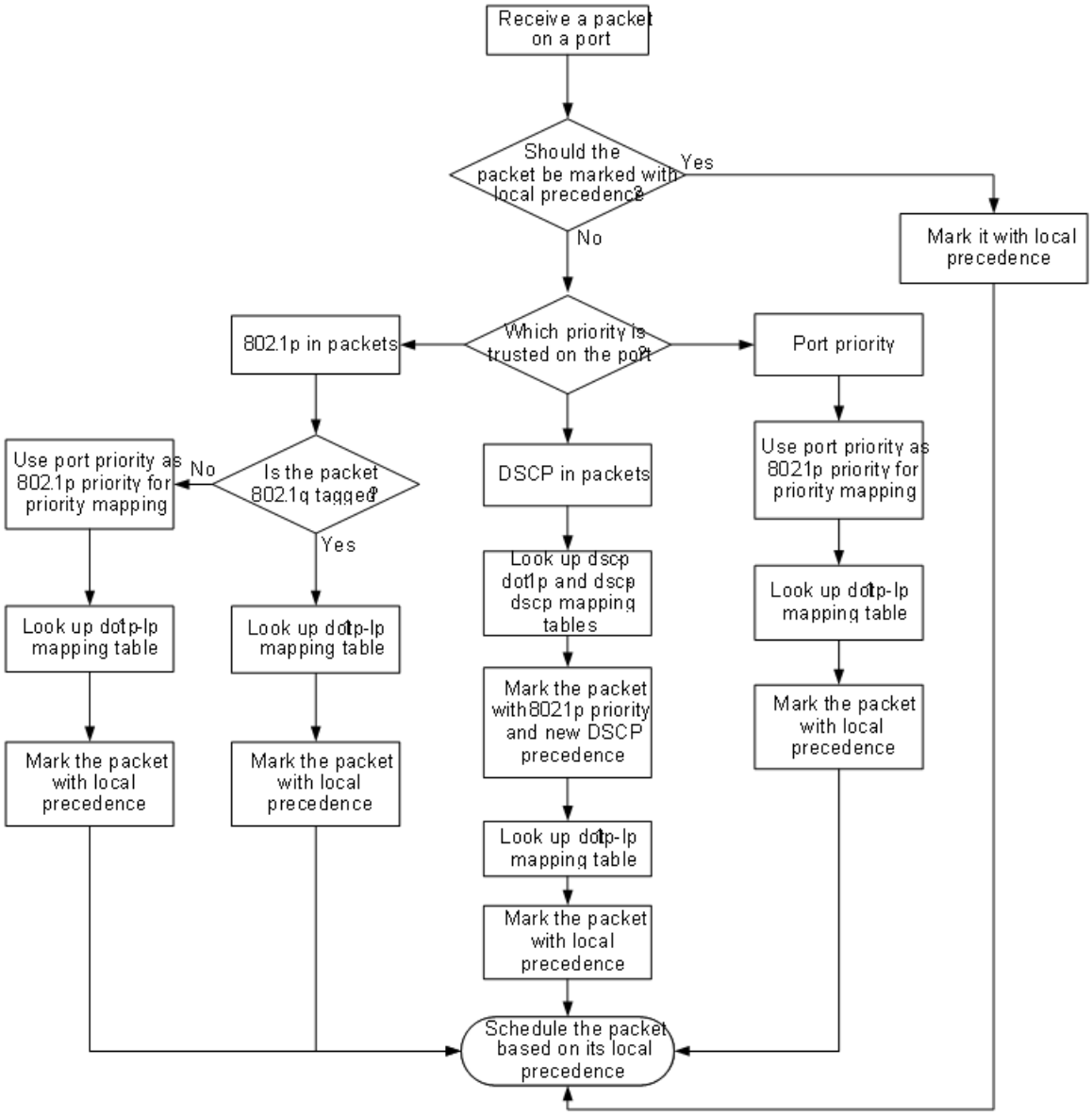
以下のいずれかの方法を使用してプライオリティマッピングを設定することができます。

- **プライオリティトラステッドモード**－この方法では、プライオリティマップの入力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）を検索するためにポートを設定します。そしてシステムはターゲットのプライオリティタイプと値としてトラステッドプライオリティ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が信用できない場合、入力ポートのポートプライオリティを使用します。ポートのポートプライオリティを変更することでポートの入力パケットのプライオリティを変更します。

4.1.4. プライオリティのマッピング手順

ポートでイーサネットパケットを受信した際、スイッチはパケットのプライオリティのスケジューリング(ローカルプレシーデンス)をマーキングします。プレシーデンスは、図 4-1 のように受信したポートのプライオリティトラステッドモードとパケットの 802.1Q タギング状態に従って行われます。

図 4-1 イーサネットパケットのプライオリティマッピング手順



詳細は、オペレーションマニュアルのセクション 7 *ACL and QoS "プライオリティマーキング"* を参照してください。

4.2. プライオリティマッピングの設定作業リスト

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

作業リスト
(必須設定項目)いずれか1つを設定してください。 1. プライオリティトラステッドモードの設定 2. 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

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 }	—
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 *7 ACL and QoS "付録"*を参照して ください。 新規に設定した値は、既存の設定に上書きします。

4.4. プライオリティトラステッドモードの設定

I. パケットプライオリティを信用するトラステッドモードの設定

ポートまたはグローバルに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スイッチを設定できます。

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、以下の内で有効なキーワードを使用します。

- **dot1p** : パケット受信に 802.1p プライオリティを使用します。
- **dscp** : パケット受信に DSCP プレシーデンスを使用します。

II. 制限とガイドライン

この章のインタフェースはレイヤ 2 Ethernet インタフェース、レイヤ 3 Ethernet インタフェースを含むインタフェースを示します。**port link-mode** コマンドを使用して Ethernet ポートをレイヤ 2 あるいはレイヤ 3 に設定することができます。(詳細はセクション 3 *アクセスオペレーションマニュアルの"Ethernet インタフェース"*を参照してください。)

III. 設定手順

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

操作	コマンド	補足
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

I. ポートプライオリティ

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、スイッチ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。

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. 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です。DSCPの値は変更されません。

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

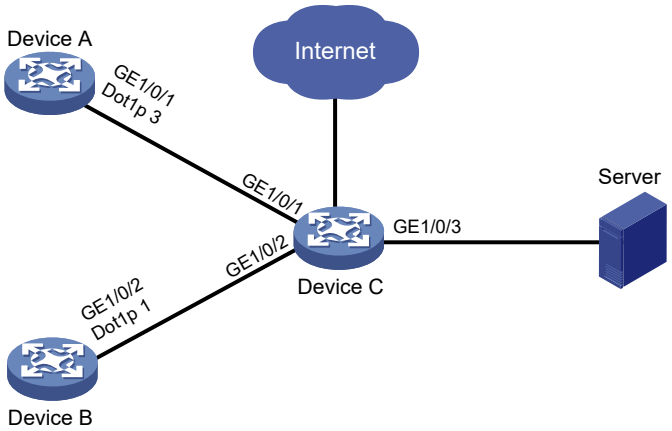
I. ネットワーク要件

図 4-2 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 802.1p プライオリティは 3 です。
- Device B から Device C へのトラフィックの 802.1p プライオリティは 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 Server 宛のパケットを優先します。

図 4-2 ネットワーク図



II. 設定手順

(方法 1) パケットプライオリティを信用し、Device C を設定します。

GigabitEthernet 1/0/1、GigabitEthernet 1/0/2 にプライオリティマッピングの 802.1p プライオリティを割り当てます。

<DeviceC> system-view

[DeviceC] interface gigabitethernet 1/0/1

[DeviceC-GigabitEthernet1/0/1] qos trust dot1p

[DeviceC-GigabitEthernet1/0/1] quit

[DeviceC] interface gigabitethernet 1/0/2

[DeviceC-GigabitEthernet1/0/2] qos trust dot1p

[DeviceC-GigabitEthernet1/0/2] quit

(方法 2) ポートプライオリティを信用し、Device C を設定します。

GigabitEthernet 1/0/1、GigabitEthernet 1/0/2 にポートプライオリティを割り当てます。GigabitEthernet 1/0/1 は GigabitEthernet 1/0/2 よりも高いプライオリティを設定し、

GigabitEthernet 1/0/1 あるいは GigabitEthernet 1/0/2 で設定されたプライオリティのタイプが信用されていな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 4-3 に示すように、プライオリティマッピングとプライオリティマーキングを設定します。

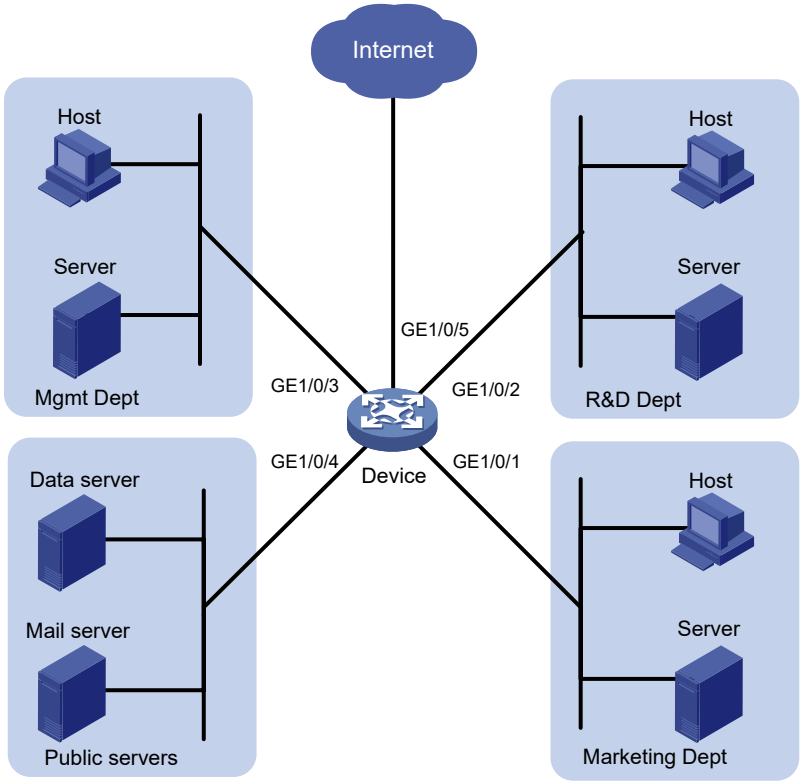
- 営業部は、Device の GigabitEthernet1/0/1 に接続します。営業部からのトラフィックの 802.1p プライオリティを 3 に設定します。
- 研究開発部は GigabitEthernet1/0/2 に接続します。研究開発部からのトラフィック 802.1p プライオリティを 4 に設定します。
- 管理部門は GigabitEthernet1/0/3 に接続します。管理部門からのトラフィック 802.1p プライオリティを 5 に設定します。

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、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

トラフィックの宛先	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>管理部門>営業部	研究開発部	6	High
		管理部門	4	Medium
		営業部	2	Low
Internet	管理部門>営業部>研究開発部	研究開発部	2	Low
		管理部門	6	High
		営業部	4	Medium

図 4-3 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. 802.1p-ローカルプライオリティのマッピングテーブルに 802.1p プライオリティ 3、4、5 をそれぞれローカルプライオリティ 2、6、4 にマッピングします。研究開発部、管理部門、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。

管理部門、営業部、研究開発部門の HTTP トラフィックの 802.1p プライオリティをそれぞれ 802.1p プライオリティ 4、5、3 にマッピングします。設定したプライオリティマッピングテーブルを使用することで、管理部門、営業部、研究開発部門のローカルプライオリティをそれぞれ 6、4、2 にマップして処理します。

HTTP トラフィックをマッチさせるために ACL 3000 を作成します。

[Device] acl advanced 3000

[Device-acl-adv-3000] rule permit tcp destination-port eq 80

[Device-acl-adv-3000] quit

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、管理部門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、QoS ポリシー**admin** のトラフィッククラス **http** とトラフィック動作 **admin** を関連付けます。

[Device] qos policy admin

[Device-qospolicy-admin] classifier http behavior admin

[Device-qospolicy-admin] quit

QoS ポリシー**admin** を GigabitEthernet 1/0/1 の入力トラフィックに適用します。

[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、QoS ポリシー**admin** のトラフィッククラス **http** とトラフィック動作 **market** を関連付けます。

[Device] qos policy market

[Device-qospolicy-market] classifier http behavior market

[Device-qospolicy-market] quit

QoS ポリシー**market** を GigabitEthernet 1/0/1 の入力トラフィックに適用します。

[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、研究開発部門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、QoS ポリシー**rd** のトラフィッククラス **http** とトラフィック動作 **rd** を関連付けます。

[Device] qos policy rd

[Device-qospolicy-rd] classifier http behavior rd

[Device-qospolicy-rd] quit

QoS ポリシー**rd** を GigabitEthernet 1/0/2 の入力トラフィックに適用します。

[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 **7-x-x** です。

5 章 トラフィックポリシング、GTS、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. トラフィックポリシング……5-3
5.1.3. GTS……5-3
5.1.4. ラインレート……5-4
5.2. 設定の制限とガイドライン……5-5
5.3. トラフィックポリシングの設定……5-5
5.4. GTS の設定……5-7
5.5. ラインレートの設定……5-7
5.6. トラフィックポリシング、GTS、ラインレートの表示と維持……5-8
5.7. トラフィックポリシング、GTS、ラインレートの設定例……5-8
5.7.1. トラフィックポリシング、GTS の設定例……5-8

5章 トラフィックポリシング、GTS、ラインレート

5.1. 概要

トラフィックポリシングは帯域幅を含むネットワークリソースの割り当て、およびネットワーク性能の向上を手助けします。たとえば、ある時間範囲内で設定したリソースのみを使用するようにフローを設定することができます。これにより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。

トラフィックポリシングと GTS(generic traffic shaping)やラインレート（レートリミット）は、特定のトラフィックが割り当てた帯域幅を上回る場合、リソースの使用量を制限します。トラフィックレートを検証するには、トークンバケットを使用します。

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。バケットに対して、バケット内のトークンの数に余裕がある場合、以下のイベントが起こります。

- トラフィックは仕様を満足します。このトラフィックは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。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。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度に検証されます。

III. 複雑な検証

より柔軟にトラフィックレートの検証をするために、それぞれ、バケット C、バケット E と呼ばれる 2 つのトークンバケットを設定できます

トークンバケットには、以下の設定可能なパラメータがあります。

より複雑な環境でトラフィックを評価し、より多くのポリシーの柔軟性を行うように 2 つのトークンバケット（バケット C、バケット E）を設定することができます。

- **1 レート 2 色**—1 つのトークンバケットと以下のパラメータを使用します。
  - **CIR**(Committed Information Rate)：バケット C に入るトークンのレートです。バケット C によって許可された平均転送レートを設定します。
  - **CBS**(Committed Burst Size)：バケット C のサイズです。バケット C が転送できるトラフィックの転送バーストを設定します。

  パケットが到達するとき、以下のルールに従います。
  - バケット C にパケットを転送するために十分なトークンがある場合、パケットは green に色分けされます。
  - そうでない場合、パケットは red に色分けされます。
- **1 レート 3 色**—2 つのトークンバケットと以下のパラメータを使用します。
  - **CIR**(Committed Information Rate)：バケット C に入るトークンのレートです。バケット C によって許可された平均転送レートを設定します。
  - **CBS**(Committed Burst Size)：バケット C のサイズです。バケット C が転送できるトラフィックの転送バーストを設定します。
  - **EBS**(Excess burst size)：バケット E のサイズからバケット C のサイズを引いたサイズです。バケット E が転送できるトラフィックの転送バーストを設定します。EBS は 0 にできません。バケット E のサイズは CBS と EBS の合計です。

  パケットが到達するとき、以下のルールに従います。
  - バケット C にパケットを転送するために十分なトークンがある場合、パケットは green に色分けされます。
  - バケット C にパケットを転送するために十分なトークンがないが、バケット E にパケットを転送するために十分なトークンがある場合、パケットは yellow に色分けされます。
  - バケット C、バケット E にパケットを転送するために十分なトークンがない場合、パケットは red に色分けされます。
- **2 レート 3 色**—2 つのトークンバケットと以下のパラメータを使用します。
  - **CIR**(Committed Information Rate)：バケット C に入るトークンのレートです。バケット C によって許可された平均転送レートを設定します。
  - **CBS**(Committed Burst Size)：バケット C のサイズです。バケット C が転送できるトラフィックの転送バーストを設定します。
  - **PIR**(Peak information rate)：バケット E に入るトークンのレートです。バケット E によって許可された平均転送レートを設定します。
  - **EBS**(Excess burst size)：バケット E のサイズです。バケット E が転送できるトラフィックの転送バーストを設定します。

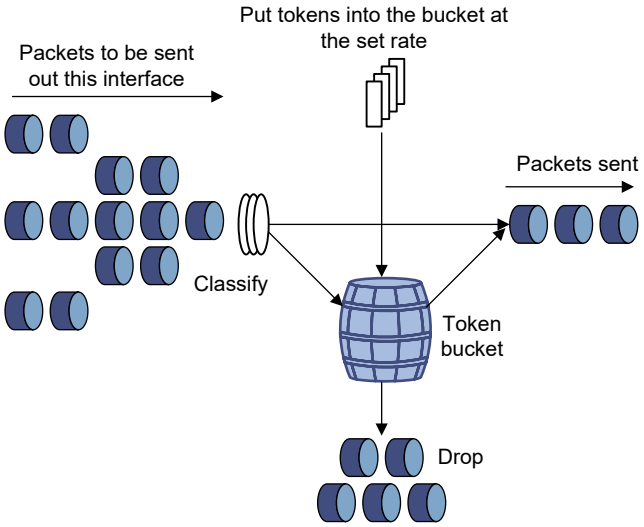
  パケットが到達するとき、以下のルールに従います。
  - バケット C にパケットを転送するために十分なトークンがある場合、パケットは green に色分けされます。
  - バケット C にパケットを転送するために十分なトークンがないが、バケット E にパケットを転送するために十分なトークンがある場合、パケットは yellow に色分けされます。
  - バケット C、バケット E にパケットを転送するために十分なトークンがない場合、パケットは red に色分けされます。

5.1.2. トラフィックポリシング

トラフィックポリシングは、入出力トラフィックのポリシーをサポートします。

一般的なトラフィックポリシングのアプリケーションは、ネットワークの特定のトラフィックを監視し、トラフィックを妥当な範囲内で制限します。別のアプリケーションは、ネットワークリソースが積極的に使用しないようにするため、余剰トラフィックの調整を行います。たとえば、HTTP パケットの帯域幅を全体の 50%未満に制限することができます。セッションのトラフィックが制限を超過すると、トラフィックポリシングはパケットの廃棄やパケットの IP プレシーデンスをリセットすることができます。図 5-1 にインタフェースの出力トラフィックのポリシングの例を示します。

図 5-1 トラフィックポリシング



トラフィックポリシングは、ISP(Internet Service Provider)のネットワークのトラフィックの制限などに広く使用されます。トラフィックポリシングはトラフィックを分類し、検証結果にもとづいて、トラフィックを事前に定義されたトラフィック動作で処理します。トラフィック動作には以下があります。

- 検証結果が適合した場合、トラフィックを転送します。
- 検証結果が余剰した場合、トラフィックを破棄します。
- 検証結果が適合である場合、リマークしたプレシーデンスに従ってパケットを転送します。リマークされた優先順位は、802.1p プライオリティ、DSCP プライオリティ、ローカルプレシーデンスが含まれます。

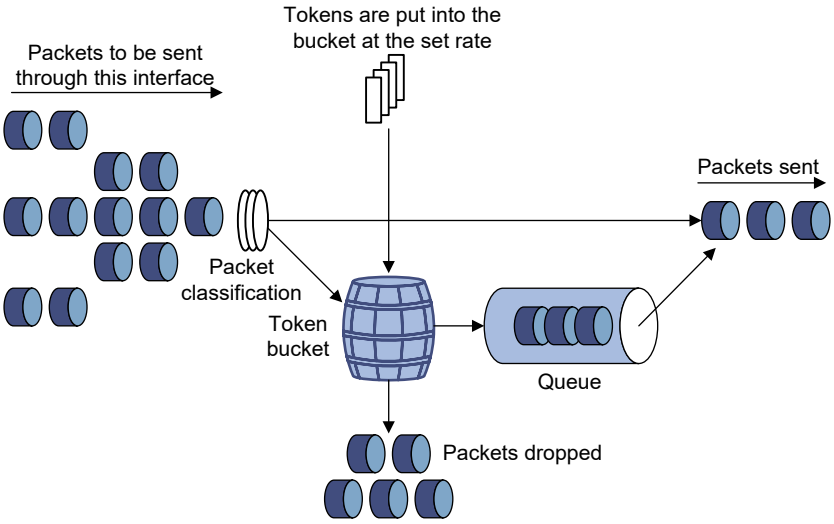
5.1.3. GTS

GTS は、出力トラフィックのシェーピングをサポートします。GTS は、超過したトラフィックをバッファすることによって、送信トラフィックの転送レートを制限します。パケットロスを防ぐため、GTS を使用することで、装置のトラフィックの出力レートを、装置に接続されたトラフィックの入力レートに適合させます。

トラフィックポリシングと GTS の違いを以下に示します。

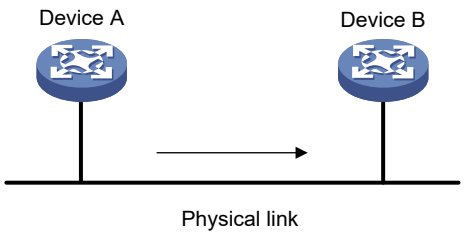
- 図 5-2 に示すように、トラフィックポリシングで廃棄されたパケットはバッファや GTS のキューに残されています。十分なトークンがトークンバケットにある場合、バッファされたパケットが適切なレートで送信されます。
- GTS は追加で遅延が生じることがありますが、トラフィックポリシングはありません。

図 5-2 GTS



たとえば、図 5-3 では、Device B は Device A からのパケットのトラフィックポリシングを行い、制限に超過したパケットを廃棄します。パケットロスを防ぐため、制限を超過しているパケットが Device A でキャッシュできるように Device A の出力インタフェースで GTS を実行します。一度リソースが解放されると、GTS はキャッシュされたパケットを取り出し、送信します。

図 5-3 GTS application アプリケーション



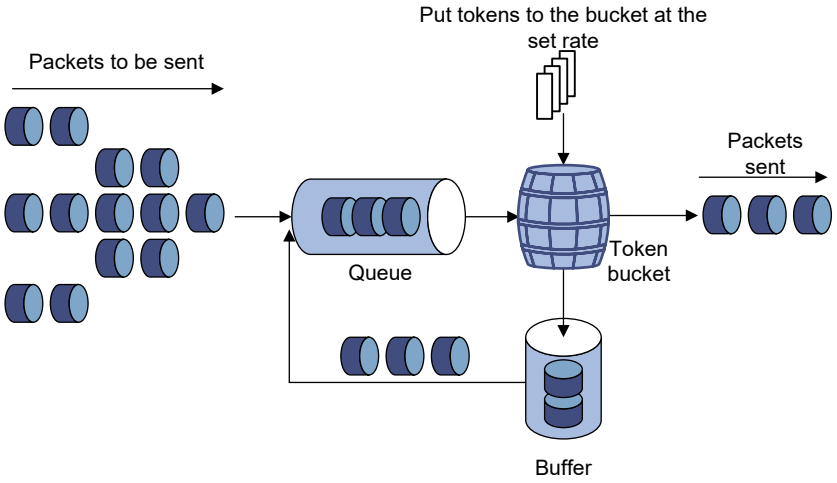
5.1.4. ラインレート

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 5-4 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. 設定の制限とガイドライン

指定された CIR はインターフレームギャップの中に送信されたトラフィックを考慮しません。インタフェースで実際に許可されたレートは指定された CIR よりも大きくなります。

インターフレームギャップはフレーム間の 12 ビットの時間間隔です。以下の役割を提供します。

- 装置が 1 つのフレームを別のフレームと区別します。
- 現在のフレームを処理し、次のフレームを受信するために準備する時間を考慮します。

5.3. トラフィックポリシングの設定

I. 制限とガイドライン

装置はトラフィックポリシングを行う際にアプリケーションの宛先として以下をサポートします。

- インタフェース
- VLAN
- グローバル

II. 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. 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. 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 Chapter7 *ACL and QoS Command References*の”*QoS policy commands*”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. トラフィックポリシングアクションを設定する	**car cir** *committed-information-rate* [**cbs** *committed-burst-size* [**ebs** *excess-burst-size*]] [**green** *action* | **red** *action* | **yellow** *action*] * **car cir** *committed-information-rate* [**cbs** *committed-burst-size*] **pir** *peak-information-rate* [**ebs** *excess-burst-size*] [**green** *action* | **red** *action* | **yellow** *action*] *	どちらか一方の設定を行います。 デフォルト：設定なし ※cirは、1000以上の単位で設定をしてください。 cbs値を指定しない場合は、cir値*62.5以上で、かつ512の整数倍になる最小値が設定されます。Cbsは、512～256000000の範囲で設定が可能です。 また、cbs値はcirに合わせて調整が必要です。詳細は本表下の重要項目をご参照ください。
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. トラフィック行動とトラフィッククラスを関連づける	**classifier** *classifier-name* **behavior** *behavior-name* [**insert-before** *before-classifier-name*]	デフォルト：設定なし
10. system view に戻る	**quit**	―
11. QoS ポリシーを適用する	Chapter7 *ACL and QoS Command References*の”*QoS policy commands*”を参照してください。	デフォルト：設定なし

重要:

TCP 通信(例 : FTP,CIFS,SMTP,HTTP 等)では、 CBS 値 が小さいと、再送処理が発生しやすくなり、速度が低下する可能性があります。
CBS 値 を十分な大きさに設定することで、再送処理を減らし、速度の低下を防ぎます。
下表及び補足に合わせ、CIR と CBS の値を設定してください。

タイプ	CIR		CBS		
	粒度(Kbps)	最大(Kbps)	粒度(B)	最小(B)	最大(B)
3	1,000	102,300,000	512	4,194,304	33,553,920
4	10,000	1,023,000,000	4,096	33,554,432	256,000,000

·CIR を 102,300,000Kbps までの範囲で設定する場合、CIR を 1000Kbps(1Mbps)単位で設定してください。CBS は 4,194,304～33,553,920B の範囲で、かつ 512 の整数倍で設定してください。
·CIR を 102,300,000Kbps を超えて設定する場合（最大 1,023,000,000Kbps まで）、CBS は 33,554,432～256,000,000B の範囲で、かつ 4,096 の整数倍で設定してください。

5.4. GTSの設定

I. 制限とガイドライン

この章のインタフェースはレイヤ 2 Ethernet インタフェース、レイヤ 3 Ethernet インタフェースを含むインタフェースを示します。**port link-mode** コマンドを使用して Ethernet ポートをレイヤ 2 あるいはレイヤ 3 に設定することができます。(詳細はセクション 3 *アクセスオペレーションマニュアルの”Ethernet インタフェース*"を参照してください。)

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. キューに GTS を設定する	**qos gts queue** *queue-number* **cir** *committed-information-rate* [**cbs** *committed-burst-size*]	デフォルト：設定なし

5.5. ラインレートの設定

I. 制限とガイドライン

この章のインタフェースはレイヤ 2 Ethernet インタフェース、レイヤ 3 Ethernet インタフェースを含むインタフェースを示します。**port link-mode** コマンドを使用して Ethernet ポートをレイヤ 2

あるいはレイヤ 3 に設定することができます。(詳細はセクション 3 *アクセスオペレーションマニュアルの”Ethernet インタフェース*"を参照してください。)

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. 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

5.6. トラフィックポリシング、GTS、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GTSの設定と統計情報を表示する	**display qos gts interface** [*interface-type interface-number*]
インタフェース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*]
QoSとACLのリソース使用状況を表示する	**display qos-acl resource** [**slot** *slot-number*]
トラフィック動作の設定を表示する	**display traffic behavior user-defined** [*behavior-name*]

5.7. トラフィックポリシング、GTS、ラインレートの設定例

5.7.1. トラフィックポリシング、GTS の設定例

I. ネットワーク要件

図 5-5 に示すように設定します。

- Server、Host A、Host B は Device A、Device B を通してインタネットにアクセスできます。
- Server、Host A、Device A の GigabitEthernet 1/0/1 は同一ネットワークセグメントにあります。

- Host B、Device A の GigabitEthernet 1/0/2 は同一ネットワークセグメントにあります。

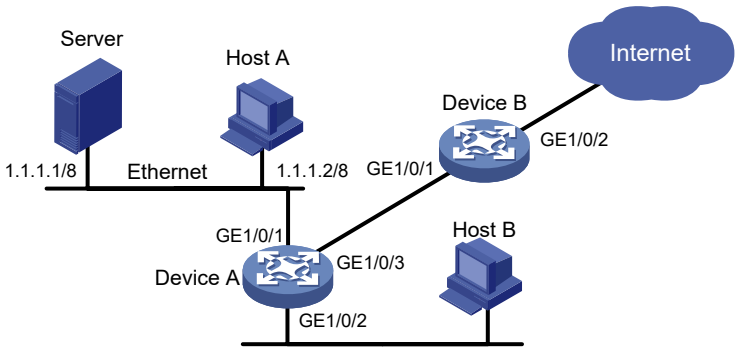
Server と Host A からのトラフィックを受信する Device A の GigabitEthernet 1/0/1 でトラフィックコントロールを設定します。

- Server からのトラフィックレートを 10240kbps に設定し、制御トラフィックを正常に転送し、余剰トラフィックに DSCP 値 0 をリマークし、トラフィックを転送します。
- Host A からのトラフィックレートを 2560kbps に設定し、制御トラフィックを正常に転送し、余剰トラフィックを廃棄します。

Device B の GigabitEthernet 1/0/1 と GigabitEthernet 1/0/2 でトラフィックの管理を行います。以下の要件に従います。

- GigabitEthernet 1/0/1 からの入力トラフィックレートを 20480kbps に設定し、余剰トラフィックを廃棄します。
- GigabitEthernet 1/0/2 の出力 HTTP トラフィックレート(インタネットにアクセスするトラフィック)を 10240kbps に設定し、余剰トラフィックを廃棄します。

図 5-5 ネットワーク図



II. 設定手順

1. Switch A を設定します。

   # Server と Host A からのトラフィックにマッチする ACL 2001、ACL 2002 をそれぞれ設定します。

   [DeviceA] acl basic 2001

   [DeviceA-acl-ipv4-basic-2001] rule permit source 1.1.1.1 0

   [DeviceA-acl-ipv4-basic-2001] quit

   [DeviceA] acl basic 2002

   [DeviceA-acl-ipv4-basic-2002] rule permit source 1.1.1.2 0

   [DeviceA-acl-ipv4-basic-2002] quit

   # トラフィッククラス **server** を作成し、一致条件に ACL2001 を適用します。

   [DeviceA] traffic classifier server

   [DeviceA-classifier-server] if-match acl 2001

   [DeviceA-classifier-server] quit

   # トラフィッククラス **host** を作成し、一致条件に ACL 2002 を適用します。

   [DeviceA] traffic classifier host

[DeviceA-classifier-host] if-match acl 2002

[DeviceA-classifier-host] quit

トラフィック動作 **server** を作成します。トラフィックポリシングアクションを設定します。CIR を 102400kbps に設定します。

[DeviceA] traffic behavior server

[DeviceA-behavior-server] car cir 10240 red remark-dscp-pass 0

[DeviceA-behavior-server] quit

トラフィック動作 **host** を作成し、CIR を 2560kbps に設定するように、トラフィックポリシングアクションを設定します。

[DeviceA] traffic behavior host

[DeviceA-behavior-host] car cir 2560

[DeviceA-behavior-host] quit

QoS ポリシー**car** を作成し、クラス **server** とトラフィック動作 **server**、クラス **host** とトラフィック動作 **host** を関連づけます。

[DeviceA] qos policy car

[DeviceA-qospolicy-car] classifier server behavior server

[DeviceA-qospolicy-car] classifier host behavior host

[DeviceA-qospolicy-car] quit

GigabitEthernet 1/0/1 のポートの入力トラフィックに QoS ポリシー**car** を適用します。

[DeviceA] interface gigabitethernet 1/0/1

[DeviceA-GigabitEthernet1/0/1] qos apply policy car inbound

2. Device B を設定します。

HTTP トラフィックにマッチする拡張 ACL 3001 を設定します。

<DeviceB> system-view

[DeviceB] acl advanced 3001

[DeviceB-acl-adv-3001] rule permit tcp destination-port eq 80

[DeviceB-acl-adv-3001] quit

トラフィッククラス **http** を作成し、一致条件に ACL3001 を適用します。

[DeviceB] traffic classifier http

[DeviceB-classifier-http] if-match acl 3001

[DeviceB-classifier-http] quit

トラフィッククラス **class** を作成し、すべてのパケットにマッチするように設定します。

[DeviceB] traffic classifier class

[DeviceB-classifier-class] if-match any

[DeviceB-classifier-class] quit

トラフィック動作 **car_inbound** を作成し、CIR を 20480kbps に設定するようにトラフィックポリシングアクションを設定します。

[DeviceB] traffic behavior car_inbound

[DeviceB-behavior-car_inbound] car cir 20480

[DeviceB-behavior-car_inbound] quit

トラフィック動作 **car_outbound** を作成し、CIR を 10240kbps に設定するようにトラフィックポリシングアクションを設定します。

[DeviceB] traffic behavior car_outbound

[DeviceB-behavior-car_outbound] car cir 10240

[DeviceB-behavior-car_outbound] quit

QoS ポリシー**car_inbound** を作成し、トラフィッククラス **class** と QoS ポリシーのトラフィック動作 **car_inbound** を関連づけます。

[DeviceB] qos policy car_inbound

[DeviceB-qospolicy-car_inbound] classifier class behavior car_inbound

[DeviceB-qospolicy-car_inbound] quit

QoS ポリシー**car_outbound** を作成し、トラフィッククラス **http** と QoS ポリシーのトラフィック動作 **car_outbound** を関連づけます。

[DeviceB] qos policy car_outbound

[DeviceB-qospolicy-car_outbound] classifier http behavior car_outbound

[DeviceB-qospolicy-car_outbound] quit

GigabitEthernet 1/0/1 の入力トラフィックに QoS ポリシー**car_inbound** を適用します。

[DeviceB] interface gigabitethernet 1/0/1

[DeviceB-GigabitEthernet1/0/1] qos apply policy car_inbound inbound

GigabitEthernet 1/0/2 の出力トラフィックに QoS ポリシー**car_outbound** を適用します。

[DeviceB] interface gigabitethernet 1/0/2

[DeviceB-GigabitEthernet1/0/2] qos apply policy car_outbound outbound

目次

このセクションのページは **7-x-x** です。

6 章 輻輳制御 6-1
6.1. 概要 6-1
6.1.1. 輻輳の原因、影響、対策 6-1
6.1.2. 輻輳制御の方法 6-1
6.2. 設定作業リスト 6-4
6.3. インタフェースのキューイングの設定 6-4
6.3.1. キューイングの設定の制限とガイドライン 6-4
6.3.2. SP キューイングの設定 6-4
6.3.3. WRR キューイングの設定 6-4
6.3.4. SP+WRR キューイングの設定 6-5
6.4. 輻輳制御の表示と維持 6-5

6章 輻輳制御

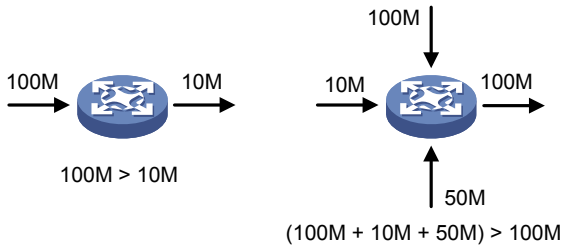
6.1. 概要

6.1.1. 輻輳の原因、影響、対策

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、統計的多重化ネットワークで起こる輻輳の典型的であり、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。

輻輳制御の鍵は、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。

6.1.2. 輻輳制御の方法

輻輳管理はポートを除外するトラフィックを区分けし、分類し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スケジューリングメカニズムをサポートします。

- SP
- WRR

I. 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

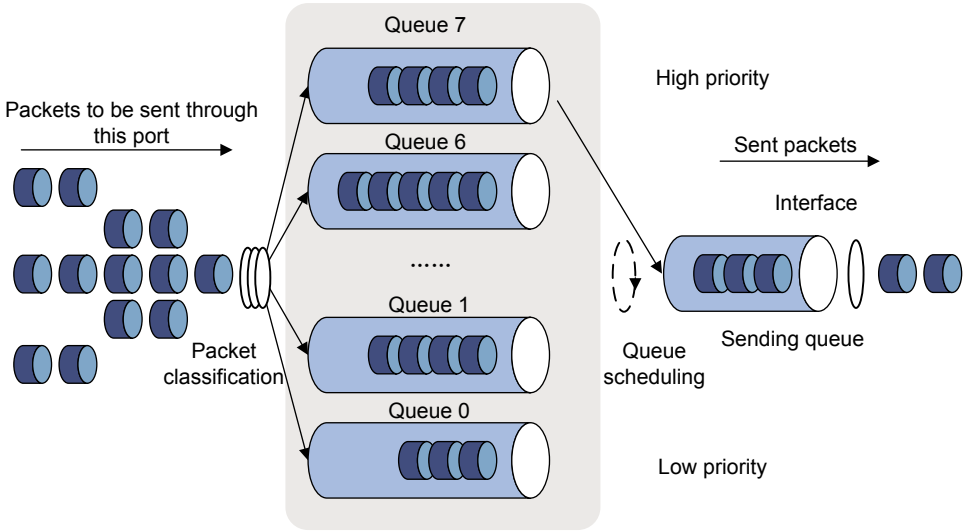


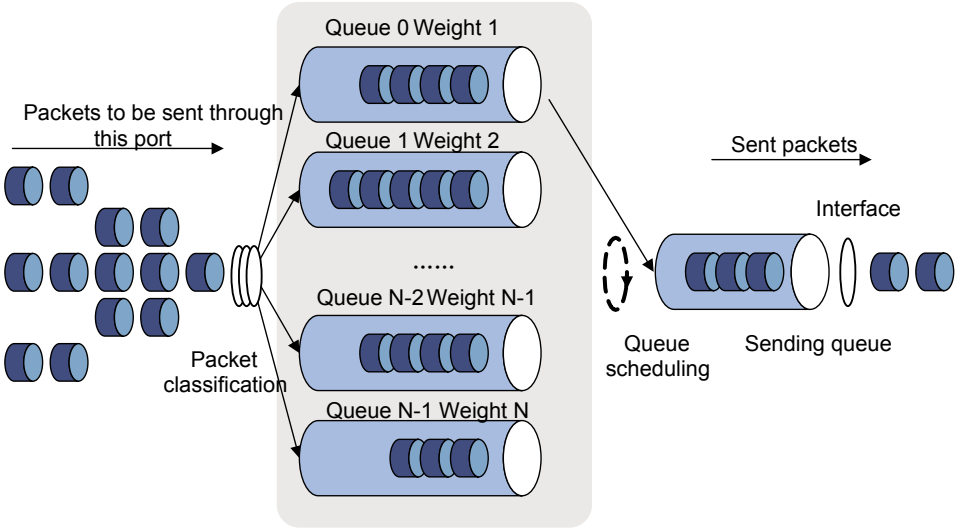
図 6-2 に示すように、SP キューイングはポートに 8 つにクラス分けしたキューを割り当てます。キューの番号 7 から 0 の順に優先順位は低くなります。

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最も優先順位が高いパケットを送信します。最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の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。

II. WRR キューイング

図 6-3 に示すように、WRR キュースケジューリングアルゴリズムは、あらゆるキューが特定のサービスタイムに割り当てられように、すべてのキューを順にスケジューリングします。

図 6-3 WR 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。

装置はキューの正確なバイト数のスケジューリング(byte-count WRR)あるいはパケットの正確な数(packet-based WRR)のスケジューリングでキューの重みづけを実装します。

byte-count WRR の例を示します。100Mbps のポートに、WRR キューイングの重み付けを 50、30、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 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がある SP キューイングの欠点が回避できます。

キューが総当たりでスケジュールした場合、各キューのサービスタイムが固定されないという WRR キューイングの別の利点があります。キューが空きの場合、次のキューはすぐにスケジューリングされます。帯域幅のリソースを効率的に使用することができます。

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。

基本 WRR キューイングは現在のソフトウェアバージョンでサポートされていません。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) キューイングの設定 輻輳管理を設定するために、以下の1つを行ってください。 • 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. インタフェースのキューイングの設定

6.3.1. キューイングの設定の制限とガイドライン

この章のインタフェースはレイヤ 2 Ethernet インタフェース、レイヤ 3 Ethernet インタフェースを含むインタフェースを示します。**port link-mode** コマンドを使用して Ethernet ポートをレイヤ 2 あるいはレイヤ 3 に設定することができます。(詳細はセクション 3 *アクセスオペレーションマニュアルの”Ethernet インタフェース*"を参照してください。)

6.3.2. 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: WRRキューイング

6.3.3. 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. WRR キューイングを有効にする	**qos wrr weight**	デフォルト : インタフェースはパケットカウントのキューイングを使用します。

操作	コマンド	補足
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：グループ1 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。

6.3.4. SP+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. byte-count あるいは packet-based の WRR キューイングを有効にする	**qos wrr weight**	デフォルト：インタフェースはパケットカウントのキューイングを使用します。
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
5. WRR グループにキューを割り当て、キューの重み付けを設定する	**qos wrr** *queue-id* **group 1 weight** *schedule-value*	デフォルト：グループ1 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。

6.4. 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
queue-basedの出力トラフィックの統計情報を表示する	**display qos queue-statistics interface outbound**
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*]

目次

このセクションのページは **7-x-x** です。

7 章 トラフィックフィルタリング 7-1
7.1. 概要 7-1
7.2. 制限とガイドライン 7-1
7.3. 設定手順 7-1
7.4. トラフィックフィルタリングの設定例 7-2
7.4.1. トラフィックフィルタリングの設定例 7-2

7章 トラフィックフィルタリング

7.1. 概要

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クラスの受信/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。

7.2. 制限とガイドライン

装置はトラフィックフィルタリングを行う際にアプリケーションの宛先として以下をサポートします。

- インタフェース
- VLAN
- グローバル

7.3. 設定手順

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 Chapter 7 *ACL and QoS Command References*の”*QoS policy commands*”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 トラフィック動作が**deny**である場合、トラフィック動作のクラスベースアカウンティングを除いたすべての他のアクションは適用されません。

操作	コマンド	補足
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	Chapter 7 *ACL and QoS Command References*の"*QoS policy commands*"を参照してください。	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。

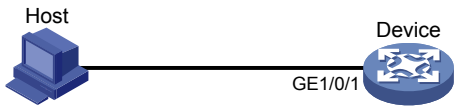
7.4. トラフィックフィルタリングの設定例

7.4.1. トラフィックフィルタリングの設定例

I. ネットワーク要件

図 7-1 に示すように、送信元ポート番号 21 の受信パケットをフィルタするために GigabitEthernet 1/0/1 で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



II. 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 neq 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 **7-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. プライオリティマーキングの設定 8-1
8.3. プライオリティマーキングの設定例 8-2
8.3.1. プライオリティマーキングの設定例 8-2

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、パケットのプライオリティを変更するため、パケットのプライオリティフィールドあるい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 プレシーデンスあるいは DSCP を設定するプライオリティマーキングを使用することができます。

パケットの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設定するため、プライオリティマーキングを設定する場合、以下の作業を行います。

1. トラフィック動作にプライオリティマーキングアクションを設定します。
2. トラフィッククラスにトラフィック動作を関連づけます。

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、セクション 7 *ACL and QoS オペレーションマニュアル*の”*プライオリティマッピング*”を参照してください。

8.2. プライオリティマーキングの設定

I. 制限とガイドライン

装置はプライオリティマーキングを行う際にアプリケーションの宛先として以下をサポートします。

- インタフェース
- VLAN
- グローバル

II. 設定手順

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、Chapter 7 *ACL and QoS Command References*の”*QoS policy commands*”を参照してください。

操作	コマンド	補足
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. プライオリティマーキングアクションを設定する	Chapter 7 *ACL and QoS Command References*の"*QoS policy commands*"の**remark** コマンドを参照してください。	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に 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	Chapter 7 *ACL and QoS Command References*の"*QoS policy commands*" を参照してください。	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

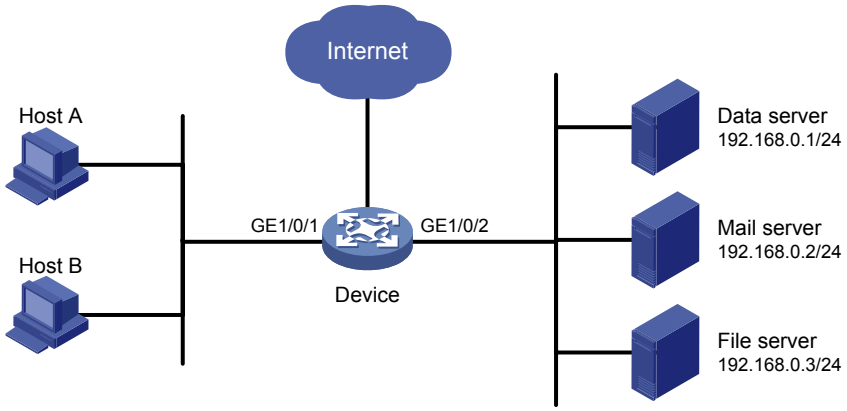
8.3.1. プライオリティマーキングの設定例

I. ネットワーク要件

図 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、Host B	Data server	High
Host A、Host B	Mail server	Medium
Host A、Host B	File server	Low

図 8-1 ネットワーク図



II. 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 ACL3002 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 **7-x-x** です。

9 章 ネスティング 9-1
9.1. 概要 9-1
9.2. 制限とガイドライン 9-1
9.3. 設定手順 9-1
9.4. ネスティングの設定例 9-2
9.4.1. ネスティングの設定例 9-2

9章 ネスティング

9.1. 概要

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。

9.2. 制限とガイドライン

装置はネスティングを行う際にアプリケーションの宛先として以下をサポートします。

- インタフェース
- VLAN
- グローバル

インタフェースで QinQ が有効で、ネスティングアクションが VLAN ID のマッチ条件に関連づけられている場合、ネスティングアクションは適用されません。ネスティングアクションを適用する場合、インタフェースで、タグ付けされたパスにマッチするパケットを許可する必要があります。

9.3. 設定手順

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 Chapter 7 *ACL and QoS Command References*の”*QoS policy commands*”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

操作	コマンド	補足
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	Chapter 7 *ACL and QoS Command References*の"*QoS policy commands*"を参照してください。	デフォルト：設定なし

9.4. ネスティングの設定例

9.4.1. ネスティングの設定例

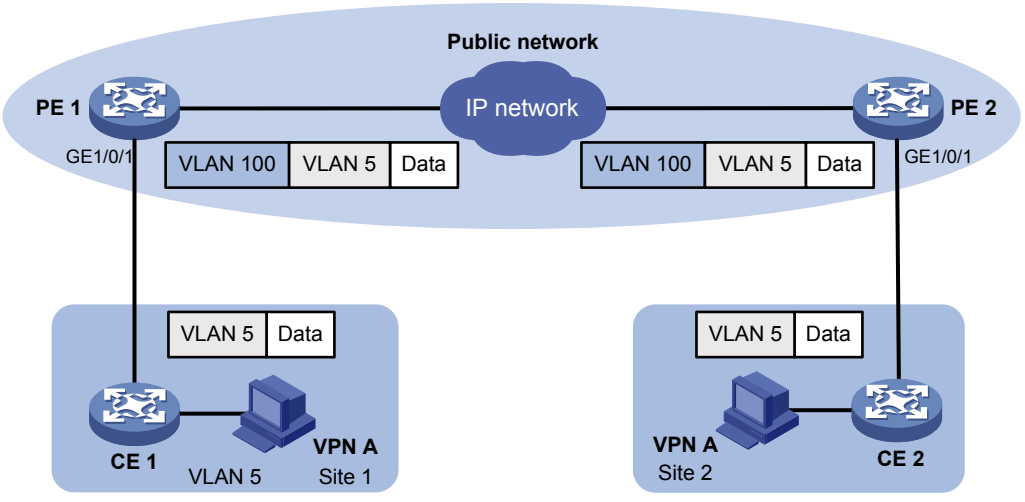
I. ネットワーク要件

図 9-1 に示すように設定します。

- 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、VLAN5 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 VLAN100 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



II. 設定手順

1. PE 1 を設定します。

   # VLAN ID 5 のパケット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、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、タグなしメンバとして 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** に受信ポート 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 **7-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. 概要……10-1
10.2. 制限とガイドライン……10-1
10.3. 設定手順……10-1
10.4. トラフィックリダイレクティングの設定例……10-2
10.4.1. トラフィックリダイレクティングの設定例……10-2

10章　トラフィックリダイレクティング

10.1. 概要

トラフィックリダイレクティングは、指定した基準でパケットをリダイレクトさせます。以下のリダイレクトアクションをサポートしています。

- **CPU へのリダイレクト** ― CPU に CPU で処理を必要とするパケットをリダイレクトします。
- **インタフェースへのリダイレクト** ― インタフェースで処理を必要があるパケットをリダイレクトします。このアクションはレイヤ 2 パケットのみ適用します。宛先インタフェースはレイヤ 2 インタフェースにする必要があります。

10.2. 制限とガイドライン

- 装置はトラフィックリダイレクティングを行う際にアプリケーションの宛先として以下をサポートします。
  - インタフェース
  - VLAN
  - グローバル
- **redirect** コマンドを複数実行した場合、最後に行った設定が適用されます。
- Ethernet インタフェースにトラフィックリダイレクティングを行う際、インタフェースが装置から取り外されたあとは、装置はリダイレクトアクションに関する表示を行いません。インタフェースモジュールが再度実装された場合、装置はリダイレクトアクションを表示することができます。

10.3. 設定手順

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 Chapter 7 *ACL and QoS Command References*の”*QoS policy commands*”を参照してください。
4. system view に戻る	**quit**	―

操作	コマンド	補足
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
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	Chapter 7 *ACL and QoS Command References*の"*QoS policy commands*"を参照してください。	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。

10.4. トラフィックリダイレクティングの設定例

10.4.1. トラフィックリダイレクティングの設定例

I. ネットワーク要件

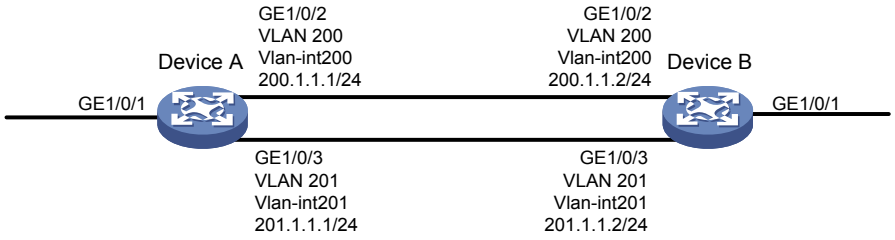
図 10-1 に示すように設定します。

- 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



II. 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の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の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 **7-x-x** です。

11 章 クラスベースアカウンティング 11-1
11.1. 概要 11-1
11.2. 制限とガイドライン 11-1
11.3. 設定手順 11-1
11.4. クラスベースアカウンティングの設定例 11-2
11.4.1. クラスベースアカウンティングの設定例 11-2

11章 クラスベースアカウンティング

11.1. 概要

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。

11.2. 制限とガイドライン

装置はクラスベースアカウンティングを行う際にアプリケーションの宛先として以下をサポートします。

- インタフェース
- VLAN
- グローバル

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. 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 Chapter 7 *ACL and QoS Command References*の”*QoS policy commands*”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**	―

操作	コマンド	補足
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	Chapter 7 *ACL and QoS Command References*の"*QoS policy commands*"を参照してください。	デフォルト：設定なし
12. (オプション設定項目) トラフィックアカウンティングの設定情報を表示する	• **display qos policy global** • **display qos policy interface** • **display qos vlan-policy**	すべてのviewで実行できます。

11.4. クラスベースアカウンティングの設定例

11.4.1. クラスベースアカウンティングの設定例

I. 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 1.1.1.1/24 のパケットのトラフィックを、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



II. 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の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 **7-x-x** です。

12 章 付録 12-1
12.1. 付録 A 頭字語 12-1
12.2. 付録 B デフォルトプライオリティマップ 12-1
12.2.1. プライオリティマップ 12-1
12.3. 付録 C パケットプレシーデンスの概要 12-3
12.3.1. IP プレシーデンスと DSCP フィールドの値 12-3
12.3.2. 802.1p プライオリティ 12-4

12章　付録

12.1. 付録A 頭字語

表 12-1 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
CIR	Committed Information Rate
DCBX	Data Center Bridging Exchange Protocol
DiffServ	Differentiated Service
DSCP	Differentiated Services Code Point
EBS	Excess Burst Size
FIFO	First in First out
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
RSVP	Resource Reservation Protocol
ToS	Type of Service
VPN	Virtual Private Network
WRR	Weighted Round Robin

12.2. 付録B デフォルトプライオリティマップ

12.2.1. 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 12-2 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 12-3 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 to 7	0
8 to 15	1
16 to 23	2
24 to 31	3
32 to 39	4
40 to 47	5
48 to 55	6
56 to 63	7

表 12-4 デフォルトのポートプライオリティーローカルプライオリティマッピング

Port priority	ローカルプレシーデンス
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7

12.3. 付録C パケットプレシーデンスの概要

12.3.1. IP プレシーデンスと DSCP フィールドの値

図 12-1 ToS、DS フィールド

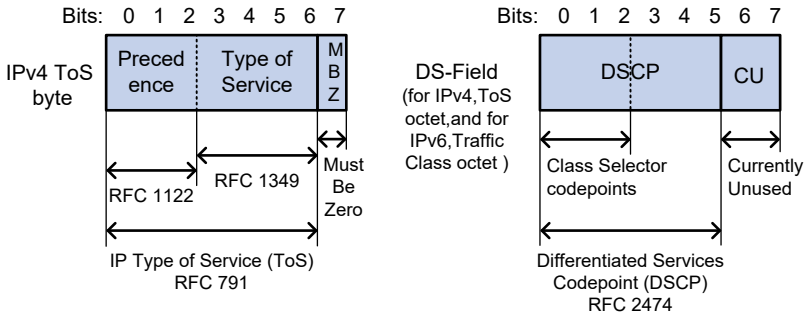


図 12-1 に示すように、IP ヘッダの ToS フィールドは 8 ビットが含まれます。最初の 3 ビット(0～2)は、0～7 までの IP プレシーデンスを示します。RFC2474 に従い、ToS フィールドは、右側の DS(Differentiated Services)フィールドとして再定義されます。ここで最初の 6 ビット(0～5)は DSCP を表し、0～63 までの値となります。残りの 2 ビット(6、7)は予約された値として使われません。

表 12-5 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 12-6 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

DSCP 値(10 進表示)	DSCP 値(2 進表示)	説明
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)

12.3.2. 802.1p プライオリティ

802.1p プライオリティは、レイヤ 2 ヘッダにあります。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 12-2 802.1Q タグヘッダの Ethernet フレーム

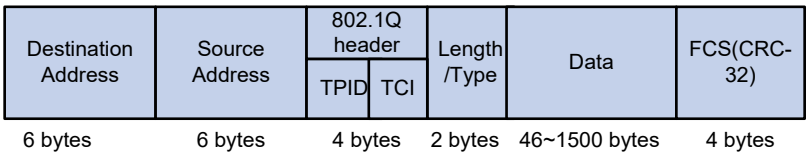


図 12-2 に示すように、4 バイトの 802.1Q タグヘッダはタグプロトコル識別子(TPID、2 バイト長)とタグ管理情報(TCI、2 バイト長)から構成されます。TPID の値は 0x8100 です。図 12-3 に、802.1Q ヘッダのフォーマットを示します。802.1Q タグヘッダのプライオリティフィールドは、IEEE802.1p で定義され、802.1p プライオリティと呼ばれます。表 12-8 に 802.1p プライオリティの値を示します。

図 12-3 802.1Q タグヘッダ

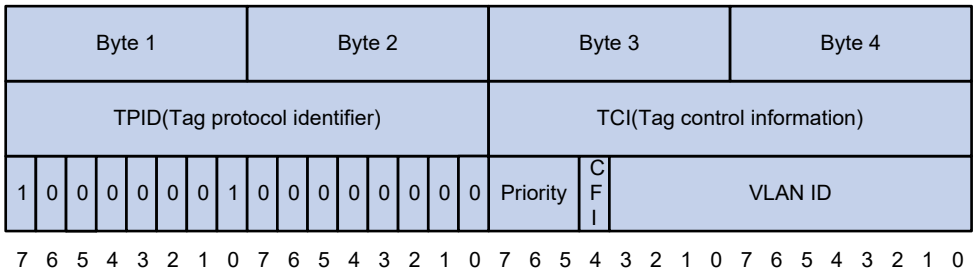


表 12-7 802.1p プライオリティの説明

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

目次

このセクションのページは **7-x-x** です。

13 章 データバッファ機能 13-1
13.1. 概要 13-1
13.1.1. データバッファのタイプ 13-1
13.1.2. セルリソースとパケットリソース 13-1
13.1.3. 専用エリアと共有エリア 13-1
13.2. 制限とガイドライン 13-2
13.3. 設定作業リスト 13-2
13.4. バースト機能の有効化 13-3
13.5. データバッファの手動設定 13-3
13.6. データバッファの表示と維持 13-4

13章 データバッファ機能

13.1. 概要

13.1.1. データバッファのタイプ

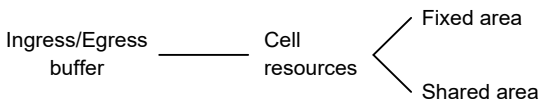
データバッファはパケットロスを避けるため、一時的にパケットを記録（バッファ）します。

以下のデータバッファがあります。

- **入力バッファ(Ingress)**－CPU がビジー状態のとき、入力パケットを記録します。
- **出力バッファ(Egress)**－ネットワークで衝突が発生したとき、出力パケットを記録します。

図 13-1 に入力バッファ、出力バッファの構造を示します。

図 13-1 データバッファの構造



13.1.2. セルリソースとパケットリソース

バッファはセルリソースを使用して、パケットサイズに基づいてパケットを格納します。セルリソースは 256 バイトです。バッファは、128 バイトのパケットに 1 つのセルリソースを割り当て、300 バイトのパケットに 2 つのセルリソースを割り当てます。

13.1.3. 専用エリアと共有エリア

リソースの各タイプには、専用エリア（Fixed area）と共有エリア（Shared area）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。輻輳が発生した場合、または CPU がビジー状態の場合は、次のルールが適用されます。

  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。

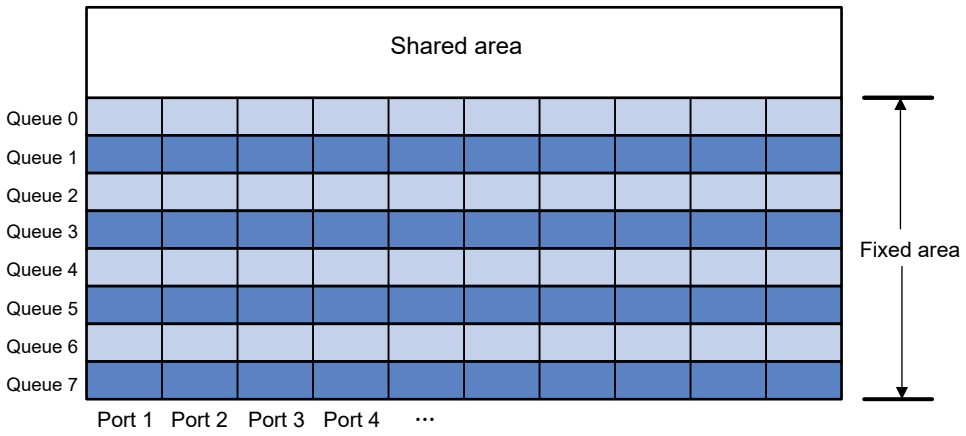
  ユーザによって指定されたキューに専用エリアが割り当てられます。キューが一杯でない場合でも、他のキューはその領域を使用できません。

同様に、キューの専用エリアが一杯でない場合に、同じキューID であっても他のインタフェースでは使用できません。

- **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。システムは共有エリアが一杯でない場合、他のキューが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 専用エリアと共有エリア



13.2. 制限とガイドライン

- データバッファ機能はデータバッファを手動または自動で設定できます。ある方法でデータバッファを設定した場合は、他の方法を使用する前に設定を削除する必要があります。それ以外の場合、新しい設定は有効になりません。
- データバッファ機能の変更が不適切であると、システムに問題が発生する可能性があります。データバッファ設定を手動で変更する前に、装置への影響を理解しておく必要があります。データバッファ設定を変更する場合は、装置の動作について事前に検証することを推奨します。

13.3. 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
バースト機能の有効化
データバッファの手動設定
データバッファの表示と維持

13.4. バースト機能の有効化

I. バースト機能

バースト機能はセル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。バースト機能を有効にすると、デフォルトのデータバッファ設定が変更されます。

- 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集中して、バーストトラフィックが発生します。
- 以下のいずれかの方法でトラフィックが入出力します。
  - 高速インタフェースから装置に入力され、低速インタフェースから出力します。
  - 複数の同じ速度のインタフェースから同時に入力し、同じ速度で 1 つのインタフェースから出力します。

II. 設定手順

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

13.5. データバッファの手動設定

I. データバッファの手動設定について

リソースのサイズを固定設定します。未設定のキューはデフォルト設定を使用します。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. キューの共有エリア比率を設定します。	**buffer egress** [**slot** *slot-number*] **cell** [**queue** *queue-id*] **shared ratio** *ratio*	デフォルトでは、ポートとキューの両方とも共有エリアの合計サイズの33%です。 各キューの実際の最大共有エリアサイズは、設定値と送受信されるパケット数に基づいて決定されます。
3. バッファ割当てルールを適用します。	**buffer apply**	適用された設定がある場合は、直接変更することはできません。設定を変更するには、**undo buffer apply**コマンドで設定を解除してから、設定を変更して再適用する必要があります。

メモ:

- **buffer shared** コマンドおよび **buffer apply** コマンドは Version7.3.24 を含む以降のソフトウェアからサポートしています。
- **buffer shared** コマンドは、SP キューイングなどの輻輳制御を使用する場合のみ設定することを推奨します。また、輻輳制御で使用する場合にはキュー0 から 7 まで以下の設定をしてください。他のパラメータを使用する場合は、使用する前にお使いの環境での事前検証を推奨します。

  buffer egress cell queue 7 shared ratio 4
  buffer egress cell queue 6 shared ratio 4
  buffer egress cell queue 5 shared ratio 4
  buffer egress cell queue 4 shared ratio 4
  buffer egress cell queue 3 shared ratio 4
  buffer egress cell queue 2 shared ratio 4
  buffer egress cell queue 1 shared ratio 4
  buffer egress cell queue 0 shared ratio 4
- **buffer apply** コマンドで設定を適用/解除する際に瞬間的（1 秒以内）に通信断が発生するため、本影響を考慮して通信が影響を受けにくい時間帯で使用することを推奨します。

13.6. データバッファの表示と維持

すべての view で display コマンドを実行できます。

操作	コマンド
バッファサイズの設定を表示する	**display buffer** [**slot** *slot-number*] [**queue** [*queue-id*]]

メモ:

- **display buffer** コマンドは Version7.3.24 を含む以降のソフトウェアからサポートしています。

目次

このセクションのページは **7-x-x** です。

14 章 タイムレンジ 14-1
14.1. 概要 14-1
14.2. 制限とガイドライン 14-1
14.3. 設定手順 14-1
14.4. タイムレンジの表示と維持 14-1
14.5. タイムレンジの設定例 14-2
14.5.1. タイムレンジの設定例 14-2

14章 タイムレンジ

14.1. 概要

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。

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。

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。

14.2. 制限とガイドライン

ハードウェアモードの ACL を設定するとき、以下の制限とガイドラインがあります。

- 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。
- 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。

14.3. 設定手順

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

14.4. 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** }

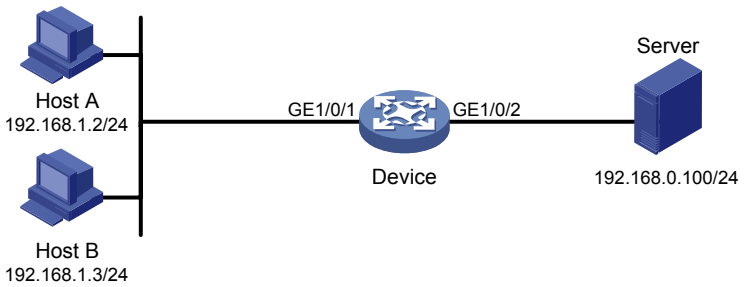
14.5. タイムレンジの設定例

14.5.1. タイムレンジの設定例

I. ネットワーク要件

ネットワーク図に示すように、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 に ACL を設定します。

図 14-1 ネットワーク図



II. 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。

<Device> system-view

[Device] 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。

[Device] acl basic 2001

[Device-acl-ipv4-basic-2001] rule permit source 192.168.1.2 0 time-range work

[Device-acl-ipv4-basic-2001] rule deny source any time-range work

[Device-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。

[Device] interface gigabitethernet 1/0/2

[Device-GigabitEthernet1/0/2] packet-filter 2001 outbound

[Device-GigabitEthernet1/0/2] quit

III. 設定の確認

Device でタイムレンジの設定と状態を表示します。

[Device] display time-range all

```
Current time is 13:58:35 6/19/2015 Friday

Time-range : work (Active)
 08:00 to 18:00 working-day
 from 00:00 6/1/2015 to 00:00 1/1/2016
```

QX-S5300G シリーズ Ethernet スイッチ

オペレーションマニュアル

8. 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-WEB 認証
06-トリプル認証
07-ポートセキュリティ
08-パスワード管理
09-公開鍵
10-PKI
11-SSH
12-SSL
13-TCP フラグメントアタックプロテクション
14-IP ソースガード
15-ARP アタックプロテクション

目次

このセクションのページは **8-x-x** です。

1 章 AAA ····· 1-1
1.1. 概要 ····· 1-1
1.1.1. AAA ····· 1-1
1.1.2. AAA のネットワーク構成 ····· 1-1
1.1.3. RADIUS ····· 1-2
1.1.4. 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 ····· 1-6
1.1.5. 認証方式、許可方式、アカウンティング方式 ····· 1-7
1.1.6. プロトコルと標準 ····· 1-8
1.2. AAA 設定要件と設定作業リスト ····· 1-9
1.3. ローカルユーザの設定 ····· 1-9
1.3.1. ローカルユーザの概要 ····· 1-9
1.3.2. ローカルユーザ設定作業リスト ····· 1-11
1.3.3. 装置管理ユーザ属性の設定 ····· 1-11
1.3.4. ネットワークアクセスユーザ属性の設定 ····· 1-13
1.3.5. ユーザグループ属性の設定 ····· 1-15
1.3.6. 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 ····· 1-16
1.4. RADIUS スキームの設定 ····· 1-17
1.4.1. 設定作業リスト ····· 1-17
1.4.2. RADIUS 設定の制限とガイドライン ····· 1-17
1.4.3. RADIUS スキームの作成 ····· 1-18
1.4.4. RADIUS 認証サーバの指定 ····· 1-18
1.4.5. RADIUS アカウンティングサーバの指定 ····· 1-19
1.4.6. セキュアな RADIUS 通信を行うための共有鍵の指定 ····· 1-20
1.4.7. RADIUS サーバのステータスの設定 ····· 1-21
1.4.8. RADIUS サーバのタイマ機能の設定 ····· 1-22
1.4.9. 出力する RADIUS パケットの送信元 IP アドレスの指定 ····· 1-24
1.4.10. 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 ····· 1-25
1.4.11. RADIUS 要求の再送信の最大試行回数の設定 ····· 1-25
1.4.12. RADIUS アカウンティング要求の最大試行回数の設定 ····· 1-26
1.4.13. RADIUS パケットの DSCP 優先度の設定 ····· 1-26
1.4.14. RADIUS アカウンティング停止要求パケットのバッファの設定 ····· 1-27
1.4.15. RADIUS accounting-on 機能の設定 ····· 1-27
1.4.16. RADIUS の SNMP notification の通知の有効化 ····· 1-28
1.4.17. 再認証を行う際の RADIUS サーバ選択モードの設定 ····· 1-28
1.4.18. RADIUS の表示と維持 ····· 1-29
1.5. ISP ドメインの作成 ····· 1-30
1.5.1. 概要 ····· 1-30
1.5.2. 制限とガイドライン ····· 1-30
1.5.3. ISP ドメインの作成 ····· 1-30
1.5.4. デフォルト ISP ドメインの指定 ····· 1-31
1.6. ISP ドメインの属性の設定 ····· 1-31
1.6.1. ISP ドメインの属性の設定 ····· 1-31
1.7. ISP ドメインの AAA 方式の設定 ····· 1-31

1.7.1. ISP ドメインの認証方式の設定……1-31
1.7.2. ISP ドメインの許可方式の設定……1-32
1.7.3. ISP ドメインのアカウンティング方式の設定……1-33
1.7.4. ISP ドメインの表示と維持……1-34
1.8. 同時ログインユーザの最大数の設定……1-34
1.9. AAA の設定例……1-35
1.9.1. SSH ユーザのローカル認証、RADIUS アカウンティングの設定例……1-35
1.10. RADIUS のトラブルシューティング……1-36
1.10.1. RADIUS 認証の失敗……1-36
1.10.2. RADIUS パケットが到達不能……1-37
1.10.3. RADIUS アカウンティングエラー……1-38
1.11. 付録……1-38
1.11.1. 一般的に使用される RADIUS 属性……1-38
1.11.2. 一般的に使われる標準 RADIUS 属性……1-40
1.11.3. QX シリーズ用 RADIUS 属性……1-42

1章 AAA

1.1. 概要

1.1.1. AAA

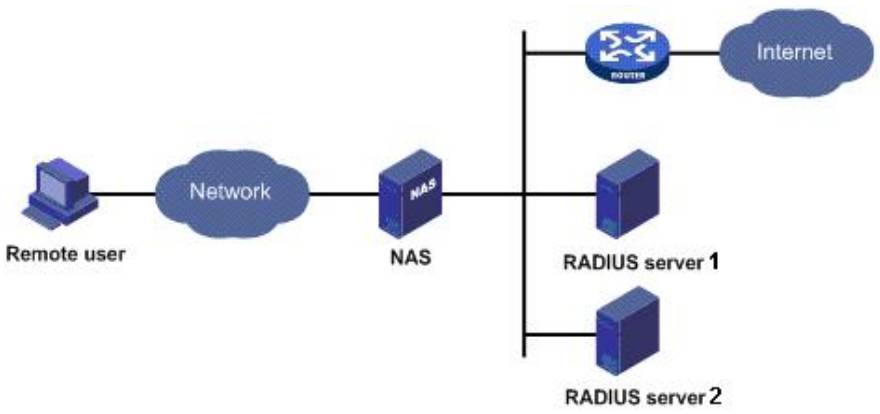
AAA は認証(Authentication)、許可(Authorization)、および課金(Accounting)というネットワークアクセス管理を行うための一定のフレームワークを提供します。以下のセキュリティ機能を提供します。

- **認証** ― リモートユーザを特定し、ユーザが有効か否かを判断します。
- **許可（認可）** ― リソースとサービスにアクセスする際、ユーザごとに異なる権限を与えます。たとえば、サーバを使用してログインするユーザに、サーバのファイルにアクセスし、印刷する権限を与えます。そしてゲストのユーザが装置上のファイルにアクセスしないようにします。
- **アカウンティング（課金）** ― サービスタイプ、開始/終了の時間、トラフィックが含まれるユーザのネットワークサービスの詳細な使用情報を記録します。これにより、課金機能は、時間ベースおよびトラフィックベースで、課金だけでなく、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。

1.1.2. AAA のネットワーク構成

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、他のネットワーク、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限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。このとき、必要に応じて、認証、許可、課金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 を課金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、課金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。

1.1.3. 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、ADSL 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 サーバは以下の処理を行います。

- 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。
- ユーザの認証、許可、アカウンティングを実行します。
- アクセス制御情報(たとえば、ユーザのアクセスリクエストを許可/拒否する)をクライアントに応答します。

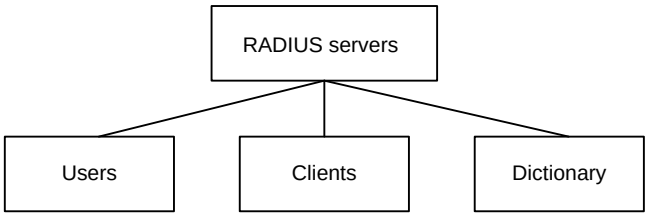
加えて RADIUS サーバは、認証プロキシのサービスを提供する別の RADIUS サーバのクライアントによって実行することができます。

通常、RADIUS サーバは、以下のデータベースを管理します。

- **Users**－ユーザ名、パスワード、適用プロトコル、IP アドレスなどのユーザ情報を記録します。
- **Clients**－共有鍵（キー）、IP アドレスなどの RADIUS クライアントの情報を記録します。

- **Dictionary**－RADIUS プロトコルの属性とその値を把握するための情報を記録します。

図 1-2 RADIUS サーバデータベース



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 バイトの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、他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とき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。

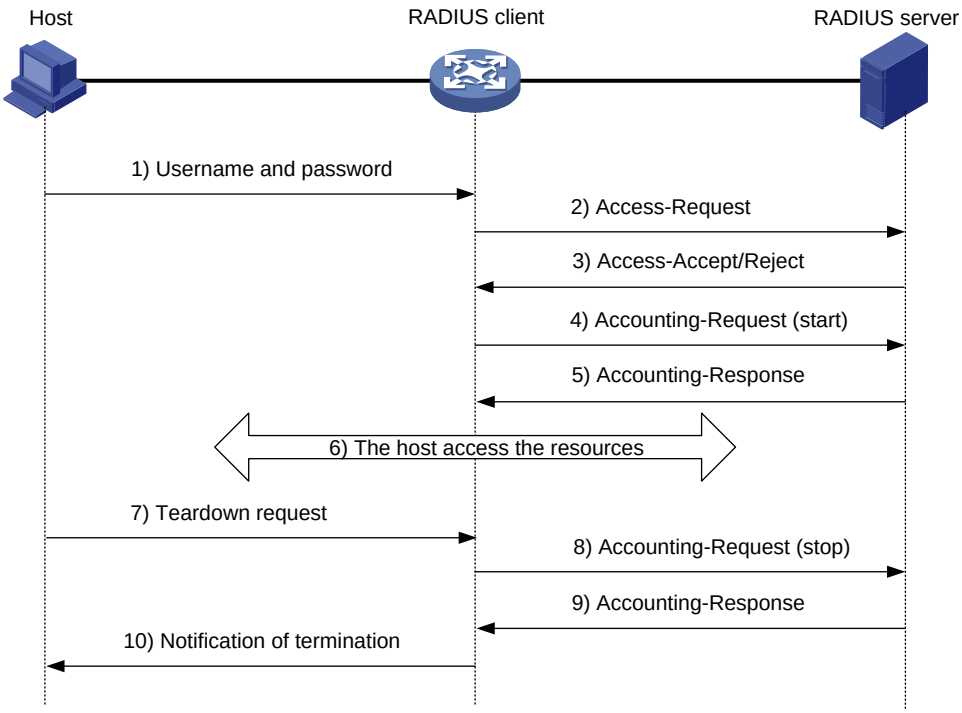
III. ユーザ認証メカニズム

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



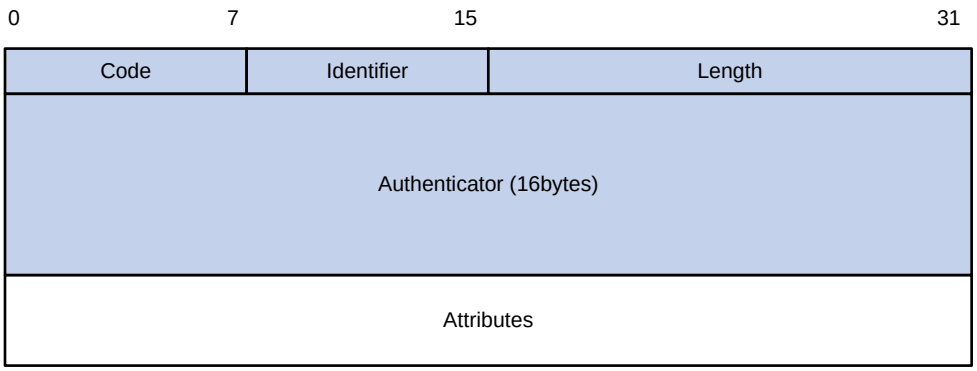
RADIUS は以下のように動作します。

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もつ認証要求(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

コード	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の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 をもちます。
- 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、セクション 8 *セキュリティ オペレーションマニュアルの”AAA”の”一般的に使われる標準 RADIUS 属性”*を参照してください。

VI. 拡張 RADIUS 属性

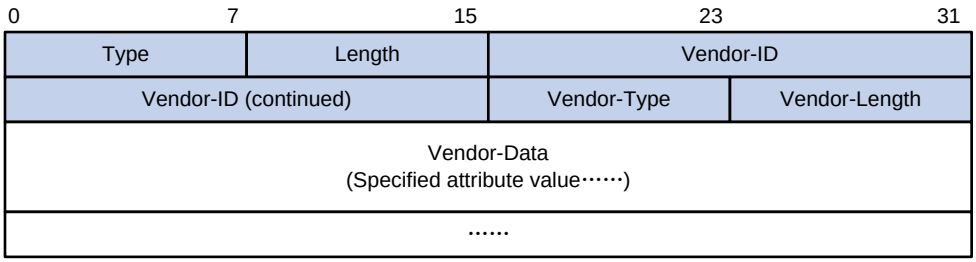
RADIUS プロトコルは優れた拡張性をもちます。RFC 2865 で定義されている属性番号 26(Vender-Specific)は、標準 RADIUS プロトコルが提供しない機能をベンダが実装するために拡張属性を定義することができます。

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、他の 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。

拡張 RADIUS 属性の詳細については、セクション 8 *セキュリティ オペレーションマニュアルの”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



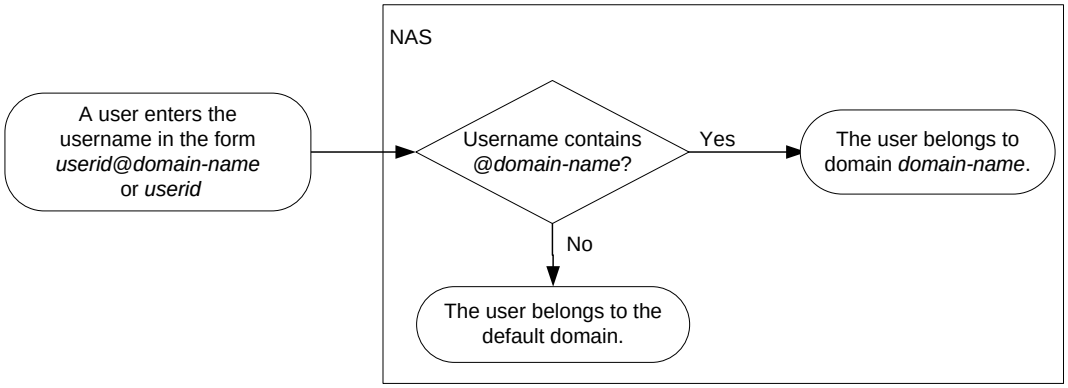
1.1.4. ISP ドメインにもとづくユーザ管理とユーザアクセスタイプ

この章は AAA のユーザ管理と方法について記載します。

AAA は ISP ドメインとアクセスタイプ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**－LAN ユーザはオンラインできるように 802.1X あるいは MAC アドレス認証にパスする必要があります。
- **ログイン**－ログインユーザは、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。

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。

1.1.5. 認証方式、許可方式、アカウンティング方式

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。

I. AAA 認証方式

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。セキュリティのため、この方式を使用しないでください。
- **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とき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。

II. 許可方式

装置は、以下の許可方式をサポートします。

- **許可なし** ― NAS は許可情報の交換を行いません。ユーザが認証にパスした後、以下のデフォルト許可情報を適用します。
  - 非ログインユーザはネットワークにアクセスできます。
  - ログインユーザはデフォルトユーザロールに割り当てられます。ユーザロールの詳細はセクション 1 *はじめにオペレーションマニュアル*の”*RBAC*”を参照してください。
  - FTP、TFTP ログインユーザは、NAS のルートディレクトリが作業ディレクトリとなりますが、ユーザはルートディレクトリにアクセスできません。
- **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。

III. アカウンティング方式

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。

1.1.6. 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*

1.2. 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 方式は設定された RADIUS スキームを参照します。

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、どちらか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) 拡張AAA機能の設定 • 同時ログインユーザの最大数の設定

1.3. ローカルユーザの設定

1.3.1. ローカルユーザの概要

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**－装置の管理を行うために、装置にログインします。
- **ネットワークアクセスユーザ**－装置を経由してネットワークのリソースにアクセスするユーザです。

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。もし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（端末）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。**blocked** のユーザは使用中のアカウンティングサービスを停止するリクエストのみ行うことができます。
- **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とき、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、パスワード管理属性、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、セクション 8 *セキュリティ オペレーションマニュアル*の”*AAA*”の”*ユーザグループ属性の設定*”を参照してください。
- **Binding 属性**－Binding 属性は、ユーザの範囲を管理し、ユーザのローカル認証を行う際に確認します。属性がローカルユーザのアカウント用に設定されたユーザの属性に一致しない場合、ユーザは認証をパスすることができません。Binding 属性は IP アドレス、アクセスポート、MAC アドレス、VLAN（Native VLAN）があります。Binding 属性の詳細は、セクション 8 *セキュリティ オペレーションマニュアル*の”*AAA*”の”*ローカルユーザ属性の設定*”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、セクション 8 *セキュリティ オペレーションマニュアル*の”*AAA*”の”*ローカルユーザ属性の設定*”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、セクション 8 *セキュリティ オペレーションマニュアル*の”*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 あるいは local user view で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は user group view で設定した許可属性よりも優先されます。

  - local user view で設定した許可属性の設定は、user group のすべてのローカルユーザに適用されます。
  - local user view で設定した許可属性の設定は、ローカルユーザでのみ適用されます。

- **パスワード管理属性**－パスワード管理属性は装置管理ユーザのパスワードのセキュリティを容易に管理するようにするサービスタイプです。パスワード管理属性は、パスワードの有効期限、最小パスワード長、パスワード構成の確認、パスワードの複雑さの確認、ログイン試行制限を含みます。

system view、user group view、local user view でパスワード管理属性を設定することができます。狭い範囲の view で設定した許可属性の設定は、優先度が高くなります。パスワード管理とグローバルパスワードの設定についての詳細は、セクション 8 *セキュリティ オペレーションマニュアル*の”*パスワード管理*”を参照してください。

1.3.2. 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 • 装置管理ユーザ属性の設定 • ネットワークアクセスユーザ属性の設定
(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

1.3.3. 装置管理ユーザ属性の設定

I. 制限とガイドライン

ローカルユーザ属性の設定を行うとき、以下のガイドラインに従ってください。

- **password-control enable** コマンドを使用して、パスワード管理機能がグローバルで有効なとき、ローカルユーザパスワードは表示されません。
- local user view あるいは user group view で許可属性、パスワード管理属性を設定することができます。local user view で設定した値が user group view で設定した値よりも優先されます。
- アプリケーション環境と目的に従って許可属性を設定してください。ユーザのサービスタイプに依存して許可属性をサポートします。
  - LAN ユーザの許可属性はユーザプロファイル、VLAN が有効です。
  - Telnet、ターミナルユーザの許可属性は idle-cut、user-role が有効です。
  - SSH ユーザの許可属性は idle-cut、user-role、work-directory が有効です。
  - FTP ユーザの許可属性は user-role、work-directory が有効です。
  - ローカルユーザの他のタイプの許可属性で有効な属性はありません。
- ユーザのサービスタイプにもとづいて binding 属性を設定します。
  - 802.1X ユーザの binding 属性は、ユーザが装置にアクセスするインタフェースとして 802.1X をサポートするレイヤ 2 Ethernet インタフェースが有効です。
  - MAC アドレス認証ユーザの binding 属性は、ユーザが装置にアクセスするインタフェースとして MAC アドレス認証をサポートするレイヤ 2 Ethernet インタフェースが有効です。

II. 設定方法

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**]	デフォルト：設定なし

操作	コマンド	補足
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** } *password*]	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	**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) ローカルユーザの許可属性を設定する	**authorization-attribute** { **idle-cut** *minute* | **user-role** *role-name* | **work-directory** *directory-name* } *	デフォルト：以下に示します。 • 装置のルートディレクトリへ許可された FTP または SFTP ユーザがアクセスする場合、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。 Telnetユーザ、端末ユーザは**user-role**の設定のみ適用されます。 SSH、FTPユーザは**user-role**、**work-directory**の設定のみ適用されます。 ローカルユーザの他のタイプは許可属性に適用されません。

操作	コマンド	補足
8. (オプション設定項目) ローカルユーザのパスワード管理属性を設定する	• パスワードエージング時間を設定する: **password-control aging** *aging-time* • 最小パスワード長を設定する: **password-control length** *length* • パスワード構成ポリシーを設定する: **password-control composition type-number** *type-number* [**type-length** *type-length*] • パスワード複雑性のポリシーを設定する: **password-control complexity** { **same-character** | **user-name** } **check** • ログイン最大再試行回数と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を設定する: **password-control login-attempt** *login-times* [**exceed** { **lock** | **lock-time** *time* | **unlock** }]	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管理の属性を使用します。 パスワード管理機能をサポートしている装置管理ユーザのみ適用されます。
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。

1.3.4. ネットワークアクセスユーザ属性の設定

I. 制限とガイドライン

許可属性は、local user view もしくは user group view で設定可能です。local user view での設定は、user group view での設定より優先して実行されます。

ユーザのサービスタイプに応じて **location** binding 属性を設定します。

- 802.1X ユーザの場合、802.1X が有効なレイヤ 2 イーサネットインタフェース、もしくはレイヤ 2 アグリゲートインタフェースを指定します。
- MAC アドレス認証ユーザの場合、MAC アドレス認証が有効なレイヤ 2 イーサネットインタフェース、もしくはレイヤ 2 アグリゲートインタフェースを指定します。

- Web 認証ユーザの場合、Web 認証が有効なレイヤ 2 イーサネットインタフェース、もしくはレイヤ 2 アグリゲートインタフェースを指定します。

II. 設定方法

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. ネットワークアクセスユーザを追加し、network access user view に移行する	**local-user** *user-name* **class 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** } *password*	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	**service-type lan-access**	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 binding 属性を指定する	**bind-attribute** { **ip** *ip-address* | **location** **interface** *interface-type interface-number* | **mac** *mac-address* | **vlan** *vlan-id* } *	デフォルト：設定なし binding属性は802.1Xを使用したLANユーザのみ適用されます。 Binding属性は、位置情報、MACアドレス、VLANです。
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* | **vlan** *vlan-id* } *	デフォルト：設定なし
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。

1.3.5. ユーザグループ属性の設定

I. ユーザグループ属性の概要

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。パスワード管理属性と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。

II. 設定方法

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**	―
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* | **vlan** *vlan-id* | **work-directory** *directory-name* } *	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) ユーザグループのパスワード管理属性を設定する	• パスワードエージング時間を設定する: **password-control aging** *aging-time* • 最小パスワード長を設定する: **password-control length** *length* • パスワード構成ポリシーを設定する: **password-control composition type-number** *type-number* [**type-length** *type-length*] • パスワード複雑性のポリシーを設定する: **password-control complexity** { **same-character** | **user-name** } **check** • ログイン最大再試行回数と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設定を使用します。 詳細は、セクション8 *セキュリティオペレーションマニュアルの”パスワード管理”* を参照してください。

1.3.6. 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* }

1.4. 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。

1.4.1. 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 RADIUS認証サーバあるいはアカウンティングサーバを設定している場合、共有鍵の設定は必要ありません。
(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) RADIUSサーバのタイマ機能の設定
(オプション設定項目) RADIUSパケットのパラメータの設定 • 出力する RADIUS パケットの送信元 IP アドレスの指定 • 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 • RADIUS 要求の再送信の最大試行回数の設定 • RADIUS アカウンティング要求の最大試行回数の設定 • RADIUS パケットの DSCP 優先度の設定
(オプション設定項目) 拡張RADIUS機能の設定 • RADIUS アカウンティング停止要求パケットのバッファの設定 • RADIUS accounting-on 機能の設定 • RADIUS の SNMP notification の通知の有効化 • 再認証を行う際の RADIUS サーバ選択モードの設定

1.4.2. RADIUS 設定の制限とガイドライン

RADIUS スキームの認証サーバが、装置の RADIUS サーバ機能により提供される場合、RADIUS スキームは以下の設定のみを含みます。

- RADIUS 認証サーバ
- RADIUS 通信を行うための共有鍵
- RADIUS サーバ間で使用するユーザ名フォーマット

1.4.3. RADIUS スキームの作成

I. 制限とガイドライン

他の 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。

II. 設定方法

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：RADIUSスキーム名がsystemのRADIUSスキームが定義されます。

1.4.4. RADIUS 認証サーバの指定

I. RADIUS 認証サーバの概要

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とき、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。

II. 制限とガイドライン

冗長性が必要とされない場合、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、他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。

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、ホスト名を設定することはできません。

III. 設定手順

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*	―

操作	コマンド	補足
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** { *host-name* | *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** { *host-name* | *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

1.4.5. RADIUS アカウンティングサーバの指定

I. RADIUS アカウンティングサーバの概要

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とき、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。

冗長性が必要とされない場合、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、他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。

II. 制限とガイドライン

冗長性が必要とされない場合、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、他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。

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、ホスト名を設定することはできません。

RADIUS は FTP、SFTP、SCP ユーザのアカウンティングをサポートしていません。

III. 設定手順

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** { *host-name* | *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** { *host-name* | *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

1.4.6. セキュアな RADIUS 通信を行うための共有鍵の指定

I. セキュアな RADIUS 通信を行うための共有鍵

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。

II. 制限とガイドライン

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。

III. 設定手順

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**	―

操作	コマンド	補足
2. RADIUS scheme view に移行する	**radius scheme** *radius-scheme-name*	―
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

1.4.7. 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ときに、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** 状態のとき、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とき、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。
  - 最も高い優先度をもつ **active** 状態のセカンダリサーバと通信するためサーバを検索します。
- もしセカンダリサーバが有効でなくなったとき、装置は以下の処理を行います。
  - 装置は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。
  - 最も高い優先度をもつ **active** 状態の次のセカンダリサーバと通信するためサーバを検索します。
- この検索プロセスは、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。有効なサーバがない場合、装置は認証あるいはアカウンティングプロセスが失敗したと認識します。
- quiet タイマが終了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。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。
- もし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。装置は最初から **active** 状態のサーバを検索します。最初にプライマリサーバ(もしある場合)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。
- プライマリサーバとセカンダリサーバの両方が **blocked** 状態の場合、装置はプライマリサーバと通信しようとします。
- 1 つ以上のサーバが **active** 状態で、他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** [{ *host-name* | *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** [{ *host-name* | *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。

1.4.8. 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とき、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とき、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とき、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 1000 以上の場合、15 分以上の間隔にしてください。

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** *minutes*	デフォルト：12分

1.4.9. 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アドレスが管理されたNASのIPアドレスかどうか確認します。

- パケットの送信元IPアドレスが管理されたNASのIPアドレスにマッチしている場合、サーバはパケットの処理を行います。
- パケットの送信元IPアドレスが管理されたNASのIPアドレスにマッチしていない場合、サーバは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、RADIUSサーバと通信するNAS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で、またはsystem viewにて、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

以下にすべてのRADIUSスキームの送信元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. 出力するRADIUSパケットの送信元IPアドレスを指定する	**radius nas-ip** { *ipv4-address* | **ipv6** *ipv6-address* }	デフォルト：RADIUSパケットを送信するインタフェースのIPアドレスが指定されます。

以下に指定されたRADIUSスキームの送信元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. 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IPアドレスを指定する	**nas-ip** { *ipv4-address* | **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。設定されていない場合、RADIUSパケットを送信するインタフェースのIPアドレスが指定されます。

1.4.10. 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通知します。トラフィックのデータフローの単位は設定可能ですが、RADIUS アカウンティングサーバで設定したトラフィックのデータフローの単位と同一にしてください。

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：RADIUSスキーム名がsystemのRADIUSスキームを除くデフォルトはwith-domainです。RADIUSスキーム名がsystemのRADIUSスキームのデフォルトはwithout-domainです。
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

1.4.11. RADIUS 要求の再送信の最大試行回数の設定

RADIUS はデータを送信する際に 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、セクション 8 *セキュリティ オペレーションマニュアル*の”*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

1.4.12. RADIUS アカウンティング要求の最大試行回数の設定

I. RADIUS アカウンティング要求の最大試行回数の設定

リアルタイムアカウンティングの最大試行回数を設定した場合、装置は指定した回数以内に応答がないユーザを切断します。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. RADIUS scheme view に移行する	**radius scheme** *radius-scheme-name*	―
3. (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

1.4.13. RADIUS パケットの DSCP 優先度の設定

ToS フィールド内の DSCP 優先度により RADIUS パケットの転送優先度が決定されます。値が大きいほど優先度は高くなります。

以下に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. RADIUS パケットに DSCP 優先度を設定する	**radius** [**ipv6**] **dscp** *dscp-value*	デフォルト：0

1.4.14. RADIUS アカウンティング停止要求パケットのバッファの設定

装置は、ホストあるいは管理者から接続切断要求を受信した場合、RADIUS アカウンティング停止要求を送信します。ただし、1回の送信で停止アカウンティング要求の応答を受信できない場合があります。アカウンティングサーバから応答を受信していない RADIUS 停止アカウンティング要求をバッファするようにします。装置は応答が受信されるまで要求を再送します。

送信間隔を制限するには、それぞれの RADIUS 停止アカウンティング要求に対して実行できる送信試行の最大数を設定します。要求に対して最大試行が行われると、装置はバッファ要求を破棄します。

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. 応答がない 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
4. (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 S る鵜	**retry stop-accounting** *retries*	デフォルト：500

1.4.15. RADIUS accounting-on 機能の設定

accounting-on 機能が有効になっている場合、装置は装置全体を再起動した後、自動的にアカウンティングパケットを RADIUS サーバに送信します。accounting-on パケットを受信すると、RADIUS サーバはすべてのオンラインユーザをログアウトさせ、装置を介して再びログインできるようにします。この機能がないと、RADIUS サーバがオンラインになると見なされるため、再起動後に再度ログインできなくなります。

装置が account-on パケットを再送する間隔と最大再試行回数を設定できます。

拡張 accounting-on 機能は分散アーキテクチャにおけるアカウンティング機能を拡張します。

拡張アカウンティング機能は LAN ユーザに有効です。ユーザデータは、ユーザがシステムにアクセスする IRF スタックメンバ装置に保存されます。拡張アカウンティング機能が有効になっている場合、メンバ装置が再起動すると、システムは自動的にアカウンティングパケットを RADIUS サーバに送信します。パケットにメンバ装置の識別子が含まれています。accounting-on パケットを受信すると、RADIUS サーバは、メンバ装置を経由してシステムにアクセスするすべてのオンラインユーザをログアウトします。メンバ装置経由でユーザがオンラインになっていない場合、IRF スタックユニットはメンバ装置の再起動後にアカウンティングパケットを送信しません。

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. RADIUS scheme view に移行する	**radius scheme** *radius-scheme-name*	ー
3. accounting-on を有効にする	**accounting-on enable** [**interval** *interval* | **send** *send-times*]	デフォルト：無効

1.4.16. RADIUS の SNMP notification の通知の有効化

RADIUS の SNMP notification が有効であるとき、SNMP エージェントは RADIUS によって作成された以下の notification をサポートします。

- **RADIUS server unreachable notification**ー RADIUS サーバに通信できません。指定した RADIUS 要求の再送信の最大試行回数以内にアカウンティング要求あるいは認証要求に対する応答を受信できない場合、RADIUS は notification を作成します。
- **RADIUS server reachable notification**ー RADIUS サーバと通信できます。RADIUS サーバが停止タイマの満了後、以前にブロックされた RADIUS サーバに対して notification を作成します。
- **Excessive authentication failures notification**ー認証を行った際、失敗した総数が指定したしきい値を超過しています。

SNMP notification の出力を制御する SNMP パラメータを設定することができます。詳細はセクション 10 *システム管理オペレーションマニュアル*の“*SNMP*”を参照してください。

以下に SNMP notification の通知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. RADIUS の SNMP notification の通知を有効にする	**snmp-agent trap enable radius** [**accounting-server-down** | **accounting-server-up** | **authentication-error-threshold** | **authentication-server-down** | **authentication-server-up**] *	デフォルト：有効

1.4.17. 再認証を行う際の RADIUS サーバ選択モードの設定

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
3. system view に移行する	**system-view**	―
4. RADIUS scheme view に移行する	**radius scheme** *radius-scheme-name*	―
5. 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**

📖 メモ：

reauthentication server-select コマンドは Version 7.1. 8 を含む以降のソフトウェアからサポートしています。

1.4.18. 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**
応答がないADIUSストップアカウンティング要求のバッファの情報を表示する	**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削除する	**reset radius statistics**
応答がないADIUSストップアカウンティング要求のバッファの情報を削除する	**reset stop-accounting-buffer** { **radius-scheme** *radius-scheme-name* | **session-id** *session-id* | **time-range** *start-time end-time* | **user-name** *user-name* }

1.5. ISPドメインの作成

1.5.1. 概要

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。もし 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。

制限とガイドライン

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。詳細はセクション 8 *セキュリティ オペレーションマニュアル*の”*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セクション 8 *セキュリティ オペレーションマニュアル*の”*AAA*”の”*RADIUS スキームの設定*”を参照してください。

複数の ISP をも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)をもち、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。もしユーザがログインするとき、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。

1.5.2. 制限とガイドライン

ISP ドメインがデフォルト ISP ドメインである場合、削除することはできません。

デフォルト ISP ドメインの設定を削除する場合、**undo domain default enable** コマンドを使用して、最初にデフォルトの ISP ドメインを変更してください。

デフォルト ISP ドメイン **system** の設定を変更することはできますが、ドメインを削除することはできません。

1.5.3. ISP ドメインの作成

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*	―

1.5.4. デフォルト ISP ドメインの指定

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) 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

1.6. 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。

1.6.1. ISP ドメインの属性の設定

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*	―
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。

1.7. ISPドメインのAAA方式の設定

1.7.1. 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とき、以下のガイドラインに従ってください。

- RADIUS スキームを参照する認証方式と、RADIUS スキームを参照しない許可方式を設定するとき、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. （オプション設定項目）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. LAN ユーザの認証方式を指定する	**authentication lan-access** { **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。
5. 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。

1.7.2. 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 ユーザのコマンド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。

1.7.3. 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とき、以下のガイドラインに従ってください。

- FTP 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 ユーザの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。

1.7.4. ISP ドメインの表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
ISPドメインの設定を表示する	**display domain** [*isp-name*]

1.8. 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

1.9. AAAの設定例

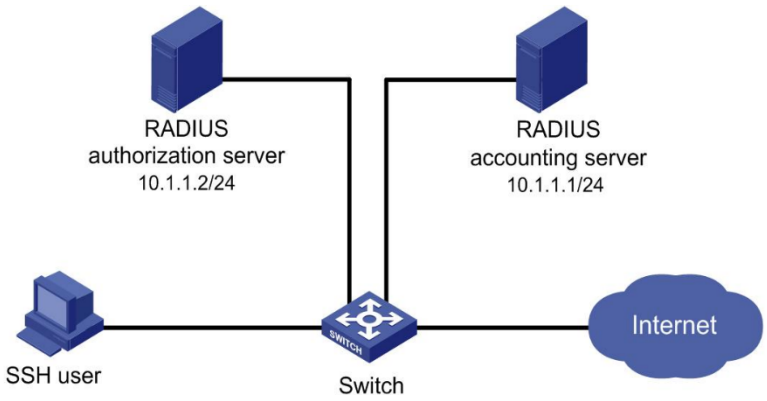
1.9.1. SSH ユーザのローカル認証、RADIUS アカウンティングの設定例

I. ネットワーク要件

図 1-7 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 1-7 ネットワーク図



II. 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

III. 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とき、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。

1.10. RADIUSのトラブルシューティング

1.10.1. RADIUS 認証の失敗

I. 症状

認証が常に失敗します。

II. 分析

問題の原因は以下のものが考えられます。

- 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

問題を解決する場合、以下を行ってください。

1) 以下の項目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。
2) 問題が解決しない場合、NEC に問い合わせてください。

1.10.2. 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

問題の原因は以下のものが考えられます。

- 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他のアプリケーションで使用されています。

III. 解決策

問題を解決する場合、以下を行ってください。

1) 以下の項目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。

2) 問題が解決しない場合、NEC に問い合わせてください。

1.10.3. RADIUS アカウンティングエラー

I. 症状

ユーザは認証と許可にパスしましたが、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。問題の原因は以下のものが考えられます。

- 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

問題を解決する場合、以下を行ってください。

1) 以下の項目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。
2) 問題が解決しない場合、NEC に問い合わせてください。

1.11. 付録

1.11.1. 一般的に使用される RADIUS 属性

一般的に使用される RADIUS 属性は、RFC 2865、RFC 2866、RFC 2867、RFC 2868 により定義されています。

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

No.	属性	No.	属性
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

1.11.2. 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。
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。

番号	属性	説明
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 です。 • 2 – Stop です。 • 3 – Interim-Update です。 • 4 – Reset-Charge です。 • 7 – Accounting-On です。(第 3 世代(3G)移動体通信システムの標準化プロジェクト)で定義されました。) • 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)で定義されました。) • 9 ～ 14–トンネルアカウンティング用に予約済みです。 • 15 – 故障用に予約済みです。
45	Acct-Authentic	ユーザによって使われる認証方式です。 • 1 – RADIUS です。 • 2 – Local です。 • 3 – Remote です。
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 です。 • 16 – ADSL のすべてのタイプです。 • 17 – ケーブル (ケーブル TV 用) です。 • 19 – WLAN-IEEE 802.11 です。 • 201 – VLAN です。 • 202 – ATM です。 もしポートが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ときに使われます。

番号	属性	説明
87	NAS-Port-Id	ユーザを認証しているNASのポートです。

1.11.3. 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への最大レートです。単位はbpsです。
2	Input-Average-Rate	ユーザからNASへの平均レートです。単位はbpsです。
3	Input-Basic-Rate	ユーザからNASへの基本レートです。単位はbpsです。
4	Output-Peak-Rate	NASからユーザへの最大レートです。単位はbpsです。
5	Output-Average-Rate	NASからユーザへの平均レートです。単位はbpsです。
6	Output-Basic-Rate	NASからユーザへの基本レートです。単位は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 です。 • 2–Terminate-Request です。 • 3–SetPolicy です。 • 4–Result です。 • 5–PortalClear です。
24	Control_Identifier	再送パケット用の識別子です。同一セッションの再送されたパケット用の属性は同じ値を使用する必要があります。異なるセッションの再送されたパケット用の属性は同じ値としてもいいです。再送パケットのクライアントの応答は、この属性をもち、属性の値は同一にしなくてはいけません。 start、stop、interim updateタイプのAccounting-Requestパケットのための Control-Identifier属性がある場合、値は意味をなしません。
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とき、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。

番号	属性	説明
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、デバイス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	SSL VPNユーザが認証をパスした後､割り当てられるユーザグループです。ユーザは複数のユーザグループに属することができます。ユーザグループは、セミコロンで区切られます｡この属性はSSL VPNデバイスと共有するために使われます。
141	Security_Level	SSL VPNユーザがセキュリティ認証をパスした後､割り当てられるセキュリティレベルです。
201	Input-Interval-Octets	実時間のアカウンティング間隔に入力したバイト数です。
202	Output-Interval-Octets	実時間のアカウンティング間隔に出力したバイト数です。
203	Input-Interval-Packets	デバイスでのユニットセットにおけるアカウンティング間隔に入力したパケット数です。
204	Output-Interval-Packets	デバイスでのユニットセットにおけるアカウンティング間隔に出力したパケット数です。
205	Input-Interval-Gigawords	4Gバイトで分割されたアカウンティング間隔に入力したバイト数の結果です。
206	Output-Interval-Gigawords	4Gバイトで分割されたアカウンティング間隔に出力したバイト数の結果です。
207	Backup-NAS-IP	RADIUSパケットを送信するためのバックアップの送信元IPアドレスです。
255	Product_ID	装置名です。

目次

このセクションのページは **8-x-x** です。

2 章 802.1X の概要 2-1
2.1. 802.1X の概要 2-1
2.1.1. 802.1X の構成 2-1
2.1.2. 制御/非制御ポートとポート許可状態 2-1
2.1.3. パケット交換方式 2-2
2.1.4. パケットフォーマット 2-3
2.1.5. 802.1X の認証プロセス 2-6
2.1.6. 802.1X 認証の開始 2-8
2.2. アクセス制御方式 2-9
2.3. 802.1X の VLAN 操作 2-9
2.3.1. 許可 VLAN 2-9
2.3.2. ゲスト VLAN 2-12
2.3.3. 制限 VLAN 2-14
2.4. ACL の割り当て 2-15
2.5. 定期的な 802.1X 再認証 2-15

2章 802.1X の概要

2.1. 802.1Xの概要

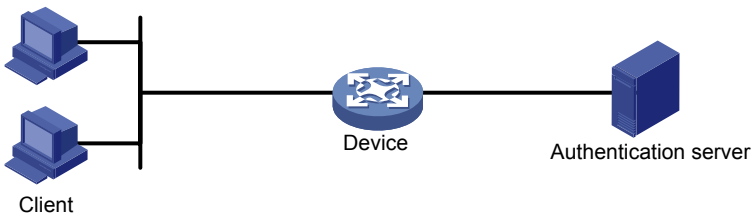
802.1X は、無線 LAN（WLAN）のセキュリティを行うため、最初に提案されたポートベースのネットワークアクセス制御プロトコルです。一般的なポートアクセス制御のメカニズムとして Ethernet で幅広く使用されています。

2.1.1. 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デバイスを認証する 802.1X ソフトウェアが必要です。
- **アクセスデバイス（オーセンティケータ）**－ネットワークアクセスデバイスは、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デバイスは、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デバイス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デバイス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デバイス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デバイスを使用することもできます。

図 2-1 802.1X の構成



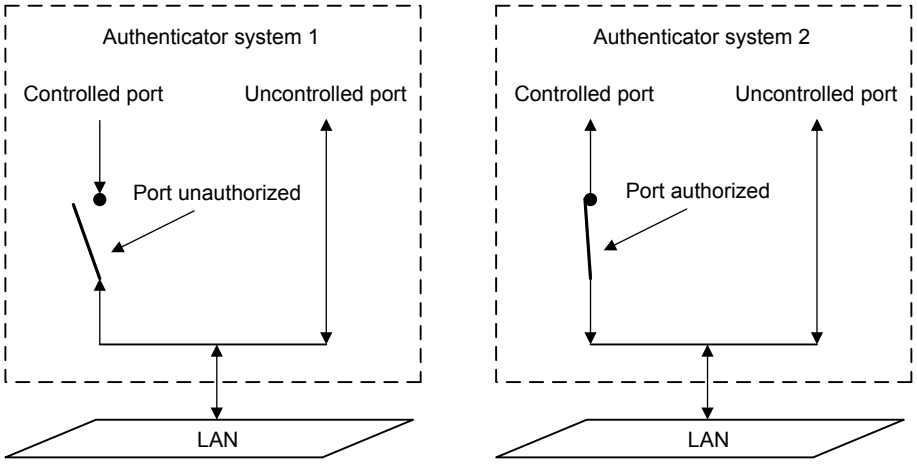
2.1.2. 制御/非制御ポートとポート許可状態

802.1X は、ネットワークのアクセスポートのために、制御ポートと非制御ポートの 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**ークライアントが認証にパスしたとき、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**ークライアントが認証にパスしないとき、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。本デバイス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



2.1.3. パケット交換方式

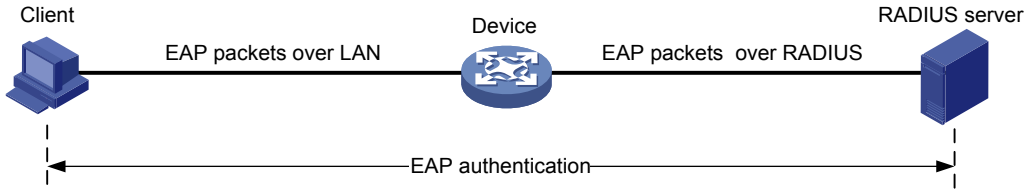
802.1X は、EAP (Extensible Authentication Protocol)を使用して、クライアント、アクセスデバイス、および認証サーバの認証情報を転送します。EAP は、クライアント/サーバモデルを使用する認証フレームワークです。このフレームワークは、MD5-Challenge、EAP-TLS(EAP-Transport Layer Security)、PEAP(Protected EAP)など、さまざまな認証方式をサポートしています。

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デバイスの間に EAP パケットを渡す EAPOL(EAP over LAN)を定義します。アクセスデバイスと認証サーバの間には、EAP relay モードまたは EAP termination モードの認証情報が 802.1X に送信されます。

I. 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、ネットワークデバイスは、図 2-3 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 2-3 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デバイス上では、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。

II. EAP termination モード

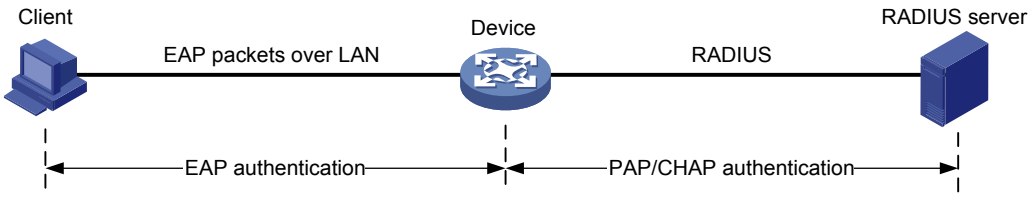
図 2-4 に示すように、アクセスデバイスは EAP termination モードで以下の動作を行います。

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 2-4 EAP termination



III. 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。 • アクセスデバイス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。

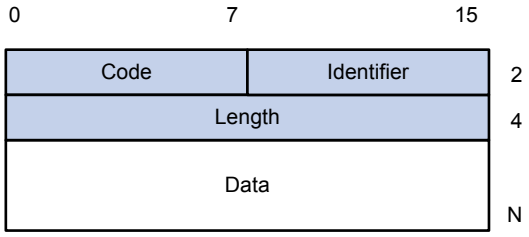
EAP termination	PAPまたはCHAP認証をサポートしている任意のRADIUSサーバと連携して動作します。	• 以下の EAP 認証方式のみをサポートします。
		  • MD5-Challenge EAP 認証
		  • ユーザ名とパスワードの EAP 認証
		• アクセスデバイス上の処理が複雑です。

2.1.4. パケットフォーマット

I. EAP パケットのフォーマット

図 2-5 に EAP パケットのフォーマットを示します。

図 2-5 EAP パケットのフォーマット

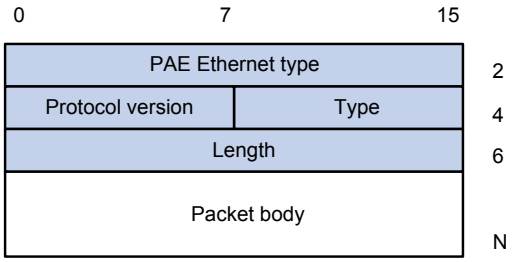


- **Code**－EAP パケットのタイプです。Request(1)、Response(2)、Success(3)、Failure(4)があります。
- **Identifier**－リクエストとレスポンスを対応づけます。
- **Length**－EAP パケット長（byte）です。Code、Identifier、Length、Data フィールドの合計です。
- **Data**－EAP パケットの中身です。このフィールドは、リクエストまたはレスポンス EAP パケットにのみあります。リクエストタイプ（またはレスポンスタイプ）とタイプデータで構成されています。タイプ 1（Identify）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 2-6 に EAPOL パケットのフォーマットを示します。

図 2-6 EAPOL パケットのフォーマット



- **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デバイスは、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デバイスにEAPOL-Startメッセージを送ります。

値	タイプ	説明
0x02	EAPOL-Logoff	クライアントは、ログオフを通知するために、アクセスデバイスにEAPOL-Logoffメッセージを送ります。

- **Length**ーデータ長（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**ー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。

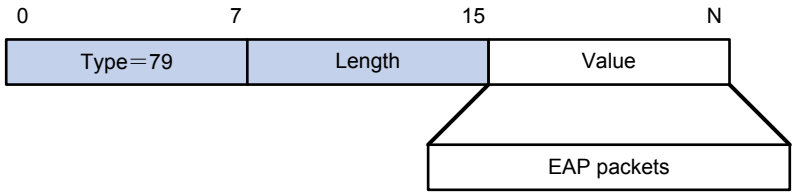
III. EAP over RADIUS

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、セクション 8 *セキュリティ オペレーションマニュアル*の"*AAA*"を参照してください。

- EAP-Message

  図 2-7 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 2-7 EAP-Message の属性フォーマット

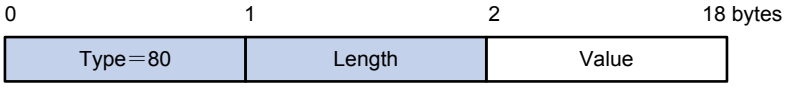


- Message-Authenticator

  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 2-8 Message-Authenticator の属性フォーマット



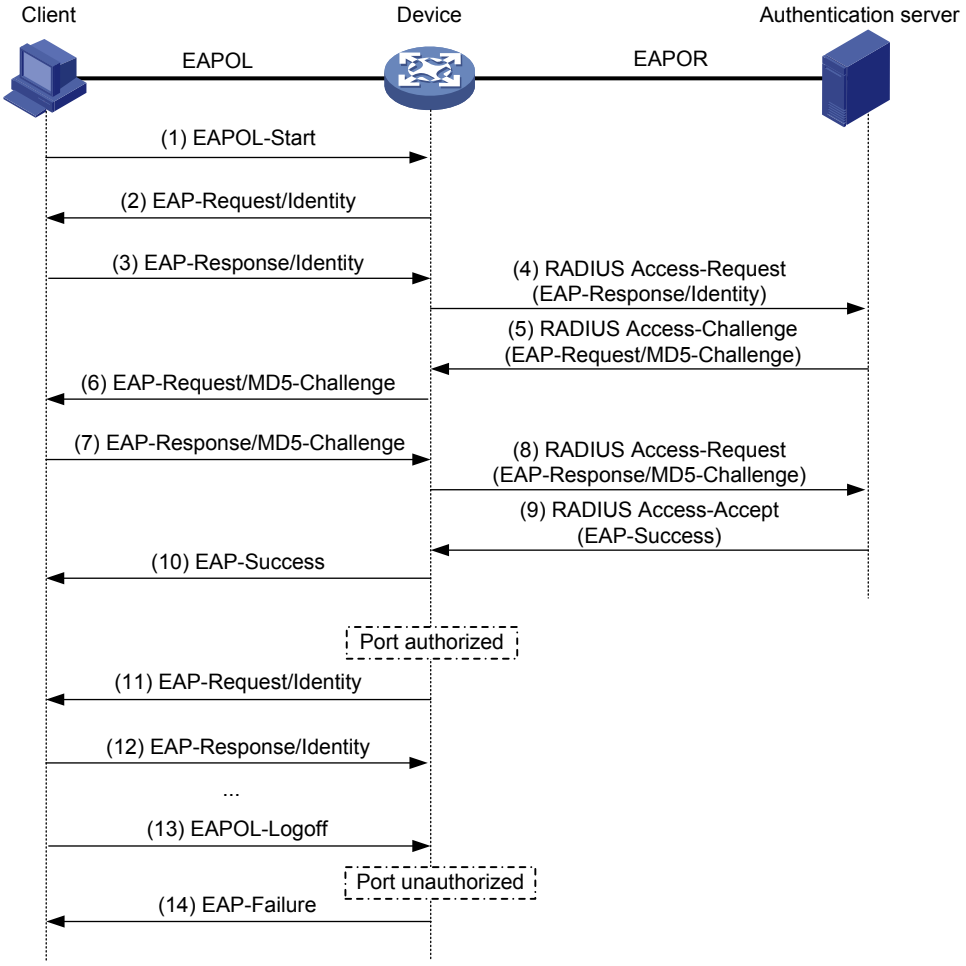
2.1.5. 802.1X の認証プロセス

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。

I. EAP relay モード

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、アクセスデバイスに EAPOL-Start パケットを送信します。
2) アクセスデバイスは、応答としてクライアントのユーザ名を要求するために Identity EAP-Request パケットを送信します。
3) Identity EAP-Request パケットの応答として、クライアントは Identity EAP-Response パケットの中にユーザ名を入れて、アクセスデバイスに送信します。
4) アクセスデバイスは、RADIUS Access-Request パケットの Identity EAP-Response 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デバイスにチャレンジ情報を送信します。

6) アクセスデバイスは、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デバイスに送信します。

8) アクセスデバイスは、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、アクセスデバイスに 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、アクセスデバイスは、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、アクセスデバイス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、デバイス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、アクセスデバイスは、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。

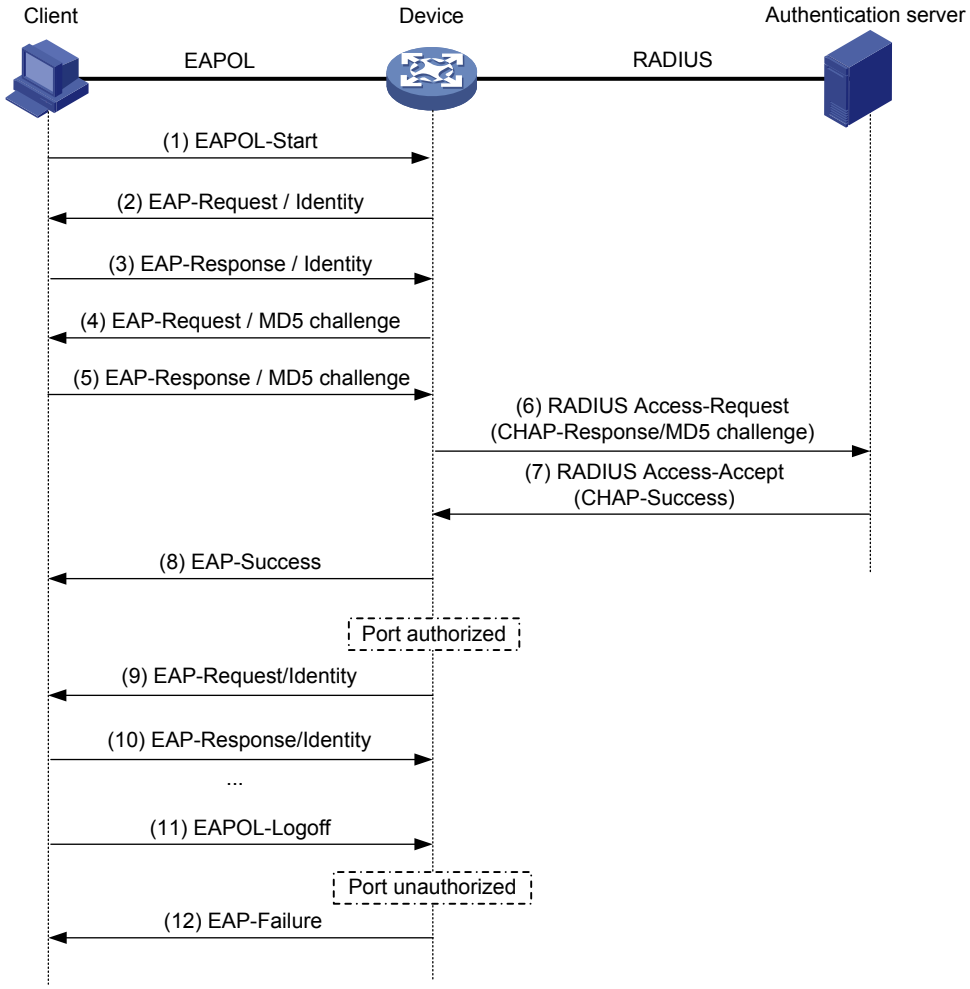
13) クライアントは、アクセスデバイスにログオフを依頼する EAPOL-Logoff パケットを送信することもできます。

14) EAPOL-Logoff パケットに応答して、アクセスデバイスは、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。

II. 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、アクセスデバイスです。アクセスデバイスは次に、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。

2.1.6. 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。

I. 802.1X クライアントからの認証開始

クライアントは、アクセスデバイスに 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デバイス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。

II. アクセスデバイスからの認証開始

クライアントが EAPOL-Start パケットを送信できない場合、アクセスデバイスが認証を開始します。たとえば 802.1X クライアントは Windows XP で使用できます。

アクセスデバイスは、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**－アクセスデバイスが、定期的に（デフォルトでは 30 秒ごと）Identity EAP-Request 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とき、アクセスデバイスは受信ポートから未知の MAC アドレスへ Identity EAP-Request 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。このプロセスは **dot1x retry** コマンドを使用してクライアントに認証要求を送信する最大試行回数になるまで行われます。

ユーザ名の要求のタイムアウトタイマはマルチキャストトリガ Identity Request 間隔とユニキャストトリガ Identity Request 間隔の両方を設定します。

2.2. 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**－ポートベースのアクセス制御では、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**－MAC ベースのアクセス制御では、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。

2.3. 802.1XのVLAN操作

2.3.1. 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. リモート VLAN 許可

リモート VLAN 認証では、リモートサーバに許可 VLAN 情報を指定する必要があります。ユーザが認証をパスすると、サーバはその情報をデバイスに割り当てます。デバイスは許可 VLAN 情報を解決し、ユーザのアクセスポートをタグ付きまたはタグなしメンバとして許可 VLAN に割り当てます。解決が失敗すると、ユーザは認証に失敗します。

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、セクション 3 *アクセス オペレーションマニュアル*の”*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。

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
- プライベート VLAN

サーバが VLAN のグループを割り当てるとき、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 2-2 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 2-2 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
	デバイスは、ポートで他のオンラインユーザがいるかどうかに依存して、許可VLANとしてVLANを選択します。
	• ポートで他のオンラインユーザがいない場合、デバイスはVLANのグループからもっとも小さいIDのVLANを選択します。
	• ポートで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。
	  • デバイス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 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、デバイスはもっとも小さい ID の VLAN を選択します。
	セクション8 *セキュリティ オペレーションマニュアル*の“*802.1X*”の“*VLAN操作*”にデバイスがVLANの割り当てを行うルールを示します。

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	• デバイス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。 • デバイスは 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。もしタグなし 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。デバイスはタグなし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。

II. 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。ユーザが装置にアクセスする際に経由するポートは、タグなしメンバとして VLAN に割り当てられます。タグ付き VLAN の割り当てはサポートされていません。

ローカルユーザの詳細はセクション 8 *セキュリティ オペレーションマニュアル*の”*AAA*”を参照してください。

III. 802.1X が有効なポートでの VLAN 許可操作

表 2-3 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 2-3 VLAN 操作

ポートアクセス制御方式	VLAN 操作
ポートベース	デバイスはPVIDとしてポートに許可VLANを割り当てます。 認証された802.1Xユーザと後続のすべての802.1Xユーザは認証なしでアクセスできます。 ユーザがログオフすると、以前のPVIDがもとに戻り、他のオンラインユーザがログオフされます。

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、デバイスは許可 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、初期に認証されたユーザの VLAN が PVID としてポートに割り当てられます。異なる VLAN が後続のユーザによって許可されると、ユーザは認証をパスすることができません。後続のユーザの認証を成功させるために、ポートのすべての 802.1X ユーザに同じ VLAN を許可してください。

重要 ：

802.1X 対応アクセスポートは、タグなしメンバとしてのみ許可 VLAN に割り当てることができます。

ハイブリッドポートは、常にタグなしメンバとして VLAN に割り当てられます。割り当てられたのち、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。

許可されていない VLAN がユーザに割り当てられている場合、ハイブリッドポートでネットワークにアクセスする 802.1X 認証ユーザは以下のいずれか処理を行います。

- VLAN のユーザからタグ付きの認証パケットを受信した場合、**port hybrid vlan** コマンドを使用して VLAN のタグ付きメンバとしてポートを設定します。
- VLAN のユーザからタグなしの認証パケットを受信した場合、**port hybrid vlan** コマンドを使用して VLAN のタグなしメンバとしてポートを設定します。

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、セクション 3 *アクセス オペレーションマニュアル*の”*VLAN*”を参照してください。

2.3.2. 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。

I. 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	デバイスは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、セクション8 *セキュリティ オペレーショマニュアルの”802.1X”の”制限VLAN”*を参照してください）が有効である場合、デバイスは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	• デバイスは 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。

⚠ **重要　：**

VLAN がゲスト VLAN ではない場合にポートが VLAN タグつきのパケットを受信すると、そのパケットはタグ付き VLAN 内に転送されます。

II. 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	デバイスはユーザの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、デバイスはユーザの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。

認証状態	VLAN 操作
802.1XゲストVLANのユーザが802.1X認証に成功した	デバイスはユーザの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、デバイスはユーザのMACアドレスをポートの初期のPVIDに再マッピングします。

2.3.3. 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。

アクセス装置は、802.1X アクセス制御方式に基づき、802.1X が有効なポートで VLAN を扱います。

I. 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	デバイスは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	デバイスは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。 🕮 **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。

II. 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	デバイスはユーザの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	デバイスはユーザの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、デバイスはユーザのMACアドレスをポートの初期のPVIDに再マッピングします。

2.4. 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、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。

ユーザのアクセス制御基準を変更する場合、以下のいずれかの方法を使用することができます。

- アクセス装置で ACL のルールを変更します。
- 認証サーバで別の許可 ACL を設定します。

サポートされている許可 ACL は以下のタイプがあります。

- 標準 ACL（ACL の番号：2000～2999）
- 拡張 ACL（ACL の番号：3000～3999）

許可 ACL を適用する場合、ACL が存在し、**counting**、**established**、**fragment**、**logging** パラメータを除く ACL ルールが存在することを確認してください。

ACL の詳細は、セクション 8 *ACL and QoS オペレーションマニュアル*の”*ACL*”を参照してください。

2.5. 定期的な802.1X再認証

定期的なオンラインユーザの再認証は、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。

ポートで定期的なオンラインユーザの再認証を有効にした場合、装置は指定された定期的な再認証の間隔でポート上のオンライン 802.1X ユーザを再認証します。再認証の間隔は、ユーザ側で設定できます。古い再認証タイマが終了した後、新しく設定された再認証の間隔が適用されます。

サーバが割り当てた session timeout タイマ（Session-Timeout 属性）と termination アクション（Termination-Action 属性）は定期的なオンラインユーザの再認証に適用します。サーバが割り当てたセッションタイムアウトタイマ（Session-Timeout 属性）と終了アクション（Termination-Action 属性）を表示する場合、**display dot1x connection** コマンドを使用します。詳細は Chapter 9 *Security Command References* の“*802.1X commands*”を参照してください。

- Termination-Action がログオフユーザ（デフォルト）である場合、定期的な再認証は、Session-Timeout よりも小さいときのみ適用されます。Termination-Action が Session-Timeout がより小さい場合、Session-Timeout タイマが終了したとき、装置は認証されたオンラインユーザをログオフします。
- Termination-Action がユーザの再認証である場合、装置で定期的な再認証は適用されません。Session-Timeout タイマが終了したのち、オンライン 802.1X ユーザを再認証します。

セッションタイムアウトがない場合、サーバによってタイマが割り当てられている場合、デバイスが定期的に 802.1X 再認証を実行するかどうかは、デバイス上の設定の定期的な再認証によって異なります。Session-Timeout 属性と Termination-Action 属性の割り当ては、サーバモデルによって異なります。

802.1X 再認証のサーバが到達不能である場合、装置はデフォルトで設定に応じてユーザをログオフする、あるいはオンラインを保持します。

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。

目次

このセクションのページは **8-x-x** です。

3 章 802.1X 3-1
3.1. 制限とガイドライン 3-1
3.2. 802.1X 設定作業リスト 3-1
3.3. 設定要件 3-2
3.4. 802.1X 認証の有効化 3-2
3.5. EAP relay または EAP termination の有効化 3-3
3.6. ポート許可状態の設定 3-3
3.7. アクセス制御方式の指定 3-4
3.8. ポートでの強制認証ドメインの設定 3-4
3.9. 802.1X 認証タイムアウトタイマの設定 3-5
3.10. 802.1X 再認証の設定 3-5
3.11. quiet タイマの設定 3-6
3.12. 802.1X ゲスト VLAN の設定 3-7
3.13. 802.1X 制限 VLAN の設定 3-8
3.14. 認証トリガ機能の設定 3-9
3.15. ポートの 802.1X ユーザの最大同時接続数の設定 3-10
3.16. 認証リクエストの最大送信数の設定 3-10
3.17. オンラインユーザハンドシェイク機能の設定 3-11
3.18. MAC アドレス移動機能の有効化 3-12
3.19. 802.1X ユーザのロギングの有効化 3-12
3.20. 802.1X の表示と維持 3-13
3.21. 802.1X 認証の設定例 3-13
3.21.1. 基本的な 802.1X 認証の設定例 3-13
3.21.2. 802.1X ゲスト VLAN と許可 VLAN の設定例 3-16
3.21.3. ACL の割り当てによる 802.1X の設定例 3-19

3章 802.1X

3.1. 制限とガイドライン

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、セクション 8 *セキュリティ オペレーションマニュアル*の”*ポートセキュリティ*”を参照してください。

許可 VLAN の割り当てを行う場合、以下の要件が満たされていることを確認してください。

- 802.1X が有効なポートでゲスト VLAN、制限 VLAN を設定している場合、認証サーバを 802.1X ユーザに割り当てるように認証サーバを設定します。

ポートの 802.1X ゲスト VLAN、制限 VLAN にユーザがある場合、ポートのリンクタイプを変更しないでください。

802.1X の設定はレイヤ 2 Ethernet インタフェース、アグリゲートインタフェースでのみサポートします。

レイヤ 2 Ethernet インタフェースがアグリゲーショングループに追加されたのち、インタフェースでの 802.1X の設定は適用されません。

インタフェースにオンライン 802.1X ユーザが存在する場合、アグリゲートインタフェースを削除しないでください。

🕮 メモ ：

QX-S5300G の認証処理速度は最大で 100 ユーザ/秒です。

3.2. 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
802.1Xの基本機能の設定 • (必須設定項目) EAP relay または EAP termination の有効化 • (必須設定項目) ポート許可状態の設定 • (必須設定項目) アクセス制御方式の指定 • (オプション設定項目) ポートでの強制認証ドメインの設定 • (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) 802.1X 再認証の設定 • (オプション設定項目) quiet タイマの設定

作業リスト
(オプション設定項目) 802.1X VLAN割り当ての設定 • 802.1X ゲスト VLAN の設定 • 802.1X 制限 VLAN の設定
(オプション設定項目)他の機能を用いた802.1Xの設定 • 認証トリガ機能の設定 802.1Xクライアントが認証を開始できない場合、設定します。 • ポートの 802.1X ユーザの最大同時接続数の設定 • 認証リクエストの最大送信数の設定 • オンラインユーザハンドシェイク機能の設定 • MAC アドレス移動機能の有効化 • 802.1X ユーザのロギングの有効化

3.3. 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。

3.4. 802.1X認証の有効化

I. 制限とガイドライン

802.1X をポートで適用する場合、グローバルとポートの両方で有効にする必要があります。

PVID が Voice VLAN である場合、802.1X はポートに適用することができません。Voice VLAN の詳細はセクション 3 *アクセス オペレーションマニュアル*の“*Voice VLAN*”を参照してください。

II. 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

3.5. EAP relayまたはEAP terminationの有効化

I. EAP モード選択の概要

EAP relay または EAP termination を設定するときに、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

II. 制限とガイドライン

- 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 CAR サーバに変更なしで認証データを送信します。**user-name-format** コマンドの詳細は Chapter 9 *Security Command Reference* の“*AAA commands*”を参照してください。
- 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。EAP termination を使用する場合、アクセス装置で CHAP 認証を有効にする必要があります。
  - 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 termination を使用する場合、アクセス装置で PAP あるいは CHAP 認証を有効にすることができます。しかしセキュリティのため、CHAP 認証を有効にしてください。
- 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 の詳細はセクション 8 *セキュリティ オペレーションマニュアルの”802.1X の概要””* を参照してください。

III. 設定手順

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

3.6. ポート許可状態の設定

I. ポート許可状態の概要

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。以下のポートの許可状態を制御できます。

- **authorized**ーポートを 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**ーポートを 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。

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. 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**

3.7. アクセス制御方式の指定

I. アクセス制御方式の指定の概要

装置はポートベースと MAC アドレスベース制御方式をサポートします。

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	**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**

3.8. ポートでの強制認証ドメインの設定

I. 強制認証ドメインの概要

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。

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*	―

操作	コマンド	補足
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

3.9. 802.1X認証タイムアウトタイマの設定

I. 802.1X 認証タイムアウトタイマの概要

ネットワークデバイスは、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ときに起動します。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ときに起動します。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。

II. 制限とガイドライン

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。

III. 設定手順

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

3.10. 802.1X再認証の設定

I. 制限とガイドライン

装置は、以下の順序で定期的な再認証タイマを選択し、802.1X 再認証を行います。

1) サーバが割り当てた再認証タイマ
2) グローバルでの再認証タイマ
3) デフォルト再認証タイマ

手動で再認証を設定した後、装置は、サーバが割り当てた再認証の属性、ポートの定期的な再認証機能にかかわらず、ポートのすべてのオンライン 802.1X ユーザを再認証します。

強制認証ドメインあるいは EAP メッセージの処理方法の変更は、オンライン 802.1X ユーザの再認証に影響しません。変更された設定は、変更後にオンラインになった 802.1X ユーザにのみ適用されます。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. (オプション設定項目) 定期的な認証タイマを設定する	• グローバルで定期的な認証タイマを設定する: **dot1x timer reauth-period** *reauth-period-value* • インタフェースで定期的な認証タイマを設定する: ○ **interface interface-type** *interface-number* ○ **dot1x timer reauth-period** *reauth-period-value* ○ **quit**	デフォルト： • グローバル：3600 秒 • インタフェース：設定されていません。グローバルの設定を使用します。
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

3.11. quietタイマの設定

I. quiet タイマの概要

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。

II. 制限とガイドライン

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。

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. quiet タイマを有効にする	**dot1x quiet-period**	デフォルト：無効
3. (オプション設定項目) quiet タイマを設定する	**dot1x timer quiet-period** *quiet-period-value*	デフォルト：60秒

3.12. 802.1Xゲスト VLANの設定

I. 制限とガイドライン

- 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。
- ポートで複数のセキュリティ機能を設定するとき、表 3-1 に示すガイドラインに従ってください。

表 3-1 802.1X 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。	セクション8 *セキュリティ オペレーションマニュアル*の”*802.1Xの概要*”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。	セクション8 *セキュリティ オペレーションマニュアル*の”*ポートセキュリティ*”を参照してください。

II. 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 の詳細はセクション 3 *アクセス オペレーションマニュアル*の”*VLAN*”を参照してください。
  - 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*	―
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

メモ：

MAC ベースダイナミック VLAN を使用する場合、**mac-vlan enable** コマンドをハイブリッドポートに設定してください。

3.13. 802.1X制限VLANの設定

I. 制限とガイドライン

- 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。
- ポートで複数のセキュリティ機能を設定するとき、表 3-2 に示すガイドラインに従ってください。

表 3-2 802.1X 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。	セクション8 *セキュリティ オペレーションマニュアル*の”*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。	セクション8 *セキュリティ オペレーションマニュアル*の”*ポートセキュリティ*”を参照してください。

II. 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 の詳細はセクション 3 *アクセス オペレーションマニュアルの”VLAN”*を参照してください。
- ポートをタグなしメンバとして 802.1X 制限 VLAN に割り当ててください。

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*	―
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

メモ：

MAC ベースダイナミック VLAN を使用する場合、**mac-vlan enable** コマンドをハイブリッドポートに設定してください。

3.14. 認証トリガ機能の設定

I. 認証トリガ機能の概要

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。セクション 8 *セキュリティ オペレーションマニュアルの“802.1X の概要”*を参照してください。

II. 制限とガイドライン

- 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。

III. 設定手順

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*	―

操作	コマンド	補足
4. 認証トリガ機能を有効にする	**dot1x** { **multicast-trigger** | **unicast-trigger** }	デフォルト： ・RJ-45：マルチキャストトリガが無効で、ユニキャストトリガが有効です。 ・RJ-45以外：マルチキャストトリガが有効で、ユニキャストトリガが無効です。

3.15. ポートの802.1Xユーザの最大同時接続数の設定

I. ポートの 802.1X ユーザの最大同時接続数の概要

この設定を行うことで、ユーザ過多によるシステムリソース不足を防ぎます。

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	**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：

QX–S5300G シリーズは 2048 まで認証動作が可能です。

3.16. 認証リクエストの最大送信数の設定

I. 認証要求再送信の概要

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。

II. 設定手順

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

3.17. オンラインユーザハンドシェイク機能の設定

I. オンラインユーザハンドシェイク機能の概要

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。

II. 制限とガイドライン

- 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。
- 装置から EAP Success パケットを受信せずに 802.1X クライアントがオフラインになる場合のみ、オンラインユーザハンドシェイク応答機能を有効にします。

III. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. (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：無効 ・RJ-45以外：有効

操作	コマンド	補足
5. (オプション設定項目) 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

3.18. 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。

もし、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。

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

3.19. 802.1Xユーザのロギングの有効化

I. 802.1X ユーザのログ機能の概要

この機能を有効にすることで装置が 802.1X ユーザのログを作成し、Information Center にログを送信します。ログの出力を行うため、装置で Information Center の設定を行う必要があります。Information Center の詳細はセクション 10 *システム管理 オペレーションマニュアル*の“*Information Center*”を参照してください。

II. 制限とガイドライン

頻繁に認証接続が発生する環境では、802.1X ユーザのログの過剰な出力を防止するため、無効にすることを推奨します。

III. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. 802.1X ユーザのログ機能を有効にする	**dot1x access-user log enable** [**abnormal-logoff** | **failed-login** | **normal-logoff** | **successful-login**] *	デフォルト：有効 パラメータを指定しない場合、802.1Xユーザのすべてのログ機能が有効になります。

3.20. 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*]
オンライン802.1Xユーザ情報を表示する	**display dot1x connection** [**open**] [**interface** *interface-type interface-number* | **slot** *slot-number* | **user-mac** *mac-addr* | **user-name** *name-string*]
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*]
802.1X統計情報をクリアする	**reset dot1x statistics** [**interface** *interface-type interface-number*]

3.21. 802.1X認証の設定例

3.21.1. 基本的な 802.1X 認証の設定例

I. ネットワーク要件

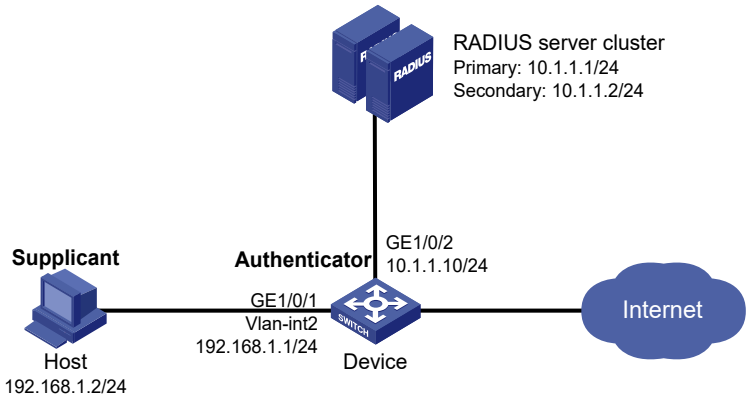
図 3-1 に示すように、アクセス装置は、GigabitEthernet 1/0/1 に接続するユーザ用に 802.1X 認証を実行します。ポート上で MAC ベースのアクセス制御を行ってください。1 ユーザのログオフは、他のオンラインの 802.1X ユーザには影響しません。

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、Chapter 8 *Security Command References* の”*AAA commands*”を参照してください。

3) アクセス装置上の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

3.21.2. 802.1X ゲスト VLAN と許可 VLAN の設定例

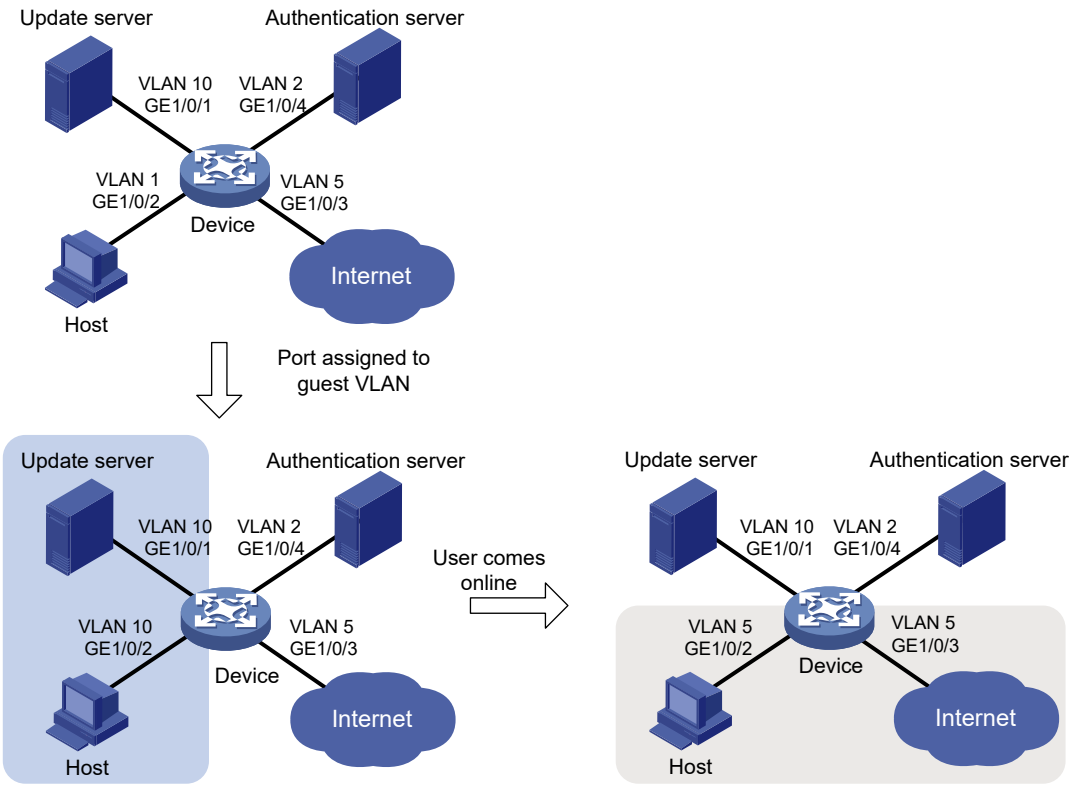
I. ネットワーク要件

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、デバイスはゲスト 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 VLAN5）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デバイス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とき、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

3.21.3. ACL の割り当てによる 802.1X の設定例

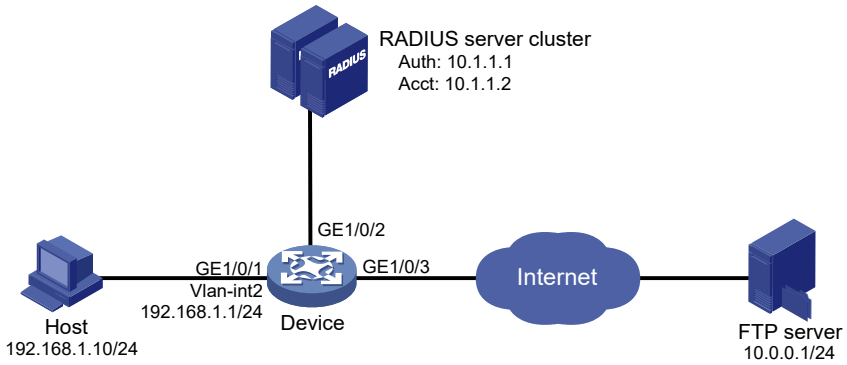
I. ネットワーク要件

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

認証サーバとデバイス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デバイス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 number 3000

[Device-acl-adv-3000] rule 0 deny ip destination 10.0.0.1 0 time-range ftp

[Device-acl-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、ACL3000 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 **8-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 4-6
4.2. 制限とガイドライン 4-6
4.3. 設定作業リスト 4-7
4.4. 設定要件 4-7
4.5. MAC アドレス認証の有効化 4-8
4.6. MAC アドレス認証ドメインの指定 4-8
4.7. ユーザアカウントフォーマットの設定 4-9
4.8. MAC アドレス認証タイマの設定 4-9
4.9. MAC アドレス認証ゲスト VLAN の設定 4-10
4.10. 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 4-11
4.11. MAC アドレス認証の開始を遅らせる遅延時間の設定 4-12
4.12. MAC アドレス移動機能の有効化 4-12
4.13. MAC アドレス認証と 802.1X 認証の並列処理の設定 4-13
4.14. MAC アドレス認証ユーザのロギングの有効化 4-14
4.15. MAC アドレス認証の表示と維持 4-14
4.16. MAC アドレス認証の設定例 4-15
4.16.1. ローカル MAC アドレス認証の設定例 4-15
4.16.2. RADIUS ベースの MAC アドレス認証の設定例 4-17
4.16.3. ACL の割り当ての設定例 4-19

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しません。ユーザは、ネットワークアクセス用のユーザ名とパスワードを入力する必要はありません。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。MAC アドレスが認証を通過した場合、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、サイレント MAC アドレスとして MAC アドレスを記憶し、パケットをドロップし、Quiet タイマを開始します。装置は、Quiet タイムの間、その MAC アドレスからのすべての後続のパケットを破棄します。この Quiet メカニズムは、短時間の間に何度も認証が行われることを回避します。

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。

- **各ユーザのための MAC ベースのユーザアカウント**－図 4-1 に示すように、アクセス装置は、MAC アドレス認証するユーザ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。このポリシーは、非セキュアな環境に適しています。
- **すべてのユーザのための共有のユーザアカウント**－図 4-2 に示すように、アクセス装置上のすべての MAC アドレス認証ユーザのために、ユーザ名とパスワードを指定します。指定するユーザ名は必ずしも MAC アドレスである必要はありません。このポリシーは、セキュアな環境に適しています。

図 4-1 MAC アドレスベースのユーザアカウントポリシー

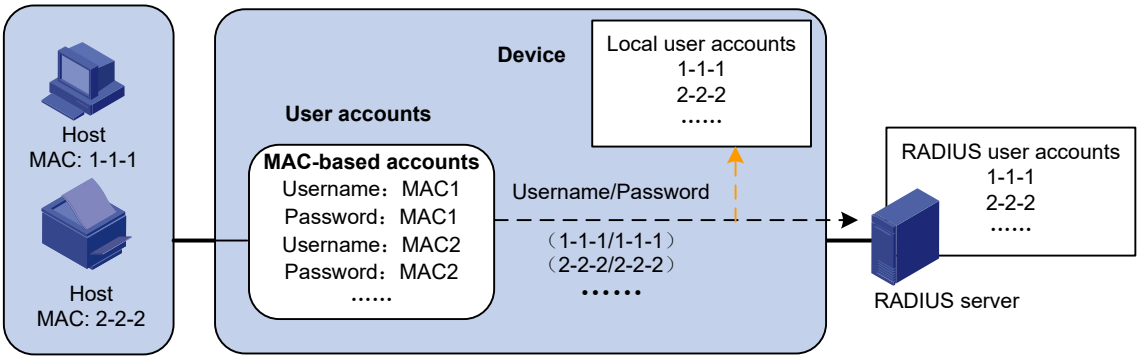
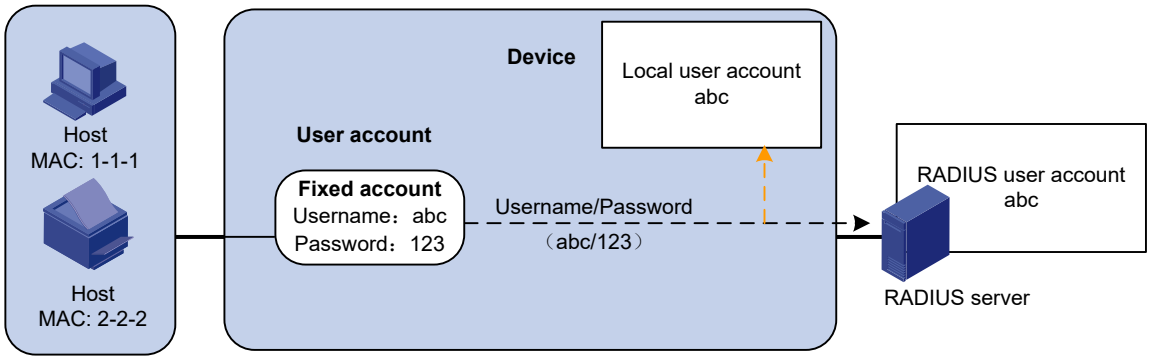


図 4-2 共有ユーザのアカウントポリシー



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。

ローカル認証と RADIUS 認証の詳細はセクション 8 *セキュリティ オペレーションマニュアル*の”*AAA*”を参照してください。

I. RADIUS 認証

- **MAC ベースアカウント**－アクセス装置は、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。
- **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。

II. ローカル認証

- **MAC ベースアカウント**－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。
- **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。

4.1.3. VLAN の割り当て

I. 許可 VLAN

許可 VLAN の制御は、許可されたネットワークリソースに MAC アドレス認証ユーザのアクセスを制限します。装置はローカルあるいはリモートサーバで割り当てられた許可 VLAN をサポートします。リモートサーバのみタグつき許可 VLAN を割り当てることができます。

II. リモート VLAN 許可

リモート VLAN 認証では、リモートサーバに許可 VLAN 情報を指定する必要があります。ユーザが認証をパスすると、サーバはその情報をデバイスに割り当てます。デバイスは許可 VLAN 情報を解決し、ユーザのアクセスポートをタグ付きまたはタグなしメンバとして許可 VLAN に割り当てます。解決が失敗すると、ユーザは認証に失敗します。

リモートサーバで 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、セクション 3 *アクセス オペレーションマニュアルの”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。

VLAN 許可では以下のタイプを指定す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
- プライベート VLAN

サーバが VLAN のグループを割り当てるとき、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 4-1 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 4-1 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	デバイスは、ポートで他のオンラインユーザがいるかどうかに依存して、許可VLANとしてVLANを選択します。 • ポートで他のオンラインユーザがいない場合、デバイスは VLAN のグループからもっとも小さい ID の VLAN を選択します。 • ポートで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。 ○ MAC ベース VLAN が有効の場合、装置は最も少ないオンラインユーザを持つ VLAN を選択します。2 つの VLAN が同じ数のオンライン 802.1X ユーザを持つ場合、装置は低い ID で VLAN を選択します。 ○ MAC ベース VLAN が無効の場合、オンラインユーザがいる VLAN が VLAN のグループにあるかどうかを調べます。VLAN がグループ内にある場合、VLAN は許可 VLAN としてユーザに割り当てられます。グループ内に VLAN が見つからない場合、VLAN 認証は失敗します。
サフィックスを持つVLAN ID	1. デバイス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. デバイスは 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。もしタグなし 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。デバイスはタグなし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。

III. 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。MACアドレス認証ユーザが装置にアクセスする際に経由するポートは、タグなしメンバとして VLAN に割り当てられます。タグ付き VLAN の割り当てはサポートされていません。

ローカルユーザの詳細はセクション 8 *セキュリティ オペレーションマニュアル*の”*AAA*”を参照してください。

IV. MAC アドレス認証が有効なポートでの VLAN 許可操作

表 4-3 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 4-2 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：** アクセスポートはタグなしVLANメンバとしてのみ許可VLANに割り当てられます。
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。

⚠ **重要：**

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。

V. 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 4-3 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 4-3 VLAN 操作

ポートタイプ	VLAN 操作
サーバに到達不能以外の理由で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。

ユーザのアクセス制御を変更するために、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。

サポートされている許可 ACL は以下のタイプがあります。

- 標準 ACL（ACL の番号：2000～2999）
- 拡張 ACL（ACL の番号：3000～3999）

許可 ACL を適用する場合、ACL が存在し、**counting**、**established**、**fragment**、**logging** パラメータを除く ACL ルールが存在することを確認してください。

4.2. 制限とガイドライン

許可 VLAN の割り当てを行う場合、以下の要件が満たされていることを確認してください。

- MAC アドレス認証が有効なポートでゲスト VLAN、制限 VLAN を設定している場合、認証サーバを MAC アドレス認証ユーザに割り当てるように認証サーバを設定します。

ポートの MAC アドレス認証ゲスト VLAN、制限 VLAN にユーザがある場合、ポートのリンクタイプを変更しないでください。

MAC アドレス認証の設定はレイヤ 2 Ethernet インタフェース、アグリゲートインタフェースでのみサポートします。

レイヤ 2 Ethernet インタフェースがアグリゲーショングループに追加されたのち、インタフェースでの MAC アドレス認証の設定は適用されません。

インタフェースにオンライン MAC アドレス認証ユーザが存在する場合、アグリゲートインタフェースを削除しないでください。

認証に失敗した MAC アドレスがスタティック MAC アドレスである場合、あるいはセキュリティの認証にパスした MAC アドレスである場合、装置は silent アドレスとして MAC アドレスを記憶しません。

メモ：

QX-S5300G の認証処理速度は最大で 100 ユーザ/秒です。

4.3. 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
MACアドレス認証の基本機能の設定 • MAC アドレス認証ドメインの指定 • 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) MACアドレス認証VLAN割り当ての設定 • MAC アドレス認証ゲスト VLAN の設定
(オプション設定項目)他の機能を用いた802.1Xの設定 • 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 • 認証の開始を遅らせる遅延時間の設定 • MAC アドレス移動機能の有効化 • MAC アドレス認証と 802.1X 認証の並列処理の設定 • MAC アドレス認証ユーザのログ機能の有効化

4.4. 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) 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セクション 8 *セキュリティ オペレーションマニュアル*の”*ポートセキュリティ*”を参照してください。

2) 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。詳細はセクション 8 *セキュリティ オペレーションマニュアル*の”*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。

4.5. MACアドレス認証の有効化

I. 制限とガイドライン

ポートで MAC アドレス認証を有効にするとき、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。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. グローバルで MAC アドレス認証を有効にする	**mac-authentication**	デフォルト：無効
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

I. MAC アドレス認証ドメインの概要

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セクション 8 *セキュリティ オペレーションマニュアル*の”*AAA*”を参照してください。

II. 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. 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 **interface** *interface-type interface-number* **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

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. MAC アドレス認証ユーザアカウントフォーマットを設定する	• 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**]] • 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** } *password*]	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

I. アクセス制御方式の指定の概要

MAC アドレス認証では以下のタイマを使用します。

- **Offline detect timer**ー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。ユーザの接続が 2 つの連続した期間でアイドル状態になっている場合、装置はユーザをログアウトし、ユーザのアカウントを停止します。
- **Quiet timer**ー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、ユーザはネットワークにアクセスすることはできません。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. 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. MACアドレス認証ゲストVLANの設定

I. 制限とガイドライン

表 4-4 にポートで MAC アドレス認証ゲスト VLAN を設定するときのガイドラインを示します。

表 4-4 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とき、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。	セクション8 *セキュリティオペレーションマニュアル*の”*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。
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。	セクション8 *セキュリティオペレーションマニュアル*の”*ポートセキュリティ*”を参照してください。

II. 設定要件

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。

- 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。
- ハイブリッドポートでタグなしメンバとして VLAN を設定します。
- ポートで MAC ベース VLAN を有効にします。

III. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. 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. ポートで MAC アドレス認証ゲスト VLAN の認証間隔を設定する	**mac-authentication guest-vlan auth-period** period-value	デフォルト：30秒

メモ：

MAC ベースダイナミック VLAN を使用する場合、**mac-vlan enable** コマンドをハイブリッドポートに設定してください。

4.10. 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

I. 概要

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を防ぎます。

II. 設定手順

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

QX-S5300G シリーズは 2048 まで認証動作が可能です。

4.11. MACアドレス認証の開始を遅らせる遅延時間の設定

I. 概要

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。

もし遅延時間内に、802.1X 認証が動作しないあるいは 802.1X 認証に失敗したとき、MAC アドレス認証を行います。

II. 制限とガイドライン

MAC アドレス認証の開始を遅らせる遅延時間を設定するとき、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、セクション 8 *セキュリティ オペレーションマニュアル*の”*ポートセキュリティ*”を参照してください。

III. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. 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** *time*	デフォルト：無効

4.12. 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。

もし、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。

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

4.13. MACアドレス認証と802.1X認証の並列処理の設定

I. MAC アドレス認証と 802.1X 認証の並列処理

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ます。
- ポートは 802.1X ユニキャストトリガ機能を有効にしています。

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。

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、セクション 8 *セキュリティ オペレーションマニュアル*の”*802.1X*”を参照してください。

II. 設定ガイドライン

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、セクション 8 *セキュリティ オペレーションマニュアル*の”*ポートセキュリティ*”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。

III. 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**	―
2. Ethernet interface view に移行する	**interface** *interface-type interface-number*	―

操作	コマンド	補足
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：無効

4.14. MACアドレス認証ユーザのロギングの有効化

I. MAC アドレス認証ユーザのロギングの概要

この機能を有効にすることで装置が MAC アドレス認証ユーザのログを作成し、Information Center にログを送信します。ログの出力を行うため、装置で Information Center の設定を行う必要があります。Information Center の詳細はセクション 10 *システム管理 オペレーションマニュアル*の“*Information Center*”を参照してください。

II. 制限とガイドライン

頻繁に認証接続が発生する環境では、MAC アドレス認証ユーザのログの過剰な出力を防止するため、無効にすることを推奨します。

この機能は、グローバルおよび該当のインタフェースの両方で有効にした場合のみ、インタフェース上で有効になります。

III. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. グローバルで MAC アドレス認証ユーザにログ機能を設定する	**mac-authentication access-user log enable** [**failed-login** | **ip-change** | **logoff** | **successful-login**] *	デフォルト：有効 パラメータを指定しない場合、MACアドレス認証ユーザに対してすべてのログ機能を有効にします。
3. Ethernet interface view に移行する	**interface** *interface-type interface-number*	―
4. ポートで MAC アドレス認証ユーザにログ機能を設定する	**mac-authentication access-user log enable** [**failed-login** | **ip-change** | **logoff** | **successful-login**] *	デフォルト：有効 パラメータを指定しない場合、MACアドレス認証ユーザに対してすべてのログ機能を有効にします。

4.15. MACアドレス認証の表示と維持

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
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** [**open**] [**interface** *interface-type interface-number* | **slot** *slot-number* | **user-mac** *mac-addr* | **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*]
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

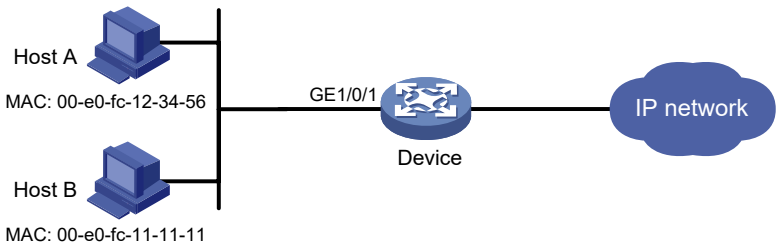
I. ネットワーク要件

図 4-3 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 4-3 ネットワーク図



II. 設定手順

ローカルユーザアを追加します。この例ではホストの MAC アドレス 00-e0-fc-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 00-e0-fc-12-34-56 class network

[Device-luser-network-00-e0-fc-12-34-56] password simple 00-e0-fc-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-00-e0-fc-12-34-56] service-type lan-access

[Device-luser-network-00-e0-fc-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
   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
   Authentication domain  : bbb
 Online MAC-auth users    : 1

 Silent MAC users:
```

```
          MAC address       VLAN ID  From port              Port index
          00e0-fc11-1111    8        GE1/0/1               1
GigabitEthernet1/0/1 is link-up
  MAC authentication          : Enabled
  Authentication domain       : Not configured
  Auth-delay timer            : Disabled
  Re-auth server-unreachable  : Logoff
  Guest VLAN                  : Not configured
  Critical VLAN               : Not configured
  Host mode                   : Single VLAN
  Max online users            : 4294967295
  Authentication attempts     : successful 1, failed 0
  Current online users        : 1
          MAC address       Auth state
          00e0-fc12-3456    Authenticated
```

4.16.2. RADIUS ベースの MAC アドレス認証の設定例

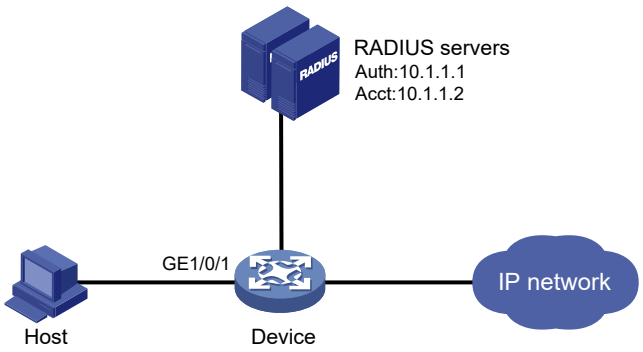
I. ネットワーク要件

図 4-4 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 4-4 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
   Authentication domain  : bbb
 Online MAC-auth users    : 1

 Silent MAC users:
          MAC address       VLAN ID  From port               Port index

 GigabitEthernet1/0/1  is link-up
   MAC authentication         : Enabled
   Authentication domain      : Not configured
   Auth-delay timer           : Disabled
   Re-auth server-unreachable : Logoff
   Guest VLAN                 : Not configured
   Critical VLAN              : Not configured
   Host mode                  : Single VLAN
   Max online users           : 4294967295
   Authentication attempts    : successful 1, failed 0
   Current online users       : 1
          MAC address       Auth state
          00e0-fc12-3456    Authenticated
```

4.16.3. ACL の割り当ての設定例

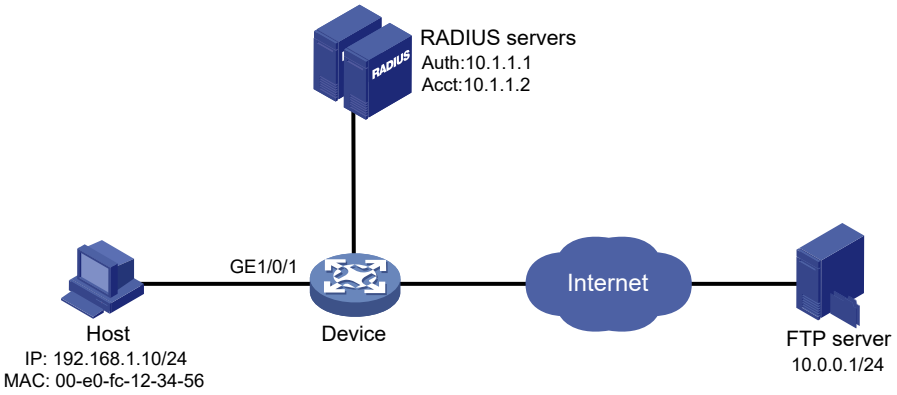
I. ネットワーク要件

図 4-5 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。
- MAC アドレス認証ユーザの MAC ベースユーザアカウントを使用します。各 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 4-5 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 number 3000

[Switch-acl-adv-3000] rule 0 deny ip destination 10.0.0.1 0

[Switch-acl-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、アカウンティング用の ISP ドメイン 2000 に RADIUS スキーム 2000 を適用します。

[Switch] domain 2000

[Switch-isp-2000] authentication default radius-scheme 2000

[Switch-isp-2000] authorization default radius-scheme 2000

[Switch-isp-2000] accounting default radius-scheme 2000

[Switch-isp-2000] quit

MAC アドレス認証の ISP ドメインを指定します。

[Switch] mac-authentication domain 2000

MAC ベースユーザアカウントを使用するために装置を設定します。各 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 00-e0-fc-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 ACL3000 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     : Enabled
   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
   Authentication domain  : bbb
 Online MAC-auth users    : 1

 Silent MAC users:
          MAC address       VLAN ID  From port               Port index

 GigabitEthernet1/0/1  is link-up
   MAC authentication         : Enabled
   Authentication domain      : Not configured
   Auth-delay timer           : Disabled
   Re-auth server-unreachable : Logoff
   Guest VLAN                 : Not configured
   Critical VLAN              : Not configured
   Host mode                  : Single VLAN
```

```
   Max online users           : 4294967295
   Authentication attempts    : successful 1, failed 0
   Current online users       : 1
          MAC address       Auth state
          00e0-fc12-3456    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、ACL3000 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 **8-x-x** です。

5 章 WEB 認証 5-1

5章 WEB 認証

WEB 認証の設定に関するコンフィグについては、別紙の共通マニュアル”*QX シリーズ Ethernet スイッチ Web 認証オペレーションマニュアル*（V7）”の“*WebAuth*”を参照してください。

目次

このセクションのページは **8-x-x** です。

6 章 トリプル認証 6-1

6章　トリプル認証

トリプル認証の設定に関するコンフィグについては、別紙の共通マニュアル”*QX シリーズ Ethernet スイッチ Web 認証オペレーションマニュアル*（V7）”の“*トリプル認証*”を参照してください。

目次

このセクションのページは **8-x-x** です。

7 章 ポートセキュリティ 7-1
7.1. 概要 7-1
7.1.1. 主要機能 7-1
7.1.2. ポートセキュリティの機能 7-1
7.1.3. ポートセキュリティのモード 7-1
7.2. 制限とガイドライン 7-5
7.3. 設定作業リスト 7-5
7.4. ポートセキュリティの有効化 7-6
7.5. ポートセキュリティモードの設定 7-6
7.6. ポートでのセキュア MAC アドレスの最大数の設定 7-8
7.7. セキュア MAC アドレスの設定 7-9
7.8. NTK の設定 7-10
7.9. 侵入防止の設定 7-11
7.10. サーバからの許可情報の無視 7-11
7.11. MAC アドレス移動機能の有効化 7-12
7.12. SNMP notification の有効化 7-12
7.13. ポートセキュリティユーザのロギングの有効化 7-13
7.14. ポートセキュリティの表示と維持 7-13
7.15. ポートセキュリティの設定例 7-14
7.15.1. autoLearn モードの設定例 7-14
7.15.2. userLoginWithOUI モードの設定例 7-16
7.15.3. macAddressElseUserLoginSecure モードの設定例 7-19
7.16. ポートセキュリティのトラブルシューティング 7-23
7.16.1. ポートセキュリティのモードが設定できない 7-23
7.16.2. セキュア MAC アドレスが設定できない 7-23

7章 ポートセキュリティ

7.1. 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。WLAN のような、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。

7.1.1. 主要機能

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。

7.1.2. 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。

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あるいはクライアントが 802.1X、MAC アドレス認証に失敗した場合、フレームは不正となります。

7.1.3. 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。

表 7-1 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 7-1 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	

モードの名前を以下に示します。

- **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** のあるセキュリティモードでは、認証リクエストのプロトコルタイプに依存して、認証方法が使用されます。

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、セクション 3 *アクセス オペレーション マニュアル*の”*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。もし 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. MAC 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 認証に失敗したとき、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ます。
  - ポートが 802.1X ユニキャストトリガが有効になっています。
  - ポートが不明の MAC アドレスのパケットを受信します。

  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。もし 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。

7.2. 制限とガイドライン

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。

この機能は、ポートの異なるユーザに異なる認証方式が必要な WLAN などのようなネットワークに適用します。

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セクション 8 *セキュリティ オペレーションマニュアル*の”*802.1X*”と”*MAC アドレス認証*”を参照してください。

autolen、secure、および userlogin-withui のポートセキュリティモードとセキュア MAC アドレス設定は、アグリゲートインタフェースではサポートされません。他のポートセキュリティ設定は、レイヤ 2 イーサネットインタフェースとアグリゲートインタフェースの両方でサポートされています。

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。

インタフェースにオンライン 802.1X あるいは MAC アドレス認証ユーザがいる場合、アグリゲートインタフェースを削除しないでください。

7.3. 設定作業リスト

作業リスト
ポートセキュリティの基本機能の設定 • （必須設定項目）ポートセキュリティの有効化 • （必須設定項目）ポートセキュリティモードの設定 • （必須設定項目）ポートでのセキュア MAC アドレスの最大数の設定 • （必須設定項目）セキュア MAC アドレスの設定 • （オプション設定項目）NTK の設定 • （オプション設定項目）侵入防止の設定
（オプション設定項目） ポートセキュリティの拡張機能の設定 • サーバからの許可情報の無視 • MAC アドレス移動機能の有効化 ポートセキュリティ機能が無効で802.1XあるいはMACアドレス認証が有効である場合、拡張ポートセキュリティ機能は適用されます。
（オプション設定項目） ポートセキュリティのSNMP notificationの通知の有効化
（オプション設定項目）ポートセキュリティユーザのロギングの有効化

7.4. ポートセキュリティの有効化

I. 制限とガイドライン

- 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。
- **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、セクション 8 *セキュリティ オペレーションマニュアル*の”*802.1X*”、”*MAC アドレス認証*”を参照してください。

II. 設定要件

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。

III. 設定手順

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

7.5. ポートセキュリティモードの設定

I. 制限とガイドライン

ポートセキュリティが無効のとき、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。

ポートセキュリティを有効にしたのち、ポートが noRestrictions モード（デフォルト）であるときのみポートのセキュリティモードを変更することができます。ほかのモードのポートセキュリティモードを変更する場合、最初に **undo port-security port-mode** コマンドを使用してデフォルトに戻してください。

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-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。

II. 設定要件

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。
- 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。

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. （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**モードのとき、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*	ー

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-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）にしたときのみ、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ときは、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。

7.6. ポートでのセキュアMACアドレスの最大数の設定

I. 概要

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セクション 3 *アクセス オペレーションマニュアル*の”*MAC アドレステーブル*”を参照してください。

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. 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** *count-value* [**vlan** [*vlan-id-list*]]	デフォルト：制限なし

7.7. セキュアMACアドレスの設定

I. 概要

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 アドレスは、スタティック、Sticky があります。

表 7-2 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とき、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。

セキュア MAC アドレスエントリが最大数に到達したとき、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。

II. 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。

- 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。

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*	―
3. セキュア MAC アドレスを設定する	**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。
4. 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 second** *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。

7.8. NTKの設定

I. 概要

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。

II. 制限とガイドライン

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 7-1 を参照してください。

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*	―
3. NTK 機能を設定する	**port-security ntk-mode** { **ntk-withbroadcasts** | **ntk-withmulticasts** | **ntkonly** }	デフォルト：無効 すべてのフレームが転送されます。

7.9. 侵入防止の設定

I. 概要

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。ブロックされた MAC アドレスからのすべての後続のフレームは廃棄されます。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。

II. 制限とガイドライン

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。

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*	―
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. （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	• system view に戻る **quit** • ポートを無効にする時間を設定する **port-security timer disableport** ***t****ime-value*	デフォルト：20秒

7.10. サーバからの許可情報の無視

I. 概要

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。

II. 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. 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。

7.11. MACアドレス移動機能の有効化

I. 概要

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。

もし 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。

II. 制限とガイドライン

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。

III. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. MAC アドレス移動機能を有効にする	**port-security mac-move permit**	デフォルト：有効

7.12. SNMP notificationの有効化

I. 概要

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、セクション 10 *システム管理 オペレーションマニュアル*の“*SNMP*”を参照してください。

II. 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. SNMP notification の通知を有効にする	**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

7.13. ポートセキュリティユーザのロギングの有効化

I. 概要

この機能は装置がポートセキュリティユーザのログを生成し、Information Center にログを送信します。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 の詳細はセクション 10 *システム管理 オペレーションマニュアル*の“*Information Center*”を参照してください。

II. 制限とガイドライン

頻繁に認証接続が発生する環境では、ポートセキュリティユーザのログの過剰な出力を防止するため、無効にすることを推奨します。

III. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. ポートセキュリティユーザのログ機能を有効にする	**port-security access-user log enable** [**failed-authorization** | **mac-learning** | **violation**] *	デフォルト：有効 パラメータを指定しない場合、ポートセキュリティユーザのすべてのログ機能を有効にします。

7.14. 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*]

操作	コマンド
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**]

7.15. ポートセキュリティの設定例

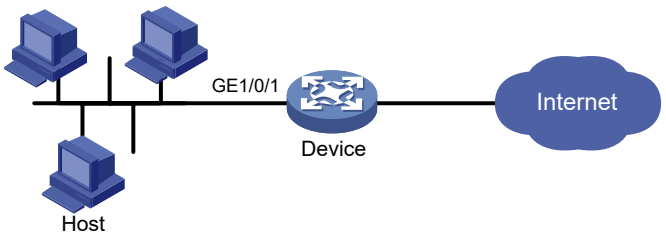
7.15.1. autoLearn モードの設定例

I. ネットワーク要件

図 7-1 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 7-1 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

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

セキュア MAC アドレスタイマを 50 秒に設定します。

[Device-GigabitEthernet1/0/1] port-security timer autolearn aging second 50

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

```
Global port security parameters:
   Port security           : Enabled
   AutoLearn aging time    : 30 min
   Disableport timeout     : 30 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
```

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）。

7.15.2. userLoginWithOUI モードの設定例

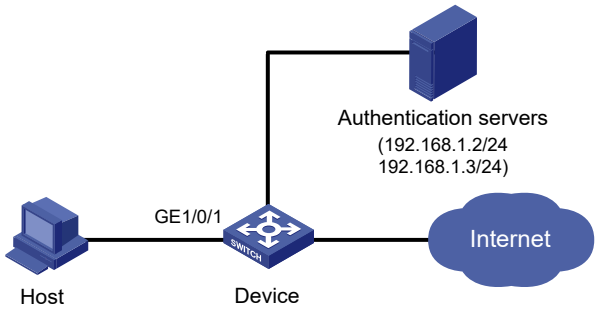
I. ネットワーク要件

図 7-2 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 7-2 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 Chapter 8 *Security Command References* の”*AAA commands*”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 を設定します。

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

GigabitEthernet 1/0/1 の 802.1X ユーザの強制認証ドメインとして 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
   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
```

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
```

7.15.3. macAddressElseUserLoginSecure モードの設定例

I. ネットワーク要件

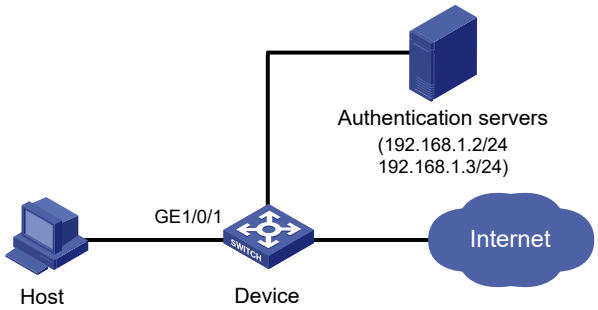
図 7-3 に示すように、GigabitEthernet 1/0/1 を通してクライアントが Device に接続されます。Device は RADIUS サーバを使用してクライアントを認証します。認証が成功すると、クライアントはインターネットにアクセスするように許可されます。

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 7-3 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。（セクション 8 *セキュリティ オペレーションマニュアル*の”*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 アドレス認証に MAC ベースのアカウントを使用します。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

802.1X ユーザの強制認証ドメインとして 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
   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
```

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
  EAD assistant function : Disabled
      EAD timeout        : 30 min
  Domain delimiter       : @
Online 802.1X 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
  Auth-Fail VSI              : Not configured
  Critical VSI               : Not configured
  Add Guest VSI delay        : Disabled

  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）

7.16. ポートセキュリティのトラブルシューティング

7.16.1. 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。

7.16.2. 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 **8-x-x** です。

8 章 パスワード管理 8-1
8.1. 概要 8-1
8.1.1. パスワードの設定 8-1
8.1.2. パスワードのアップデートと有効期限の終了 8-3
8.1.3. ユーザログイン管理 8-4
8.1.4. すべての形式でのパスワードの非表示 8-5
8.1.5. ロギング 8-5
8.2. 制限とガイドライン 8-5
8.3. パスワード管理設定作業リスト 8-6
8.4. パスワード管理の有効化 8-6
8.5. グローバルパスワード管理パラメータの設定 8-6
8.6. ユーザグループパスワード管理パラメータの設定 8-8
8.7. ローカルユーザパスワード管理パラメータの設定 8-8
8.8. super パスワード管理パラメータの設定 8-10
8.9. パスワード管理の表示と維持 8-10
8.10. パスワード管理の設定例 8-10
8.10.1. パスワード管理の設定例 8-10

8章 パスワード管理

8.1. 概要

パスワード管理は、以下の機能ができます。

- 装置の管理者のログインと 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。

ローカルユーザは装置管理者とネットワークアクセスユーザの 2 つのタイプに分類されます。この機能は装置管理者についてのみ適用されます。ローカルユーザについての詳細は、セクション 8 *セキュリティ オペレーションマニュアル*の”*AAA*”を参照してください。

8.1.1. 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. パスワード構成のポリシー

パスワードは以下のタイプの組み合わせで構成されます。

- 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 8-1 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	―	キャロット	^
コロン	:	コンマ	,
ダラーマーク	$	ドット	.

文字名	記号	文字名	記号
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 8-2 にパスワード構成のポリシーを示します。

表 8-2 パスワード構成のポリシー

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
Level 3	3	1
Level 4	4	1

すべてのパスワード組み合わせのレベルが有効です。

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。

8.1.2. 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。

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。

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。

8.1.3. 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 や 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）
- コンソールあるいは AUX 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。ユーザが指定した試行回数後に正しいパスワードの入力に失敗した場合、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。

8.1.4. 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。

8.1.5. 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。

8.2. 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。

8.3. 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

8.4. 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と、指定したパスワード管理の設定が適用されます。

II. 制限とガイドライン

- グローバルパスワード管理機能を有効にした後、対応する **display** コマンドを使用してパスワードと装置管理者用の super パスワードを表示することができません。ネットワークにアクセスするユーザパスワードの設定を表示させることができます。
- 装置管理者の初回パスワードが設定されている場合、少なくとも 4 文字は異なるようにしてください。

III. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. グローバルでパスワード機能を有効にする	**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

8.5. 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反映されます。

パスワードの有効期限、最小パスワード長、パスワード構成ポリシーは system view、user group view、local user view で設定することができます。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。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 でのグローバル設定は、すべてのユーザグループのローカルユーザに適用されます。

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
5. パスワード構成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1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：ポリシーなし
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-num*	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

8.6. 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、セクション 8 *セキュリティ オペレーションマニュアル*の”*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。
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. パスワード構成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構成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。

8.7. 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**	―

操作	コマンド	補足
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**	デフォルト : ローカルユーザは存在しません。 ネットワークアクセスユーザの代わりにローカルユーザパスワード管理が、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、セクション 8 *セキュリティ オペレーションマニュアル*の”*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. パスワード構成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構成ポリシーと同一です。ユーザグループのパスワード構成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。
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。

8.8. 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**	―
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. パスワード構成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1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。

8.9. 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** *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。

8.10. パスワード管理の設定例

8.10.1. 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:          Enabled (20 days)
  Password length:         Enabled (24 characters)
  Password composition:    Enabled (4 types, 5 characters per type)
```

目次

このセクションのページは **8-x-x** です。

9 章 公開鍵 9-1
9.1. 概要 9-1
9.1.1. 非対象鍵アルゴリズムの概要 9-1
9.1.2. 非対象鍵アルゴリズムの使用 9-1
9.2. 公開鍵設定作業リスト 9-2
9.3. ローカル鍵ペアの作成 9-2
9.4. ローカルホスト公開鍵の分配 9-3
9.4.1. 概要 9-3
9.4.2. ホスト公開鍵のエクスポート 9-4
9.4.3. ホスト公開鍵の表示 9-4
9.5. ピアホスト公開鍵の設定 9-4
9.5.1. 概要 9-4
9.5.2. 制限とガイドライン 9-5
9.5.3. 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 9-5
9.5.4. ピアの公開鍵の入力 9-5
9.6. ローカル鍵ペアの削除 9-6
9.7. 公開鍵の表示と維持 9-6
9.8. 公開鍵の設定例 9-7
9.8.1. ピアのホスト公開鍵の入力例 9-7
9.8.2. 公開鍵ファイルからの公開鍵のインポート例 9-9

9章 公開鍵

9.1. 概要

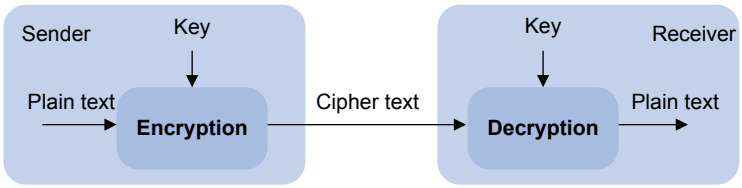
この章では、以下の非対称鍵アルゴリズムの公開鍵の管理について記載します。

- RSA(Revest-Shamir-Adleman)アルゴリズム
- DSA(Digital Signature Algorithm)アルゴリズム

9.1.1. 非対象鍵アルゴリズムの概要

セキュリティアプリケーションは、図 9-1 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 9-1 暗号化と復号化



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。

9.1.2. 非対象鍵アルゴリズムの使用

SSH、SSL、PKI 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。

9.2. 公開鍵設定作業リスト

作業リスト
ローカル鍵ペアの作成
ローカルホスト公開鍵の分配 以下の作業から1つを選択してください。 • 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 • ホスト公開鍵の表示 ローカル装置を認証するようにピアの装置を有効にするため、ローカル装置の公開鍵をピアの装置に分配してください。
ピアホスト公開鍵の設定 以下の作業から1つを選択してください。 • 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 • ホスト公開鍵の入力 ピアの装置に送信する情報を暗合する、あるいはピアの装置のデジタル署名を認証するために、ローカル装置にあるピアの装置の公開鍵を設定してください。
（オプション設定項目）ローカル鍵ペアの削除

9.3. ローカル鍵ペアの作成

I. 制限とガイドライン

ローカル鍵ペアを作成するとき、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。表 9-1 に非対称鍵ペアの異なるタイプの比較を示します。
- 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。もし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 9-1 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	• 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。

タイプ	鍵ペアの数	鍵の長さ、推奨値
	ルト名です。	
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。

II. 設定手順

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

9.4. ローカルホスト公開鍵の分配

9.4.1. 概要

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。

9.4.2. ホスト公開鍵のエクスポート

I. 制限とガイドライン

ホスト公開鍵をエクスポートするとき、以下の制限とガイドラインに従ってください。

- コマンドのファイル名を指定する場合、コマンドは指定したファイルに鍵をエクスポートします。
- ファイル名を指定しない場合、コマンドはモニタ画面に鍵をエクスポートします。手動でファイルに表示された鍵を保存してください。

II. 設定手順

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*]

9.4.3. ホスト公開鍵の表示

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。

9.5. ピアホスト公開鍵の設定

9.5.1. 概要

ピアの装置に送信する情報を暗号化する、あるいはピアの装置のデジタル署名を認証する場合、ローカル装置でピアの装置の公開鍵を設定してください。

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）

装置のホスト公開鍵を取得する方法についてはセクション 8 *セキュリティ オペレーションマニュアル*の“*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。

9.5.2. 制限とガイドライン

ピアのホスト公開鍵を設定するとき、以下の制限とガイドラインに従ってください。

- ピアのホスト公開鍵を手動で設定するとき、入力した鍵が正しいフォーマットであ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。

9.5.3. 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

I. 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、セクション 8 *セキュリティ オペレーションマニュアル*の”*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。

II. 設定手順

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。

9.5.4. ピアの公開鍵の入力

I. 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。

ホスト公開鍵の表示については、セクション 8 *セキュリティ オペレーションマニュアル*の”*公開鍵*”の”*ホスト公開鍵の表示*”を参照してください。

II. 設定手順

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

9.6. ローカル鍵ペアの削除

I. 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

  ローカル証明書の詳細は別紙の共通マニュアル”*QX シリーズ Ethernet スイッチ Web 認証オペレーションマニュアル（V7）*”の“*PKI*”を参照してください。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. ローカル鍵ペアを削除する	**public-key local destroy** { **dsa** | **rsa** } [**name** *key-name*]	—

9.7. 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** [**name** *key-name*]
ピアのホスト公開鍵を表示する	**display public-key peer** [**brief** | **name** *publickey-name*]

9.8. 公開鍵の設定例

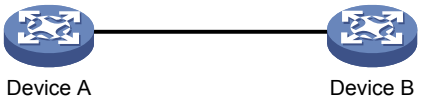
9.8.1. ピアのホスト公開鍵の入力例

I. ネットワーク要件

図 9-2 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、Device B 上で Device A の公開鍵を設定します。

- Device A の認証に RSA の非対称鍵アルゴリズムを使用するために Device B を設定します。
- Device B 上で、Device A の公開鍵ペアのホスト公開鍵を手動で指定します。

図 9-2 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 ~ 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.
```

   # 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:
   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
```

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]30819F300D06092A864886F70D010101050003818D003081890

2818100DA3B90F59237347B

[DeviceB-pkey-public-key-devicea]8D41B58F8143512880139EC9111BFD31EB84B6B7C7A1470027A

C8F04A827B30C2CAF79242E

[DeviceB-pkey-public-key-devicea]45FDFF51A9C7E917DB818D54CB7AEF538AB261557524A7441D2

88EC54A5D31EFAE4F681257

[DeviceB-pkey-public-key-devicea]6D7796490AF87A8C78F4A7E31F0793D8BA06FB95D54EBB9F94E

B1F2D561BF66EA27DFD4788

[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 B に設定されたピアのホスト公開鍵が 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:
   30819F300D06092A864886F70D010101050003818D003081890281810 0DA3B90F59237347B
   8D41B58F8143512880139EC9111BFD31EB84B6B7C7A1470027AC8F04A827B30C2CAF79242E
   45FDFF51A9C7E917DB818D54CB7AEF538AB261557524A7441D288EC54A5D31EFAE4F681257
```

```
    6D7796490AF87A8C78F4A7E31F0793D8BA06FB95D54EBB9F94EB1F2D561BF66EA27DFD4788
    CB47440AF6BB25ACA50203010001
```

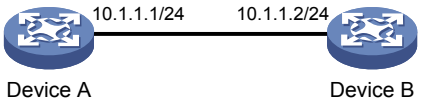
9.8.2. 公開鍵ファイルからの公開鍵のインポート例

I. ネットワーク要件

図 9-3 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、Device B 上で Device A の公開鍵を設定します。

- Device A の認証に RSA の非対称鍵アルゴリズムを使用するために Device B を設定します。
- 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 9-3 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 ~ 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.
```

   # 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

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

Device B に設定されたピアのホスト公開鍵が 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 **8-x-x** です。

10 章 PKI……10-1

10章 PKI

PKI 設定に関するコンフィグについては、別紙の共通マニュアル”*QX シリーズ Ethernet スイッチ Web 認証オペレーションマニュアル*（V7）”の“*PKI*”を参照してください。

目次

このセクションのページは **8-x-x** です。

11 章 SSH 11-1
11.1. 概要 11-1
11.1.1. SSH アプリケーション 11-1
11.1.2. SSH の動作 11-1
11.1.3. SSH 認証方式 11-2
11.2. SSH サーバの設定 11-4
11.2.1. SSH サーバ設定作業リスト 11-4
11.2.2. ローカル鍵ペアの作成 11-4
11.2.3. Stelnet サーバの有効化 11-5
11.2.4. SFTP サーバの有効化 11-5
11.2.5. SCP サーバの有効化 11-6
11.2.6. SSH ログインのユーザラインの設定 11-6
11.2.7. クライアントのホスト公開鍵の設定 11-7
11.2.8. SSH ユーザの設定 11-8
11.2.9. SSH 管理パラメータの設定 11-10
11.2.10. SSH セッションの切断 11-12
11.3. Stelnet クライアントの設定 11-12
11.3.1. Stelnet クライアントの設定作業リスト 11-12
11.3.2. ローカル鍵ペアの作成 11-12
11.3.3. SSH パケットの送信元 IP アドレスの指定 11-13
11.3.4. Stelnet サーバとの接続の確立 11-14
11.4. SFTP クライアントの設定 11-15
11.4.1. SFTP クライアントの設定作業リスト 11-15
11.4.2. ローカル鍵ペアの作成 11-15
11.4.3. SFTP パケットの送信元 IP アドレスの指定 11-15
11.4.4. SFTP サーバとの接続の確立 11-16
11.4.5. SFTP ディレクトリの操作 11-17
11.4.6. SFTP ファイルの操作 11-19
11.4.7. ヘルプ情報の表示 11-20
11.4.8. SFTP サーバの接続の切断 11-21
11.5. SCP クライアントの設定 11-21
11.5.1. SCP クライアントの設定作業リスト 11-21
11.5.2. ローカル鍵ペアの作成 11-21
11.5.3. SCP サーバとの接続の確立 11-22
11.6. SSH2 のアルゴリズムの指定 11-23
11.6.1. SSH2 のアルゴリズム 11-23
11.6.2. SSH2 の鍵交換アルゴリズムの指定 11-23
11.6.3. SSH2 の公開鍵アルゴリズムの指定 11-23
11.6.4. SSH2 の暗号化アルゴリズムの指定 11-24
11.6.5. SSH2 の HMAC アルゴリズムの指定 11-24
11.7. SSH の表示と維持 11-25
11.8. Stelnet 設定例 11-26
11.8.1. パスワード認証を有効にした Stelnet サーバ設定例 11-26

11.8.2. 公開鍵認証を有効にした Stelnet サーバの設定例 ……11-28
11.8.3. パスワード認証を有効にした Stelnet クライアント設定例……11-34
11.8.4. 公開鍵認証を有効にした Stelnet クライアント設定例……11-38
11.9. SFTP 設定例……11-40
11.9.1. パスワード認証を有効にした SFTP サーバの設定例……11-40
11.9.2. 公開鍵認証を有効にした SFTP クライアント設定例……11-42
11.10. SCP 設定例……11-46
11.10.1. パスワード認証を有効にした SCP の設定例 ……11-46

11章 SSH

11.1. 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、SSH はセキュリティ対策が行われていないネットワークを通過して、安全にリモートアクセスを行い、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。

11.1.1. SSH アプリケーション

装置は以下のアプリケーションをサポートします。

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。

- **SFTP（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 を通して、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 spoofing やプレーンテキストパスワード乗っ取りのような攻撃者に対して装置を保護することができます。装置は Stelnet サーバや 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、SFTP は安全なファイル転送を提供するために SSH 接続を使用します。安全なファイル管理と転送を行うためにリモートユーザが SFTP サーバにログインし、装置は SFTP サーバとして動作することができます。装置はユーザが安全なファイル転送を行うため装置からリモート装置にログインすることを許可し、SFTP クライアントとして動作することができます。
- **SCP（Secure Copy）**–SSH2 をもとに、SCP は安全にファイルをコピーします。安全なファイルのアップロードとダウンロードを行うためにユーザが装置にログインし、装置は SCP サーバとして動作することができます。装置はユーザが安全なファイル転送を行うため装置からリモート装置にログインすることを許可し、SCP クライアントとして動作することができます。

SSH クライアントあるいはサーバとして動作するとき、装置は以下の 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とき、装置は SSH2 のみをサポートします。
- Stelnet、SFTP、SCP サーバとして動作するとき、装置は SSH2、SSH1 の両方をサポートします。

11.1.2. 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。

表 11-1 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。
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、SCP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。

11.1.3. 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とき、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とき、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、セクション 8 *セキュリティ オペレーションマニュアル*の”*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。公開鍵認証の処理を以下に示します。

1. クライアントはユーザ名、公開鍵、公開鍵のアルゴリズム名が含まれる公開鍵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必要になる場合、クライアントは認証要求の中にデジタル署名もカプセル化します。デジタル署名はクライアントの公開鍵情報を運びます。
2. サーバはクライアントの公開鍵を確認します。
   - 公開鍵が無効である場合、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、クライアントにデジタル署名を要求します。デジタル署名を受信した後、サーバはデジタル署名を確認するため公開鍵を使用します。認証結果をクライアントに通知します。

装置が SSH サーバとして動作するとき、装置はデジタル署名を確認するために公開鍵アルゴリズム DSA と RSA をサポートします。

装置が SSH クライアントとして動作するとき、装置はデジタル署名を作成するために公開鍵アルゴリズム DSA と RSA をサポートします。

公開鍵の設定についての詳細は、セクション 8 *セキュリティ オペレーションマニュアル*の”*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、どちらか 1 つの認証のみ必要とします。

IV. すべての認証

サーバはパスワード認証あるいは公開鍵のどちらかにパスするように要求します。

11.2. SSHサーバの設定

11.2.1. SSH サーバ設定作業リスト

作業リスト	補足
(必須設定項目)ローカル鍵ペアの作成	―
(必須設定項目) SSHサーバの有効化 • Stelnet サーバの有効化 • SFTP サーバの有効化 • SCP サーバの有効化	―
(必須設定項目)SSHログインのユーザラインの設定	Stelnetでは必須設定項目です。
(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、パスワード認証あるいはすべて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、パスワード認証あるいはすべて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	認証、接続管理の設定のようなSSH管理の設定はSSH接続のセキュリティを向上させます。
(オプション設定項目) SSHセッションの切断	―

11.2.2. ローカル鍵ペアの作成

I. ローカル鍵ペア

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場合も使用します。クライアントがサーバを認証するとき、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てサーバから受信したデジタル署名を認証します。デジタル署名が一致している場合、認証は成功します。

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。

- **RSA 鍵ペア**－SSH サーバは 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。
- **DSA 鍵ペア**－SSH サーバは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 アプリケーションを実行させるため、装置の SSH コマンドを実行するとき、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。

II. 制限とガイドライン

SSH のローカル DSA と RSA 鍵ペアはデフォルトの名前を使用します。鍵ペアに名前を割り当てることができません。

装置にデフォルト名の RSA 鍵ペアがない場合、SSH が開始したときに RSA サーバ鍵ペアと RSA ホスト鍵ペアを自動で作成します。鍵ペアはデフォルト名を使用します。

装置で SSH サーバコマンドを使用するとき、SSH アプリケーションが開始します。

SSH サーバで DSA 鍵ペアを作成するとき、鍵の長さは 2048 ビットよりも短くしてください。

III. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	－
2. ローカル鍵ペアを作成する	**public-key local create** { **dsa** | **rsa** }	－

11.2.3. Stelnet サーバの有効化

I. 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、クライアントが Stelnet を通して装置と通信できます。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	－
2. Stelnet サーバ機能を有効にする	**ssh server enable**	デフォルト：無効

11.2.4. SFTP サーバの有効化

I. SFTP サーバの有効化

装置で SFTP サーバ機能を有効にした後、クライアントは、クライアントが SFTP を通して装置にログインすることができます。

II. 制限とガイドライン

SSH 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。

III. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. SFTP サーバ機能を有効にする	**sftp server enable**	デフォルト：無効

11.2.5. SCP サーバの有効化

I. SCP サーバの有効化

装置で SCP サーバ機能を有効にした後、クライアントは、クライアントが SCP を通して装置にログインすることができます。

II. 制限とガイドライン

SCP 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 SCP 接続をサポートしません。

III. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. SCP サーバ機能を有効にする	**scp server enable**	デフォルト：無効

11.2.6. SSH ログインのユーザラインの設定

I. 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依存して、SSH クライアントは Stelnet、SFTP、SCP クライアントを行うことができます。

Stelnet クライアントではユーザラインの設定が必要です。SFTP クライアントはユーザラインを使用しないで装置にアクセスできます。ユーザラインの設定は次回ログインしたクライアントにのみ適用します。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. VTY line view に移行する	**line vty** *number* [*ending-number*]	—

操作	コマンド	補足
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、Chapter1 *Fundamentals Command Referencesの”Login management commands”*を参照してください。

11.2.7. クライアントのホスト公開鍵の設定

I. クライアントのホスト公開鍵

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、あるいはすべての認証を使用する 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。
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。

   もし装置が 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。

II. クライアントのホスト公開鍵の設定方法

以下の方法を使用してクライアントのホスト公開鍵を設定することができます。

- サーバでクライアントのホスト公開鍵の内容を手動で入力

  a. クライアントのホスト公開鍵を表示し、鍵を記録します。

  b. サーバでクライアントのホスト公開鍵の文字列を入力、あるいはコピー、ペーストします。

  手動で入力した鍵は変換しないで DER 復号形式にする必要があります。クライアントが NEC の装置であるとき表示された鍵を要件に合わせるため、**display public-key local public** コマンドを使用します。別の方法で表示された公開鍵の形式(たとえば **public-key local export** コマンド)は正確ではない可能性があります。鍵が正しい形式ではない場合、システムは鍵を廃棄します。
- 公開鍵ファイルからクライアントのホスト公開鍵のインポート

  a. サーバにクライアントのホスト公開鍵ファイルを保存します。たとえば FTP あるいは TFTP を通して、バイナリモードでサーバにクライアントの公開鍵ファイルを転送します。

  b. ローカルに保存された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。

III. 制限とガイドライン

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。

クライアントのホスト公開鍵のインポートすることを推奨します。

IV. クライアントのホスト公開鍵の入力

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*	—
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とき、空白と改行は自動で削除されます。 詳細は、セクション8 *セキュリティ オペレーションマニュアル*の”*公開鍵*”を参照してください。
4. system view に戻る	**peer-public-key end**	—

V. 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

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*

11.2.8. SSH ユーザの設定

I. SSH ユーザ

認証方式に依存して SSH ユーザ、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。
  - ローカル認証では SSH サーバでローカルユーザを設定します。
  - リモート認証では 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 ユーザを作成する必要がありません。しかし集中管理を行うためパスワードのみの 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である場合、SSH ユーザは以下の処理の 1 つを行う必要があります。
  - ローカル認証では SSH サーバでローカルユーザを設定します。
  - リモート認証では 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。

  いずれの場合においてもリモート認証サーバで設定されたローカルユーザあるいは 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。

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、セクション 8 *セキュリティ オペレーションマニュアル*の”*AAA*”を参照してください。

II. 制限とガイドライン

SSH ユーザがすでにログインしている際、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ときに適用されます。

SFTP、SCP ユーザの作業ディレクトリは認証方式に依存します。

- パスワード認証が使用される場合、作業ディレクトリは AAA によって許可されます。
- 認証方式が公開鍵あるいはパスワード公開鍵である場合、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。

SSH ユーザでは、ユーザロールは認証方式に依存します。

- パスワード認証が使用される場合、ユーザロールはリモート AAA サーバあるいはローカル装置によって許可されます。
- 認証方式が公開鍵あるいはパスワード公開鍵である場合、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。

パスワード認証を除くすべての認証方式は、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存在する必要があります。公開鍵の詳細は、セクション 8 *セキュリティ オペレーションマニュアル*の”*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。

III. 設定手順

操作	コマンド	補足
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** | **netconf** | **scp** | **sftp** | **stelnet** } **authentication-type** { **password** | { **any** | **password-publickey** | **publickey** } [**assign publickey** *keyname*&<1-6>] }	SSHサーバは1024までのSSHユーザをサポートします。

11.2.9. SSH 管理パラメータの設定

I. SSH サーバでの SSH1 クライアントのサポートの有効化

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. 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

II. RSA サーバ鍵ペアのアップデート間隔の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. RSA サーバ鍵ペアのアップデート間隔を設定する	**ssh server rekey-interval** *hours*	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。

III. SSH ユーザ認証タイムアウト時間の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. SSH ユーザ認証タイムアウト時間を設定する	**ssh server authentication-timeout** *time-out-value*	デフォルト：60秒 この設定はTCP接続の悪意のある占有を防止します。 タイムアウト時間が終了したとき、ユーザ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。

IV. SSH 認証の最大試行回数の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. 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 この設定は悪意のあるユーザ名、パスワードのハッキングを防止します。 公開鍵認証とパスワード認証の試行回数は上限を超過することができません。

V. SSH ユーザ接続を制御するため ACL の指定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. SSH ユーザ接続を制御するため ACL を指定する	• IPv4 SSH ユーザ接続を制御する **ssh server acl** { *advanced-acl-number* | *basic-acl-number* | **mac** *mac-acl-number* } • IPv6 SSH ユーザ接続を制御する **ssh server ipv6 acl** { **ipv6** { *advanced-acl-number* | *basic-acl-number* } | **mac** *mac-acl-number* }	デフォルト：設定なし す サーバにSSH接続を開始化するSSHクライアントをフィルタするためACLを使用します。

VI. SSH サーバが SSH クライアントに送信するパケットの DSCP の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. 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 パケットのDSCPはSSHサーバによって送信されます。このフィールドはパケットを転送する優先度を決定します。DSCPが大きいほど高い優先度となります。

VII. SFTP 接続アイドルタイムアウト時間の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. SFTP 接続アイドルタイムアウト時間を設定する	**sftp server idle-timeout** *time-out-value*	デフォルト：10分 SFTP接続のアイドル時間が指定したしきい値を超えたとき、システムは自動的に接続を切断します。

VIII. オンライン SSH ユーザの最大同時接続数の指定

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とき、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。

11.2.10. SSH セッションの切断

I. SSH セッションの切断

装置は同時にログインするセッションをサポートします。設定を邪魔している SSH ログインユーザを避けるため、SSH ログインユーザを切断することができます。

II. 設定手順

user view で実行できます。

操作	コマンド
SSHセッションを切断する	**free ssh** { **user-ip** { *ip-address* | **ipv6** *ipv6-address* } [**port** *port-number*] | **user-pid** *pid-number* | **username** *username* }

11.3. Stelnetクライアントの設定

11.3.1. Stelnet クライアントの設定作業リスト

設定リスト	
(必須設定項目)ローカル鍵ペアの作成	認証方法が公開鍵、パスワード-公開鍵あるいはすべての方法を使用する場合、必須設定項目です。
(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	—

11.3.2. ローカル鍵ペアの作成

I. ローカル鍵ペアの作成

Stelnet サーバが公開鍵、パスワード-公開鍵あるいはすべての方法を使用する場合、Stelnet クライアントでローカル鍵ペアを作成する必要があります。

II. 制限とガイドライン

SSH のローカル DSA と RSA 鍵ペアはデフォルトの名前を使用します。鍵ペアに名前を割り当てることができません。

SSH サーバで DSA 鍵ペアを作成するとき、鍵の長さは 2048 ビットよりも短くしてください。

III. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. ローカル鍵ペアを作成する	**public-key local create** { **dsa** | **rsa** }	—

11.3.3. SSH パケットの送信元 IP アドレスの指定

I. SSH パケットの送信元 IP アドレスの指定

Stelnet クライアントで送信する SSH パケットの送信元 IP アドレスを指定した後、クライアントは Stelnet サーバと通信するため指定された IP アドレスを使用します。

II. 制限とガイドライン

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。

III. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
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 IPv4 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ルーティングエントリ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 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。

11.3.4. Stelnet サーバとの接続の確立

I. Stelnet サーバとの接続の確立

装置で Stelnet クライアント機能を有効にし、Stelnet サーバと通信を確立するため、この機能を使用します。接続中に使用される公開鍵アルゴリズム、暗号化アルゴリズム、HMAC アルゴリズム、鍵交換アルゴリズムを指定します。

Stelnet サーバにアクセスするとき、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する必要があります。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。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。ダウンロードされた公開鍵は後続のアクセスでサーバの認証に使用します。

  サーバに接続するときサーバの公開鍵を指定しない場合、装置はサーバの公開鍵を公開鍵に保存します。サーバの公開鍵は設定ファイルに保存されません。
- 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。

II. 制限とガイドライン

Stelnet クライアントは IPv4、IPv6 Stelnet サーバの両方の接続を確立することができません。

III. IPv4 Stelnet サーバの接続の確立

user view で実行できます。

操作	コマンド
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* }] *

IV. IPv6 Stelnet サーバの接続の確立

user view で実行できます。

操作	コマンド
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* }] *

11.4. SFTPクライアントの設定

11.4.1. SFTP クライアントの設定作業リスト

作業リスト	
(必須設定項目)ローカル鍵ペアの作成	認証方法が公開鍵、パスワード-公開鍵あるいはすべての方法を使用する場合、必須設定項目です。
(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	—

11.4.2. ローカル鍵ペアの作成

I. ローカル鍵ペアの作成

SFTP クライアントが公開鍵、パスワード-公開鍵あるいはすべての方法を使用する場合、SFTP クライアントでローカル鍵ペアを作成する必要があります。

II. 制限とガイドライン

SSH のローカル DSA と RSA 鍵ペアはデフォルトの名前を使用します。鍵ペアに名前を割り当てることができません。

SSH サーバで DSA 鍵ペアを作成するとき、鍵の長さは 2048 ビットよりも短くしてください。

III. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. ローカル鍵ペアを作成する	**public-key local create** { **dsa** | **rsa** }	—

11.4.3. SFTP パケットの送信元 IP アドレスの指定

I. SFTP パケットの送信元 IP アドレスの指定

SFTP クライアントで送信する SFTP パケットの送信元 IP アドレスを指定した後、クライアントは SFTP サーバと通信するため指定された IP アドレスを使用します。

II. 制限とガイドライン

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。

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. 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ルーティングエントリ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 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。

11.4.4. SFTP サーバとの接続の確立

I. SFTP サーバとの接続の確立

装置で SFTP クライアント機能を有効にし、SFTP サーバと通信を確立するため、この機能を使用します。接続中に使用される公開鍵アルゴリズム、暗号化アルゴリズム、HMAC アルゴリズム、鍵交換アルゴリズムを指定します。

SFTP サーバにアクセスするとき、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する必要があります。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。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。ダウンロードされた公開鍵は後続のアクセスでサーバの認証に使用します。

  サーバに接続するときサーバの公開鍵を指定しない場合、装置はサーバの公開鍵を公開鍵に保存します。サーバの公開鍵は設定ファイルに保存されません。
- 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。

II. 制限とガイドライン

SFTP クライアントは IPv4、IPv6 SFTP サーバの両方の接続を確立することができません。

III. IPv4 SFTP サーバの接続の確立

user view で実行できます。

操作	コマンド
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* }] *

IV. IPv6 SFTP サーバの接続の確立

user view で実行できます。

操作	コマンド
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* }] *

11.4.5. SFTP ディレクトリの操作

I. SFTP ディレクトリの操作

SFTP サーバと接続を確立したのち、SFTP サーバのディレクトリを操作することができます。

II. SFTP サーバの作業ディレクトリの変更

操作	コマンド	補足
1. SFTP client view に移行する	セクション8 *セキュリティオペレーションマニュアル*の“*SSH*”の“*SFTPサーバとの接続の確立*”を参照してください。	—
2. SFTP サーバの作業ディレクトリを変更する	**cd** [*remote-path*]	—
3. （オプション項目）上位のディレクトリに戻る	**cdup**	—

III. SFTP サーバの現在の作業ディレクトリの表示

操作	コマンド	補足
1. SFTP client view に移行する	セクション8 *セキュリティオペレーションマニュアル* の“*SSH*”の“*SFTP サーバとの接続の確立*”を参照してください。	—
2. SFTP サーバの現在の作業ディレクトリを表示する	**pwd**	—

IV. 指定したディレクトリにあるファイルの表示

操作	コマンド	補足
1. SFTP client view に移行する	セクション8 *セキュリティオペレーションマニュアル* の“*SSH*”の“*SFTP サーバとの接続の確立*”を参照してください。	—
2. 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*]	**dir**コマンドは**ls**コマンドと同一です。

V. SFTP サーバの指定したディレクトリ名の変更

操作	コマンド	補足
1. SFTP client view に移行する	セクション8 *セキュリティオペレーションマニュアル* の“*SSH*”の“*SFTP サーバとの接続の確立*”を参照してください。	—
2. SFTP サーバの指定したディレクトリ名を変更する	**rename** *oldname newname*	—

VI. SFTP サーバで新しいディレクトリの作成

操作	コマンド	補足
1. SFTP client view に移行する	セクション8 *セキュリティオペレーションマニュアル* の“*SSH*”の“*SFTP サーバとの接続の確立*”を参照してください。	—
2. SFTP サーバで新しいディレクトリを作成する	**mkdir** *remote-path*	—

VII. SFTP サーバのディレクトリの削除

操作	コマンド	補足
1. SFTP client view に移行する	セクション8 *セキュリティオペレーションマニュアル* の“*SSH*”の“*SFTPサーバとの接続の確立*”を参照してください。	—
2. 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*	—

11.4.6. SFTP ファイルの操作

I. SFTP ファイルの操作

SFTP サーバと接続を確立したのち、SFTP サーバのファイルを操作することができます。

II. SFTP サーバのファイル名の変更

操作	コマンド	補足
1. SFTP client view に移行する	セクション8 *セキュリティオペレーションマニュアル* の“*SSH*”の“*SFTPサーバとの接続の確立*”を参照してください。	—
2. SFTP サーバの指定したファイル名を変更する	**rename** *old-name new-name*	—

III. リモートサーバからファイルのダウンロードおよびローカルへの保存

操作	コマンド	補足
1. SFTP client view に移行する	セクション8 *セキュリティオペレーションマニュアル* の“*SSH*”の“*SFTPサーバとの接続の確立*”を参照してください。	—
2. リモート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*]	—

IV. SFTP サーバへのローカルファイルのアップロード

操作	コマンド	補足
1. SFTP client view に移行する	セクション8 *セキュリティオペレーションマニュアル* の“*SSH*”の“*SFTPサーバとの接続の確立*”を参照してください。	—

操作	コマンド	補足
2. 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*]	—

V. ディレクトリにあるファイルの表示

操作	コマンド	補足
1. SFTP client view に移行する	セクション8 *セキュリティオペレーションマニュアル* の“*SSH*”の“*SFTPサーバとの接続の確立*”を参照してください。	—
2. 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*]	**dir**コマンドは**ls**コマンドと同一です。

VI. SFTP サーバからディレクトリの削除

操作	コマンド	補足
1. SFTP client view に移行する	セクション8 *セキュリティオペレーションマニュアル* の“*SSH*”の“*SFTPサーバとの接続の確立*”を参照してください。	—
2. 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	**delete**コマンドは**remove**コマンドと同一です。

11.4.7. ヘルプ情報の表示

I. ヘルプ情報の表示

SFTP サーバと接続を確立したのち、SFTP クライアントの Syntax、パラメータの設定が含まれるヘルプ情報を表示することができます。

II. 設定手順

操作	コマンド	補足
1. SFTP client view に移行する	セクション8 *セキュリティオペレーションマニュアル* の“*SSH*”の“*SFTPサーバとの接続の確立*”を参照してください。	—
2. SFTP クライアントコマンドのヘルプ情報を表示する	• **help** • **?**	**help**コマンドは**?**コマンドと同一です。

11.4.8. SFTP サーバの接続の切断

操作	コマンド	補足
1. SFTP client view に移行する	セクション8 *セキュリティオペレーションマニュアル* の“*SSH*”の“*SFTPサーバとの接続の確立*”を参照してください。	―
2. SFTP サーバの接続を切断し、user view に戻る	• **bye** • **exit** • **quit**	3つのコマンドは同一機能です。

11.5. SCPクライアントの設定

11.5.1. SCP クライアントの設定作業リスト

作業リスト	
(必須設定項目)ローカル鍵ペアの作成	認証方法が公開鍵、パスワード-公開鍵あるいはすべての方法を使用する場合、必須設定項目です。
(必須設定項目) SCPサーバとの接続の確立	―

11.5.2. ローカル鍵ペアの作成

I. ローカル鍵ペアの作成

SCP クライアントが公開鍵、パスワード-公開鍵あるいはすべての方法を使用する場合、SCP クライアントでローカル鍵ペアを作成する必要があります。

II. 制限とガイドライン

SSH のローカル DSA と RSA 鍵ペアはデフォルトの名前を使用します。鍵ペアに名前を割り当てることができません。

SSH サーバで DSA 鍵ペアを作成するとき、鍵の長さは 2048 ビットよりも短くしてください。

III. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. ローカル鍵ペアを作成する	**public-key local create** { **dsa** | **rsa** }	―

11.5.3. SCP サーバとの接続の確立

I. SCP サーバとの接続の確立

装置で SCP クライアント機能を有効にし、SCP サーバと通信を確立するため、この機能を使用します。接続中に使用される公開鍵アルゴリズム、暗号化アルゴリズム、HMAC アルゴリズム、鍵交換アルゴリズムを指定します。

SCP サーバにアクセスするとき、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する必要があります。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。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。ダウンロードされた公開鍵は後続のアクセスでサーバの認証に使用します。

  サーバに接続するときサーバの公開鍵を指定しない場合、装置はサーバの公開鍵を公開鍵に保存します。サーバの公開鍵は設定ファイルに保存されません。
- 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。

II. 制限とガイドライン

SCP クライアントは IPv4、IPv6 SCP サーバの両方の接続を確立することができません。

III. IPv4 SCP サーバの接続の確立

user view で実行できます。

操作	コマンド
IPv4 SCPサーバの接続を確立する	**scp** *server* [*port-number*] { **put** | **get** } *source-file-name* [*destination-file-name*] [**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** }] * [**public-key** *keyname* | **source** { **interface** *interface-type interface-number* | **ip** *ip-address* }] *

IV. IPv6 SCP サーバの接続の確立

user view で実行できます。

操作	コマンド
IPv6 SCPサーバの接続を確立する	**scp ipv6** *server* [*port-number*] [**-i** *interface-type interface-number*] { **put** | **get** } *source-file-name* [*destination-file-name*] [**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** }] * [**public-key** *keyname* | **source** { **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }] *

11.6. SSH2のアルゴリズムの指定

11.6.1. SSH2 のアルゴリズム

SSH2 クライアントおよびサーバは、Stelnet、SFTP、または SCP セッションの確立時に、アルゴリズムネゴシエーションに次のタイプのアルゴリズムを使用します。

- 鍵交換アルゴリズム
- 公開鍵アルゴリズム
- 暗号化アルゴリズム
- HMAC アルゴリズム

アルゴリズムを指定すると、SSH2 は指定されたアルゴリズムのみをアルゴリズムネゴシエーションに使用します。クライアントは指定されたアルゴリズムを使用してネゴシエーションを起動し、サーバはクライアントとのネゴシエートに一致するアルゴリズムを使用します。同じタイプの複数のアルゴリズムが指定された場合、ネゴシエーション期間中は、先に指定されたアルゴリズムの方が優先されます。

11.6.2. SSH2 の鍵交換アルゴリズムの指定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. SSH2 の鍵交換アルゴリズムを指定する	**ssh2 algorithm key-exchange** { **dh-group-exchange-sha1** | **dh-group1-sha1** | **dh-group14-sha1** | **ecdh-sha2-nistp256** | **ecdh-sha2-nistp384** } *	デフォルト：SSH2は、アルゴリズムネゴシエーションの優先度の高い順に、鍵交換アルゴリズム **ecdh-sha2-nistp256**、**ecdh-sha2-nistp384**、**dh-group-exchange-sha1**、**dh-group14-sha1**、および **dh-group1-sha1**を使用します。

メモ:

ssh2 algorithm key-exchange コマンドは Version7.2.17 を含む以降のソフトウェアからサポートしています。

11.6.3. SSH2 の公開鍵アルゴリズムの指定

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. SSH2 の公開鍵アルゴリズムを指定する	**ssh2 algorithm public-key** { **dsa** | **ecdsa-sha2-nistp256** | **ecdsa-sha2-nistp384** | **rsa** | **x509v3-ecdsa-sha2-nistp256** | **x509v3-ecdsa-sha2-nistp384** } *	デフォルト：SSH2は、アルゴリズムネゴシエーションの優先度の高い順に、公開鍵アルゴリズム **x509v3-ecdsa-sha2-nistp256**、**x509v3-ecdsa-sha2-nistp384**、**ecdsa-sha2-nistp256**、**ecdsa-sha2-nistp384**、**rsa**、および**dsa**を使用します。

🕮 **メモ:**

ssh2 algorithm public-key コマンドは Version7.2.17 を含む以降のソフトウェアからサポートしています。

11.6.4. SSH2 の暗号化アルゴリズムの指定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. SSH2 の暗号化アルゴリズムを指定する	**ssh2 algorithm cipher** { **3des-cbc** | **aes128-cbc** | **aes128-ctr** | **aes128-gcm** | **aes192-ctr** | **aes256-cbc** | **aes256-ctr** | **aes256-gcm** | **des-cbc** } *	デフォルト：SSH2は、アルゴリズムネゴシエーションの優先度の高い順に、暗号化アルゴリズム**aes128-ctr**、**aes192-ctr**、**aes256-ctr**、**aes128-gcm**、**aes256-gcm**、**aes128-cbc**、**3des-cbc**、**aes256-cbc**、**des-cbc**を使用します。

🕮 **メモ:**

ssh2 algorithm cipher コマンドは Version7.2.17 を含む以降のソフトウェアからサポートしています。

11.6.5. SSH2 の HMAC アルゴリズムの指定

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. SSH2 の HMAC アルゴリズムを指定する	**ssh2 algorithm mac** { **md5** | **md5-96** | **sha1** | **sha1-96** | **sha2-256** | **sha2-512** } *	デフォルト：SSH2は、アルゴリズムネゴシエーションの優先度の高い順に、HMACアルゴリズム**sha2-256**、**sha2-512**、**sha1**、**md5**、**sha1-96**、**md5-96**を使用します。

メモ:

ssh2 algorithm mac コマンドは Version7.2.17 を含む以降のソフトウェアからサポートしています。

11.7. 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
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*]
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**
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*]
アルゴリズムネゴシエーション段階でSSH2によって使用されるアルゴリズムを表示する	**display ssh2 algorithm**

メモ:

display ssh2 algorithm コマンドは Version7.2.17 を含む以降のソフトウェアからサポートしています。

display public-key local コマンド、**display public-key peer** コマンドの詳細は Chapter 8 *Security Command References* の“*Public key management commands*”を参照してください。

11.8. Stelnet設定例

別の方法で記載されていない限り、設定例の装置は動作します。

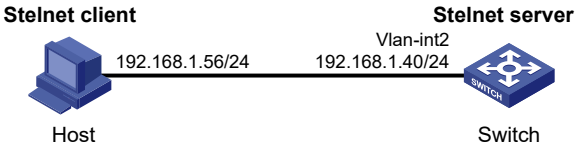
11.8.1. パスワード認証を有効にした Stelnet サーバ設定例

I. ネットワーク要件

図 11-1 に示すように設定します。

- Switch は Stelnet サーバとして動作し、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 クライアントソフトウェア（SSH2）を使用して Stelnet クライアントとして動作します。Stelnet を通して Switch にログインすることができます。ログインした後、設定の管理を行うため、ユーザロール network-admin が割り当てられます。

図 11-1 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 ~ 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 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.
```

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** に設定します。

[Switch-luser-manage-client001] password simple aabbcc

ユーザのサービスタイプを **ssh** に設定します。

[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。

[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。

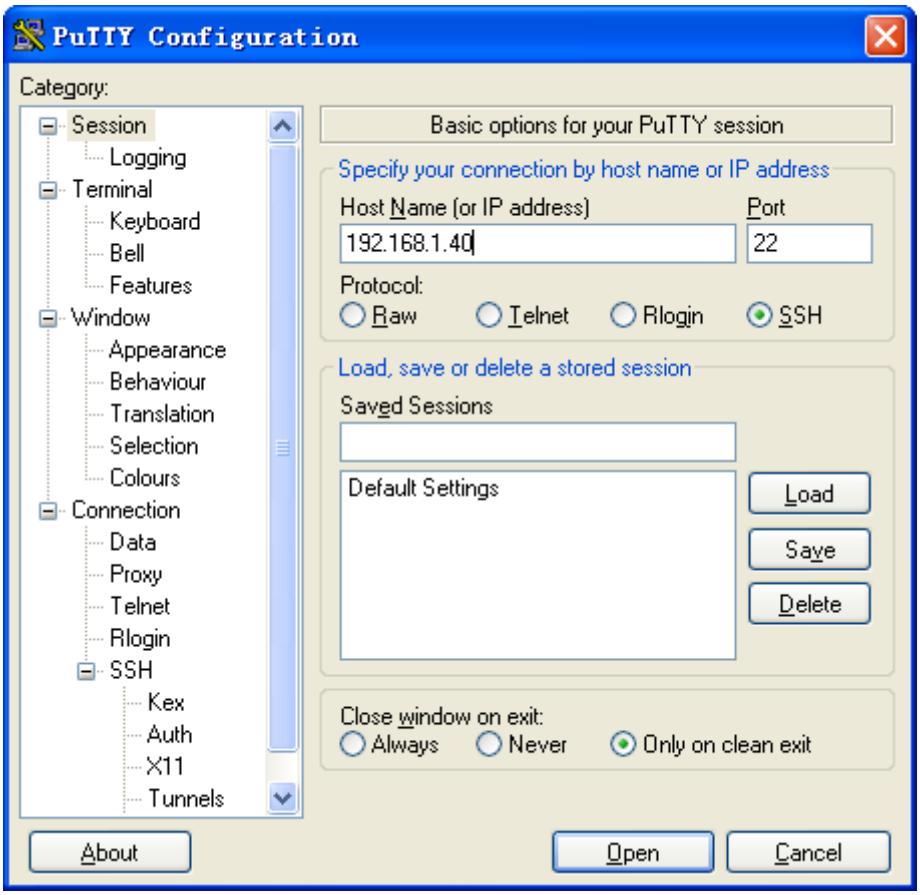
   Stelnet サーバとの接続を確立します。

   a. 図 11-2 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. サーバに接続するため、**Open** をクリックします。

図 11-2 ホスト名(あるいは IP アドレス)の指定



d. Stelnet サーバにログインするため、ユーザ名 **client001**、パスワード **aabbcc** を入力します。

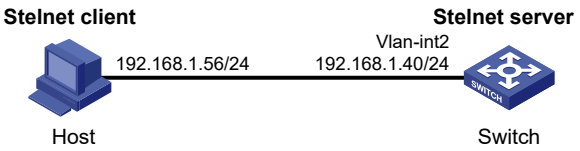
11.8.2. 公開鍵認証を有効にした Stelnet サーバの設定例

I. ネットワーク要件

図 11-3 に示すように設定します。

- Switch は Stelnet サーバとして動作し、公開鍵認証と RSA 公開鍵アルゴリズムを使用します。
- ホストは Stelnet クライアントソフトウェア（SSH2）を使用して Stelnet クライアントとして動作します。Stelnet を通して Switch にログインすることができます。ログインした後、設定の管理を行うため、ユーザロール network-admin が割り当てられます。

図 11-3 ネットワーク図



II. 設定手順

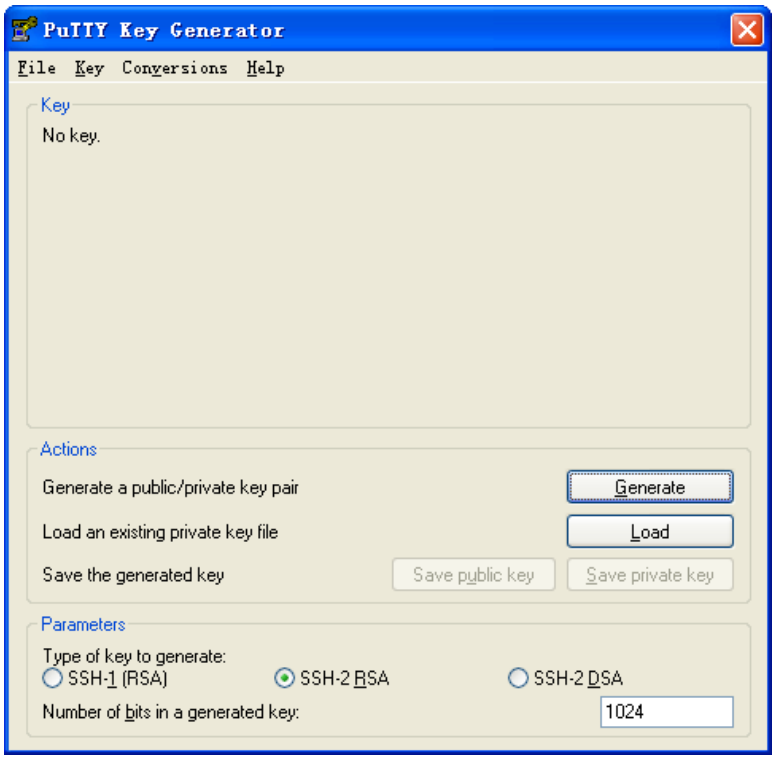
サーバの設定では、クライアントのホスト公開鍵が必要となります。Stelnet サーバを設定する前に、クライアントで RSA 鍵ペアを作成するため、クライアントソフトウェアを使用します。

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。

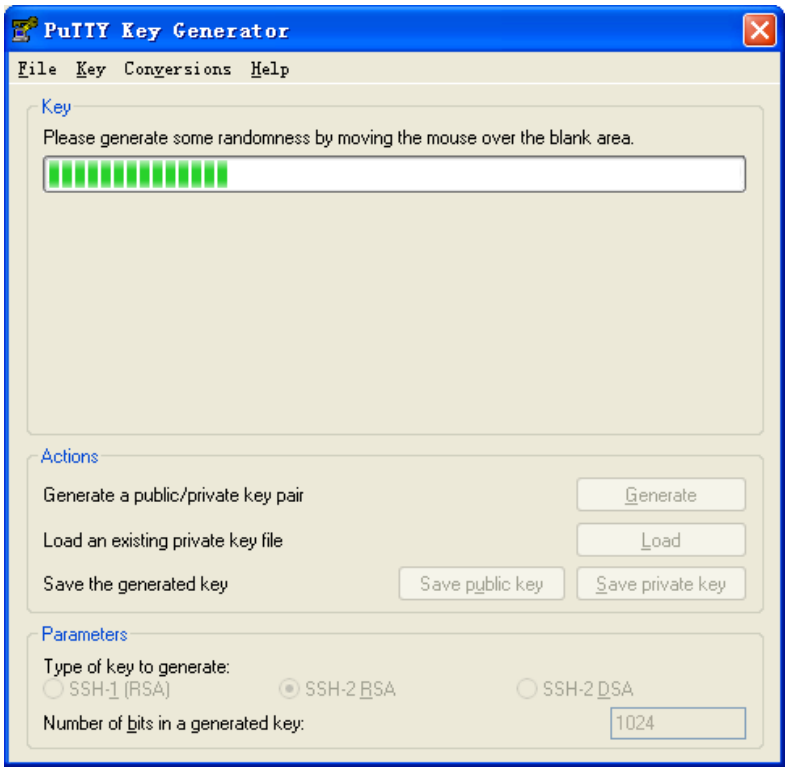
1. Stelnet クライアントで RSA 鍵ペアを作成します。
   a. クライアントで PuTTY.exe を起動させ、SSH-2 RSA を選択し、Generate をクリックします。

図 11-4 クライアントの鍵ペアの作成



   b. 鍵ペアを作成しているとき、マウスを継続して動かしてください。図 11-5 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。そうしなければ、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。

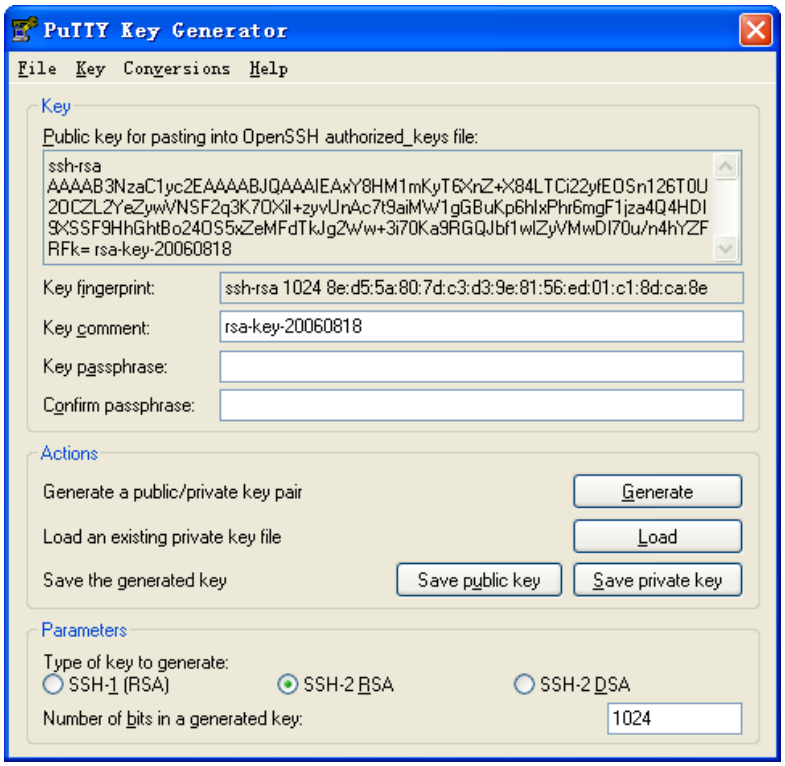
図 11-5 プロセスの作成



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 11-6 クライアントの鍵ペアの保存



d. 図 11-6 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。

e. **Yes** をクリックします。

f. 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。

g. 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 ~ 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 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.
```

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。

[Switch] local-user client002 class manage

ユーザのサービスタイプを **ssh** に設定します。

[Switch-luser-manage-client002] service-type ssh

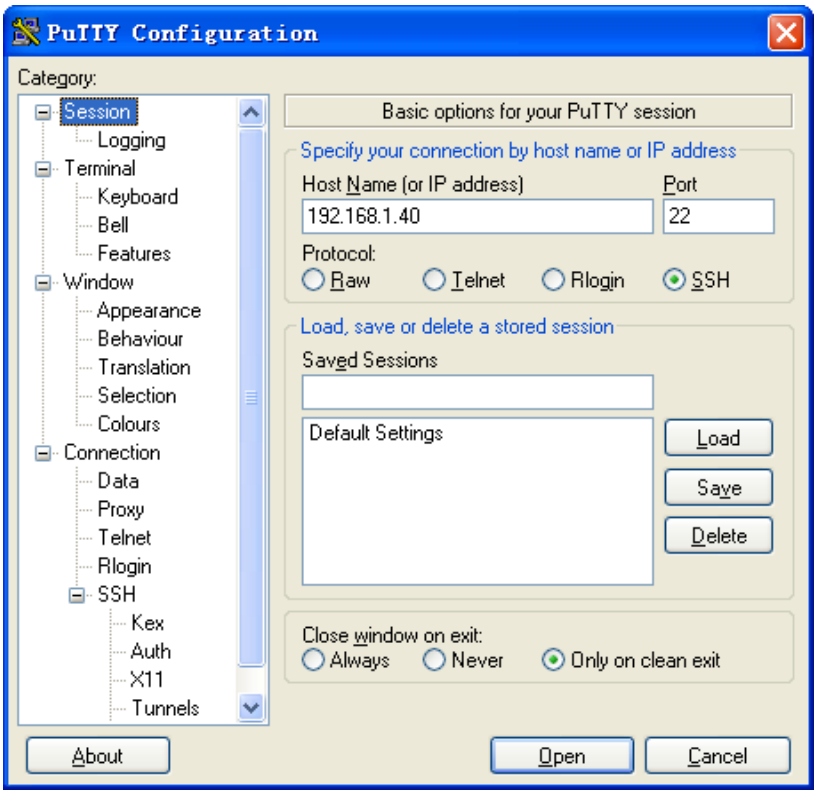
ユーザロールを **network-admin** に設定します。

[Switch-luser-manage-client002] authorization-attribute user-role network-admin

[Switch-luser-manage-client002] quit

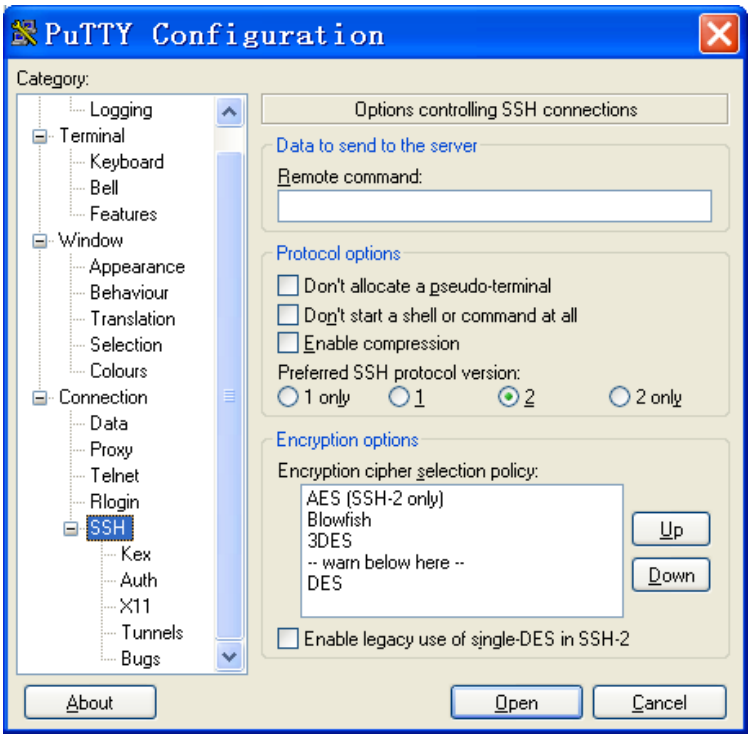
3. 秘密鍵ファイルを指定し、Stelnet サーバとの接続を確立します。
   a. 図 11-7 に示すように Stelnet クライアントで PuTTY.exe を起動させ、インタフェースに移行します。
   b. **Host Name** フィールド(あるいは **IP address**)で、Stelnet サーバの IP アドレス 192.168.1.40 を入力します。

図 11-7 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 11-8 に示すようにウィンドウ画面を表示します。

図 11-8 SSH バージョンの指定

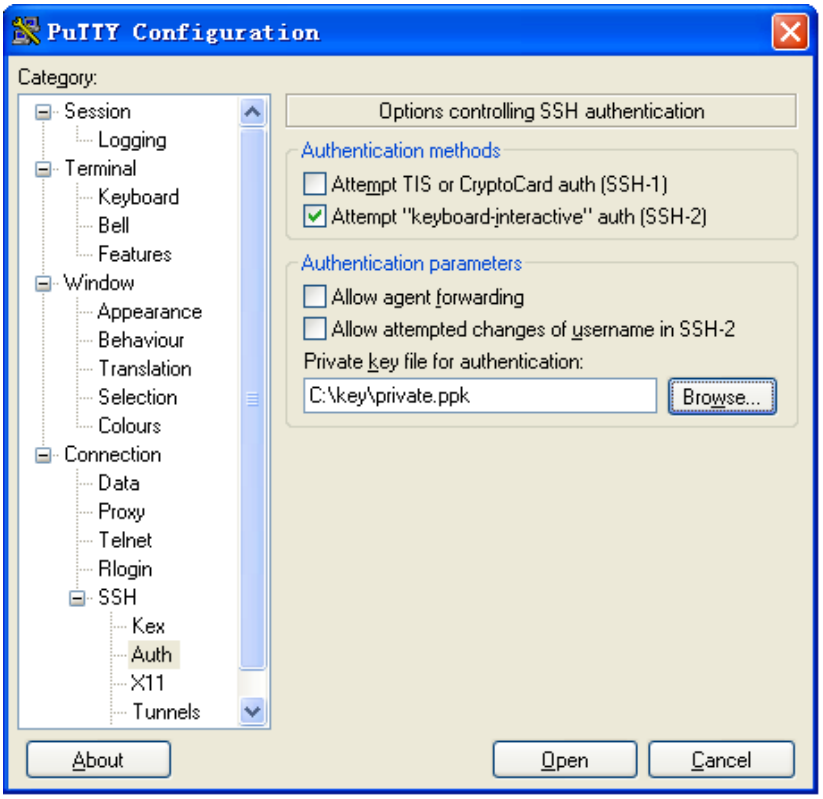


d. ナビゲーションツリーから **Connection** を選択し、**SSH** を選択し、**Auth** を選択します。図 11-9 に示すようにウィンドウ画面を表示します。

e. 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。

f. サーバに接続するため、**Open** をクリックします。

図 11-9 秘密鍵ファイルの指定



h. Stelnet サーバに接続するため、ユーザ名（**client002**）を入力します。

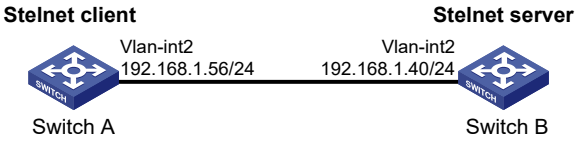
11.8.3. パスワード認証を有効にした Stelnet クライアント設定例

l. ネットワーク要件

図 11-10 示すように設定します。

- Switch B は Stelnet サーバとして動作し、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 B に保存されます。
- Switch A の Stelnet クライアントを通して、Switch B にログインすることができます。ログインした後、設定の管理を行うため、ユーザロール network-admin が割り当てられます。

図 11-10 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 ~ 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 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

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** に指定します。

[SwitchB-luser-manage-client001] password simple aabbcc

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。

2. [SwitchB] ssh user client001 service-type stelnet authentication-type passwordStelnet 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

     Enter public key view. Return to system view with "peer-public-key end" command.

     [SwitchA-pkey-public-key-key1]308201B73082012C06072A8648CE3804013082011F02818100D757262C4584C44C211F18BD96E5F0

     [SwitchA-pkey-public-key-key1]61C4F0A423F7FE6B6B85B34CEF72CE14A0D3A5222FE08CECE65BE6C265854889DC1EDBD13EC8B274

     [SwitchA-pkey-public-key-key1]DA9F75BA26CCB987723602787E922BA84421F22C3C89CB9B06FD60FE01941DDD77FE6B12893DA76E

     [SwitchA-pkey-public-key-key1]EBC1D128D97F0678D7722B5341C8506F358214B16A2FAC4B368950387811C7DA33021500C773218C

     [SwitchA-pkey-public-key-key1]737EC8EE993B4F2DED30F48EDACE915F028181008226900 9E14EC474BAF2932E69D3B1F18517AD95

     [SwitchA-pkey-public-key-key1]94184CCDFCEAE96EC4D5EF93133E84B47093C52B20CD35D02492B3959EC6499625BC4FA5082E22C5

[SwitchA-pkey-public-key-key1]B374E16DD00132CE71B020217091AC717B612391C76C1FB2E88317C1BD8171D41ECB83E210C03CC9

[SwitchA-pkey-public-key-key1]B32E810561C21621C73D6DAAC028F4B1585DA7F42519718CC9B09EEF0381840002818000AF995917

[SwitchA-pkey-public-key-key1]E1E570A3F6B1C2411948B3B4FFA256699B3BF871221CC9C5DF257523777D033BEE77FC378145F2AD

[SwitchA-pkey-public-key-key1]D716D7DB9FCABB4ADBF6FB4FDB0CA25C761B308EF53009F7101F7C62621216D5A572C379A32AC290

[SwitchA-pkey-public-key-key1]E55B394A217DA38B65B77F0185C8DB8095522D1EF044B465E8716261214A5A3B493E866991113B2D

[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とき、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、**Y** 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 **aabbcc** 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。次回接続を行うとき、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。

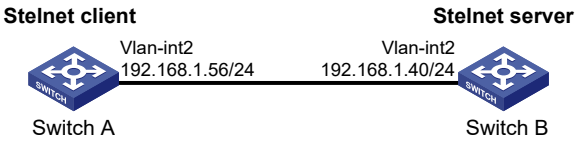
11.8.4. 公開鍵認証を有効にした Stelnet クライアント設定例

I. ネットワーク要件

図 11-11 に示すように設定します。

- Switch 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。
- Switch A で動作する Stelnet クライアントを通して、Switch B にログインすることができます。ログインした後、設定の管理を行うため、ユーザロール network-admin が割り当てられます。

図 11-11 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 ~ 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 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。

[SwitchB] local-user client002 class manage

ユーザのサービスタイプを SSH に指定します。

[SwitchB-luser-manage-client002] service-type ssh

ユーザにユーザロール **network-admin** を割り当てます。

[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 **Y** を選択し、サーバのホスト公開鍵をダウンロードします。次回接続を行うとき、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。

11.9. SFTP設定例

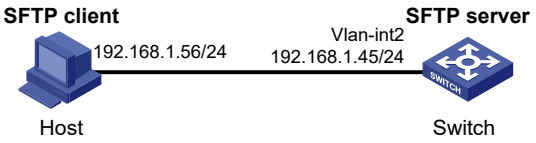
11.9.1. パスワード認証を有効にした SFTP サーバの設定例

I. ネットワーク要件

図 11-12 に示すように設定します。

- SFTP サーバとして Switch が動作し、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。
- ホストで動作する SFTP クライアントを通して Switch にログインすることができます。ログインした後、ファイルの管理と転送を行うため、ユーザロール network-admin が割り当てられます。

図 11-12 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 ~ 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 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。

[Switch] local-user client002 class manage

プレーンテキストのパスワードを **aabbcc** とします。

[Switch-luser-manage-client002] password simple aabbcc

サービスタイプを **ssh** とします。

[Switch-luser-manage-client002] 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。

[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。

[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。

メモ:

PSFTP はパスワード認証のみサポートしています。

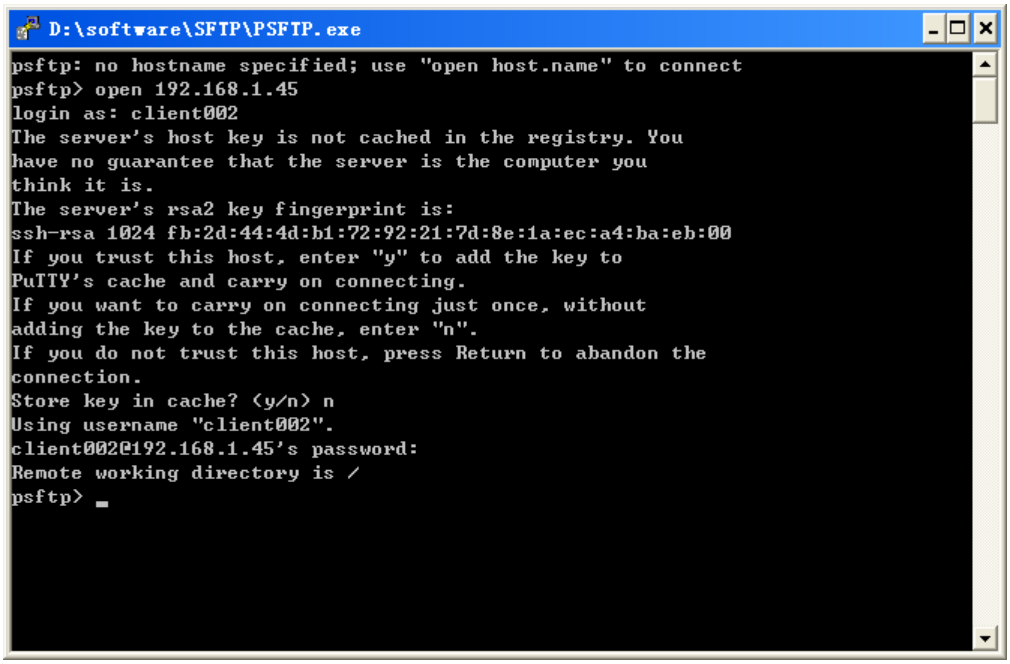
SFTP サーバへの接続を確立するために、以下を行います。

a. 図 11-13 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 サーバに接続するため、パスワード **aabbcc** を入力します。

図 11-13 SFTP クライアントインタフェース



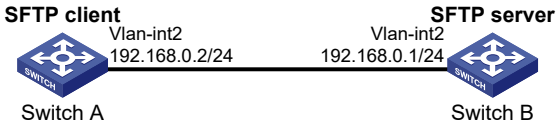
11.9.2. 公開鍵認証を有効にした SFTP クライアント設定例

I. ネットワーク要件

図 11-14 に示すように設定します。

- SFTP サーバとして Switch 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。
- Switch A で動作する SFTP クライアントを通して Switch B にログインすることができます。ログインした後、ファイルの管理と転送を行うため、ユーザロール network-admin が割り当てられます。

図 11-14 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 ~ 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.
```

   # 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 ~ 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 鍵ペアを作成します。

[SwitchB] public-key local create dsa

```
The range of public key size 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** を作成します。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>
```

11.10. SCP設定例

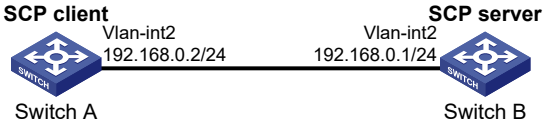
11.10.1. パスワード認証を有効にした SCP の設定例

I. ネットワーク要件

図 11-15 に示すように設定します。

- SCP サーバとして Switch B が動作し、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 B に保存されます。
- SCP クライアントとして Switch A が動作します。Switch A のユーザが SCP を通して Switch B にログインした後、ネットワーク管理者として Switch 間のファイルを転送することができます。

図 11-15 ネットワーク図



II. 設定手順

1. SCP 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 ~ 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 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.
```

SCP サーバ機能を有効にします。

[SwitchB] scp server enable

VLAN インタフェース 2 に IP アドレスを割り当てます。クライアントは SCP 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

ローカル装置管理ユーザ **client001** を作成します。

[SwitchB] local-user client001 class manage

プレーンテキストのパスワードを **aabbcc** とします。

[SwitchB-luser-manage-client001] password simple aabbcc

サービスタイプを **ssh** とします。

[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。ユーザの認証モードを **password**、サービスタイプを **scp** に設定します。

[SwitchB] ssh user client001 service-type scp authentication-type password

2. SCP クライアントの VLAN インタフェース 2 を IP アドレスに設定します。

<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

[SwitchA] quit

3. SCP サーバに接続し、サーバからファイル **remote.bin** をダウンロードし、ローカルファイル **local.bin** に保存します。

<SwitchA> scp 192.168.0.1 get remote.bin local.bin

```
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
client001@192.168.0.1's password:
remote.bin                                    100% 2875     2.8KB/s   00:00
```

目次

このセクションのページは **8-x-x** です。

12 章 SSL 12-1

12章 SSL

SSL の設定に関するコンフィグについては、別紙の共通マニュアル”*QX シリーズ Ethernet スイッチ Web 認証オペレーションマニュアル*（V7）”の“*SSL*”を参照してください。

目次

このセクションのページは **8-x-x** です。

13 章 TCP フラグメントアタックプロテクション 13-1
13.1. 概要 13-1
13.2. 検出、保護可能な攻撃の種類 13-1
13.2.1. TCP フラグメントアタック 13-1
13.3. TCP フラグメントアタックプロテクション機能の設定 13-1

13章 TCP フラグメントアタックプロテクション

13.1. 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。

13.2. 検出、保護可能な攻撃の種類

この章は装置が検出、保護できる攻撃について記載します。

13.2.1. TCP フラグメントアタック

RFC 1858 で定義されているように、TCP フラグメントは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。

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リングができないために、2 番目以降のフラグメントも透過してしまいます。受信ホストがフラグメントパケットを再構築すると TCP フラグメントアタックが行われます。

TCP フラグメントアタックを防ぐため 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。

13.3. 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。装置は CPU を通して転送された TCP フラグメントのみを検出します。

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**	デフォルト：有効

目次

このセクションのページは **8-x-x** です。

14 章 IP ソースガード 14-1
14.1. 概要 14-1
14.1.1. IP ソースガード動作メカニズム 14-1
14.1.2. スタティック IP ソースガードのバインディング 14-1
14.1.3. ダイナミック IP ソースガードのバインディング 14-2
14.2. IP ソースガードの設定作業リスト 14-3
14.3. IPv4 ソースガード機能の設定 14-3
14.3.1. インタフェースの IPv4 ソースガードの有効化 14-3
14.3.2. スタティック IPv4 ソースガードバインディングの設定 14-4
14.4. IPv6 ソースガード機能の設定 14-5
14.4.1. インタフェースでの IPv6 ソースガードの有効化 14-5
14.4.2. スタティック IPv6 ソースガードバインディングの設定 14-5
14.5. IP ソースガードの表示と維持 14-6
14.6. IP ソースガードの設定 14-6
14.6.1. DHCP snooping を使用したダイナミック IPv4 ソースガードの設定例 14-6
14.6.2. スタティック IPv6 ソースガード設定例 14-8

14章 IP ソースガード

14.1. 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。この機能はユーザ側のインタフェースで一般的に設定されます。

14.1.1. IP ソースガード動作メカニズム

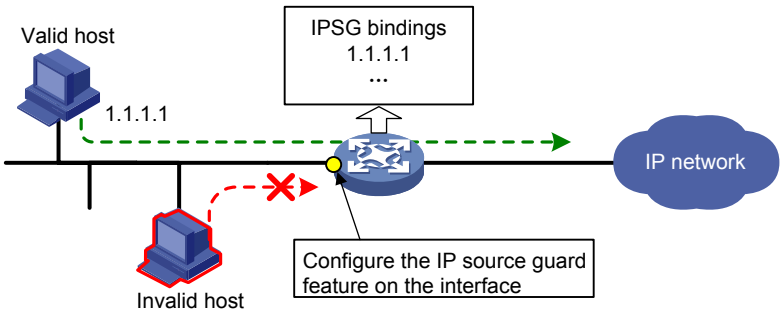
IP ソースガードバインディングテーブルは、IP アドレス、MAC アドレス、VLAN、あるいはそれらの組み合わせが含まれます。IP ソースガードは入力パケットに一致するバインディングを使用します。バインディングが一致した場合、パケットは転送されます。一致しない場合、パケットは廃棄されます。

IP ソースガードはインタフェースごとにパケットをフィルタします。あるインタフェースで IP ソースガードを設定した場合、他のインタフェースの転送には影響しません。

IP ソースガードのバインディングはスタティックあるいはダイナミックがあります。

図 14-1 に示すように IP ソースガードは IP ソースガードバインディングに一致するパケットのみ転送します。

図 14-1 IP ソースガードアプリケーション



14.1.2. スタティック IP ソースガードのバインディング

スタティック IP ソースガードバインディング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。

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以下の機能を実装します。

- インタフェースで受信する IPv4 あるいは IPv6 パケットをフィルタします。

- ユーザの妥当性を確認するため IPv4 の ARP 検出機能と連携します。ARP 検出についての詳細は、セクション 8 *セキュリティ オペレーションマニュアル*の"*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グローバルあるいは指定したインタフェースで行うことができます。

- **グローバルのスタティックバインディング**－system view で IP アドレスと MAC アドレスを割り当てます。ユーザのなりすまし攻撃を防止するため、パケットをフィルタするためすべてのインタフェースで適用します。
- **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-S5300G 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。

14.1.3. ダイナミック IP ソースガードのバインディング

IP ソースガードは自動的にダイナミックバインディングを作成するため、他のモジュールからユーザ情報を取得します。ダイナミック IP ソースガードは MAC アドレス、IPv4 アドレス、IPv6 アドレス、VLAN タグ、入力インタフェース、バインディングタイプが含まれます。送信元モジュールは DHCP relay、DHCP snooping、DHCP サーバが含まれます。

DHCP ベースの 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 snooping の装置あるいは DHCP リレーエージェントで設定されます。DHCP snooping エントリあるいは DHCP リレー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を作成します。IP ソースガードは通過にパスした 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
Layer 2 Ethernet インタフェース	DHCP snooping 802.1X	パケットフィルタリング
	ARP snooping	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。
VLANインタフェース	DHCP relayエージェント	パケットフィルタリング
	DHCP server	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

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
		リティサービスを提供します。

802.1X についての詳細はセクション 8 *セキュリティ オペレーションマニュアルの“802.1X”*を参照してください。

DHCP snooping、DHCP リレー、DHCP サーバについての詳細は、セクション 4 *IP サービス オペレーションマニュアルの”DHCP snooping”、”DHCP リレー”、”DHCP サーバ”*を参照してください。

II. ダイナミック IPv6 ソースガード

IPv6 ソースガードは、パケットフィルタリングの IPv6 ソースガードバインディングエントリを作成するため、DHCPv6 snooping エントリから情報を取得します。

メモ：

QX-S5300G シリーズはダイナミック IPv6 ソースガードをサポートしていません。

14.2. IPソースガードの設定作業リスト

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ソースガードバインディングの設定

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ソースガードバインディングの設定

14.3. IPv4ソースガード機能の設定

14.3.1. インタフェースの IPv4 ソースガードの有効化

I. インタフェースの IPv4 ソースガード

インタフェースで IP ソースガードを有効にするとき、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。詳細はセクション 8 *セキュリティ オペレーションマニ*

*ュアルの“IP ソースガード”の“スタティック IPv4 ソースガードバインディングの設定”*を参照してください。

- 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。

II. 制限とガイドライン

ダイナミック IPv4 ソースガードを実装するため、ネットワークで 802.1X、ARP snooping、DHCP snooping、DHCP リレー、DHCP サーバが正常に動作することを確認してください。

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*	以下のインタフェースをサポートします。 • 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。

14.3.2. スタティック IPv4 ソースガードバインディングの設定

I. 制限とガイドライン

- 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、**ip-address** *ip-address* パラメータ、**mac-address** *mac-address* パラメータ、**vlan** *vlan-id* パラメータが必要です。
- ARP 検出機能は指定された VLAN で有効にする必要があります。

II. インタフェースでのスタティック IPv4 ソースガードバインディングの設定

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*	以下のインタフェースをサポートします。 • レイヤ 2 Ethernet インタフェース • VLAN インタフェース
3. 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 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。

14.4. IPv6ソースガード機能の設定

14.4.1. インタフェースでの IPv6 ソースガードの有効化

I. インタフェースでの IPv6 ソースガード

インタフェースで IPv6 ソースガードを有効にするとき、スタティック IPv6 ソースガードが有効となります。

- 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。詳細はセクション 8 *セキュリティ オペレーションマニュアルの“IP ソースガード”の“スタティック IPv6 ソースガードバインディングの設定”*を参照してください。
- IPv6 ソースガードは **ipv6 verify source** コマンドで指定された条件をもとにして受信 IPv6 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。

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*	以下のインタフェースをサポートします。 • 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。

14.4.2. スタティック IPv6 ソースガードバインディングの設定

I. 制限とガイドライン

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、**vlan** *vlan-id* パラメータが必要です。

II. インタフェースでのスタティック IPv6 ソースガードバインディングの設定

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. interface view に移行する	**interface** *interface-type interface-number*	以下のインタフェースをサポートします。 • 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 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。

14.5. 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。

操作	コマンド
IPv4ソースガードバインディングを表示する	**display ip source binding** [**static** | [**arp-suppression** | **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*]
IPv6ソースガードバインディングを表示する	**display ipv6 source binding** [**static** | [**dhcpv6-snooping**]] [**ip-address** *ipv6-address*] [**mac-address** *mac-address*] [**vlan** *vlan-id*] [**interface** *interface-type interface-number*] [**slot** *slot-number*]

14.6. IPソースガードの設定

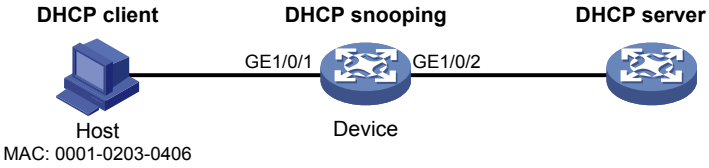
14.6.1. DHCP snooping を使用したダイナミック IPv4 ソースガードの設定例

I. ネットワーク要件

図 14-2 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 14-2 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、セクション 4 *IP サービス オペレーションマニュアル*の”*DHCP サーバ*”を参照してください。

2. Device 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。

   <Device> system-view

   [Device] 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。

   [Device] interface gigabitethernet 1/0/2

   [Device-GigabitEthernet1/0/2] dhcp snooping trust

   [Device-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。

   [Device] interface gigabitethernet 1/0/1

   [Device-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。

   [Device-GigabitEthernet1/0/1] dhcp snooping binding record

   [Device-GigabitEthernet1/0/1] quit

III. 設定の確認

DHCP snooping エントリをもとにして作成されたダイナミック IPv4 ソースガードバインディングを確認します。

[Device] 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
```

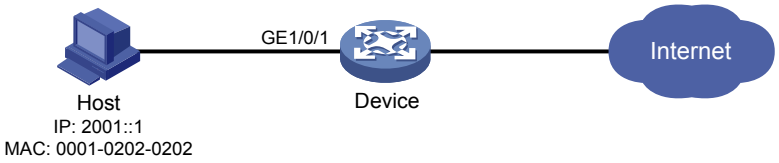
GigabitEthernet 1/0/1 は IPv4 ソースガードバインディングをもとにパケットをフィルタすることができます。

14.6.2. 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 14-3 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を設定します。

図 14-3 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。

<Device> system-view

[Device] interface gigabitethernet 1/0/1

[Device-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を設定します。

[Device-GigabitEthernet1/0/1] ipv6 source binding ip-address 2001::1 mac-address 0001-0202-0202

[Device-GigabitEthernet1/0/1] quit

III. 設定の確認

Switch でスタティック IPv6 ソースガードバインディングが正常に設定されていることを確認します。

[Device] 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
```

目次

このセクションのページは **8-x-x** です。

15 章 ARP アタックプロテクション……15-1
15.1. 概要……15-1
15.2. ARP アタックプロテクション設定作業リスト……15-1
15.3. 宛先不明の IP アタックプロテクションの設定……15-2
15.3.1. 概要……15-2
15.3.2. ARP 送信元抑制機能の設定……15-2
15.3.3. ARP ブラックホールルーティング機能の有効化……15-3
15.3.4. 宛先不明の IP アタックプロテクションの表示と維持……15-3
15.3.5. 宛先不明の IP アタックプロテクションの設定例……15-3
15.4. ARP パケットレートリミットの設定……15-4
15.5. 送信元 MAC アドレスにもとづく ARP アタック detection の設定……15-6
15.5.1. 概要……15-6
15.5.2. 制限とガイドライン……15-6
15.5.3. 設定手順……15-6
15.5.4. 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……15-7
15.5.5. 送信元 MAC アドレスにもとづく ARP アタック detection の設定例……15-7
15.6. ARP パケット送信元 MAC アドレス正当性チェックの設定……15-8
15.6.1. ARP パケット送信元 MAC アドレス正当性チェック……15-8
15.6.2. 設定手順……15-9
15.7. ARP 確認応答の設定……15-9
15.8. ARP アタック detection の設定……15-9
15.8.1. ARP アタック detection……15-9
15.8.2. ユーザ正当性の確認……15-10
15.8.3. ARP パケット正当性の確認の設定……15-11
15.8.4. ARP 制限転送の設定……15-12
15.8.5. ARP アタック detection の表示と維持……15-13
15.9. ARP ゲートウェイプロテクションの設定……15-13
15.9.1. ARP ゲートウェイプロテクション……15-13
15.9.2. 制限とガイドライン……15-13
15.9.3. 設定手順……15-14
15.9.4. ARP ゲートウェイプロテクションの設定例……15-14
15.10. ARP フィルタリングの設定……15-15
15.10.1. ARP フィルタリング……15-15
15.10.2. 制限とガイドライン……15-15
15.10.3. 設定手順……15-15
15.10.4. ARP フィルタリングの設定……15-15

15章 ARP アタックプロテクション

15.1. 概要

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。

- 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。
- 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。

15.2. ARPアタックプロテクション設定作業リスト

作業リスト
• （オプション設定項目）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 　○ ARP パケットレートリミットの設定 　○ 送信元 MAC アドレスにもとづく ARP アタック detection の設定
• （オプション設定項目）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 　○ ARP 確認応答の設定 　○ ARP アタック detection の設定 　○ ARP パケット正当性の確認の設定 　○ ARP 制限転送の設定 　○ ARP ゲートウェイプロテクションの設定 　○ ARP フィルタリングの設定

15.3. 宛先不明のIPアタックプロテクションの設定

15.3.1. 概要

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。ブラックホールルートはエージングタイマ（25 秒）が終了する、あるいはルートが到達可能になったときに、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とき、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を持つかどうかにかかわらず、適用可能です。

15.3.2. 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

15.3.3. ARP ブラックホールルーティング機能の有効化

I. 制限とガイドライン

ARP ブラックホールのルートを調査する間隔は 25 のような大きい値を設定してください。装置が一時的に宛先 IP アドレスに到達できず、調査するカウントが小さすぎる場合、すべての調査は問題が解決するまえに完了してしまう可能性があります。その結果、攻撃パケット以外のパケットが廃棄されてしまいます。この機能はこの問題を避けることができます。

II. 設定手順

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

15.3.4. 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**

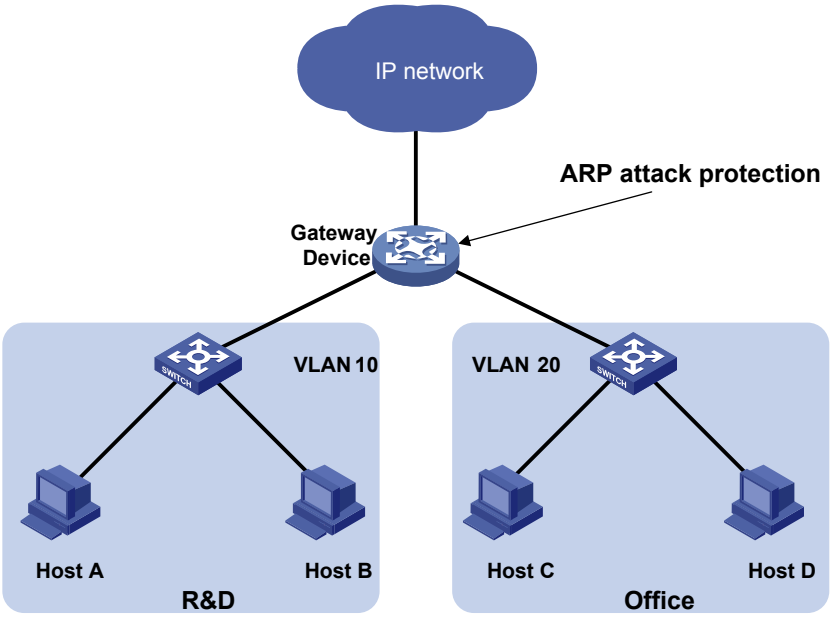
15.3.5. 宛先不明の IP アタックプロテクションの設定例

I. ネットワーク要件

図 15-1 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 15-1 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 送信元抑制機能を有効にします。

  # ARP 送信元抑制機能を有効にします。

  <Device> system-view

  [Device] arp source-suppression enable

  # ホストからの宛先不明のパケットを 5 秒間に受信できる最大値を 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、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

15.4. 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。

ARP パケットレートリミットにより SNMP モジュールへの notification あるいはログメッセージの送信を有効にすることができます。

- notification の送信が有効の場合、装置は notification の送信間隔以内に、もっとも高いしきい値と交差した ARP パケットのレートを、SNMP モジュールへ送信します。notification タイプ（inform あるいは trap）、宛先ホストを設定するため、**snmp-agent target-host** コマンドを

使用する必要があります。notification の詳細はセクション 10 *システム管理 オペレーションマニュアル*の”*SNMP*”を参照してください。

- ARP のログメッセージの送信が有効である場合、装置はログメッセージの送信間隔以内に、もっとも高いしきい値と交差した ARP パケットのレートを、information center へ送信します。information center の出力ルールを設定することができます。information center の詳細はセクション 10 *システム管理 オペレーションマニュアル*の”*information center*”を参照してください。

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。

過剰な notification とログメッセージが送信された場合、ARP パケットレートリミットの設定によって、notification とログメッセージの送信間隔を増やすことができます。

アグリゲートインタフェースで ARP パケットレートリミット機能の notification、ログメッセージの送信を有効にした場合、すべてのアグリゲーションメンバポートに適用します。

III. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. （オプション設定項目）ARP パケットレートリミットの notification の送信を有効にする	**snmp-agent trap enable arp** [*rate-limit*]	デフォルト：無効
3. （オプション設定項目）ARP パケットレートリミットのロギングを有効にする	**arp rate-limit log enable**	デフォルト：無効
4. （オプション設定項目）ARP パケットレートリミットの notification、ログメッセージを送信する送信間隔を設定する	**arp rate-limit log interval** *interval*	デフォルト：60秒
5. Layer 2 Ethernet interface あるいは Layer 2 aggregate interface view に移行する	**interface** *interface-type interface-number*	—
6. 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

15.5. 送信元MACアドレスにもとづくARPアタックdetectionの設定

15.5.1. 概要

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。

ARP ロギング機能を有効にする場合、**arp check log enable** コマンドを使用します。詳細はセクション 4 *IP サービス オペレーションマニュアル*の“*ARP*”を参照してください。

ARP アタックエントリのエージングタイマが終了したとき、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。

15.5.2. 制限とガイドライン

ARP アタック detection の処理モードをモニタからフィルタに変更した場合、設定はすぐに適用されます。処理モードをフィルタからモニタに変更した場合、装置は既存の攻撃エントリに一致するパケットをフィルタし続けます。

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。

15.5.3. 設定手順

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

操作	コマンド	補足
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

15.5.4. 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。

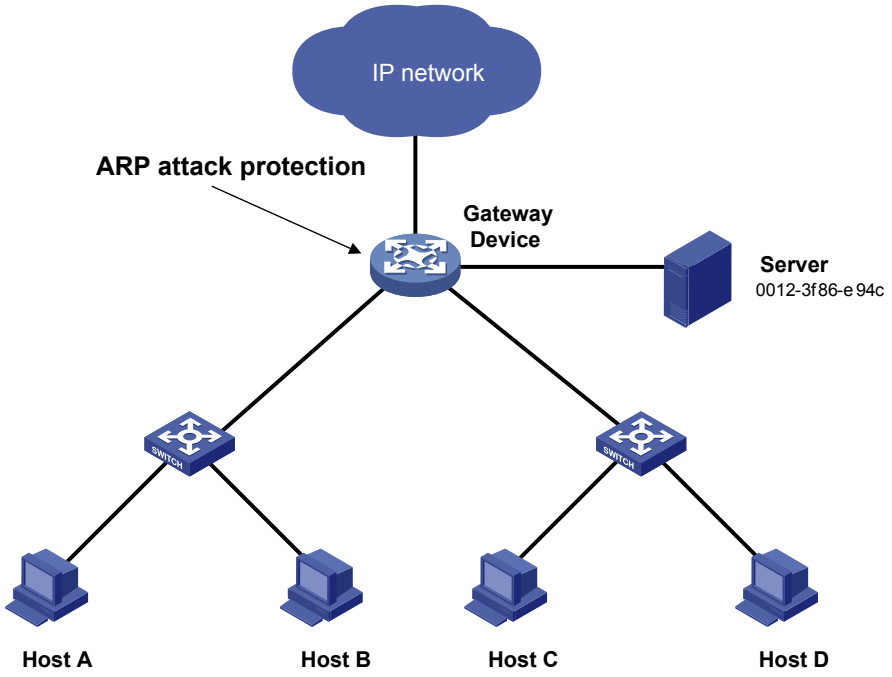
操作	コマンド
送信元MACアドレスにもとづくARPアタックdetectionで検出されたARPアタックエントリを表示する	**display arp source-mac** { **interface** *interface-type interface-number* | **slot** *slot-number* }

15.5.5. 送信元 MAC アドレスにもとづく ARP アタック detection の設定例

I. ネットワーク要件

図 15-2 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 15-2 ネットワーク図



II. 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

ARP アタック detection から MAC アドレス 0012-3f86-e94c を除外します。

[Device] arp source-mac exclude-mac 0012-3f86-e94c

15.6. ARPパケット送信元MACアドレス正当性チェックの設定

15.6.1. ARP パケット送信元 MAC アドレス正当性チェック

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。

15.6.2. 設定手順

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

15.7. ARP確認応答の設定

I. ARP 確認応答

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。

II. 設定手順

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

15.8. ARPアタックdetectionの設定

15.8.1. ARP アタック detection

ARP 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、認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 は以下の機能を提供します。

- ユーザの正当性の確認
- ARP パケット正当性の確認
- ARP 制限転送

ARP パケット正当性とユーザ正当性の確認の両方が有効である場合、ARP パケットの正当性の確認が最初に適用され、ユーザ正当性の確認が次に適用されます。

ARP アタック detection と ARP snooping を同時に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。

15.8.2. ユーザ正当性の確認

I. ユーザ正当性の確認

ユーザ正当性の確認機能は ARP トラステッドインタフェースから受信した ARP パケットを確認しません。以下の設定が行われている場合、ARP の非トラステッドインタフェースから ARP パケットを受信すると、装置は受信した 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。

1. スタティック IP ソースガードバインディング、802.1X セキュリティエントリ、DHCP snooping エントリ
   - 一致した場合、装置は ARP パケットを転送します。
   - 一致しない場合、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は **ip source binding** コマンド使用して作成されます。詳細はセクション 8 *セキュリティ オペレーションマニュアルの“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、セクション 4 *IP サービス オペレーションマニュアルの”DHCP snooping”*を参照してください。

802.1X セキュリティエントリは 802.1X クライアントの IP-MAC アドレスのマッピングを記録します。クライアントが 802.1X 認証にパスし、ARP アタック detection が有効な装置に IP アドレスをアップロードしたのち、装置は自動で 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。詳細はセクション 8 *セキュリティ オペレーションマニュアルの“802.1X”*を参照してください。

II. 制限とガイドライン

ユーザ正当性の確認を設定するとき、以下の機能が 1 つ以上設定されていることを確認してください。

- ユーザの正当性の確認
- 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、ARP 非トラステッドポートから受信された ARP パケットは廃棄されます。

IP ソースガードバインディングエントリを設定する場合、IP アドレス、MAC アドレス、VLAN を指定する必要があります。そうでなければ ARP パケットは、IP ソースガードバインディングエントリに一致することができません。

III. 設定手順

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. ARP detection を有効にする	**arp detection enable**	デフォルト：無効

操作	コマンド	補足
4. (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インタフェースを設定する	• system view に戻る **quit** • Ethernet interface view あるいは aggregate interface view に移行する **interface** *interface-type interface-number* • ARP 検出を除外するトラステッドインタフェースとしてインタフェースを設定する **arp detection trust**	デフォルト : 非トラステッドインタフェース

15.8.3. ARP パケット正当性の確認の設定

I. 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。

II. 設定要件

ARP パケット正当性の確認の設定を行う前に、ユーザ正当性の確認の設定を最初に行ってください。詳細はセクション 8 *セキュリティ オペレーションマニュアル*の“*ARP アタックプロテクション*”の“*ユーザ正当性の確認*”を参照してください。

III. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. VLAN view に移行する	**vlan** *vlan-id*	—
3. ARP detection を有効にする	**arp detection enable**	デフォルト：無効

操作	コマンド	補足
4. 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	• system view に戻る **quit** • 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
5. (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インタフェースを設定する	• Ethernet interface view あるいは aggregate interface view に移行する **interface** *interface-type interface-number* • ARP 検出を除外するトラステッドインタフェースとしてインタフェースを設定する **arp detection trust**	デフォルト：非トラステッドインタフェース

15.8.4. ARP 制限転送の設定

I. ARP 制限転送

ARP トラステッドインタフェースで受信された ARP パケットは ARP 制限転送に適用されません。正常に ARP パケットを転送します。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。

II. 制限とガイドライン

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。

III. 設定要件

ARP 制限転送の設定を行う前に、ユーザ正当性の確認の設定を最初に行ってください。詳細はセクション 8 *セキュリティ オペレーションマニュアル*の“*ARP アタックプロテクション*”の“*ユーザ正当性の確認*”を参照してください。

IV. 設定手順

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. ARP 制限転送を有効にする	**arp restricted-forwarding enable**	デフォルト：無効

15.8.5. 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アタックdetectionが有効なVLANを表示する	**display arp detection**
ARPアタックdetectionの送信元の統計情報を表示する	**display arp detection statistics attack-source slot** *slot-number*
ARPアタックdetectionによって廃棄されたパケットの統計情報を表示する	**display arp detection statistics packet-drop** [**interface** *interface-type interface-number*]
ARPアタックdetectionの送信元の統計情報を削除する	**reset arp detection statistics attack-source** [**slot** *slot-number*]
ARPアタックdetectionによって廃棄されたパケットの統計情報を削除する	**reset arp detection statistics packet-drop** [**interface** *interface-type interface-number*]

15.9. ARPゲートウェイプロテクションの設定

15.9.1. ARP ゲートウェイプロテクション

ゲートウェイスプーフィング攻撃を防ぐため、ゲートウェイに接続されていないインタフェースで設定してください。

インタフェースで ARP パケットを受信した場合、パケットの送信元 IP アドレスが保護されているゲートウェイの送信元 IP アドレスと一致しているかどうかを確認します。一致した場合、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。

15.9.2. 制限とガイドライン

インタフェースで最大 8 つのゲートウェイの ARP ゲートウェイプロテクションを有効にすることができます。

インタフェースで **arp filter source** コマンドと **arp filter binding** コマンドを同時に設定しないでください。

ARP ゲートウェイプロテクションと ARP アタック detection を同時に設定した場合、ARP ゲートウェイプロテクションが最初に適用されます。

15.9.3. 設定手順

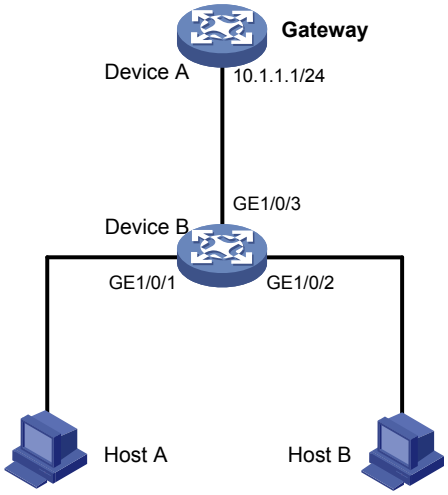
操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. Ethernet interface view あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	—
3. ARP ゲートウェイプロテクションを有効にする	**arp filter** *source ip-address*	デフォルト：無効

15.9.4. ARP ゲートウェイプロテクションの設定例

I. ネットワーク要件

図 15-3 に示すように、Host B は Device B にゲートウェイスプーフィング攻撃を行います。Device B が Device A に送信するトラフィックは Host B に送信されます。Device B で攻撃をブロックします。

図 15-3 ネットワーク図



II. 設定手順

Device B で 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. 設定の確認

GigabitEthernet 1/0/1 と GigabitEthernet 1/0/2 で、送信元 IP アドレスがゲートウェイの IP アドレスである入力 ARP パケットを廃棄していることを確認します。

15.10. ARPフィルタリングの設定

15.10.1. ARP フィルタリング

ARP フィルタリング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では、受信された ARP パケットの送信元 IP アドレスと MAC アドレスが許可されたエントリであるかどうか確認します。一致した場合、パケットが正しいと認識して処理します。一致しない場合、パケットを廃棄します。

15.10.2. 制限とガイドライン

インタフェースで最大 8 つの ARP フィルタリングの許可されたエントリを設定することができます。

インタフェースで **arp filter source** コマンドと **arp filter binding** コマンドを同時に設定しないでください。

ARP ゲートウェイプロテクションと ARP アタック detection を同時に設定した場合、ARP ゲートウェイプロテクションが最初に適用されます。

15.10.3. 設定手順

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. ARP フィルタリングと許可されたエントリを設定する	**arp filter binding** *ip-address mac-address*	デフォルト：無効

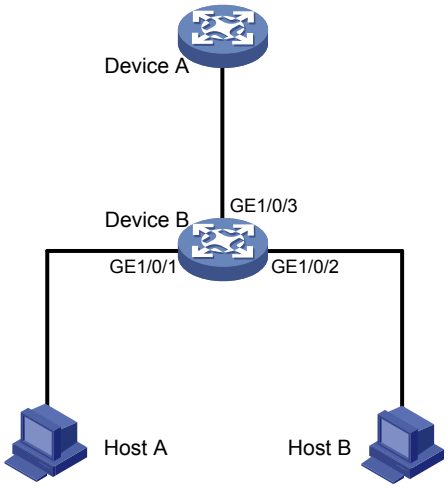
15.10.4. ARP フィルタリングの設定

I. ネットワーク要件

図 15-4 に示すように Host A の IP アドレスと MAC アドレスはそれぞれ 10.1.1.2、000f-e349-1233 です。Host B の IP アドレスと MAC アドレスはそれぞれ 10.1.1.3、000f-e349-1234 です。

Device B の GigabitEthernet 1/0/1 と GigabitEthernet 1/0/2 で Host A と Host B からの ARP パケットのみ許可するように設定します。

図 15-4 ネットワーク図



II. 設定手順

Device B で 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. 設定の確認

GigabitEthernet 1/0/1 で Host A からの ARP パケットを許可し、他の ARP パケットを廃棄することを確認します。

GigabitEthernet 1/0/2 で Host B からの ARP パケットを許可し、他の ARP パケットを廃棄することを確認します。

QX-S5300G シリーズ Ethernet スイッチ

オペレーションマニュアル

9. 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-Ethernet OAM

02-CFD

03-DLDP

04-RRPP

05-Smart Link

06-Monitor Link

07-BFD

08-Track

目次

このセクションのページは **9-x-x** です。

1 章 Ethernet OAM 1-1
1.1. Ethernet OAM について 1-1
1.1.1. Ethernet OAM の主な機能 1-1
1.1.2. Ethernet OAMPDU 1-1
1.1.3. Ethernet OAM の動作 1-2
1.1.4. プロトコルと標準 1-4
1.2. 制限とガイドライン 1-4
1.3. Ethernet OAM 設定作業リスト 1-4
1.4. Ethernet OAM の基本機能の設定 1-5
1.5. Ethernet OAM 接続検出タイマの設定 1-5
1.5.1. Ethernet OAM 接続検出タイマについて 1-5
1.5.2. 制限とガイドライン 1-5
1.5.3. グローバルでの Ethernet OAM 接続検出タイマの設定 1-6
1.5.4. ポートでの Ethernet OAM 接続検出タイマの設定 1-6
1.6. エラーシンボルイベント検出の設定 1-6
1.6.1. 制限とガイドライン 1-6
1.6.2. グローバルでのエラーシンボルイベント検出の設定 1-6
1.6.3. ポートでのエラーシンボルイベント検出の設定 1-7
1.7. エラーフレームイベント検出の設定 1-7
1.7.1. 制限とガイドライン 1-7
1.7.2. グローバルでのエラーフレームイベント検出の設定 1-7
1.7.3. ポートでのエラーフレームイベント検出の設定 1-7
1.8. エラーフレーム期間イベント検出の設定 1-8
1.8.1. 制限とガイドライン 1-8
1.8.2. グローバルでのエラーフレーム期間イベント検出の設定 1-8
1.8.3. ポートでのエラーフレーム期間イベント検出の設定 1-8
1.9. エラーフレーム秒イベント検出の設定 1-8
1.9.1. 制限とガイドライン 1-8
1.9.2. グローバルでのエラーフレーム秒イベント検出の設定 1-9
1.9.3. ポートでのエラーフレーム秒イベント検出の設定 1-9
1.10. リモートエンドから Ethernet OAM イベント受信後のポートのアクション設定 1-9
1.11. ポートの Ethernet OAM リモートループバックの有効化 1-10
1.11.1. Ethernet OAM リモートループバックについて 1-10
1.11.2. 制限とガイドライン 1-10
1.11.3. system view での Ethernet OAM リモートループバックの有効化 1-11
1.11.4. interface view での Ethernet OAM リモートループバックの有効化 1-11
1.12. リモートポートからの Ethernet OAM リモートループバックリクエストの拒否 1-11
1.13. Ethernet OAM の表示と維持 1-12
1.14. Ethernet OAM の設定例 1-12
1.14.1. Ethernet OAM の設定例 1-12

1章 Ethernet OAM

1.1. Ethernet OAMについて

Ethernet OAM(Ethernet Operation, Administration and Maintenance)はレイヤ 2 リンク状態をモニタし、「ラストマイル」に関するリンク関連の問題に対処するツールです。Ethernet OAM を使用することで、2 台の直接接続された装置間のポイントツーポイント接続の状態をモニタできます。

1.1.1. Ethernet OAM の主な機能

以下に Ethernet OAM の主な機能を示します。

- リンクパフォーマンスのモニタ—パケットロス、遅延、ジッタを含むリンクの性能指標をモニタし、様々なタイプのトラフィック統計情報を収集します。
- 障害検出とアラーム—リンク異常が発生したとき、OAM プロトコルデータ単位(OAMPDU)とレポートをネットワーク管理者に送ることによって、リンクの接続性をチェックします。
- リモートループバック—ループバック OAMPDU によってリンク品質の確認とリンクエラーの検出を行います。

1.1.2. Ethernet OAMPDU

Ethernet OAM はデータリンクレイヤで動作します。Ethernet OAM は、管理者が効率的にネットワークを管理できるように、装置間で定期的に OAMPDU を交換することによってリンクの状態を通知します。

表 1-1 に Ethernet OAMPDU のタイプによる違いを示します。

表 1-1 OAMPDU の異なるタイプによる機能

OAMPDU タイプ	機能
Information OAMPDU	リモートEthernet OAMエンティティとOAM接続を維持するため、Ethernet OAMエンティティの転送状態の情報に使用します。この情報はローカルデバイス、リモートデバイス、カスタマイズ情報を含みます。
Event Notification OAMPDU	リンクモニタリングによりリンク間で問題を検出したとき、リモートOAMエンティティに通知するために使用します。
Loopback Control OAMPDU	リモートループバック制御に使用します。ループバック制御OAMPDUにループバックの有効／無効情報を挿入することにより、リモートOAMエンティティのループバックを有効／無効にすることができます。

メモ:

この章では Ethernet OAM が有効なポートは Ethernet OAM エンティティあるいは OAM エンティティと呼びます。

1.1.3. Ethernet OAM の動作

この章では Ethernet OAM の動作手順について記載します。

I. Ethernet OAM 接続の確立

Ethernet OAM 機能を使用するためには、最初にリモートとの接続の確立が必要となります。Ethernet OAM 接続の確立とは、Ethernet OAM エンティティがリモート OAM エンティティを発見し、セッションを確立するディスカバリフェーズです。

このフェーズでは、2 つの接続された OAM エンティティは、リモートの OAM 設定と機能を Information OAMPDU を交換することにより通知し、Ethernet OAM 接続が確立できるか判断します。Information OAMPDU のループバック接続、リンク検出、リンクイベントの設定が一致している場合、OAM エンティティは OAM 接続を確立します。Ethernet OAM 接続が確立後は Ethernet OAM が有効になります。

OAM エンティティはアクティブモードあるいはパッシブモードで動作します。アクティブモードの OAM エンティティは OAM 接続を開始します。パッシブモードの OAM エンティティは相手からの OAM 接続要求を待ち、応答します。2 つの OAM エンティティ間の OAM 接続を行うため、少なくとも 1 つのモードはアクティブモードに設定する必要があります。

以下に異なるモードで装置が実行する動作を示します。

表 1-2 アクティブ Ethernet OAM モードとパッシブ Ethernet OAM モード

アイテム	アクティブ Ethernet OAM モード	パッシブ Ethernet OAM モード
Initiating OAM Discovery	可能	不可
Responding to OAM Discovery	可能	可能
Transmitting Information OAMPDUs	可能	可能
Transmitting Event Notification OAMPDUs	可能	可能
Transmitting Information OAMPDUs without any TLV	可能	可能
Transmitting Loopback Control OAMPDUs	可能	不可
Responding to Loopback Control OAMPDUs	双方がアクティブOAMモードのとき可能	可能

Ethernet OAM 接続が確立した後、Ethernet OAM エンティティは Information OAMPDU を定期的に交換し Ethernet OAM 接続を保持します。Ethernet OAM エンティティが Information OAMPDU を Ethernet OAM タイムアウトタイマ内に受信しない場合、Ethernet OAM 接続は切断されます。

II. リンクモニタリング

Ethernet のエラー検出は、困難を伴います。特にネットワークが物理的に切断されていないが、ネットワークパフォーマンスが徐々に低下している状況では、検出が困難になります。

リンクモニタリングは様々な環境でリンクエラーを検出するために使用します。Ethernet OAM のリンクモニタリングは Event Notification OAMPDU の交換により確立します。表 1-3 に示す Ethernet OAM リンクエラーイベントを検出すると、ローカル OAM エンティティは Event Notification OAMPDU をリモート OAM エンティティに送信します。ログ情報を取得することによりネットワーク管理者は速やかにネットワークステータスの変更を追跡できます。

表 1-3 Ethernet OAM リンクエラーイベント

Ethernet OAM リンクイベント	説明
Errored symbol event	検出ウィンドウ（受信したシンボル数）内に、所定のしきい値を超過したエラーシンボルを検出したときにエラーシンボルイベントが発生します。
Errored frame event	検出ウィンドウ（検出期間）内に、所定のしきい値を超過したエラーフレームを検出したときにエラーフレームイベントが発生します。
Errored frame period event	検出ウィンドウ（受信したフレーム数）内に、エラーフレームが所定のしきい値を超過したときにエラーフレーム期間イベントが発生します。
Errored frame seconds event	検出ウィンドウ（検出期間）内に、ポートでエラーフレーム秒（エラーフレームが1秒以内に発生したエラーフレーム）の数が設定しきい値を超過したときにエラーフレーム秒イベントが発生します。

III. リモート障害検知

Information OAMPDU は、OAM 接続が確立された Ethernet OAM エンティティ間で定期的に交換されます。装置の障害または使用不能により通信が中断したネットワークでは、Ethernet OAM エンティティがピアにエラー情報を送信するために Information OAMPDU のフラグフィールドを使用できます。現在のリンク状態を追跡するため、ログ情報を使用し、問題を早急にトラブルシュートすることができます。

表 1-4 クリティカルリンクイベント

タイプ	説明	OAMPDU 送信間隔
Link Fault	ピアのリンク信号がロストしました。	1秒に1回
Dying Gasp	電源障害のような予測不能な障害が発生しました。	ノンストップ
Critical Event	不確定なクリティカルイベントが発生しました。	ノンストップ

IV. リモートループバック

リモートループバックは Ethernet OAM コネクションが確立された後のみ利用可能です。リモートループバックを有効にすると、アクティブモードの Ethernet OAM エンティティは non-OAMPDU

をピアに送信します。フレームを受信したのち、ピアは送信先アドレスへは転送せずにオリジナルパスで返信します。

リモートループバックはリンク状態やリンク障害箇所を確認するために使用します。定期的なリモートループバックの実行は、ネットワーク障害を速やかに検出するのに役立ちます。さらにネットワークセグメントでのリモートループバックの実行は、ネットワーク障害箇所の検出の手助けとなります。

1.1.4. プロトコルと標準

IEEE 802.3ah, *Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications*

1.2. 制限とガイドライン

クリティカルリンクイベントを持つ Information OAMPDU の送受信について、装置のサポートは下記です。

- クリティカルリンクイベントを持つ Information OAMPDU を受信することができます。
- Link Fault イベントを持つ Information OAMPDU を送信できます。
- 装置の再起動や関連したポートが手動で shutdown された際の Dying Gasp イベントを持つ Information OAMPDU の送信することができます。IRF スタックポートは、この information OAMDPU を送信することができません。
- クリティカルリンクイベントを持つ information OAMPDU の送信はできません。

1.3. Ethernet OAM設定作業リスト

作業リスト
(必須設定項目) Ethernet OAMの基本機能の設定
(オプション設定項目) Ethernet OAM接続検出タイマの設定
(オプション設定項目) リンクモニタリングの設定 • エラーシンボルイベント検出の設定 • エラーフレームイベント検出の設定 • エラーフレーム期間イベント検出の設定 • エラーフレーム秒イベント検出の設定
(オプション設定項目) リモートエンドからEthernet OAMイベント受信後のポートのアクション設定
(オプション設定項目) Ethernet OAMリモートループバックの設定 • ポートの Ethernet OAM リモートループバックの有効化 • リモートポートからの Ethernet OAM リモートループバックリクエストの拒否

1.4. Ethernet OAMの基本機能の設定

I. Ethernet OAM モードについて

2 つの Ethernet OAM エンティティ間で Ethernet OAM 接続を確立するために、装置を少なくとも 1 つをアクティブモードに設定します。アクティブモードでのみ Ethernet OAM エンティティはコネクションを開始することができます。

II. 制限とガイドライン

Ethernet OAM が有効になったポートの Ethernet OAM モードを変更するには、最初に Ethernet OAM を無効にする必要があります。

III. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Ethernet interface view に移行する	**interface** *interface-type interface-number*	―
3. Ethernet OAM モードを設定する	**oam mode** { **active** | **passive** }	デフォルト：**active**
4. Ethernet OAM を有効にする	**oam enable**	デフォルト：無効

1.5. Ethernet OAM接続検出タイマの設定

1.5.1. Ethernet OAM 接続検出タイマについて

Ethernet OAM の接続が確立された後、Ethernet OAM エンティティは、Ethernet OAM 接続が有効であるか検出するため、指定された間隔で Ethernet OAM ハンドシェークパケットとして Information OAMPDU の交換を行います。Ethernet OAM が有効になっているポートで Ethernet OAM コネクションタイムアウトの前に Information OAMPDU を受信しない場合は、Ethernet OAM 接続が切断されたと判断します。

ハンドシェークパケットの転送間隔と接続タイムアウトタイマを調整することで、Ethernet OAM の検出時間を変更することができます。

1.5.2. 制限とガイドライン

- このコマンドは system view あるいは interface view で設定することができます。system view での設定はすべてのポートで適用され、interface view での設定は指定されたポートで適用されます。interface view での設定が優先されます。
- Ethernet OAM 接続のタイムアウトタイマが終了した後、ローカル OAM エンティティは、OAM 接続を切断し、ピアの OAM エンティティの接続を終了させます。Ethernet OAM 接続を安定的に維持するために、Ethernet OAM コネクションタイムアウト値は Ethernet OAM ハンドシェークパケットの送信間隔の少なくとも 5 倍以上にすることを推奨します。

1.5.3. グローバルでの Ethernet OAM 接続検出タイマの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Ethernet OAM ハンドシェークパケットの送信間隔を設定する	**oam global timer hello** *interval*	デフォルト：1000ms
3. Ethernet OAM コネクションタイムアウトタイマを設定する	**oam global timer keepalive** *interval*	デフォルト：5000ms

1.5.4. ポートでの Ethernet OAM 接続検出タイマの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Ethernet interface view に移行する	**interface** *interface-type interface-number*	―
3. Ethernet OAM ハンドシェークパケットの送信間隔を設定する	**oam timer hello** *interval*	デフォルト：グローバルに設定された値を使用します。
4. Ethernet OAM コネクションタイムアウトタイマを設定する	**oam timer keepalive** *interval*	デフォルト：グローバルに設定された値を使用します。

1.6. エラーシンボルイベント検出の設定

1.6.1. 制限とガイドライン

このコマンドは system view あるいは interface view で設定することができます。system view での設定はすべてのポートで適用され、interface view での設定は指定されたポートで適用されます。interface view での設定が優先されます。interface view での設定が優先されます。

1.6.2. グローバルでのエラーシンボルイベント検出の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. エラーシンボルイベント検出数を設定する	**oam global errored-symbol-period window** *window-value*	デフォルト：100,000,000
3. エラーシンボルイベント検出のしきい値を設定する	**oam global errored-symbol-period threshold** *threshold-value*	デフォルト：1

1.6.3. ポートでのエラーシンボルイベント検出の設定

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. エラーシンボルイベント検出数を設定する	**oam errored-symbol-period window** *window-value*	デフォルト : グローバルに設定された値を使用します。
4. エラーシンボルイベント検出のしきい値を設定する	**oam errored-symbol-period threshold** *threshold-value*	デフォルト : グローバルに設定された値を使用します。

1.7. エラーフレームイベント検出の設定

1.7.1. 制限とガイドライン

このコマンドは system view あるいは interface view で設定することができます。system view での設定はすべてのポートで適用され、interface view での設定は指定されたポートで適用されます。interface view での設定が優先されます。

1.7.2. グローバルでのエラーフレームイベント検出の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. エラーフレームイベント検出期間を設定する	**oam global errored-frame window** *window-value*	デフォルト：1000 ms
3. エラーフレームイベント検出のしきい値を設定する	**oam global errored-frame threshold** *threshold-value*	デフォルト：1

1.7.3. ポートでのエラーフレームイベント検出の設定

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. エラーフレームイベント検出期間を設定する	**oam errored-frame window** *window-value*	デフォルト : グローバルに設定された値を使用します。
4. エラーフレームイベント検出のしきい値を設定する	**oam errored-frame threshold** *threshold-value*	デフォルト : グローバルに設定された値を使用します。

1.8. エラーフレーム期間イベント検出の設定

1.8.1. 制限とガイドライン

このコマンドは system view あるいは interface view で設定することができます。system view での設定はすべてのポートで適用され、interface view での設定は指定されたポートで適用されます。interface view での設定が優先されます。

1.8.2. グローバルでのエラーフレーム期間イベント検出の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. エラーフレーム期間イベント検出のフレーム数を設定する	**oam global errored-frame-period window** *window-value*	デフォルト：10000000
3. エラーフレーム期間イベント検出のしきい値を設定する	**oam global errored-frame-period threshold** *threshold-value*	デフォルト：1

1.8.3. ポートでのエラーフレーム期間イベント検出の設定

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. エラーフレーム期間イベント検出のフレーム数を設定する	**oam errored-frame-period window** *window-value*	デフォルト：グローバルに設定された値を使用します。
4. エラーフレーム期間イベント検出のしきい値を設定する	**oam errored-frame-period threshold** *threshold-value*	デフォルト：グローバルに設定された値を使用します。

1.9. エラーフレーム秒イベント検出の設定

1.9.1. 制限とガイドライン

- このコマンドは system view あるいは interface view で設定することができます。system view での設定はすべてのポートで適用され、interface view での設定は指定されたポートで適用されます。interface view での設定が優先されます。

- エラーフレーム秒イベントを動作させるために、エラーフレーム秒検出しきい値は、エラーフレーム秒イベントの検出期間より小さくする必要があります。そうでなければエラーフレーム秒イベントが動作しません。

1.9.2. グローバルでのエラーフレーム秒イベント検出の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. エラーフレーム秒イベント検出を設定する	**oam global errored-frame-seconds window** *window-value*	デフォルト：60000ms
3. エラーフレーム秒イベント検出のしきい値を設定する	**oam global errored-frame-seconds threshold** *threshold-value*	デフォルト：1

1.9.3. ポートでのエラーフレーム秒イベント検出の設定

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. エラーフレーム秒イベント検出を設定する	**oam errored-frame-seconds window** *window-value*	デフォルト：グローバルに設定された値を使用します。
4. エラーフレーム秒イベント検出のしきい値を設定する	**oam errored-frame-seconds threshold** *threshold-value*	デフォルト：グローバルに設定された値を使用します。

1.10. リモートエンドからEthernet OAMイベント受信後のポートのアクション設定

I. 本機能について

この機能によって、ポートはイベントのログを有効にし、OAM 接続を自動で終了させ、リンク状態をダウンさせます。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Ethernet interface view に移行する	**interface** *interface-type interface-number*	―

操作	コマンド	補足
3. リモートエンドから Ethernet OAM イベントを受信した後のポートのアクションを設定する	**oam remote-failure** { **connection-expired** | **critical-event** | **dying-gasp** | **link-fault** } **action error-link-down**	デフォルト：設定なし（ポートはリモートエンドからEthernet OAMイベントを受信した際のEthernet OAMイベントのログのみを行います）

1.11. ポートのEthernet OAMリモートループバックの有効化

注意:

OAM リモートループバック機能は、他のサービスに大きな影響を与える可能性があるので、注意して使用してください。

1.11.1. Ethernet OAM リモートループバックについて

ポートで OAM リモートループバックを有効にすると、ポートはリモートポートに Loopback Control OAMPDU を送信し、リモートポートがループバック状態になります。ポートはリモートポートにテストフレームを送信します。このテストフレームのポートでの受信数をチェックすることで、パケットロス率によるリンク性能の評価ができます。

1.11.2. 制限とガイドライン

- Ethernet OAM リモートループバックは、Ethernet OAM 接続が確立され、Ethernet OAM エンティティがアクティブ Ethernet OAM モードであるとき実行可能です。
- リモートループバックは、リモートループバックを行う両端の通信モードが全 2 重である必要があります。
- Ethernet OAM リモートループバックは、リモートポートと送信ポートの両方でサポートしている必要があります。
- Ethernet OAM リモートループバックはデータ通信に割り込みます。Ethernet OAM リモートループバックを無効化した後、関係するすべてのポートがシャットダウンしたのちアップします。 Ethernet OAM リモートループバックは、以下のイベントのいずれによっても無効にすることができます。
  - Ethernet OAM の無効化
  - Ethernet OAM リモートループバックの無効化
  - Ethernet OAM 接続のタイムアウト
- リモートループバックテストを行っているポートで内部ループバックテストを有効にするとリモートループバックテストを終了できます。ループバックテストについての詳細は、セクション 3 *アクセス オペレーションマニュアル*の"*Ethernet インタフェース*"を参照してください。

- user view、system view、Ethernet interface view で Ethernet OAM リモートループバックを有効にすることができ、設定時の効果は同じです。

1.11.3. system view での Ethernet OAM リモートループバックの有効化

操作	コマンド	補足
1. (オプション設定項目) system view に移行する	**system-view**	―
2. 指定したポートで Ethernet OAM リモートループバックを有効にする	**oam remote-loopback start interface** *interface-type interface-number*	デフォルト：無効 このコマンドはuser viewあるいはsystem viewで実行できます。

1.11.4. interface view での Ethernet OAM リモートループバックの有効化

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Ethernet interface view に移行する	**interface** *interface-type interface-number*	―
3. ポートの Ethernet OAM リモートループバックを有効にする	**oam remote-loopback start**	デフォルト：無効

1.12. リモートポートからのEthernet OAMリモートループバックリクエストの拒否

I. 本機能について

Ethernet OAM リモートループバック機能は、他のサービスに影響を与えます。この問題を解決するために、リモートポートから送信された Loopback Control OAMPDU によって制御されるポートを無効にすることができます。ローカルポートはリモートポートからの Ethernet OAM リモートループバック要求を拒否することができます。

II. 制限とガイドライン

この設定はポートで実行されたループバックテストには影響しません。ポートで次にループバックが行われるときに適用されます。

III. 設定手順

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

操作	コマンド	補足
2. Ethernet interface view に移行する	**interface** *interface-type interface-number*	―
3. リモートポートからの Ethernet OAM リモートループバック要求を拒否する	**oam remote-loopback reject-request**	デフォルト：拒否しません。

1.13. Ethernet OAM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、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
Ethernet OAMの接続を表示する	**display oam** { **local** | **remote** } [**interface** *interface-type interface-number*]
Ethernet OAMの設定を表示する	**display oam configuration** [**interface** *interface-type interface-number*]
Ethernet OAM確立後のクリティカルイベントの統計情報を表示する	**display oam critical-event** [**interface** *interface-type interface-number*]
Ethernet OAM確立後の Ethernet OAMリンクエラーイベントの統計情報を表示する	**display oam link-event** { **local** | **remote** } [**interface** *interface-type interface-number*]
Ethernet OAMパケットと Ethernet OAMリンクエラーイベントの統計情報を削除する	**reset oam** [**interface** *interface-type interface-number*]

1.14. Ethernet OAMの設定例

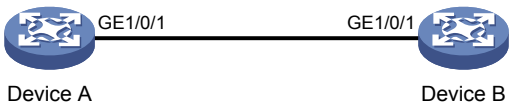
1.14.1. Ethernet OAM の設定例

I. ネットワーク要件

図 1-1 に示すように、以下の動作を実行します。

- 2 台の装置間でリンクエラーを自動検出するため、Device A と Device B で Ethernet OAM を有効にします。
- Device A が受信するエラーフレームの統計情報を収集することによって、Device A と Device B 間のリンク性能を測定できます。

図 1-1 ネットワーク図



II. 設定手順

1. Device A を設定します。

アクティブ Ethernet OAM モードで動作するように、GigabitEthernet 1/0/1 を設定し、Ethernet OAM を有効にします。

<DeviceA> system-view

[DeviceA] interface gigabitethernet 1/0/1

[DeviceA-GigabitEthernet1/0/1] oam mode active

[DeviceA-GigabitEthernet1/0/1] oam enable

エラーフレーム検出期間を 20000ms に設定し、エラーフレームイベント検出しきい値を 10 に設定します。

[DeviceA-GigabitEthernet1/0/1] oam errored-frame window 200

[DeviceA-GigabitEthernet1/0/1] oam errored-frame threshold 10

[DeviceA-GigabitEthernet1/0/1] quit

2. Device B を設定します。

#パッシブ Ethernet OAM モード(デフォルト)で動作するように、GigabitEthernet 1/0/1 を設定し、Ethernet OAM を有効にします。

<DeviceB> system-view

[DeviceB] interface gigabitethernet 1/0/1

[DeviceB-GigabitEthernet1/0/1] oam mode passive

[DeviceB-GigabitEthernet1/0/1] oam enable

[DeviceB-GigabitEthernet1/0/1] quit

III. 設定の確認

display oam critical-event コマンドを使用し、Ethernet OAM クリティカルリンクイベントの統計情報を表示します。

Device A のすべてのポートの Ethernet OAM クリティカルリンクイベントの統計情報を表示します。

[DeviceA] display oam critical-event

```
-----------[GigabitEthernet1/0/1] -----------
 Local link status    : UP
 Event statistics
   Link fault         : Not occurred
   Dying gasp         : Not occurred
   Critical event     : Not occurred
```

出力は、Device A と Device B 間のリンクでクリティカルリンクイベントが発生していないことを示します。

display oam link-event コマンドを使用し、Ethernet OAM リンクイベントの統計情報を表示します。

Device A のリモートエンドの Ethernet OAM リンクエラーイベントの統計情報を表示します。

```
[DeviceA] display oam link-event local
------------ [GigabitEthernet1/0/1] -----------
 Link status: UP
 OAM local errored frame event
   Event time stamp        : 5789 x 100 milliseconds
   Errored frame window    : 200 x 100 milliseconds
   Errored frame threshold : 10 error frames
   Errored frame           : 13 error frames
   Error running total     : 350 error frames
   Event running total     : 17 events
```

出力は下記を示します。

- Device A 上で Ethernet OAM が有効になった後、350 回エラーが発生しました。
- エラーフレームによって 17 のエラーが発生しました。
- リンクは不安定です。

目次

このセクションのページは **9-x-x** です。

2 章 CFD 2-1
2.1. 概要 2-1
2.1.1. CFD の基本概念 2-1
2.1.2. CFD レベル 2-2
2.1.3. MP のパケット処理 2-4
2.1.4. CFD 機能 2-4
2.1.5. プロトコルと標準 2-5
2.2. 制限とガイドライン 2-5
2.3. CFD の設定作業リスト 2-6
2.4. CFD のための必要条件 2-6
2.5. CFD の基本設定 2-6
2.5.1. CFD の有効化 2-6
2.5.2. イーサネットサービスインスタンスの設定 2-7
2.5.3. MEP の設定 2-7
2.5.4. MIP 自動生成ルールの作成 2-8
2.6. CFD function 機能の設定 2-8
2.6.1. CC の設定 2-8
2.6.2. LB の設定 2-10
2.6.3. LT の設定 2-10
2.7. CFD の表示と管理 2-11
2.8. CFD の設定例 2-11
2.8.1. CFD の設定例 2-11

2章 CFD

2.1. 概要

Connectivity Fault Detection (CFD)は、IEEE 802.1ag Connectivity Fault Management (CFM)と ITU-T Y.1731 に準拠し、1VLAN あたりの end-to-end のリンクレイヤ OAM メカニズムです。CFD は

リンク接続性検出、故障検証、障害箇所検出のために使用されます。

2.1.1. CFD の基本概念

I. MD(Maintenance domain)

MD(Maintenance domain)は、CFD が役割を果たすネットワークまたはネットワークの一部を定義します。MD はその MD 名によって識別されます。

II. MA(Maintenance association)

MA(maintenance association)は MD の一部です。必要に応じて、MD の中で複数の MA を設定することができます。MA は MD 名+MA の名によって識別されます。

MA は指定された VLAN を利用するか、どの VLAN も利用しません。VLAN を利用する MA は、VLAN 属性を送信します。VLAN を利用しない MA は、VLAN 属性がないと判断します。

III. MP(Maintenance point)

MP(Maintenance point)はポートで設定され、MA に属します。MP は、MEP(maintenance association end points)と MIP(maintenance association intermediate points) の 2 つのタイプに分類されます。

MEP は MA の境界を定義します。各 MEP は MEP ID によって識別されます。

MEP は内側向きの MEP と外側向きの MEP に分類されます。

- 外側向きの MEP はホストがあるポートにパケットを送信します。
- 内側向き MEP はホストがあるポートにパケットを送信しません。装置上の他のポートにパケットを送信します。

MIP は MA の内部にあります。それは自ら CFD パケットを送信することができないけれども、それは扱い、CFD パケットに反応することができます。MIP は機器によって自動的に作成されます。MEP と協力することによって、MIP は ping と経路探索に類似している機能を実行することができます。

IV. MEP リスト

MEP リストは、同じ MA 内に設定されたローカルな MEP と、モニタのためのリモート MEP のリストです。同じ MA 内のデバイスに設定されるすべての MEP が一覧表示されます。MEP はすべて固有な ID を持っています。MEP はリモートデバイスから、MA の MEP リストに含まれない MEP の ID を転送する CCM(Continuity Check Message)を受信すると、そのメッセージを廃棄します。ローカル装置は、リモート障害表示(RDI)フラグビットを転送する CCM メッセージを送らなければなりません。そうでなければ、隣接装置は確実な障害を検知することができません。MA 内の少なくと

もーつのローカル MEP が、MEP リストから他のすべてのリモート MEP を学習していないとき、MEP は CCM の RDI(Remote Detect Indication)フラグを転送できません。

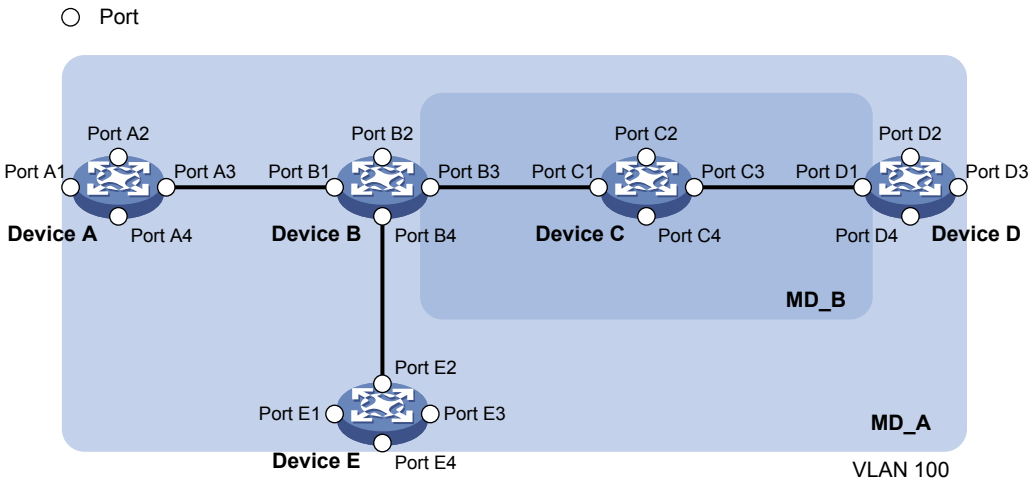
2.1.2. CFD レベル

I. MD レベル

正確に障害個所を見つけるために、CFD は MD に 8 つのレベル（0 から 7 まで）を導入します。数値が大きいほど高レベルであり、カバー可能な領域も大きくなります。ドメインをタッチしたり、入れ子にできたりしますが(外のドメインに入れ子にされたものより高いレベルがある場合)、交差や重複はできません。MD レベルは障害個所の特定を容易にして、障害箇所をより明確にします。

図 2-1 に、MD_A をライトブルー、MD_B を濃いブルーで示します。MD_A で接続障害が発生した場合、Device E を通して Device A を含む MD_A における機器のどの装置にも問題がある可能性があります。MD_B の境界で障害が発生した場合は、Device B、Device C、Device D の間のどこかが問題点となります。MD_B の装置で障害が発生していなければ、少なくとも Device C は操作が可能です。

図 2-1 2 つの入れ子の MD



CFD はメッセージを交換し、ドメイン単位でオペレーションを実行します。ネットワークで正しく MD を決め、CFD を構築することにより、問題点を早く見つけ出すことができます。

II. MA と MP のレベル

MA のレベルは MA が属している MD のレベルと同一です。

MEP のレベルは MEP が属している MD のレベルと同一です。

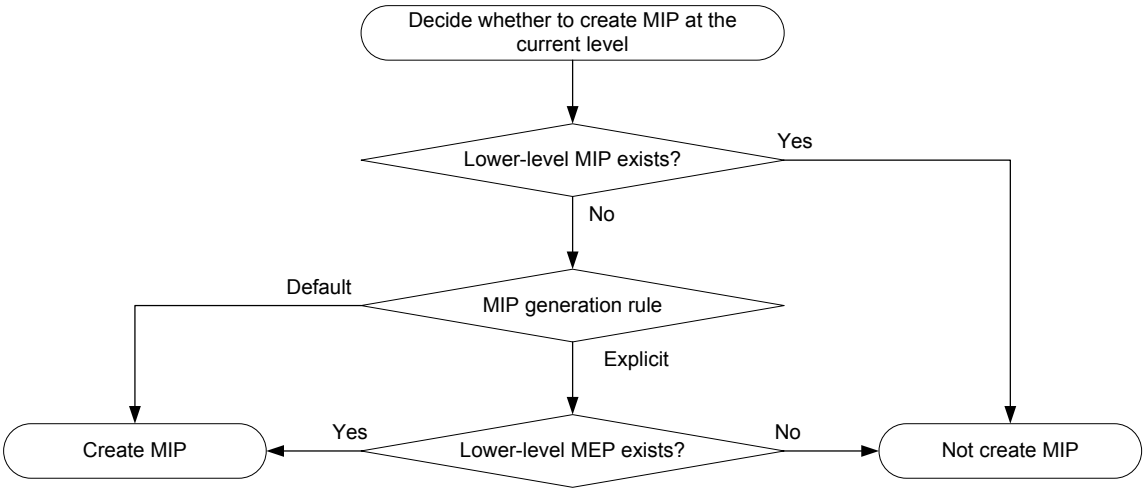
MIP のレベルは生成ルールと MIP が属している MD と生成ルールによって定義されます。MIP は以下に示す MIP 生成ルールにしたがって各ポートで自動的に作成されます。

- **デフォルトルール**—インタフェースで低いレベルの MIP が存在しない場合、MIP は現在のレベルで作成されます。MIP はインタフェースで MEP が設定されていなくても作成することができます。

- **明示ルール**—インタフェースで低いレベルの MIP と低いレベルの MEP がない場合、MEP は現在のレベルで作成されます。MIP はインタフェースで低いレベルの MEP が作成されたときのみ MIP を作成することができます。

ポートが MIP を持たないとき、システムは各 MD(低いレベルから高いレベル)の MA を確認し、現在のレベルで MIP を作成するか作成しないか、図 2-2 に記載されている手順に従います。

図 2-2 MIP の作成手順

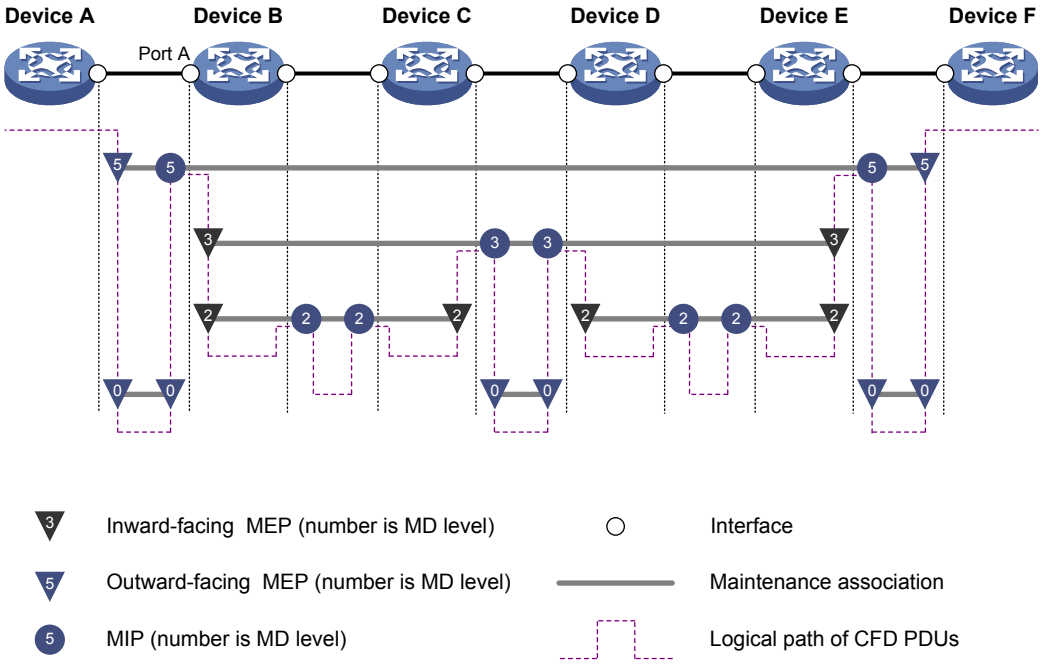


III. CFD の等級づけの例

図 2-3 に CFD モジュールの等級づけの例を示します。MD の 4 つのレベル(0、2、3、5)があります。大きい値は高いレベルで、大きい範囲がサポートされます。MP は Device A から Device F のポートで設定されます。Device B のポートは、以下の MP で設定されます。

- レベル 5 の MIP
- レベル 3 の内側向き MEP
- レベル 2 の内側向き MEP
- レベル 0 の外側向き MEP

図 2-3 CFD grading example



2.1.3. MP のパケット処理

VLAN 属性を運ぶ MA では、MA の MP は MA が提供する VLAN にのみパケットを送信します。MP によって送信されたパケットのレベルは MP が所属している MD のレベルと同一です。

MA が VLAN 属性を持っていない MA では、MA の MPs は外部の MEP のみに対応できます。外向き MEP によって送信されるパケットのレベルは、MEP が属する MD のレベルと等しくなります。

MEP は、処理なしでパケットを上位レベルに転送し、そのレベル以下のパケットのみを処理します。

MIP は、処理を行わずに異なるレベルのパケットを転送し、そのレベルのパケットのみを処理します。

2.1.4. CFD 機能

MP によって実装される CFD 機能は以下です。

- Continuity check (CC)
- Loopback (LB)
- Linktrace (LT)

I. Continuity check

接続障害は、装置障害または設定エラーに起因します。Continuity check は、MEP の接続性をチェックします。この機能は MEP によって CCM(continuity check massage)を定期的に送信することで実行されます。1 つの MEP から送信された CCM は、同じ MA 内のすべての MEP で受信されることを意図しています。MEP を 3.5 回 送信する間に CCM を受信しない場合、リンクが確立していな

いと判断し、ログが生成されます。複数の MEP が同時に CCM を送信すると、多点から多点へのリンクチェックが行われます。CCM はマルチキャストフレームです。

II. Loopback

IP レイヤの ping と同様に、loopback はローカルデバイスと宛先デバイスの接続性を検証します。この機能を実行するために、ローカル MEP は、宛先 MEP に LBM(loopback massage)を送信します。ローカル MEP が宛先 MEP からの LBR(loopback reply massage）を受信するかどうかで、2 つの間のリンク状態をチェックします。

LBM と LBR は、ユニキャストフレームとユニキャストフレームです。装置はユニキャストフレームの送受信とマルチキャスト LBM フレームの受信をサポートします。マルチキャスト LBM フレームの送信をサポートしていません。LBR フレームはユニキャストフレームです。

III. Linktrace

Linktrace は、traceroute と同様です。ソース MEP と宛先 MEP の間のパスを識別します。ソース MEP は、宛先 MEP に LTM(linktrace messages)を送信します。メッセージ受信後、宛先 MEP および MIP は、LTM フレームのソース MEP に LTR(linktrace reply massage)を送り返します。reply メッセージにもとづいて、ソース MEP は、宛先 MEP までの経路を識別できます。LTR はユニキャストフレームですが、LTM はマルチキャストフレームとなります。

2.1.5. プロトコルと標準

- IEEE 802.1ag, *Virtual Bridged Local Area Networks Amendment 5: Connectivity Fault Management*
- ITU-T Y.1731, *OAM functions and mechanisms for Ethernet based networks*

2.2. 制限とガイドライン

- 他の CFD を設定するために、リモート MEP の MEP ID を使用する前に CC を設定してください。他の CFD を設定するために、リモート MEP の MAC アドレスを使用する場合は例外です。
- 一般的に、スパニングツリーによってブロックポートとなった場合、以下のケースを除いて、CFD メッセージの送受信ができません。
  - ポートは外側向き MEP として設定されています。
  - ポートは、CCM メッセージを除く CFD メッセージを送受信できるよう設定された内側向きの MEP あるいは MIP として設定されています。

スパニングツリーの詳細は、セクション 3 *アクセス オペレーションマニュアル*の"*STP*"を参照してください。

2.3. CFDの設定作業リスト

作業リスト
CFDの基本設定 • (必須設定項目) CFD の有効化 • (必須設定項目) サービスインスタンスの設定 • (必須設定項目) MEP の設定 • (必須設定項目) MIP 自動生成ルールの設定
CFD機能の設定: • (必須設定項目) CC の設定 • (オプション設定項目) LB の設定 • (オプション設定項目) LT の設定

2.4. CFDのための必要条件

CFD が正しく動作するように、以下の作業を実行して、ネットワークを設計する必要があります。

- 全体のネットワークで MD のレベル付けを行い、各 MD の境界を定義してください。
- MD ごとに名前を割り当ててください。同じ MD 内にある装置は同じ MD の名前を使用していることを確認してください。
- 監視したい VLAN にしたがって、各 MD の MA を定義してください。
- MA ごとに名前を割り当ててください。同じ MD 内の同じ MA の装置が、同じ MA の名前を使用することを確認してください。
- 各 MD で各 MA の MEP リストを決定してください。同じ MA の装置が同じ MEP リストを持っていることを確認してください。
- MD と MA はエッジ、MEP はデバイスポートに設定する必要があります。MIP は、エッジではない装置またはポートに設計することができます。

2.5. CFDの基本設定

2.5.1. CFD の有効化

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. CFD を有効にする	**cfd enable**	デフォルト：無効

2.5.2. イーサネットサービスインスタンスの設定

I. イーサネットサービスインスタンスについて

MEP と MIP を設定する前に、最初にサービスインスタンスを設定する必要があります。サービスインスタンスはサービスアクセスポイント(SAP)で、MD 中の MA に属しています。

MD と MA は、サービスインスタンスの MP によって処理されたメッセージのレベルと VLAN 属性を定義します。VLAN 属性がない MA の MP は、VLAN に属していません。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. MD を作成する	**cfd md** *md-name* [**index** *index-value*] **level** *level-value*	デフォルト：設定なし
3. サービスインスタンスを作成する	**cfd service-instance** *instance-id* **ma-id** { **icc-based** *ma-name* | **integer** *ma-num* | **string** *ma-name* | **vlan-based** [*vlan-id*] } [**ma-index** *index-value*] **md** *md-name* [**vlan** *vlan-id*]	デフォルト：設定なし

2.5.3. MEP の設定

I. MEP について

CFD は MEP のオペレーションを通して実行されます。MEP はサービスインスタンス上で構成され、MD レベルとサービスインスタンスの VLAN 属性は MEP の属性になります。

II. 制限とガイドライン

- インタフェースが同一レベルで、VLAN 属性なしで 1 つの MA の外側向けの MEP を設定することができます。
- VLAN 属性がない MA の MEP がリモート MEP から 3.5 CCM 間隔以内に CCM メッセージを受信しない場合、ローカル MEP はインタフェースをリンクダウン状態に設定します。このローカル MEP の動作により、RRPP あるいは Smart Link の高速切り替えが容易になります。

III. 設定要件

MEP を設定する前にイーサネットサービスを作成して下さい。

IV. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. MEP リストを設定する	**cfd meplist** *mep-list* **service-instance** *instance-id*	デフォルト：設定なし

操作	コマンド	補足
3. Layer 2 interface view あるいは Layer 2 aggregate interface view に移行する	**interface** *interface-type interface-number*	―
4. MEP を作成する	**cfd mep** *mep-id* **service-instance** *instance-id* { **inbound** | **outbound** }	デフォルト：設定なし

2.5.4. MIP 自動生成ルールの作成

I. MIP 自動生成ルールについて

サービスインスタンスの機能的な実体として、MIP は、LTM フレーム、LBM フレームなどの様々な CFD フレームに応答します。システムは MIP 自動作成ルールにもとづいて MIP を自動的に作成します。

cfd mip-rule コマンドが設定された後、以下の要因によって MIP を作成あるいは削除することができます。

- CFD の有効化あるいは無効化
- ポートの MEP の作成あるいは削除
- ポートの VLAN 属性の変更
- **cfd mip-rule** コマンドで指定されるルールの変更

II. 制限とガイドライン

- VLAN 属性がない MA は主にダイレクトリンクの状態を検出するのに使用されます。その VLAN 属性がない MA は MIP を生成することはできません。
- VLAN 属性がある MA で、インタフェースで同一以上のレベルの MEP が存在する場合、MA 用の MIP はインタフェースで作成されません。

III. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. MIP 自動生成ルールを設定する	**cfd mip-rule** { **default** | **explicit** } **service-instance** *instance-id*	デフォルト：生成ルールは設定されておらず、自動的に MIPを作成しません。

2.6. CFD function機能の設定

2.6.1. CC の設定

I. CC について

CC を設定したのち、MA の MEP は接続性のチェックを行うために定期的に CCM フレームを送信できます。

他の CFD を設定するために、リモート MEP の MEP ID を使用する前に CC を設定してください。他の CFD を設定するために、リモート MEP の MAC アドレスを使用する場合は例外です。

CCM フレームのタイムアウト時間が終了したとき、MEP はリンクが切断されたと認識します。CCM の interval フィールドを設定するとき、表 2-1 .に示す値を使用します。

表 2-1 CCM の interval フィールドの変換

CCM の interval フィールドの値	CCM の送信間隔	最大 CCM ライフタイム時間
1	10/3 ミリ秒	35/3 ミリ秒
2	10 ミリ秒	35 ミリ秒
3	100 ミリ秒	350 ミリ秒
4	1 秒	3.5 秒
5	10 秒	35 秒
6	60 秒	210 秒
7	600 秒	2100 秒

メモ ：

- Interval フィールドの設定範囲は 1 ～7 です。1 および 2 の値を設定した場合、ハードウエア性能によって値と異なる動作をする場合があります。
- cfd cc interval コマンドの interval フィールドの 1～3 の CCM メッセージは short-interval の CCM メッセージです。interval フィールドの 4～7 の CCM メッセージは long-interval の CCM メッセージです。

II. 制限とガイドライン

MEP で CC を設定するとき、以下のガイドラインに従ってください。

- 同一 MA 内のすべての MEP は、同一 CCM の interval フィールドの値を設定してください。
- CCM の interval フィールドを変更したのち、MEP は、CCM を送る前に別の CCM 間隔を待たなければなりません。

III. 設定手順

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) MEP から送信される CCM メッセージの送信間隔を設定する	**cfd cc interval** *interval-value* **service-instance** *instance-id*	デフォルト：4
3. Layer 2 interface view あるいは Layer 2 aggregate interface view に移行する	**interface** *interface-type interface-number*	―

操作	コマンド	補足
4. MEP 上で CCM の送信を有効にする	**cfd cc service-instance** *instance-id* **mep** *mep-id* **enable**	デフォルト：無効

2.6.2. LB の設定

LB は、ローカル MEP、リモート MEP、あるいは MIP の間のリンクの状態を確認することができます。

操作	コマンド	補足
LBを有効にする	**cfd loopback service-instance** *instance-id* **mep** *mep-id* { **target-mac** *mac-address* | **target-mep** *target-mep-id* } [**number** *number*]	すべてのviewで設定可能です。

2.6.3. LT の設定

I. LT について

LT はソース MEP とターゲット MEP の間で経路をたどることができ、自動的に LT メッセージを送信することで、リンク障害を検出します。2 つの機能は、以下のようにして実装されます。

- **経路確認**—最初の機能を実装するため、ソース MEP は、ターゲット MEP に LTM にメッセージを送信します。LTM メッセージに応答した LTR メッセージにより、2 つの MEP 間の経路確認ができます。
- **LT メッセージの自動送信**—LT メッセージの自動送信－LT メッセージの自動送信が有効になると、ソース MEP が 3.5 回送信する間にターゲット MEP からの CCM フレームを受信しなれば、2 つの間のリンクは不完全であると考えられ、LTM フレーム（宛先がターゲットの MEP で、LTM フレームの TTL フィールドに最大値 255 がセットされています）が送信されます。MIP が応答した LTR にもとづいて、障害場所の特定ができます。

II. 設定要件

VLAN 属性を送信する MA の MEP で LT を設定する前に、MA が所属する VLAN を作成してください。

III. 設定手順

操作	コマンド	補足
1. ソース MEP とターゲット MEP 間のパスを検出する	**cfd linktrace service-instance** *instance-id* **mep** *mep-id* { **target-mac** *mac-address* | **target-mep** *target-mep-id* } [**ttl** *ttl-value*] [**hw-only**]	すべてのviewで設定可能です。
2. system view に移行する	**system-view**	―

操作	コマンド	補足
3. LT メッセージの自動送信を有効にする	**cfd linktrace auto-detection** [**size** *size-value*]	デフォルト：無効

2.7. CFDの表示と管理

すべての view で **display** コマンドを実行できます。

操作	コマンド
MEPで受信したLTR情報を表示する	**display cfd linktrace-reply** [**service-instance** *instance-id* [**mep** *mep-id*]]
LTMに自動応答したLTRメッセージの受信情報を表示する	**display cfd linktrace-reply auto-detection** [**size** *size-value*]
MD設定情報を表示する	**display cfd md**
MEPの属性と稼動状況を表示する	**display cfd mep** *mep-id* **service-instance** *instance-id*
サービスインスタンスのMEPリストを表示する	**display cfd meplist** [**service-instance** *instance-id*]
MP情報を表示する	**display cfd mp** [**interface** *interface-type interface-number*]
リモートMEP情報を表示する	**display cfd remote-mep service-instance** *instance-id* **mep** *mep-id*
サービスインスタンス設定情報を表示する	**display cfd service-instance** [*instance-id*]
CFDの状態を表示する	**display cfd status**

2.8. CFDの設定例

2.8.1. CFD の設定例

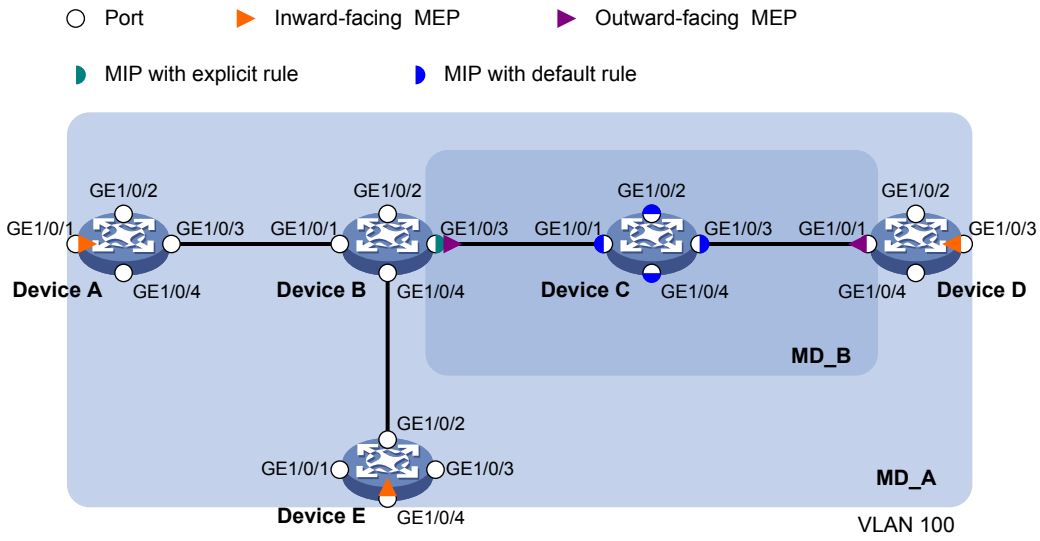
I. ネットワーク要件

図 2-4 に示すように以下の設定を行います。

- ネットワークには 5 つの装置があり、MD_A(Level 5)、MD_B(Level 3)の 2 つの MD に分かれています。すべてのポートは VLAN100 に属し、2 つの MD の MA はすべて VLAN100 で動作しています。Device A～Device E の MAC アドレスを、それぞれ 0010-FC00-6511、0010-FC00-6512、0010-FC00-6513、0010-FC00-6514、0010-FC00-6515 とします。
- MD_A は Device A の GigabitEthernet 1/0/1、Device D の GigabitEthernet 1/0/3、Device E の GigabitEthernet 1/0/4 の 3 つのエッジポートがあります。すべて内向き MEP(Inward-facing MEP)です。MD_B は Device B の GigabitEthernet 1/0/3、Device D の GigabitEthernet 1/0/1 の 2 つのエッジポートがあります。そのポートは外向き MEP(Outward-facing MEP)です。

- MD_A では、Device B のポートは、低レベルの MEP が設定されたときに MIP を持つように設計されています。GigabitEthernet 1/0/3 は MD_B の MEP と設定され、MD_A の MIP がこのポートに設定されます。MD_A の MIP 生成ルールを明示的にする必要があります。
- Device C のすべてのポートで MD_B の MIP が設定されています。デフォルトの MIP 生成ルールを設定します。
- ソース MEP とターゲット MEP の間の経路、またはリンク障害を検出するために、LT を使用してください。
- ネットワーク全体のステータス情報が得られた後に、リンク障害を検出するために、LT を使って回線障害を見つけます。

図 2-4 ネットワーク図



II. 設定手順

1. VLAN を作成し、ポートを割り当てます。

   図 2-4 に示すように各 Device で、VLAN 100 を作成し、GigabitEthernet 1/0/1～GigabitEthernet 1/0/4 に VLAN100 を割り当てます。

2. CFD を有効にします。

   # Enable CFD on Device A.

   <DeviceA> system-view

   [DeviceA] cfd enable

   # Device A の設定と同様に、Device B～Device E で CFD を有効にします。（詳細は省略します）

3. イーサネットサービスインスタンスを作成します。

   # Device A で MD_A(level 5)、サービスインスタンス 1 を作成します。サービスインスタンス 1 では MA は VLAN によって識別され、VLAN100 を提供します。

   [DeviceA] cfd md MD_A level 5

   [DeviceA] cfd service-instance 1 ma-id vlan-based md MD_A vlan 100

   # Device A の設定と同様に Device E を設定します。（詳細は省略します）

Device B で MD_A(level 5)を作成し、サービスインスタンス 1 を作成します。サービスインスタンス 1 では MA は VLAN によって識別され、VLAN100 を提供します。

[DeviceB] cfd md MD_A level 5

[DeviceB] cfd service-instance 1 ma-id vlan-based md MD_A vlan 100

MD_B(level 3)を作成し、サービスインスタンス 2 を作成します。サービスインスタンス 2 では MA は VLAN によって識別され、VLAN100 を提供します。

[DeviceB] cfd md MD_B level 3

[DeviceB] cfd service-instance 2 ma-id vlan-based md MD_B vlan 100

Device B の設定と同様に Device D を設定します。（詳細は省略します）

Device C で MD_B(level 3)を作成し、サービスインスタンス 2 を作成します。サービスインスタンス 2 では MA は VLAN によって識別され、VLAN100 を提供します。

[DeviceC] cfd md MD_B level 3

[DeviceC] cfd service-instance 2 ma-id vlan-based md MD_B vlan 100

4. MEP を設定します。

Device A で、サービスインスタンス 1 の MEP リストを設定し、GigabitEthernet 1/0/1 のサービスインスタンス 1 の内向き MEP 1001 を作成します。

[DeviceA] cfd meplist 1001 4002 5001 service-instance 1

[DeviceA] interface gigabitethernet 1/0/1

[DeviceA-GigabitEthernet1/0/1] cfd mep 1001 service-instance 1 inbound

[DeviceA-GigabitEthernet1/0/1] quit

Device B でサービスインスタンス 1、2 の MEP リストを設定します。

[DeviceB] cfd meplist 1001 4002 5001 service-instance 1

[DeviceB] cfd meplist 2001 4001 service-instance 2

Device B で GigabitEthernet 1/0/3 のサービスインスタンス 2 の外向き MEP 2001 を作成します。

[DeviceB] interface gigabitethernet 1/0/3

[DeviceB-GigabitEthernet1/0/3] cfd mep 2001 service-instance 2 outbound

[DeviceB-GigabitEthernet1/0/3] quit

Device D でサービスインスタンス 1、2 の MEP リストを設定します。

[DeviceD] cfd meplist 1001 4002 5001 service-instance 1

[DeviceD] cfd meplist 2001 4001 service-instance 2

Device D で GigabitEthernet 1/0/1 のサービスインスタンス 2 の外向き MEP 4001 を作成します。

[DeviceD] interface gigabitethernet 1/0/1

[DeviceD-GigabitEthernet1/0/1] cfd mep 4001 service-instance 2 outbound

[DeviceD-GigabitEthernet1/0/1] quit

Device D で GigabitEthernet 1/0/3 のサービスインスタンス 1 の内向き MEP 4002 を作成します。

[DeviceD] interface gigabitethernet 1/0/3

[DeviceD-GigabitEthernet1/0/3] cfd mep 4002 service-instance 1 inbound

[DeviceD-GigabitEthernet1/0/3] quit

Device E でサービスインスタンス 1 の MEP リストを設定します。

[DeviceE] cfd meplist 1001 4002 5001 service-instance 1

Device E で GigabitEthernet 1/0/4 のサービスインスタンス 1 の内向き MEP 5001 を作成します。

[DeviceE] interface gigabitethernet 1/0/4

[DeviceE-GigabitEthernet1/0/4] cfd mep 5001 service-instance 1 inbound

[DeviceE-GigabitEthernet1/0/4] quit

5. MIP の設定をします。

Device B のサービスインスタンス 1 で MIP の作成ルールを明示的に設定します。

[DeviceB] cfd mip-rule explicit service-instance 1

Device C のサービスインスタンス 2 で MIP のデフォルトの作成ルールを明示的に設定します。

[DeviceC] cfd mip-rule default service-instance 2

6. CC の設定をします。

Device A の GigabitEthernet 1/0/1 で、サービスインスタンス 1 の MEP 1001 用の CCM フレームの送信を有効にします。

[DeviceA] interface gigabitethernet 1/0/1

[DeviceA-GigabitEthernet1/0/1] cfd cc service-instance 1 mep 1001 enable

[DeviceA-GigabitEthernet1/0/1] quit

Device B の GigabitEthernet 1/0/3 で、サービスインスタンス 2 の MEP 2001 用の CCM フレームの送信を有効にします。

[DeviceB] interface gigabitethernet 1/0/3

[DeviceB-GigabitEthernet1/0/3] cfd cc service-instance 2 mep 2001 enable

[DeviceB-GigabitEthernet1/0/3] quit

Device D の GigabitEthernet 1/0/1 で、サービスインスタンス 2 の MEP 4001 用の CCM フレームの送信を有効にします。

[DeviceD] interface gigabitethernet 1/0/1

[DeviceD-GigabitEthernet1/0/1] cfd cc service-instance 2 mep 4001 enable

[DeviceD-GigabitEthernet1/0/1] quit

Device D の GigabitEthernet 1/0/3 で、サービスインスタンス 1 の MEP 4002 用の CCM フレームの送信を有効にします。

[DeviceD] interface gigabitethernet 1/0/3

[DeviceD-GigabitEthernet1/0/3] cfd cc service-instance 1 mep 4002 enable

[DeviceD-GigabitEthernet1/0/3] quit

Device E の GigabitEthernet 1/0/4 で、サービスインスタンス 1 の MEP 5001 用の CCM フレームの送信を有効にします。

[DeviceE] interface gigabitethernet 1/0/4

[DeviceE-GigabitEthernet1/0/4] cfd cc service-instance 1 mep 5001 enable

[DeviceE-GigabitEthernet1/0/4] quit

III. 設定の確認

1. CC 機能がリンク障害を検出した場合、LB 機能を確認します。

   # Device A で LB 機能を有効にし、サービスインスタンス 1 の MEP 1001 と MEP 5001 間のリンクステータスをチェックします。

   [DeviceA] cfd loopback service-instance 1 mep 1001 target-mep 5001

   ```
   Loopback to MEP 5001 with the sequence number start from 1001-43404:
   Reply from 0010-fc05-6515: sequence number=1001-43404 time=5ms
   Reply from 0010-fc05-6515: sequence number=1001-43405 time=5ms
   Reply from 0010-fc05-6515: sequence number=1001-43406 time=5ms
   Reply from 0010-fc05-6515: sequence number=1001-43407 time=5ms
   Reply from 0010-fc05-6515: sequence number=1001-43408 time=5ms
   Sent: 5        Received: 5        Lost: 0
   ```

2. すべてのネットワークのステータス状態を CC 機能で取得した後、LT 機能を確認します。

   # Device A のサービスインスタンス 1 で MEP 1001 と MEP 5001 間の経路を確認します。

   [DeviceA] cfd linktrace service-instance 1 mep 1001 target-mep 5001

   ```
   Linktrace to MEP 5001 with the sequence number 1001-43462:
   MAC address               TTL     Last MAC         Relay action
   0010-fc05-6515            63      001
   ```

目次

このセクションのページは **9-x-x** です。

3 章 DLDP 3-1
3.1. 概要 3-1
3.1.1. アプリケーションシナリオ 3-1
3.1.2. 基本概念 3-2
3.1.3. DLDP の仕組み 3-4
3.2. 制限とガイドライン 3-6
3.3. DLDP 設定作業リスト 3-6
3.4. DLDP の有効化 3-7
3.5. Advertisement パケット送信間隔の設定 3-7
3.6. DelayDown タイマの設定 3-7
3.7. ポートシャットダウンモードの設定 3-8
3.8. DLDP 認証の設定 3-9
3.9. DLDP の表示および保守コマンド 3-9
3.10. DLDP 設定例 3-10
3.10.1. 自動ポートシャットダウンモードの設定例 3-10
3.10.2. 手動ポートシャットダウンモードの設定例 3-13

3章 DLDP

3.1. 概要

オートネゴシエーションなどの物理層検出メカニズムは、物理信号と障害を検出できます。ただし、物理レイヤが接続状態にある単方向リンクの通信障害は検出できません。

データリンクとして DLDP（Device Link Detection Protocol)は、次のことが可能です。

- リンク層の光ファイバリンクまたはツイストペアリンクのステータスを監視します。
- 物理層プロトコルと協力して、リンクが正しく接続されているかどうか、およびリンクの両端が正しくパケットを交換できるかどうかを確認します。

DLDP が単方向リンクを検出すると、ネットワークの問題を回避するために、障害のあるポートを自動的にシャットダウンできます。または、ユーザーは手動で障害のあるポートをシャットダウンできます。

3.1.1. アプリケーションシナリオ

リンクの一方の端だけが他方の端からパケットを受信できる場合、リンクは片方向になります。

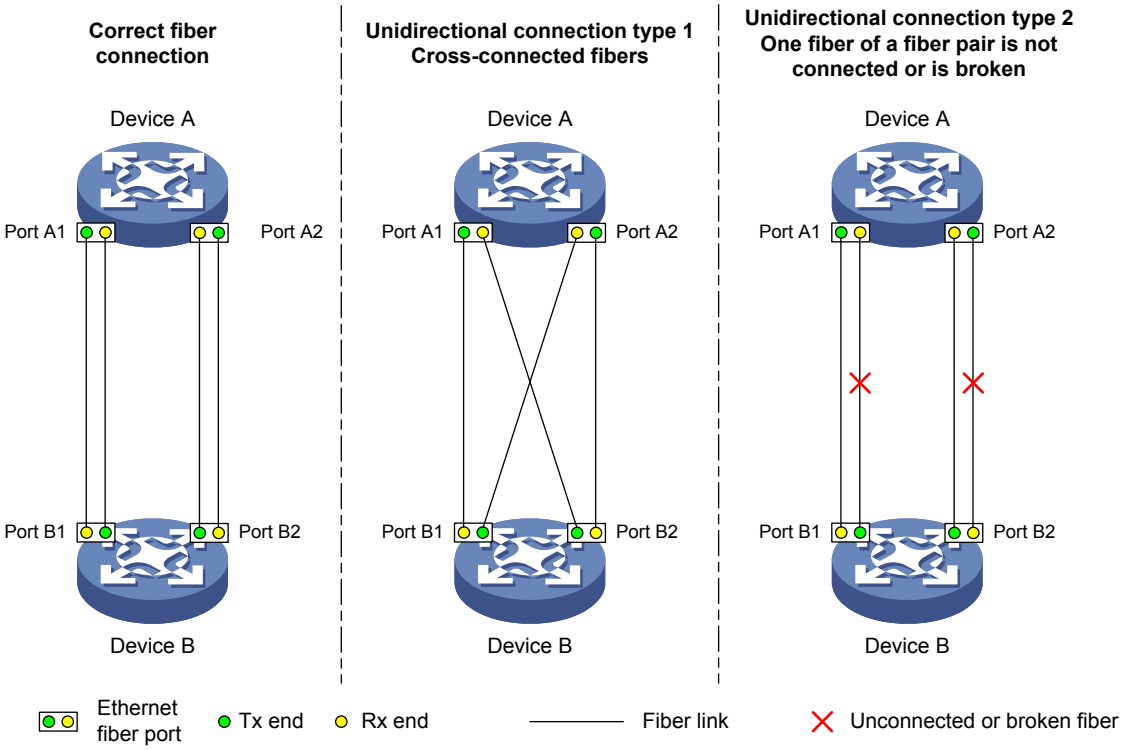
単方向ファイバリンクは、次の場合に発生します。

- ファイバは相互接続されています。
- ファイバが 1 つの端部に接続されていないか、ファイバペアのファイバが 1 つ破損しています。

図 3-1 に正しいファイバ接続と 2 種類の片方向のファイバ接続を示します。

DLDP が単方向リンクを検出すると、ネットワークの問題を回避するために、障害のあるポートを自動的にシャットダウンできます。または、ユーザーは手動で障害のあるポートをシャットダウンできます。

図 3-1 ファイバの正常な接続と異常な接続



3.1.2. 基本概念

I. DLDP 隣接状態

ポート A が同じリンク上のポート B からリンク層パケットを受信できる場合、ポート B はポート A の DLDP ネイバであり、パケット交換可能な 2 つのポートは隣接ルータです。

表 3-1 DLDP 隣接状態

DLDP タイマ	説明
確認済み	DLDPネイバへのリンクは双方向です。
未確認	新しく検出されたネイバへのリンクの状態は決定されません。

II. DLDP ポート状態

DLDP 対応ポートは、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、その状態は DLDP 隣接状態によって異なります。

表 3-2 DLDP ポート状態

状態	説明
初期	DLDPはポートで有効になっていますが、グローバルに無効になっています。
非アクティブ	DLDPはポート上で有効になり、リンクは物理的にダウンします。
双方向	DLDPはポート上で有効になり、確認済み状態では少なくとも1つの

状態	説明
	ネイバが存在します。
単方向	DLDPはポート上で有効になり、確認済み状態に隣接していません。この状態では、ポートは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 3-3 DLDP タイマ

DLDP タイマ	説明
Advertisement タイマ	パケット送信間隔です。(デフォルトは5秒です。設定可能です。)
Probeタイマ	Probeパケット送信間隔です。このタイマは1秒に設定されています。
Echoタイマ	新しいネイバ用にProbe状態になったとき、Echoタイマが開始します。ネイバ情報はタイマが切れると削除されます。このタイマは10秒に設定されています。
入力タイマ	新しい隣接ルータが結合されると、ネイバエントリが作成され、隣接ルータが確認済み状態にある場合に、対応するエントリタイマが開始します。アドバタイズメントを受信すると、デバイスは対応するネイバエントリとエントリタイマを更新します。 Entryタイマが満了すると、ネイバのエンハンスタイマとEchoタイマが開始します。 入力タイマの値はAdvertisementタイマの3倍です。
拡張タイマ	Probeパケット送信間隔です。このタイマは1秒に設定されています。 エントリタイマが満了すると、Enhancedタイマがトリガされ、Probeパケットが送信されます。 同時に、Echoタイマがトリガされます。
DelayDownタイマ	ポートが物理的にダウンしている場合、デバイスは対応するネイバエントリを削除するのではなく、DelayDownタイマをトリガします。 デフォルトのDelayDownタイマは1秒で設定可能です。 DelayDownタイマが期限切れになると、デバイスはポートがダウンしている場合に対応するDLDPネイバ情報を削除し、ポートがアップしている場合は操作を実行しません。
RecoverProbeタイマ	このタイマは2秒に設定されています。 単方向のポートは、定期的にRecoverProbeパケットを送信して、片方向リンクが双方向に復元されたかどうかを検出します。

IV. DLDP 認証モード

DLDP 認証を使用して、ネットワーク攻撃や不正検出を防止できます。

表 3-4 DLDP 認証モード

認証モード	DLDP パケット送信側での処理	DLDP パケット受信側での処理
非認証	送信側は、DLDPパケットの認証フィールドを0に設定します。	受信側は受信したDLDPパケットの認

認証モード	DLDP パケット送信側での処理	DLDP パケット受信側での処理
平文認証	送信側は、平文で設定されたパスワードに認証フィールドを設定します。	証情報を調べ、認証情報がローカル構成と競合するパケットを廃棄します。
MD5認証	送信側は、MD5アルゴリズムを使用してユーザー設定パスワードを暗号化し、ダイジェストを認証フィールドに割り当てます。	

3.1.3. DLDP の仕組み

I. 隣接機器を検出する

2 つのデバイスが光ファイバまたはネットワークケーブルを介して接続されている場合は、DLDP がネイバへの片方向リンクを検出できるようにします。 次の 2 つのケースで、単方向リンク検出プロセスを示します。

- 片方向リンクは、DLDP を有効にする前に発生します。

図 3-2 クロス接続ファイバ

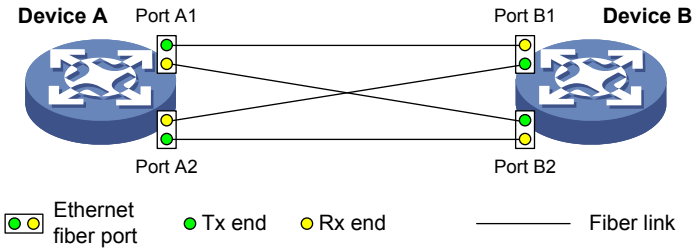


図 3-2 に示すように、DLDP を有効にする前に、デバイス A とデバイス B 間の光ファイバが相互接続されています。 DLDP を有効にした後、4 つのポートはすべて、片方向状態であり、RecoverProbe パケットを送信します。 単方向リンク検出プロセスを示す例として、ポート A1 を使用します。

a. ポート A1 は、ポート B2 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 B2 は、ポート A1 から RecoverEcho パケットを受信できません。したがってポート B2 はポート A1 のネイバになることはできません。

c. ポート B1 は、ポート A1 から RecoverEcho パケットを受信できますが、ポート B1 は目的の宛先ではなく、ポート B1 のネイバになることはできません。

同じプロセスが他の 3 つのポートで発生します。 4 つのポートはすべて片方向の状態です。

- 片方向リンクは、DLDP を有効にした後に発生します。

図 3-3 ファイバの故障

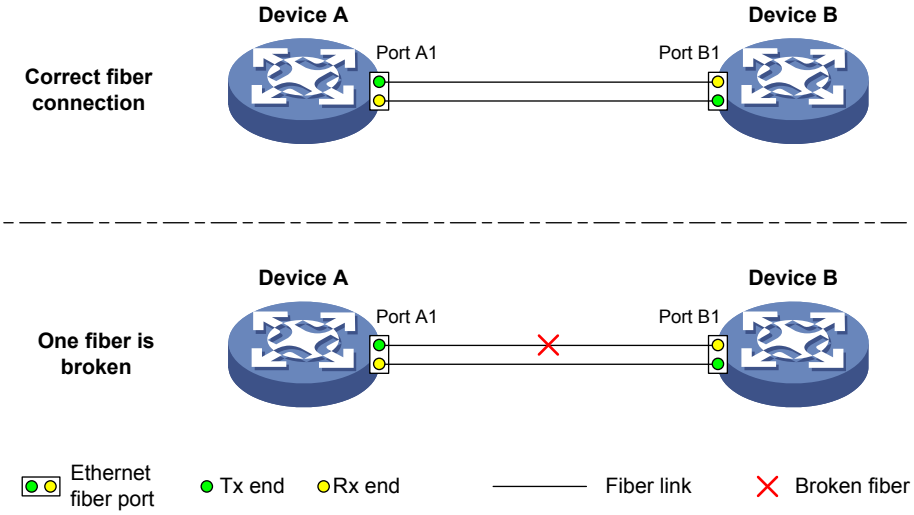


図 3-3 に示すように、Device A および Device B は、光ファイバを介して接続されます。DLDP を有効にした後、ポート A1 とポート B1 は双方向の隣接を次のように設定します。

a. 物理的にアップするポート A1 は、単方向状態に入り、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 B1 は RecoverEcho パケットを返します。

c. ポート A1 が RecoverEcho パケットを受信した後、パケット内のネイバ情報を調べます。近隣情報がローカル情報と一致する場合、ポート A1 はポート B1 を持つ近隣を確立し、双方向状態に移行します。 ポート A1 は入力タイマを開始し、定期的に Advertisement パケットを送信します。

d. ポート B1 がアドバタイズメントパケットを受信した後、ポート A1 を使用して Unconfirmed 近隣ルータを確立します。 ポート B1 は、Echo タイマと Probe タイマを起動し、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 A1 は Echo パケットを返します。

f. ポート B1 が Echo パケットを受信した後、パケット内の隣接情報を調べます。 ネイバ情報がローカル情報と一致する場合、ポート A1 のネイバ状態は確認されます。 次に、ポート B1 は双方向状態に移行し、Entry タイマを開始します。そして定期的にアドバタイズメントパケットを送信します。

ポート A1 とポート B1 の間の双方向の隣接が確立されました。

その後、ポート B1 の Rx 端が信号を受信できない場合、ポート B1 は物理的にダウンし、非アクティブ状態になります。 ポート B1 の Tx エンドはポート A1 に信号を送信できるため、ポート A1 は引き続きアップします。 ポート B1 のエントリタイマが期限切れになると、ポート A1 は Enhanced タイマと Echo タイマを起動し、Probe パケットをポート B1 に送信します。ポート A1 の Tx ラインが壊れているため、Echo タイマが満了した後、Port A1 はポート B1 から Echo パケットを受信できません。 ポート A1 は、単方向状態に入り、Disable パケットをポート B1 に送信します。 同時にポート A1 は、ポート B1 で近隣を削除し、RecoverProbe タイマを起動します。 このプロセス中、ポート B1 は非アクティブ状態になります。

インタフェースが物理的にダウンしているが、インタフェースの Tx 終端が動作中である場合、DLDP は LinkDown パケットを送信して、関連するネイバエントリを削除します。

II. 複数の隣接機器を検出する

ハブを介して複数のデバイスが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で DLDP を有効にして、ネイバ間の片方向リンクを検出します。 確認済みネイバが存在しない場合、インタフェースは単方向状態に入ります。

図 3-4 ネットワーク図

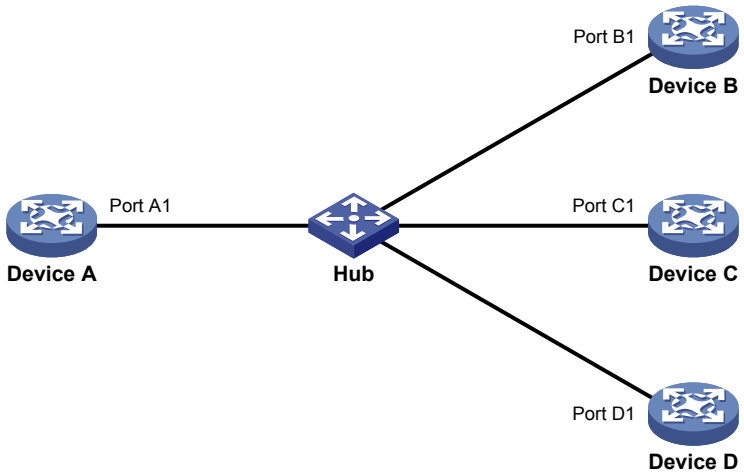


図 3-4 に示すように、Device A から Device D はハブを介して接続され、DLDP が有効になっています。ポート 1、ポート 2、ポート 3 がポート 4 のリンクが故障したと検出したとき、ポート 4 との隣接関係を削除しますが、Bidirectional 状態を維持します。

3.2. 制限とガイドライン

DLDP を設定する場合は、次の制限とガイドラインに従ってください。

- DLDP が正しく動作するためには、両側で DLDP を有効にし、次の設定が同一であることを確認します。
  - アドバタイズメントパケットを送信する間隔。
  - DLDP 認証モード。
  - パスワード。
- DLDP が正しく動作するには、リンクの両端にあるポートの全二重モードを設定し、2 つのポートに対して同じ速度を設定します。

3.3. 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

作業リスト
(オプション設定項目) DLDP認証の設定

3.4. DLDP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*	ー
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はリンクダウンが直ちに発生します。

3.5. Advertisementパケット送信間隔の設定

I. 概要

ネットワークパフォーマンスが低下する前に、DLDPが片方向リンクを検出できるようにするには、ネットワーク環境に適したAdvertisement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。

II. 手順

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

3.6. DelayDownタイマの設定

I. DelayDown タイマの設定について

Tx ラインに障害が発生すると、一部のポートがダウンして再び立ち上がり、Rx ライン上に光信号ジッタが発生します。デバイスがそのような場合に隣接エントリを削除しないようにするには、デバイスの DelayDown タイマを設定します。Tx 回線障害によりポートがダウンすると、デバイスは DelayDown タイマを起動します。 タイマが期限切れになったときにポートがダウンした場合、デバイスは DLDP ネイバ情報を削除します。 ポートが起動すると、デバイスは動作しません。

II. 手順

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

3.7. ポートシャットダウンモードの設定

I. ポートのシャットダウンモードについて

片方向リンクを検出すると、DLDP は次のいずれかのモードでポートをシャットダウンします。

- **自動モード**--DLDP が単方向リンクを検出すると、単方向ポートをシャットダウンします。リンクが双方向になると、シャットダウンされたポートが表示されます。
- **手動モード**-DLDP が単方向リンクを検出すると、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。リンクステータスを確認するには、**undo shutdown** コマンドを使用してポートを起動します。 リンクが双方向になると、ポートは双方向になります。 このモードを使用して、次の場合に、単一方向リンクレポートのために通常のリンクがシャットダウンされないようにします。
  - ネットワークのパフォーマンスが低い状態です。
  - デバイスがビジー状態です。
  - CPU 使用率が高い状態です。

II. 制限とガイドライン

system view 内のすべてのインタフェース、または interface view の一つのインタフェースのポートシャットダウンモードを設定できます。interface view の設定は、system view の設定よりも優先されます。

DLDP ポートでリモート OAM ループバックを有効にするには、ポートシャットダウンモードを手動に設定します。それ以外の場合、DLDP は自動的にパケットを受信したときにポートをシャットダウンします。 これにより、リモート OAM ループバック障害が発生します。 Ethernet OAM の詳細については、セクション 9 *高可用性 オペレーションマニュアル*の“*Ethernet OAM の設定*”を参照してください。

III. グローバルでのポートシャットダウンモードの設定

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

IV. インタフェースでのポートシャットダウンモードの設定

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. Ethernet interface view に移行する	**interface** *interface-type interface-number*	—
3. 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**

3.8. DLDP認証の設定

I. DLDP 認証について

適切な DLDP 認証モードを設定して、平文認証または MD5 認証を行うことができるように、攻撃や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は、認証しないことを選択できます。

II. 手順

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。

3.9. DLDPの表示および保守コマンド

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
グローバルおよびポートのDLDP構成を表示する	**display dldp** [**interface** *interface-type interface-number*]
ポートを通過するDLDPパケットに関する統計情報を表示する	**display dldp statistics** [**interface** *interface-type interface-number*]
ポートを通過するDLDPパケットの統計情報をクリアする	**reset dldp statistics** [**interface** *interface-type interface-number*]

3.10. DLDP設定例

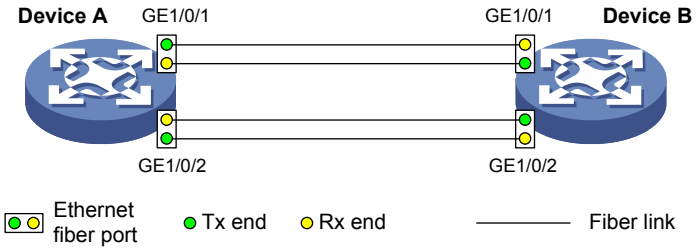
3.10.1. 自動ポートシャットダウンモードの設定例

I. ネットワーク要件

図 3-5 に示すように、Device A および Device B は、2 つのファイバペアを介して接続されています。

単一方向リンクを検出したときに、障害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起動するように設定します。

図 3-5 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 を全二重モードおよび 1000Mbps で動作するように設定し、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 を全二重モードおよび 1000Mbps で動作するように設定し、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

   #グローバルでポートの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 を全二重モードおよび 1000Mbps で動作するように設定し、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 を全二重モードおよび 1000Mbps で動作するように設定し、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

#グローバルポートのシャットダウンモードを auto に設定します。

[DeviceB] dldp unidirectional-shutdown auto

III. 構成の確認

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 port unidirectional-shutdown mode: None
 Number of the port's neighbors: 1
  Neighbor MAC address: 0023-8956-3600
  Neighbor port index: 1
  Neighbor state: Confirmed
  Neighbor aged time: 11s

Interface GigabitEthernet1/0/2
 DLDP port state: Bidirectional
 DLDP port unidirectional-shutdown mode: None
 Number of the port's neighbors: 1
```

```
  Neighbor MAC address: 0023-8956-3600
  Neighbor port index: 2
  Neighbor state: Confirmed
  Neighbor aged time: 12s
```

出力は両方とも GigabitEthernet 1/0/1 と GigabitEthernet 1/0/2 は双方向です。

DeviceA の現在の端末でログの監視を有効にします。現在の端末に出力できるログのもっとも低いレベルを 6 に設定します。

[DeviceA] quit

<DeviceA> terminal monitor

<DeviceA> terminal logging level 6

DeviceA には、次のログ情報が表示されます。

```
<DeviceA>%Jul 11 17:40:31:089 2012 DeviceA IFNET/3/PHY_UPDOWN: GigabitEthernet1/0/1 link status is DOWN.
%Jul 11 17:40:31:091 2012 DeviceA IFNET/5/LINK_UPDOWN: Line protocol on the interface GigabitEthernet1/0/1 is DOWN.
%Jul 11 17:40:31:677 2012 DeviceA IFNET/3/PHY_UPDOWN: GigabitEthernet1/0/2 link status is DOWN.
%Jul 11 17:40:31:678 2012 DeviceA IFNET/5/LINK_UPDOWN: Line protocol on the interface GigabitEthernet1/0/2 is DOWN.
%Jul 11 17:40:38:544 2012 DeviceA IFNET/3/PHY_UPDOWN: GigabitEthernet1/0/1 link status is UP.
%Jul 11 17:40:38:836 2012 DeviceA IFNET/3/PHY_UPDOWN: GigabitEthernet1/0/2 link status is UP.
```

出力は次のとおりです。

- 両方のポートステータス GigabitEthernet 1/0/1 と GigabitEthernet 1/0/2 がダウンしています。
- 両方のリンクステータス GigabitEthernet 1/0/1 と GigabitEthernet 1/0/2 は常にダウンしています。

#グローバルおよびすべての DLDP 対応ポートの DLDP 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 port unidirectional-shutdown mode: None
 Number of the port's neighbors: 0 (Maximum number ever detected: 1)

Interface GigabitEthernet1/0/2
 DLDP port state: Unidirectional
 DLDP port unidirectional-shutdown mode: None
```

```
Number of the port's neighbors: 0 (Maximum number ever detected: 1)
```

出力は、両方の DLDP ポートステータスが GigabitEthernet 1/0/1 と GigabitEthernet 1/0/2 は片方向です。DLDP は、それらの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 によってシャットダウンされたポートは自動的にリカバリされ、Device A は次のログ情報を表示します。

```
<DeviceA>%Jul 11 17:42:57:709 2012 DeviceA IFNET/3/PHY_UPDOWN: GigabitEthernet1/0/1 link status is DOWN.
%Jul 11 17:42:58:603 2012 DeviceA IFNET/3/PHY_UPDOWN: GigabitEthernet1/0/2 link status is DOWN.
%Jul 11 17:43:02:342 2012 DeviceA IFNET/3/PHY_UPDOWN: GigabitEthernet1/0/1 link status is 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 on the interface GigabitEthernet1/0/1 is UP.
%Jul 11 17:43:02:357 2012 DeviceA IFNET/3/PHY_UPDOWN: GigabitEthernet1/0/2 link status is 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 on the interface GigabitEthernet1/0/2 is UP.
```

出力は、両方のポートステータスとリンクステータスが GigabitEthernet 1/0/1 と GigabitEthernet 1/0/2 がアップし、DLDP ネイバが決定されます。

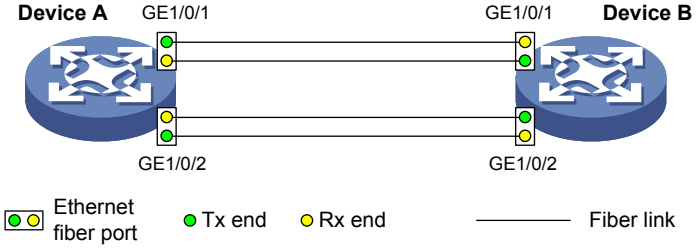
3.10.2. 手動ポートシャットダウンモードの設定例

I. ネットワーク構成

図 3-6 に示すように、Device A および Device B は、2 つのファイバペアを介して接続されています。

単一方向リンクを検出するように DLDP を設定します。 片方向リンクが検出されると、管理者は手動でポートをシャットダウンする必要があります。

図 3-6 ネットワーク図



II. 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 を全二重モードおよび 1000Mbps で動作するように設定し、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 を全二重モードおよび 1000Mbps で動作するように設定し、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

   #グローバルポートのシャットダウンモードを手動に設定します。

   [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 を全二重モードおよび 1000Mbps で動作するように設定し、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 1/0/21 を全二重モードおよび 1000Mbps で動作するように設定し、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

#グローバルポートのシャットダウンモードを手動に設定します。

[DeviceB] dldp unidirectional-shutdown manual

III. 構成の確認

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 port unidirectional-shutdown mode: None
 Number of the port's neighbors: 1
  Neighbor MAC address: 0023-8956-3600
  Neighbor port index: 1
  Neighbor state: Confirmed
  Neighbor aged time: 11s

Interface GigabitEthernet1/0/2
 DLDP port state: Bidirectional
 DLDP port unidirectional-shutdown mode: None
 Number of the port's neighbors: 1
  Neighbor MAC address: 0023-8956-3600
  Neighbor port index: 2
  Neighbor state: Confirmed
  Neighbor aged time: 12s
```

出力は両方とも GigabitEthernet 1/0/1 と GigabitEthernet 1/0/2 は双方向状態で、両方のリンクが双方向であることを意味します。

Device A の現在の端末でログの監視を有効にします。現在の端末に出力できるログのもっとも低いレベルを 6 に設定します。

[DeviceA] quit

<DeviceA> terminal monitor

<DeviceA> terminal logging level 6

Device A には、次のログ情報が表示されます。

```
<DeviceA>%Jul 12 08:29:17:786 2012 DeviceA IFNET/3/PHY_UPDOWN: GigabitEthernet1/0/1 link
status is DOWN.
%Jul 12 08:29:17:787 2012 DeviceA IFNET/5/LINK_UPDOWN: Line protocol on the interface
GigabitEthernet1/0/1 is DOWN.
%Jul 12 08:29:17:800 2012 DeviceA IFNET/3/PHY_UPDOWN: GigabitEthernet1/0/2 link status
is DOWN.
```

```
%Jul 12 08:29:17:800 2012 DeviceA IFNET/5/LINK_UPDOWN: Line protocol on the interface
GigabitEthernet1/0/2 is DOWN.
%Jul 12 08:29:25:004 2012 DeviceA IFNET/3/PHY_UPDOWN: GigabitEthernet1/0/1 link status
is UP.
%Jul 12 08:29:25:005 2012 DeviceA IFNET/5/LINK_UPDOWN: Line protocol on the interface
GigabitEthernet1/0/1 is UP.
%Jul 12 08:29:25:893 2012 DeviceA IFNET/3/PHY_UPDOWN: GigabitEthernet1/0/2 link status
is UP.
%Jul 12 08:29:25:894 2012 DeviceA IFNET/5/LINK_UPDOWN: Line protocol on the interface
GigabitEthernet1/0/2 is UP.
```

出力は、両方のポートステータスとリンクステータスが GigabitEthernet 1/0/1 と GigabitEthernet 1/0/2 がダウンしています。

#グローバルおよびすべての DLDP 対応ポートの DLDP 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 port unidirectional-shutdown mode: None
 Number of the port's neighbors: 0 (Maximum number ever detected: 1)

Interface GigabitEthernet1/0/2
 DLDP port state: Unidirectional
 DLDP port unidirectional-shutdown mode: None
 Number of the port's neighbors: 0 (Maximum number ever detected: 1)
```

出力は、両方の DLDP ポートステータスが GigabitEthernet 1/0/1 と GigabitEthernet 1/0/2 は片方向です。 DLDP は 2 つのポートの片方向リンクを検出しますが、シャットダウンしません。

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

Device A には、次のログ情報が表示されます。

```
[DeviceA-GigabitEthernet1/0/1]%Jul 12 08:34:23:717 2012 DeviceA IFNET/3/PHY_UPDOWN:
GigabitEthernet1/0/1 link status is DOWN.
%Jul 12 08:34:23:718 2012 DeviceA IFNET/5/LINK_UPDOWN: Line protocol on the interface
GigabitEthernet1/0/1 is DOWN.
%Jul 12 08:34:23:778 2012 DeviceA IFNET/3/PHY_UPDOWN: GigabitEthernet1/0/2 link status
is DOWN.
```

```
%Jul 12 08:34:23:779 2012 DeviceA IFNET/5/LINK_UPDOWN: Line protocol on the interface
GigabitEthernet1/0/2 is DOWN.
```

出力は、両方のポートステータスとリンクステータスが GigabitEthernet 1/0/1 と GigabitEthernet 1/0/2 がダウンしました。

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
```

Device A には、次のログ情報が表示されます。

```
[DeviceA-GigabitEthernet1/0/2]%Jul 12 08:46:17:677 2012 DeviceA IFNET/3/PHY_UPDOWN:
GigabitEthernet1/0/2 link status is UP.
%Jul 12 08:46:17:678 2012 DeviceA IFNET/5/LINK_UPDOWN: Line protocol on the interface
GigabitEthernet1/0/2 is 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、ポートステータスとリンクステータスが GigabitEthernet 1/0/2 がアップし、その DLDP ネイバが決定されます。

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

Device A には、次のログ情報が表示されます。

```
[DeviceA-GigabitEthernet1/0/1]%Jul 12 08:48:25:952 2012 DeviceA IFNET/3/PHY_UPDOWN:
GigabitEthernet1/0/1 link status is 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 on the interface
GigabitEthernet1/0/1 is 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、ポートステータスとリンクステータスが GigabitEthernet 1/0/1 がアップし、その DLDP ネイバが決定されます。

目次

このセクションのページは **9-x-x** です。

4 章 RRPP 4-1
4.1. 概要 4-1
4.1.1. RRPP ネットワーク 4-1
4.1.2. RRPPDU 4-4
4.1.3. RRPP タイマ 4-4
4.1.4. RRPP の動作 4-5
4.1.5. RRPP の典型的なネットワーク 4-6
4.2. 制限とガイドライン 4-8
4.3. RRPP の設定作業リスト 4-9
4.4. RRPP の設定要件 4-9
4.5. RRPP ドメインの作成 4-10
4.6. コントロール VLAN の設定 4-10
4.7. プロテクト VLAN の設定 4-11
4.8. RRPP リングの設定 4-11
4.8.1. 設定要件 4-11
4.8.2. RRPP ポートの設定 4-11
4.8.3. RRPP ノードの設定 4-12
4.9. RRPP ドメインの有効化 4-14
4.10. RRPP タイマの設定 4-15
4.11. RRPP リンググループの設定 4-15
4.12. RRPP に関する SNMP notification の有効化 4-16
4.13. RRPP の表示と維持 4-16
4.14. RRPP の設定例 4-17
4.14.1. シングルリングの設定例 4-17
4.14.2. 交差リング（Intersecting リング、マルチリング）の設定例 4-20
4.15. RRPP のトラブルシューティング 4-27
4.15.1. リンクの状態が正常なとき、マスタノードが Hello パケットを受信できない 4-27

4章 RRPP

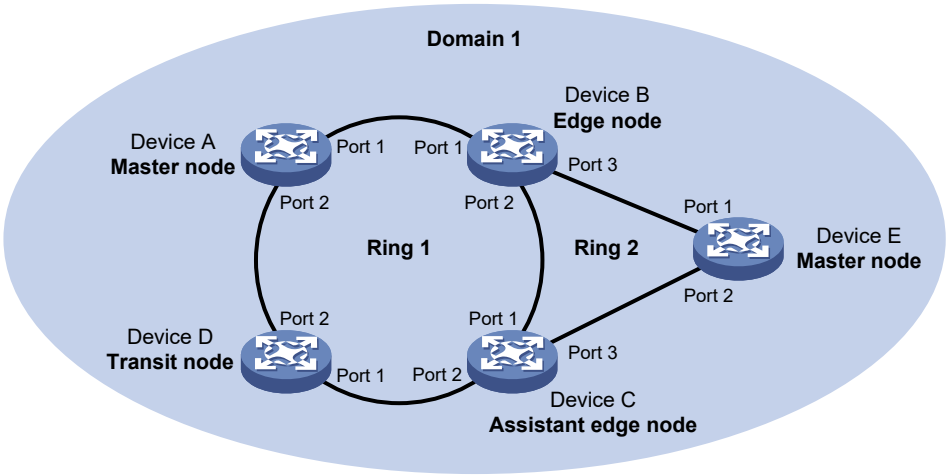
4.1. 概要

RRPP（Rapid Ring Protection Protocol）はイーサネットリング専用のリンクレイヤプロトコルです。RRPP は、イーサネットリングを構成したときのデータループによるブロードキャストストームの発生を効果的に防止することができます。そして、リング上のノード間のリンクが切断されたとき、ノード間の通信パスをすばやく復旧させることができます。RRPP の収束時間はイーサネットリング上のノード数に影響されません。RRPP は大規模ネットワークに適用することができます。

4.1.1. RRPP ネットワーク

図 4-1 に 2 つのイーサネットリングと複数ノードを持つ一般的な RRPP ネットワークを示します。RRPP はノード間で RRPPDU（Rapid Ring Protection Protocol Data Units）を交換することで、リング状態を検出し、トポロジの変更情報を送信します。

図 4-1 RRPP ネットワーク



I. RRPP ドメイン

RRPP ドメインは、ドメイン ID によって一意に識別されます。同じドメイン ID を持った相互接続された装置とコントロール VLAN は RRPP ドメインを構成します。RRPP ドメインは以下の要素で構成されます。

- プライマリリングとサブリング
- コントロール VLAN
- マスタノード、トランジットノード、アシスタントエッジノード
- プライマリポート、セカンダリポート、共通ポート、エッジノード

図 4-1 に示すように、ドメイン 1 は Ring 1、Ring 2 の RRPP リングから構成される RRPP ドメインです。2 つのリング上のすべてのノードは RRPP ドメインに所属しています。

II. RRPP リング

リング型のイーサネットトポロジを RRPP リングと呼びます。RRPP リングにはプライマリリングとサブリングが含まれます。リングレベルを指定することにより、リングをプライマリリングもしくはサブリングのどちらかに設定することができます。レベル 0 がプライマリリング、レベル 1 がサブリングです。複数の RRPP リングにより構成された RRPP ドメインは、1 つのプライマリリングとそれ以外のサブリングにより構成されます。

リングは以下のどちらかの状態になります。

- **Health 状態**－イーサネットリング上のすべての物理リンクが接続されています。
- **Disconnect 状態**－イーサネットリング上のいくつかの物理リンクが接続されていません。

図 4-1 において、Domain1 は 2 つの RRPP リング（Ring 1 と Ring 2）を含みます。Ring 1 のレベルは 0 に設定され、Ring 2 のレベルは 1 に設定されています。Ring 1 はプライマリリングで、Ring 2 はサブリングとなります。

III. コントロール VLAN とプロテクト VLAN

1. コントロール VLAN

   RRPP ドメインにおいて、コントロール VLAN は RRPPDU（Rapid Ring Protection Protocol Data Units）を転送するための専用の VLAN です。装置で RRPP リングにアクセスしているポートはリングのコントロール VLAN に所属します。そのポートのみがコントロール VLAN に加わることができます。

   RRPP ドメインは以下のコントロール VLAN が設定されます。

   - プライマリコントロール VLAN です。これはプライマリリングのためのプライマリコントロール VLAN です。
   - セカンダリコントロール VLAN です。これはサブリングのためのセカンダリコントロール VLAN です。

   プライマリコントロール VLAN として VLAN を指定した後、システムは自動的にセカンダリコントロール VLAN を設定します。VLAN ID はプライマリコントロール VLAN の VLAN-ID に 1 を追加したものとなります。同一の RRPP ドメイン上のすべてのサブリングは同じセカンダリコントロール VLAN を共有します。コントロール VLAN インタフェースで IP アドレスの設定は行うことができません。

2. プロテクト VLAN

   プロテクト VLAN はデータパケットを転送するための VLAN です。RRPP ポートと非 RRPP ポートはプロテクト VLAN に割り当てることができます。

IV. ノードの役割

RRPP リング上の各装置はノードと呼ばれます。ノードの役割を設定することができます。RRPP は以下のノードがあります。

- **マスタノード**－各リングには必ずマスタノードが 1 つあります。マスタノードはポーリングメカニズムを初期化し、トポロジが変更された後の動作を決定します。
- **トランジットノード**－プライマリリングで、マスタノードを除くすべてのノードをトランジットノードとなります。サブリングで、マスタノードを除くすべてのノードと、プライマリリングとサブリングが交差するノードはトランジットノードとなります。トランジットノードは、直接接続された RRPP リンクの状態をモニタし、リンク状態の変更がある場合、変更をマスタノードに通知します。リンク状態の変更にもとづいて、マスタノードは実行される動作を決定します。

- **エッジノード**－プライマリリングとサブリングの両方に同時に所属する特別なノードです。エッジノードは、プライマリリングではマスタノードあるいはトランジットノードとして動作し、サブリングではエッジノードとなります。
- **アシスタントエッジノード**－プライマリリングとサブリングの両方に同時に所属する特別なノードです。エッジノードは、プライマリリングではマスタノードあるいはトランジットノードとして動作し、サブリングではエッジノードとなります。アシスタントエッジノードは、プライマリリングの正常性を検出しループガードを行うため、エッジノードと連携します。

図 4-1 に示すように、Ring 1 はプライマリリング、Ring 2 はサブリングです。Device A は Ring 1 のマスタノード、Device B、Device C、Device D は Ring 1 のトランジットノードです。Device E は Ring 2 のマスタノード、Device B は Ring 2 のエッジノード、Device C は Ring 2 のアシスタントエッジノードです。

V. ポートの役割

1. プライマリポートとセカンダリポート

   マスタノードあるいはトランジットノードはそれぞれ RRPP リングに接続する 2 つのポートを持ちます。1 つはプライマリポート、もう 1 つはセカンダリポートとして動作します。ポートの役割はユーザが設定できます。

   マスタノードにおいて、プライマリポートとセカンダリポートの動作の違いを以下に示します。

   - プライマリポートは Hello パケットを送信し、セカンダリポートは Hello パケットを受信します。
   - RRPP リングが正常（Health 状態）である場合、マスタノードのセカンダリポートは論理的にデータ VLAN のパケットをブロックし、コントロール VLAN のパケットのみ通過を許可します。
   - RRPP リングに障害（Disconnect 状態）が発生した場合、マスタノードのセカンダリポートはデータ VLAN のパケットの受信を許可し、そのパケットを転送します。

   トランジットノードのプライマリポートとセカンダリポートに動作の違いはありません。両方とも RRPP リング上でリングプロトコルパケットとデータパケットを転送するように設計されています。

   図 4-1 に示すように、Device A は Ring 1 のマスタノードです。Port 1 と Port 2 はそれぞれ Ring 1 のマスタノードのプライマリポートとセカンダリポートです。Device B と Device C と Device D は Ring 1 のトランジットノードです。これらの Port 1 と Port 2 はそれぞれ Ring 1 上でプライマリポートとセカンダリポートです。

2. 共有ポートとエッジポート

   共有ポートは、エッジノードとアシスタントエッジノードからプライマリリングに接続されているポートを示します。エッジポートはエッジノードとアシスタントエッジノードからサブリングにのみ接続されているポートです。

   図 4-1 に示すように、Device B と Device C は Ring 1 と Ring 2 上にあります。Device B の Port 1 と Port 2、Device C の Port 1 と Port 2 はプライマリリングに接続されているので、これらのポートは共有ポートとなります。Device B の Port 3 と Device C の Port 3 はサブリングにのみ接続されているので、これらのポートはエッジポートとなります。

VI. RRPP リンググループ

Edge-Hello パケットのトラフィックを減らすため、エッジノードまたはアシスタントエッジノード上でサブリングのグループを設定することができます。これらのサブリングのエッジノードとして装置を設定し、サブリングのアシスタントエッジノードとして別の装置を設定する必要があります。また同じサブリングパケットをプライマリリング（SRPT）にトンネルする

ため、エッジノードのサブリングとアシスタントエッジノードを接続する必要があります。これらのサブリングのエッジノードの Edge-Hello パケットは、同じリンクを通ってアシスタントエッジノードへ転送されます。

エッジノードで設定された RRPP リンググループはエッジノード RRPP リンググループです。アシスタントエッジノードで設定された RRPP リンググループはアシスタントエッジノード RRPP リンググループです。エッジノード RRPP リンググループの中の 1 つのサブリングのみが、Edge-Hello パケットを送信することができます。

4.1.2. RRPPDU

サブリングの RRPPDU はプライマリリングのデータパケットとして転送され、プライマリリングの RRPPDU のみがプライマリリング内に転送することができます。

表 4-1 RRPPDU タイプと機能

タイプ	説明
Hello	マスタノードはHelloパケット（Healthパケットして知られます）を送信し、ネットワークのリングが正常であるかを確認します。
Link-Down	リンクに障害が発生した場合、トランジットノード、エッジノード、アシスタントエッジノードのポートはLink-Downパケットを送信し、リングが解除されたことをマスタノードに通知します。
Common-Flush-FDB	RRPPリングがDisconnect状態になった場合、マスタノードはCommon-Flush-FDBパケットをトランジットノードに対して送信し、MACエントリとARPエントリを更新するように通知します。(FDBはForwarding Databaseを示します)
Complete-Flush-FDB	RRPPリングがHealth状態になった場合、マスタノードはComplete-Flush-FDBパケットを以下のために送信します。 • トランジットノードに対して送信し、MAC エントリと ARP エントリを更新します。 • ポートのブロックを一時的に解除します。
Edge-Hello	エッジノードはEdge-Helloパケットを送信し、エッジノードとアシスタントエッジノード間のSRPTを確認します。
Major-Fault	エッジノードとアシスタントエッジノード間のSRPTが切断された場合、アシスタントエッジノードはMajor-Faultパケットを送信し、障害をエッジノードに通知します。

4.1.3. RRPP タイマ

RRPP はイーサネットリングのリング状態を決定するとき、以下のタイマを使用します。

I. Hello タイマ

マスタノードのプライマリポートから送信する Hello パケットの送信間隔です。

II. Fail タイマ

セカンダリポートがマスタノードからの Hello パケットを受信する最大遅延時間（タイムアウト時間）です。もし Fail タイマが終了する前に、セカンダリポートがローカルのマスタノードによって送信された Hello パケットを受信した場合、リングは Health 状態となります。受信しない場合、リングは Disconnect 状態となります。

RRPP ドメインにおいて、トランジットノードは、受信した Hello パケットを通してマスタノードの Fail タイマの値を学習します。これはリングネットワークのすべてのノードで Fail タイマの設定が一致していることを保証します。

4.1.4. RRPP の動作

I. ポーリングメカニズム

ポーリングメカニズムはリングネットワークの Health 状態を確認するために、RRPP のマスタノードによって使用されます。

マスタノードはプライマリポートから Hello パケットを定期的に送信します。Hello パケットはリング上の各トランジットノードを順番に通過します。

- リングが正常な場合、マスタノードのセカンダリポートは Fail タイマの期限が切れる前に Hello パケットを受信し、マスタノードはセカンダリポートをブロック状態に維持します。
- リングが切断されている場合、マスタノードのセカンダリポートは Fail タイマの期限が切れる前に Hello パケットを受信することができません。これにより、マスタノードはセカンダリポートがデータ VLAN をブロックするのを解除して、Common-Flush-FDB を送信してすべてのトランジットノードに MAC アドレスエントリと ARP エントリの更新を通知します。

II. LinkDown アラームメカニズム

RRPP において、トランジットノード、エッジノード、アシスタントエッジノードは RRPP ドメインに属するいずれかのポートがダウンしたことを検出すると、すぐにマスタノードへ Link-Down パケットを送信します。Link-Down パケットを受信すると、マスタノードは以下のアクションを行います。

- セカンダリポートのデータ VLAN のブロック状態を解除します。
- Common-Flush-FDB パケットを送信し、すべてのトランジットノード、エッジノード、アシスタントエッジノードに MAC アドレスエントリと ARP エントリを更新するように通知します。

各ノードがエントリを更新した後、トラフィックは通常のリンクに転送されます。

III. リングの復旧

RRPP ドメインのトランジットノード、エッジノード、アシスタントエッジノードに所属するポートが再度アップするとき、リングは復旧します。しかしマスタノードは一定時間後にリングの復旧を認識する可能性があります。この間、データ VLAN で一時的にループが発生することがあります。この結果、ブロードキャストストームが発生します。

一時的なループを防ぐために、マスタノード以外のノードはリングに接続するポートが再度アップしたことを検出するとすぐにそのポートをブロックします。コントロール VLAN のパケットの通過のみ許可します。ノードがポートでループが発生しないことを確認したときのみ、ブロック状態のポートのブロックが解除されます。

IV. SRPT 障害時のマルチホームサブリングのブロードキャストストーム抑制メカニズム

図 4-5 に示すように、Ring 1 はプライマリリング、Ring 2 と Ring 3 はサブリングです。エッジノードとアシスタントエッジノード間の 2 つのリンク（SRPT）がダウンした場合、Ring 2 と Ring 3 のマスタノードはそれぞれセカンダリポートのブロック状態を解除します。そしてこれにより Device B と Device C と Device E と Device F の間でループが作られます。この結果、ブロードキャストストームが発生します。

この場合、ループの発生を防ぐためにエッジノードはエッジポートを一時的にブロック状態にします。エッジノードがエッジポートでループが発生しないことを確認したときのみ、ブロック状態のエッジポートのブロックが解除されます。

V. RRPP リンググループ

エッジノード RRPP リンググループでは、最小のドメイン ID とリング ID を持つアクティブなサブリングのみが Edge-Hello パケットを送信することができます。アシスタントエッジノード RRPP リンググループでは、Edge-Hello パケットを受信したいずれかのアクティブなサブリングがそのパケットを他のアクティブなサブリングに転送します。エッジノード RRPP リンググループとアシスタントエッジノード RRPP リンググループが設定されるとき、以下の理由により CPU の負荷が軽減します。

- エッジノードの 1 つのサブリングのみが Edge-Hello パケットを送信します。
- アシスタントエッジノードの 1 つのサブリングのみが Edge-Hello パケットを受信します。

図 4-5 に示すように、Device B は Ring 2 と Ring 3 のエッジノードです。Device C は Ring 2 と Ring 3 のアシスタントエッジノードです。Device B と Device C は Edge-Hello パケットを頻繁に送信または受信します。より多くのサブリングが設定されたり、より多くのドメインによるロードバランシングが行われたりする場合、Device B と Device C は多くの Edge-Hello パケットを送信または受信することになります。

Edge-Hello パケットのトラフィックを削減するため、以下のことを行います。

- エッジノードの Device B 上で Ring 2 と Ring 3 を RRPP リンググループに割り当てます。
- アシスタントエッジノードの Device C 上で Ring 2 と Ring 3 を RRPP リンググループに割り当てます。

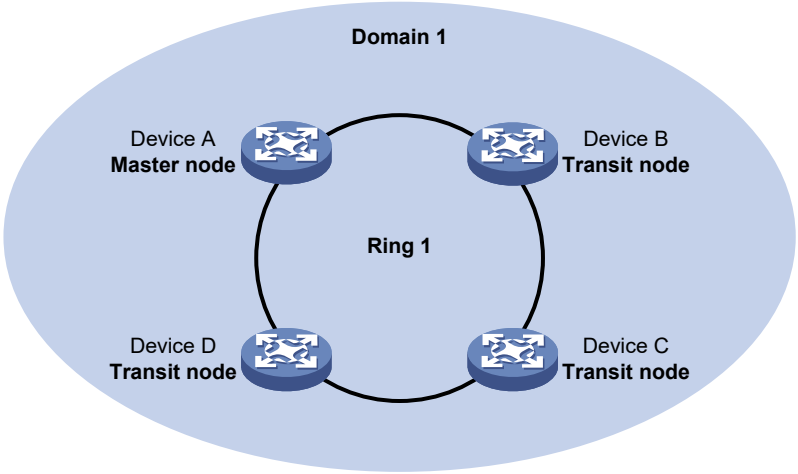
すべてのリングがアクティブな場合、Device B の Ring 2 のみが Edge-Hello パケットを送信します。

4.1.5. RRPP の典型的なネットワーク

I. シングルリング

図 4-2 にシングルリングのネットワークトポロジを示します。RRPP ドメインのみ定義することができます。

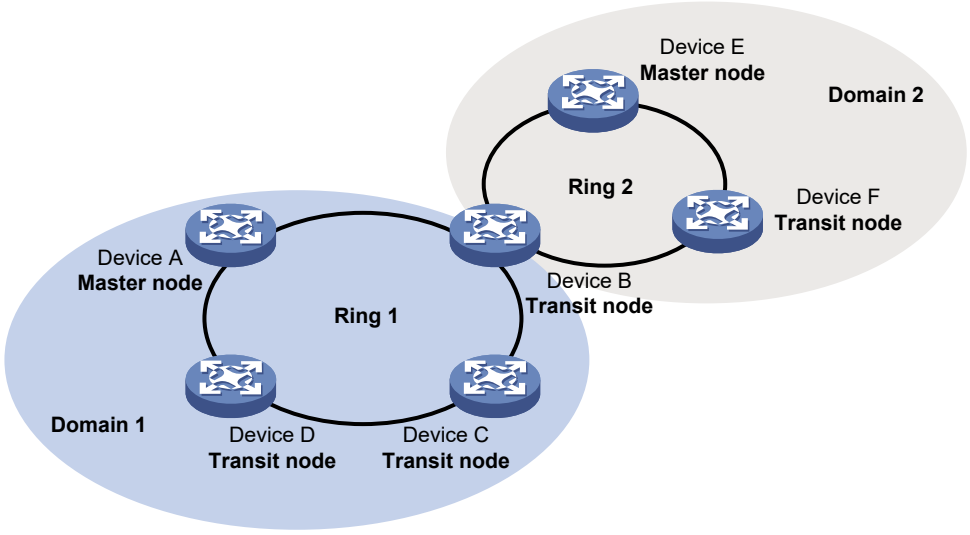
図 4-2 シングルリングのネットワークトポロジ



II. タンジェントリング（接面リング、トランジットリング）

図 4-3 にタンジェントリングのネットワークトポロジを示します。2 つ以上のリングが存在します。リング間に 1 つの共通ノードがあります。各リングに RRPP ドメインを定義する必要があります。

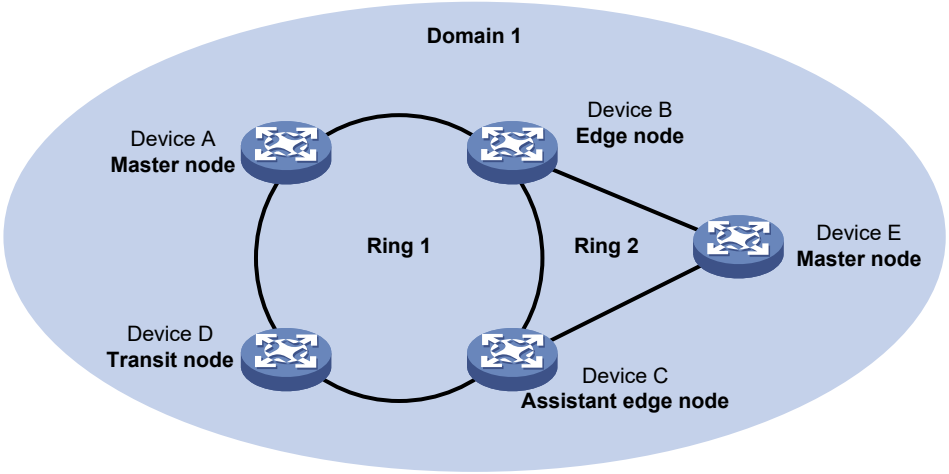
図 4-3 タンジェントリングのネットワークトポロジ



III. 交差リング（Intersecting リング、マルチリング）

図 4-4 に交差リングのネットワークトポロジを示します。2 つ以上のリングが存在します。リング間に 2 つの共通ノードがあります。各リングに RRPP ドメインを定義し、1 つのプライマリリング、それ以外のサブリングを設定する必要があります。

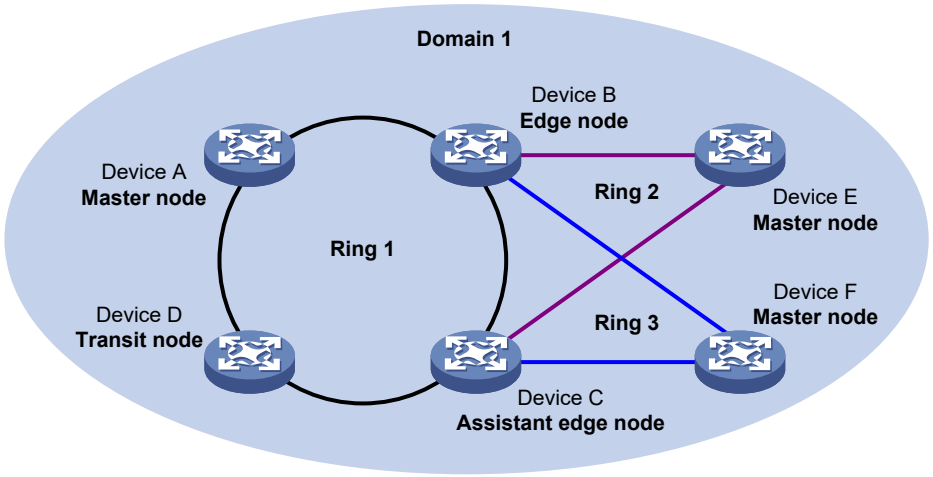
図 4-4 交差リングのネットワークトポロジ



IV. デュアルホームリング

図 4-5 にデュアルホームリングのネットワークトポロジを示します。2 つ以上のリングが存在します。リング間に 2 つの類似した共通ノードがあります。各リングに RRPP ドメインを定義し、1 つのプライマリリング、それ以外のサブリングを設定する必要があります。

図 4-5 デュアルホームリングのネットワークトポロジ



4.2. 制限とガイドライン

- RRPP は自動選択メカニズムがありません。リングネットワークをモニタし、保護するため、RRPP の各ノードを正しく設定してください。
- 以下の順番で RRPP を設定してください。
  - サービスの計画にもとづいて RRPP ドメインを作成してください。
  - 各 RRPP ドメインのコントロール VLAN、データ VLAN を指定してください。
  - 各 RRPP ドメインのトラフィックパスにもとづいてリングの役割、ノードの役割を定義してください。

4.3. RRPPの設定作業リスト

作業		補足
（必須設定項目）RRPPドメインの作成		RRPPドメインのノードとして設定する装置でこのタスクを実行してください。
（必須設定項目）コントロールVLANの設定		RRPPドメインのすべてのノード上でこのタスクを実行してください。
（必須設定項目）プロテクトVLANの設定		RRPPドメインのすべてのノード上でこのタスクを実行してください。
（必須設定項目）RRPP リングの設定	1. RRPP ポートの設定	RRPPリングにアクセスする各ノードのポートでこのタスクを実行してください。
	2. RRPP ノードの設定	RRPPドメインのすべてのノード上でこのタスクを実行してください。
（必須設定項目）RRPPドメインの有効化		RRPPドメインのすべてのノード上でこのタスクを実行してください。
（オプション設定項目）RRPPタイマの設定		RRPPドメインのマスタノード上でこのタスクを実行してください。
（オプション設定項目）RRPPリンググループの設定		RRPPドメインのエッジノード、およびアシスタントエッジノードでこのタスクを実行してください。
（オプション設定項目）RRPPに関するSNMP notification の有効化		—

注意:

RRPP とループ検知機能を併用する場合は、RRPP リングを構成する各ノードのプライマリポートとセカンダリポートでループ保護アクションを設定しないで下さい。プライマリポートとセカンダリポートでループ保護アクションを設定すると、RRPP のノード上のどこかでループが発生したとき、ループ検知の保護アクションにより RRPP の Hello パケットが途切れて、マスタノードのセカンダリポートのブロックが解除されます。それにより、ループ検知の保護アクションが発生したノードのもう一方の RRPP ポートでも保護アクションが動作して自動復旧できなくなります。

4.4. RRPPの設定要件

RRPP を設定する前に、物理的にリング状の Ethernet トポロジを構成してください。

4.5. RRPPドメインの作成

I. RRPP ドメインの作成

RRPP ドメインを作成するとき、RRPP ドメインに固有の RRPP ドメイン ID を指定してください。同じ RRPP ドメイン内のすべての装置は、同じ RRPP ドメイン ID で構成する必要があります。

II. 制限とガイドライン

RRPP ドメインのノードとして設定する装置でこのタスクを実行してください。

III. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	–
2. RRPP ドメインを作成し、RRPP domain view に移行する	**rrpp domain** *domain-id*	–

4.6. コントロールVLANの設定

I. 制限とガイドライン

- RRPP ドメインのすべてのノード上でこのタスクを実行してください。
- RRPP ドメインで RRPP リングを設定する前に RRPP ドメインのすべてのノードに同じコントロール VLAN を設定してください。RRPP ドメインにプライマリコントロール VLAN のみを設定してください。システムは自動でセカンダリコントロール VLAN を設定します。セカンダリコントロール VLAN ID はプライマリコントロール VLAN ID に 1 を追加したものを使用します。コントロール VLAN を正常に設定するため､2 つのコントロール VLAN の ID が連続しており、既存の ID でないことを確認してください。
- コントロール VLAN として RRPP リングにアクセスするポートのデフォルト VLAN を設定しないでください。
- RRPPDU を正常に転送するため、コントロール VLAN で QinQ、VLAN マッピングを有効にしないでください。有効にした場合、RRPPDU を正常に転送することができません。
- RRPP ドメインの RRPP リングを設定した後、ドメインのプライマリコントロール VLAN を削除あるいは修正することはできません。**undo control-vlan** コマンドを使用してプライマリコントロール VLAN を削除のみすることができます。
- RRPP が設定されていない装置で透過的に RRPPDU を転送するため、RRPP リングにアクセスする 2 つのポートのみ、コントロール VLAN からのパケットを許可できるようにしてください。そうでない場合、他の VLAN からのパケットはトランスペアレント転送モードのコントロール VLAN に入り、RRPP リングと衝突する可能性があります。

II. 設定手順

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

操作	コマンド	補足
2. RRPP domain view に移行する	**rrpp domain** *domain-id*	—
3. RRPP ドメインのプライマリコントロール VLAN を設定する	**control-vlan** *vlan-id*	—

4.7. プロテクトVLANの設定

I. 制限とガイドライン

- RRPP ドメインのすべてのノード上でこのタスクを実行してください。
- RRPP ドメインで RRPP リングを設定する前に、最初に RRPP ドメインのすべてのノードに同じプロテクト VLAN を設定してください。 RRPP ポートが割り当てられるすべての VLAN は、RRPP ドメインによって保護されていなければなりません。

II. 設定要件

プロテクト VLAN を設定する前に、MST region と VLAN-インスタンスマッピングを設定してください。MST region の詳細はセクション 3 *アクセス オペレーションマニュアル*の“*STP*”を参照してください。

III. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	–
2. RRPP domain view に移行する	**rrpp domain** *domain-id*	—
3. RRPP ドメインのプロテクト VLAN を設定する	**protected-vlan reference-instance** *instance-id-list*	—

4.8. RRPPリングの設定

RRPP リングを設定する場合、ノードを設定する前に、各ノードを RRPP リングに接続しているポートを設定してください。

4.8.1. 設定要件

RRPP リングを設定する前に、コントロール VLAN とプロテクト VLAN を設定してください。

4.8.2. RRPP ポートの設定

I. 制限とガイドライン

- RRPP リングにアクセスする各ノードのポートでこのタスクを実行してください。

- RRPP ポートで OAM リモートループバック機能を有効にしないでください。一時的なブロードキャストストームを引き起こす恐れがあります。
- トポロジの収束を加速するため、RRPP ポートでリンクダウンの通知を抑制する **link-delay** コマンドを使用してください。**link-delay** コマンドは、物理状態の変更を通知するリンクダウンの抑制の時間を 0 秒に変更します。**link-delay** コマンドの詳細は Chapter 3 *Layer 2 - LAN Switching Command References* の”*Spanning tree commands*”を参照してください。

II. 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 view または Layer 2 aggregation interface view へ移行する	**interface** *interface-type interface-number*	—
3. インタフェースの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 コマンドの詳細はChapter 3 *Layer 2 - LAN Switching Command References*の”*Spanning tree commands*”を参照してください。
4. トランクポートを RRPP ドメインのプロテクト VLAN に割り当てる	**port trunk permit vlan** { *vlan-id-list* | **all** }	デフォルト：VLAN1パケットのみ許可します。 RRPPポートはコントロールVLANからのパケットを許可します。 コマンドの詳細はChapter 3 *Layer 2 - LAN Switching Command References*の”*Spanning tree commands*”を参照してください。
5. スパニングツリーを無効にする	**undo stp enable**	デフォルト：有効 コマンドの詳細はChapter 3 *Layer 2 - LAN Switching Command References*の”*Spanning tree commands*”を参照してください。

4.8.3. RRPP ノードの設定

I. 制限とガイドライン

- RRPP ドメインのすべてのノード上でこのタスクを実行してください。
- 装置が RRPP ドメインで複数の RRPP リングを運ぶ場合、サブリングのエッジノードあるいはアシスタントエッジノードでのみできます。
- エッジノードあるいはアシスタントエッジノードを設定するとき、サブリングを設定する前にプライマリリングを設定してください。

II. マスタノードの指定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. RRPP domain view に移行する	**rrpp domain** *domain-id*	—
3. 装置をマスタノードに設定し、プライマリポート、セカンダリポートを設定する	**ring** *ring-id* **node-mode master** [**primary-port** *interface-type interface-number*] [**secondary-port** *interface-type interface-number*] **level** *level-value*	—

III. トランジットノードの指定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. RRPP domain view に移行する	**rrpp domain** *domain-id*	—
3. 装置をトランジットノードに指定し、プライマリポート、セカンダリポートを指定する	**ring** *ring-id* **node-mode transit** [**primary-port** *interface-type interface-number*] [**secondary-port** *interface-type interface-number*] **level** *level-value*	—

IV. エッジノードの指定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. RRPP domain view に移行する	**rrpp domain** *domain-id*	—
3. 装置をプライマリリングのマスタノードあるいはトランジットノードに指定し、プライマリポート、セカンダリポートを指定する	**ring** *ring-id* **node-mode** { **master** | **transit** } [**primary-port** *interface-type interface-number*] [**secondary-port** *interface-type interface-number*] **level** *level-value*	—
4. 装置をサブリングのエッジノードに指定し、エッジポートを指定する	**ring** *ring-id* **node-mode edge** [**edge-port** *interface-type interface-number*]	—

V. アシスタントエッジノードの指定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. RRPP domain view に移行する	**rrpp domain** *domain-id*	—
3. 装置をプライマリリングのマスタノードあるいはトランジットノードに指定し、プライマリポート、セカンダリポートを指定する	**ring** *ring-id* **node-mode** { **master** | **transit** } [**primary-port** *interface-type interface-number*] [**secondary-port** *interface-type interface-number*] **level** *level-value*	デフォルト：設定なし
4. 装置をサブリングのアシスタントエッジノードに指定し、エッジポートを指定する	**ring** *ring-id* **node-mode assistant-edge** [**edge-port** *interface-type interface-number*]	デフォルト：設定なし

4.9. RRPPドメインの有効化

I. 制限とガイドライン

- RRPP ドメインのすべてのノード上でこのタスクを実行してください。
- 現在の装置で RRPP ドメインを有効にする前、現在の装置の RRPP ドメインの RRPP プロトコルと RRPP リングを有効にしてください。
- 装置でサブリングを有効にする前にプライマリリングを有効にしてください。装置でプライマリリングを無効にする前に、すべてのサブリングを無効にしてください。そうでない場合、システムは画面にエラー表示を行います。
- サブリングの Hello パケットがプライマリリングでループすることを防止するため、最初にマスタノードでプライマリリングを有効にしてください。そして別のマスタノードでサブリングを有効にしてください。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. RRPP を有効にする	**rrpp enable**	デフォルト：無効
3. RRPP domain view に移行する	**rrpp domain** *domain-id*	—
4. 指定した RRPP リングを有効にする	**ring** *ring-id* **enable**	デフォルト：無効

4.10. RRPPタイマの設定

I. 制限とガイドライン

- RRPP ドメインのマスタノード上でこのタスクを実行してください。
- Fail タイマは Hello タイマの 3 倍以上の値である必要があります。
- デュアルホームリングネットワークにおいて、サブリングのマスタノードの Fail タイマとプライマリリングのマスタノードの Fail タイマの差分が、サブリングのマスタノードの Hello タイマの 2 倍以上であることを確認してください。そうでない場合プライマリリングで障害が発生したときに一時的なループが発生します。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. RRPP domain view に移行する	**rrpp domain** *domain-id*	—
3. RRPP ドメインの Hello タイマと Fail タイマを設定する	**timer hello-timer** *hello-value* **fail-timer** *fail-value*	デフォルト： Helloタイマ：1秒 Failタイマ：3秒

4.11. RRPPリンググループの設定

I. RRPP リンググループの設定

Edge-Hello パケットのトラフィックを減らすために、RRPP リンググループに同じエッジノード、アシスタントエッジノードでサブリングを割り当てます。RRPP リンググループは、エッジノードとアシスタントエッジノードの両方で設定する必要があります。RRPP リンクグループは、エッジノードとアシスタントエッジノードにのみ設定することができます。

II. 制限とガイドライン

- RRPP ドメインのエッジノード、およびアシスタントエッジノードでこのタスクを実行してください。
- 1 つの RRPP リンググループにのみサブリングを割り当てることができます。エッジノードで設定された RRPP リンググループと、アシスタントエッジノードで設定された RRPP リンググループが同じサブリングに含まれていることを確認してください。同じサブリングに含まれていない場合、RRPP リンググループは正常に動作することができません。
- RRPP リンググループのサブリングが同じエッジノードとアシスタントエッジノードを共有していること、エッジノードとアシスタントエッジノードが同じ SRPT を持っていることを確認してください。
- 装置が RRPP リンググループのサブリングでエッジノードあるいはアシスタントエッジノードであることを確認してください。
- エッジノード上の RRPP リンググループとアシスタントエッジノード上の RRPP リンググループは、同じ設定で同じ動作状態であることを確認してください。

- RRPP リンググループ内のすべてのサブリングが同じ SRPT を持っていることを確認してください。これらのサブリングの SRPT の設定が異なる場合、RRPP リンググループは正常に動作することができません。

III. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. RRPP domain view に移行する	**rrpp domain** *domain-id*	—
3. 指定したサブリングを RRPP リンググループに割り当てる	**domain** *domain-id* **ring** *ring-id-list*	デフォルト：設定なし

4.12. RRPPに関するSNMP notificationの有効化

I. RRPP に関する SNMP notification の有効化

SNMP notification を有効にすることで、RRPP に関する重要なイベントを NMS に通知します。NMS は設定された出力ルールにしたがって notification を出力する方法を決定します。SNMP notification の詳細はセクション 10 *システム管理 オペレーションマニュアル*の "*SNMP*" を参照してください。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. RRPP に関する SNMP notification の送信を有効にする	**snmp-agent trap enable rrpp** [**major-fault** | **multi-master** | **ring-fail** | **ring-recover**] *	デフォルト：無効

4.13. RRPP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
RRPPの概要情報を表示する	**display rrpp brief**
RRPPグループの設定情報を表示する	**display rrpp ring-group** [*ring-group-id*]
RRPPDUの統計情報を表示する	**display rrpp statistics domain** *domain-id* [**ring** *ring-id*]
RRPPの詳細情報を表示する	**display rrpp verbose domain** *domain-id* [**ring** *ring-id*]
RRPPDUの統計情報を削除する	**reset rrpp statistics domain** *domain-id* [**ring** *ring-id*]

4.14. RRPPの設定例

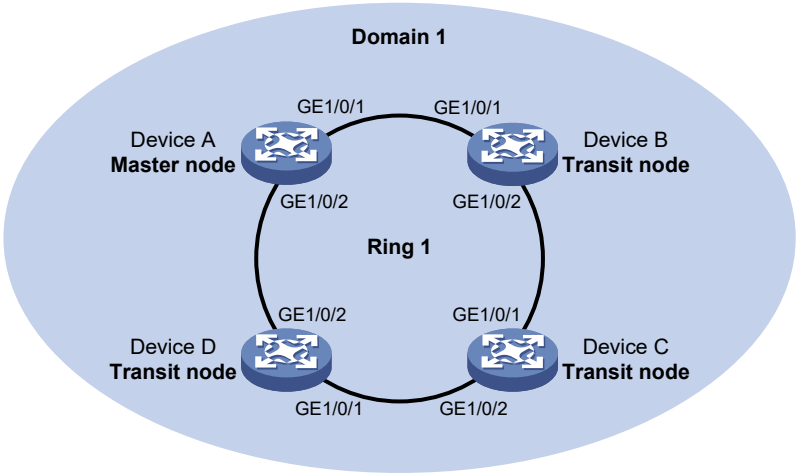
4.14.1. シングルリングの設定例

I. ネットワーク要件

図 4-6 に示すように設定します。

- Device A、Device B、Device C、Device D、Device E は RRPP ドメイン 1 を構成します。VLAN4092 を RRPP ドメイン 1 のプライマリコントロール VLAN に指定します。RRPP ドメイン 1 のプロテクト VLAN に VLAN1～30 を設定します。
- Device A、Device B、Device C、Device D はプライマリリング 1 を構成します。
- Device A をプライマリリング 1 のマスタノードに指定し、GigabitEthernet 1/0/1 をプライマリポート、GigabitEthernet 1/0/2 をセカンダリポートに指定します。
- Device B と Device C と Device D をプライマリリング 1 のトランジットノードに指定します。各装置の GigabitEthernet 1/0/1 をプライマリポート、GigabitEthernet 1/0/2 をセカンダリポートとします。

図 4-6 ネットワーク図



II. 設定手順

1. 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

   # MSTI インスタンス 1 に VLAN をマッピングします。

   [DeviceA] stp region-configuration

   [DeviceA-mst-region] instance 1 vlan 1 to 30

   # MST region の設定を有効にします。

   [DeviceA-mst-region] active region-configuration

   [DeviceA-mst-region] quit

物理状態の変更があった場合、GigabitEthernet 1/0/1 のリンクダウンの通知を抑制する時間を 0 秒に設定します。

[DeviceA] interface gigabitethernet 1/0/1

[DeviceA-GigabitEthernet1/0/1] link-delay 0

ポートでスパニングツリー機能を無効にします。

[DeviceA-GigabitEthernet1/0/1] undo stp enable

ポートをトランクポートに設定します。

[DeviceA-GigabitEthernet1/0/1] port link-type trunk

VLAN 1～VLAN 30 にポートを割り当てます。

[DeviceA-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30

[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] link-delay 0

[DeviceA-GigabitEthernet1/0/2] undo stp enable

[DeviceA-GigabitEthernet1/0/2] port link-type trunk

[DeviceA-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30

[DeviceA-GigabitEthernet1/0/2] quit

RRPP ドメイン 1 を作成します。

[DeviceA] rrpp domain 1

RRPP ドメイン 1 のプライマリコントロール VLAN として VLAN 4092 を設定します。

[DeviceA-rrpp-domain1] control-vlan 4092

RRPP ドメイン 1 のプロテクト VLAN として MSTI 1 にマッピングした VLAN を設定します。

[DeviceA-rrpp-domain1] protected-vlan reference-instance 1

プライマリリング 1 のマスタノードとして Device A を設定します。プライマリポートを GigabitEthernet 1/0/1、セカンダリポートを GigabitEthernet 1/0/2 に設定します。リング 1 を有効にします。

[DeviceA-rrpp-domain1] ring 1 node-mode master primary-port gigabitethernet 1/0/1 secondary-port gigabitethernet 1/0/2 level 0

[DeviceA-rrpp-domain1] ring 1 enable

[DeviceA-rrpp-domain1] quit

RRPP を有効にします。

[DeviceA] rrpp enable

2. 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

MSTI 1 に VLAN をマッピングします。

[DeviceB] stp region-configuration

[DeviceB-mst-region] instance 1 vlan 1 to 30

MST region の設定を有効にします。

[DeviceB-mst-region] active region-configuration

[DeviceB-mst-region] quit

物理状態の変更があった場合、GigabitEthernet 1/0/1 のリンクダウンの通知を抑制する時間を 0 秒に設定します。

[DeviceB] interface gigabitethernet 1/0/1

[DeviceB-GigabitEthernet1/0/1] link-delay 0

ポートでスパニングツリー機能を無効にします。

[DeviceB-GigabitEthernet1/0/1] undo stp enable

[DeviceB-GigabitEthernet1/0/1] port link-type trunk

VLAN 1～VLAN 30 にポートを割り当てます。

[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30

[DeviceB-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。

[DeviceB] interface gigabitethernet 1/0/2

[DeviceB-GigabitEthernet1/0/2] link-delay 0

[DeviceB-GigabitEthernet1/0/2] undo stp enable

[DeviceB-GigabitEthernet1/0/2] port link-type trunk

[DeviceB-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30

[DeviceB-GigabitEthernet1/0/2] quit

RRPP ドメイン 1 を作成します。

[DeviceB] rrpp domain 1

RRPP ドメイン 1 のプライマリコントロール VLAN として VLAN 4092 を設定します。

[DeviceB-rrpp-domain1] control-vlan 4092

RRPP ドメイン 1 のプロテクト VLAN として MSTI 1 にマッピングした VLAN を設定します。

[DeviceB-rrpp-domain1] protected-vlan reference-instance 1

プライマリリング 1 のトランジットノードとして Device B を設定します。プライマリポートを GigabitEthernet 1/0/1、セカンダリポートを GigabitEthernet 1/0/2 に設定します。リング 1 を有効にします。

[DeviceB-rrpp-domain1] ring 1 node-mode transit primary-port gigabitethernet 1/0/1 secondary-port gigabitethernet 1/0/2 level 0

[DeviceB-rrpp-domain1] ring 1 enable

[DeviceB-rrpp-domain1] quit

RRPP を有効にします。

[DeviceB] rrpp enable

3. Device C を設定します。

   # Device B の設定と同様に Device C を設定します。

4. Device D を設定します。

Device B の設定と同様に Device D を設定します。

III. 設定の確認

display コマンドを使用し、各 Device の RRPP 設定と動作情報を表示します。

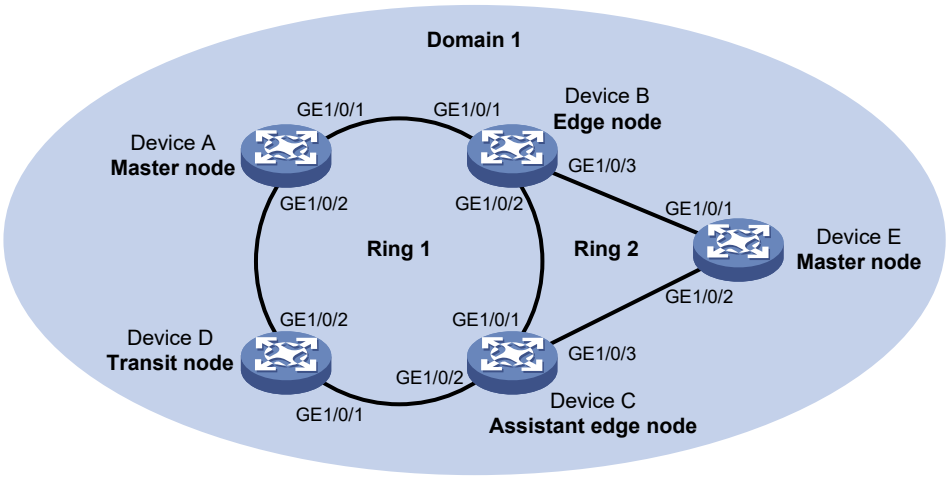
4.14.2. 交差リング（Intersecting リング、マルチリング）の設定例

I. ネットワーク要件

図 4-7 に示すように設定します。

- Device A、Device B、Device C、Device D、Device E は RRPP ドメイン 1 を構成します。VLAN4092 を RRPP ドメイン 1 のプライマリコントロール VLAN に指定します。RRPP ドメイン 1 のプロテクト VLAN に VLAN1～30 を設定します。
- Device A、Device B、Device C、Device D はプライマリリング 1 を構成します。Device B、Device C、Device E はサブリング 2 を構成します。
- Device A をプライマリリング 1 のマスタノードに指定し、GigabitEthernet 1/0/1 をプライマリポート、GigabitEthernet 1/0/2 をセカンダリポートに指定します。
- Device E をサブリング 2 のマスタノードに指定し、GigabitEthernet 1/0/1 をプライマリポート、GigabitEthernet 1/0/2 をセカンダリポートに指定します。
- Device B をプライマリリング 1 のトランジットノード、サブリング 2 のエッジノードに指定し、GigabitEthernet 1/0/3 をエッジポートに指定します。
- Device C をプライマリリング 1 のトランジットノード、サブリング 1 のアシスタントエッジノードに指定し、GigabitEthernet 1/0/3 をエッジポートに指定します。
- Device D をプライマリリング 1 のトランジットノードに指定し、GigabitEthernet 1/0/1 をプライマリポート、GigabitEthernet 1/0/2 をセカンダリポートに指定します。

図 4-7 ネットワーク図



II. 設定手順

1. 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

MSTI インスタンス 1 に VLAN をマッピングします。

[DeviceA] stp region-configuration

[DeviceA-mst-region] instance 1 vlan 1 to 30

MST region の設定を有効にします。

[DeviceA-mst-region] active region-configuration

[DeviceA-mst-region] quit

物理状態の変更があった場合、GigabitEthernet 1/0/1 のリンクダウンの通知を抑制する時間を 0 秒に設定します。

[DeviceA] interface gigabitethernet 1/0/1

[DeviceA-GigabitEthernet1/0/1] link-delay 0

ポートでスパニングツリー機能を無効にします。

[DeviceA-GigabitEthernet1/0/1] undo stp enable

ポートをトランクポートに設定します。

[DeviceA-GigabitEthernet1/0/1] port link-type trunk

VLAN 1～VLAN 30 にポートを割り当てます。

[DeviceA-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30

[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] link-delay 0

[DeviceA-GigabitEthernet1/0/2] undo stp enable

[DeviceA-GigabitEthernet1/0/2] port link-type trunk

[DeviceA-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30

[DeviceA-GigabitEthernet1/0/2] quit

RRPP ドメイン 1 を作成します。

[DeviceA] rrpp domain 1

RRPP ドメイン 1 のプライマリコントロール VLAN として VLAN 4092 を設定します。

[DeviceA-rrpp-domain1] control-vlan 4092

RRPP ドメイン 1 のプロテクト VLAN として MSTI 1 にマッピングした VLAN を設定します。

[DeviceA-rrpp-domain1] protected-vlan reference-instance 1

プライマリリング 1 のマスタノードとして Device A を設定します。プライマリポートを GigabitEthernet 1/0/1、セカンダリポートを GigabitEthernet 1/0/2 に設定します。リング 1 を有効にします。

[DeviceA-rrpp-domain1] ring 1 node-mode master primary-port gigabitethernet 1/0/1 secondary-port gigabitethernet 1/0/2 level 0

[DeviceA-rrpp-domain1] ring 1 enable

[DeviceA-rrpp-domain1] quit

RRPP を有効にします。

[DeviceA] rrpp enable

2. 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

MSTI 1 に VLAN をマッピングします。

[DeviceB] stp region-configuration

[DeviceB-mst-region] instance 1 vlan 1 to 30

MST region の設定を有効にします。

[DeviceB-mst-region] active region-configuration

[DeviceB-mst-region] quit

物理状態の変更があった場合、GigabitEthernet 1/0/1 のリンクダウンの通知を抑制する時間を 0 秒に設定します。

[DeviceB] interface gigabitethernet 1/0/1

[DeviceB-GigabitEthernet1/0/1] link-delay 0

ポートでスパニングツリー機能を無効にします。

[DeviceB-GigabitEthernet1/0/1] undo stp enable

ポートをトランクポートに設定します。

[DeviceB-GigabitEthernet1/0/1] port link-type trunk

VLAN 1～VLAN 30 にポートを割り当てます。

[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30

[DeviceB-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。

[DeviceB] interface gigabitethernet 1/0/2

[DeviceB-GigabitEthernet1/0/2] link-delay 0

[DeviceB-GigabitEthernet1/0/2] undo stp enable

[DeviceB-GigabitEthernet1/0/2] port link-type trunk

[DeviceB-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30

[DeviceB-GigabitEthernet1/0/2] quit

GigabitEthernet 1/0/1 の設定と同様に GigabitEthernet 1/0/3 を設定します。

[DeviceB] interface gigabitethernet 1/0/3

[DeviceB-GigabitEthernet1/0/3] link-delay 0

[DeviceB-GigabitEthernet1/0/3] undo stp enable

[DeviceB-GigabitEthernet1/0/3] port link-type trunk

[DeviceB-GigabitEthernet1/0/3] port trunk permit vlan 1 to 30

[DeviceB-GigabitEthernet1/0/3] quit

RRPP ドメイン 1 を作成します。

[DeviceB] rrpp domain 1

RRPP ドメイン 1 のプライマリコントロール VLAN として VLAN 4092 を設定します。

[DeviceB-rrpp-domain1] control-vlan 4092

RRPP ドメイン 1 のプロテクト VLAN として MSTI 1 にマッピングした VLAN を設定します。

[DeviceB-rrpp-domain1] protected-vlan reference-instance 1

プライマリリング 1 のトランジットノードとして Device B を設定します。プライマリポートを GigabitEthernet 1/0/1、セカンダリポートを GigabitEthernet 1/0/2 に設定します。リング 1 を有効にします。

[DeviceB-rrpp-domain1] ring 1 node-mode transit primary-port gigabitethernet 1/0/1 secondary-port gigabitethernet 1/0/2 level 0

[DeviceB-rrpp-domain1] ring 1 enable

サブリング 2 のエッジノードとして Device B を設定します。エッジポートを GigabitEthernet 1/0/3 に設定します。サブリング 2 を有効にします。

[DeviceB-rrpp-domain1] ring 2 node-mode edge edge-port gigabitethernet 1/0/3

[DeviceB-rrpp-domain1] ring 2 enable

[DeviceB-rrpp-domain1] quit

RRPP を有効にします。

[DeviceB] rrpp enable

3. 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 インスタンス 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 の設定を有効にします。

[DeviceC-mst-region] active region-configuration

[DeviceC-mst-region] quit

物理状態の変更があった場合、GigabitEthernet 1/0/1 のリンクダウンの通知を抑制する時間を 0 秒に設定します。

[DeviceC] interface gigabitethernet 1/0/1

[DeviceC-GigabitEthernet1/0/1] link-delay 0

ポート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

ポートをトランクポートに設定します。

[DeviceC-GigabitEthernet1/0/1] port link-type trunk

VLAN 1～VLAN 30 にポートを割り当てます。

[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] link-delay 0

[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

GigabitEthernet 1/0/1 の設定と同様に GigabitEthernet 1/0/3 を設定します。

[DeviceC] interface gigabitethernet 1/0/3

[DeviceC-GigabitEthernet1/0/3] link-delay 0

[DeviceC-GigabitEthernet1/0/3] undo stp enable

[DeviceC-GigabitEthernet1/0/3] port link-type trunk

[DeviceC-GigabitEthernet1/0/3] port trunk permit vlan 1 to 30

[DeviceC-GigabitEthernet1/0/3] quit

RRPP ドメイン 1 を作成します。

[DeviceC] rrpp domain 1

RRPP ドメイン 1 のプライマリコントロール VLAN として VLAN 4092 を設定します。

[DeviceC-rrpp-domain1] control-vlan 4092

RRPP ドメイン 1 のプロテクト VLAN として MSTI 1 にマッピングした VLAN を設定します。

[DeviceC-rrpp-domain1] protected-vlan reference-instance 1

プライマリリング 1 のトランジットノードとして Device C を設定します。プライマリポートを GigabitEthernet 1/0/1、セカンダリポートを GigabitEthernet 1/0/2 に設定します。リング 1 を有効にします。

[DeviceC-rrpp-domain1] ring 1 node-mode transit primary-port gigabitethernet 1/0/1 secondary-port gigabitethernet 1/0/2 level 0

[DeviceC-rrpp-domain1] ring 1 enable

サブリング 2 のアシスタントエッジノードとして Device C を設定します。エッジポートを GigabitEthernet 1/0/3 に設定します。サブリング 2 を有効にします。

[DeviceC-rrpp-domain1] ring 2 node-mode assistant-edge edge-port gigabitethernet 1/0/3

[DeviceC-rrpp-domain1] ring 2 enable

[DeviceC-rrpp-domain1] quit

RRPP を有効にします。

[DeviceC] rrpp enable

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

MSTI インスタンス 1 に VLAN をマッピングします。

[DeviceD] stp region-configuration

[DeviceD-mst-region] instance 1 vlan 1 to 30

MST region の設定を有効にします。

[DeviceD-mst-region] active region-configuration

[DeviceD-mst-region] quit

物理状態の変更があった場合、GigabitEthernet 1/0/1 のリンクダウンの通知を抑制する時間を 0 秒に設定します。

[DeviceD] interface gigabitethernet 1/0/1

[DeviceD-GigabitEthernet1/0/1] link-delay 0

ポートでスパニングツリー機能を無効にします。

[DeviceD-GigabitEthernet1/0/1] undo stp enable

ポートをトランクポートに設定します。

[DeviceD-GigabitEthernet1/0/1] port link-type trunk

VLAN 1～VLAN 30 にポートを割り当てます。

[DeviceD-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30

[DeviceD-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。

[DeviceD] interface gigabitethernet 1/0/2

[DeviceD-GigabitEthernet1/0/2] link-delay 0

[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

RRPP ドメイン 1 を作成します。

[DeviceD] rrpp domain 1

RRPP ドメイン 1 のプライマリコントロール VLAN として VLAN 4092 を設定します。

[DeviceD-rrpp-domain1] control-vlan 4092

RRPP ドメイン 1 のプロテクト VLAN として MSTI 1 にマッピングした VLAN を設定します。

[DeviceD-rrpp-domain1] protected-vlan reference-instance 1

プライマリリング 1 のトランジットノードとして Device D を設定します。プライマリポートを GigabitEthernet 1/0/1、セカンダリポートを GigabitEthernet 1/0/2 に設定します。リング 1 を有効にします。

[DeviceD-rrpp-domain1] ring 1 node-mode transit primary-port gigabitethernet 1/0/1 secondary-port gigabitethernet 1/0/2 level 0

[DeviceD-rrpp-domain1] ring 1 enable

[DeviceD-rrpp-domain1] quit

Enable RRPP.

[DeviceD] rrpp enable

5. 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

MSTI 1 に VLAN をマッピングします。

[DeviceE] stp region-configuration

[DeviceE-mst-region] instance 1 vlan 1 to 30

MST region の設定を有効にします。

[DeviceE-mst-region] active region-configuration

[DeviceE-mst-region] quit

物理状態の変更があった場合、GigabitEthernet 1/0/1 のリンクダウンの通知を抑制する時間を 0 秒に設定します。

[DeviceE] interface gigabitethernet 1/0/1

[DeviceE-GigabitEthernet1/0/1] link-delay 0

ポートでスパニングツリー機能を無効にします。

[DeviceE-GigabitEthernet1/0/1] undo stp enable

ポートをトランクポートに設定します。

[DeviceE-GigabitEthernet1/0/1] port link-type trunk

VLAN 1～VLAN 30 にポートを割り当てます。

[DeviceE-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30

[DeviceE-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。

[DeviceE] interface gigabitethernet 1/0/2

[DeviceE-GigabitEthernet1/0/2] link-delay 0

[DeviceE-GigabitEthernet1/0/2] undo stp enable

[DeviceE-GigabitEthernet1/0/2] port link-type trunk

[DeviceE-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30

[DeviceE-GigabitEthernet1/0/2] quit

RRPP ドメイン 1 を作成します。

[DeviceE] rrpp domain 1

RRPP ドメイン 1 のプライマリコントロール VLAN として VLAN 4092 を設定します。

[DeviceE-rrpp-domain1] control-vlan 4092

RRPP ドメイン 1 のプロテクト VLAN として MSTI 1 にマッピングした VLAN を設定します。

[DeviceE-rrpp-domain1] protected-vlan reference-instance 1

サブリング 2 のマスタノードとして Device E を設定します。プライマリポートを GigabitEthernet 1/0/1、セカンダリポートを GigabitEthernet 1/0/2 に設定します。サブリング 2 を有効にします。

[DeviceE-rrpp-domain1] ring 2 node-mode master primary-port gigabitethernet 1/0/1 secondary-port gigabitethernet 1/0/2 level 1

[DeviceE-rrpp-domain1] ring 2 enable

[DeviceE-rrpp-domain1] quit

RRPP を有効にします。

[DeviceE] rrpp enable

III. 設定の確認

display コマンドを使用し、各 Device の RRPP 設定と動作情報を表示します。

4.15. RRPPのトラブルシューティング

4.15.1. リンクの状態が正常なとき、マスタノードが Hello パケットを受信できない

I. 症状

リンクの状態が正常なとき、マスタノードが Hello パケットを受信できず、マスタノードがセカンダリポートのブロック状態を解除しました。

II. 分析

問題の原因は以下のものが考えられます。

- RRPP リング内のいくつかのノードで RRPP が有効になっていません。
- RRPP リング内のノードにドメイン ID またはプライマリコントロール VLAN-ID が他のノードと異なっているノードがあります。
- ポートに異常があります。

III. 解決策

問題を解決する場合、以下を行ってください。

1. **display rrpp brief** コマンドで、すべてのノードで RRPP が有効かどうかを確認してください。RRPP が有効になっていないノードがある場合、そのノードで **rrpp enable** コマンドと **ring enable** コマンドを使用して RRPP と RRPP リングを有効にしてください。
2. **display rrpp brief** コマンドで、すべてのノードでドメイン ID とプライマリコントロール VLAN の ID が同じかどうかを確認してください。ドメイン ID またはプライマリコントロール VLAN の ID が異なるノードがある場合、そのノードの設定を他のノードと同じドメイン ID とプライマリコントロール VLAN の ID に変更してください。
3. **display rrpp verbose** コマンドで、各リングの各ポートのリンク状態を確認してください。
4. **debugging rrpp** コマンドで、各ノードで Hello パケットを送受信しているかどうかを確認してください。
5. 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。

5 章 Smart Link 5-1
5.1. 概要 5-1
5.1.1. アプリケーションシナリオ 5-1
5.1.2. 用語の説明 5-2
5.1.3. Smart Link の動作 5-3
5.1.4. Smart Link と Monitor Link のコラボレーション 5-3
5.1.5. Smart Link と Track のコラボレーション 5-4
5.2. 制限とガイドライン 5-4
5.3. Smart Link 設定作業リスト 5-4
5.4. Smart Link 装置の設定: 5-4
5.4.1. 設定要件 5-4
5.4.2. Smart Link グループのプロテクト VLAN の設定 5-5
5.4.3. Smart Link グループのメンバポートの設定 5-6
5.4.4. Smart link グループの Preemption モードの設定 5-7
5.4.5. Flush メッセージの送信の有効化 5-7
5.4.6. Smart と Track のコラボレーションの設定 5-8
5.5. Flush メッセージを受信する関連装置の有効化 5-8
5.6. Smart Link の表示と維持 5-9
5.7. Smart Link の設定例 5-9
5.7.1. 単一 Smart Link グループの設定例 5-9
5.7.2. 複数 Smart Link グループのロードバランスの設定例 5-15
5.7.3. Smart Link と Track のコラボレーション設定例 5-19

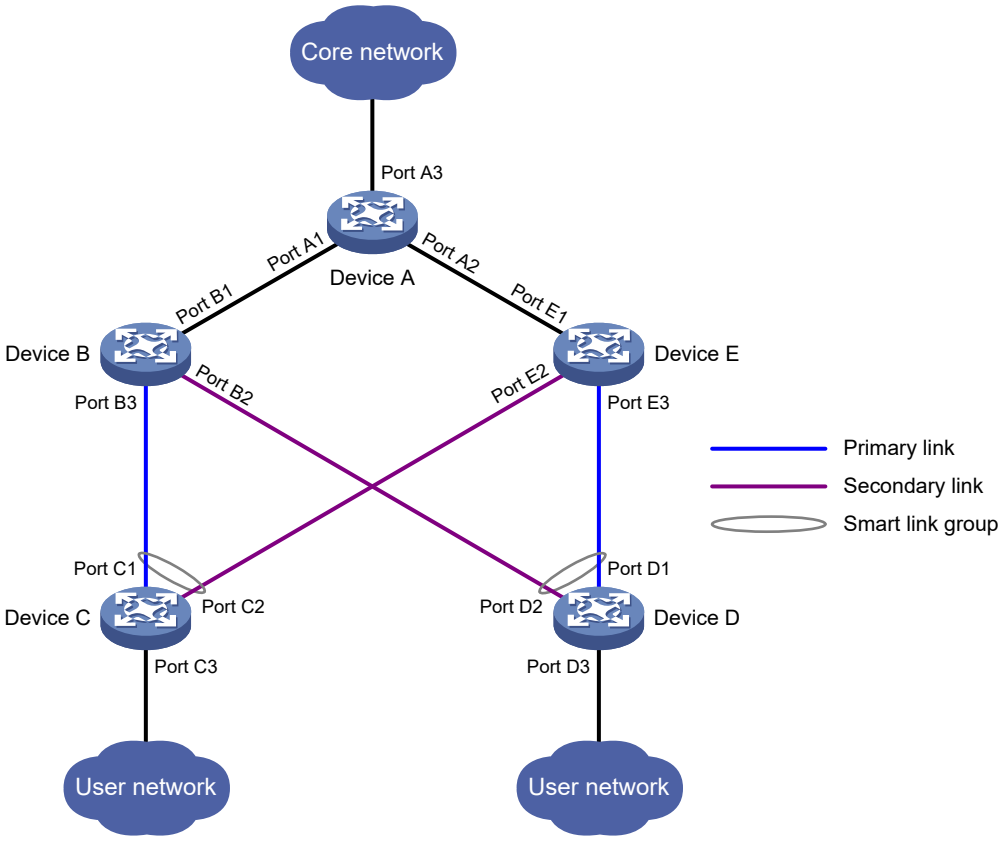
5章 Smart Link

5.1. 概要

5.1.1. アプリケーションシナリオ

単一ポイントの故障を避ける、あるいはネットワークの信頼性を保障するために、図 5-1 に示すようにダウンリンクのデバイスはアップリンクのデバイスにデュアルホームの 2 重で接続する冗長構成のネットワークを築きます。

図 5-1 2 つのアップリンクを持つネットワーク



Smart Link ネットワークは以下の装置があります。

- **Smart Link 装置**–2 つのアップリンクがあります。Smart Link 装置は Smart Link グループの設定と、Flush メッセージを送信する送信制御 VLAN の設定を行う必要があります。図 5-1 の Device C と Device D が Smart Link 装置です。
- **関連装置**–関連装置は Smart Link 装置が接続されているアップリンク装置です。関連装置は Smart Link をサポートし、関連する制御 VLAN から送信された Flush メッセージを受信します。プライマリ/セカンダリのリンクの切り替えが発生したとき、関連装置は受信した Flush メッ

セージに従い、MAC アドレスエントリと ARP エントリをアップデートします。図 5-1 の Device A、Device B、Device E が Smart Link 装置です。

5.1.2. 用語の説明

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 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 5-1 では、Device C の Port C1 と Port C2 が、Smart Link グループを形成し、Device D の Port D1 と Port D2 が、別の Smart Link グループを形成します。Port C1 が active で、Port C2 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 しているときには、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 5-1 では、Device C の Port C1 と Device D の Port D1 を primary ポートとして、Device C の Port D2 と Device D の Port D2 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、Smart link グループでリンクの切り替えが発生したときに、MAC アドレス転送エントリと ARP エントリをリフレッシュするよう他のデバイス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 5-1 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 5-1 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 アドレス転送エントリと ARP エントリをリフレッシュさせます。

5.1.3. Smart Link の動作

I. リンクバックアップ

図 5-1 で示すように、Device C の Port C1 のリンクは primary リンクです。Device C の Port D2 のリンクは secondary リンクです。Port C1 は転送状態で、Port C2 は Standby 状態です。primary リンクで障害が発声した場合、Port C2 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、Port C1 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、すべてのデバイスの MAC アドレス転送エントリと ARP 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 Flush アップデートメカニズムが提供されます。

このメカニズムでは、Smart Link が有効な装置は上流装置へのバックアップリンクを介して Flush メッセージを送信することで情報をアップデートします。このメカニズムは上流装置が MAC アドレス転送エントリと ARP エントリをアップデートするため、Smart Link Flush メッセージを認識する必要があります。

III. Preemption モード

図 5-1 では、Device C の Port C1 のリンクは primary link です。Device C の Port C2 のリンクは secondary link です。primary link で障害が発生すると、Port C1 は自動的にブロッキングされ standby 状態になります。そして、Port C2 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 Preemption モード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 port C1 は、active に切り替わりません。port C2 でリンク障害が発生したときに、port C1 は active に切り替わります。
- Smart Link グループに Preemption モードを設定した場合、port C1 のリンクが復旧するとすぐに active に切り替わります。port C2 は自動的にブロッキングされ standby 状態になります。

IV. ロードバランス

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、ロードバランス（負荷分散）を行います。

ロードバランスを行うために、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、セクション 3 *アクセス オペレーションマニュアル*の "*STP*"を参照してください。

5.1.4. 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ときや障害が復旧したとき、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、ダウンリンクのデバイス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、セクション 9 *高可用性 オペレーションマニュアルの ”Monitor Link"*を参照してください。

5.1.5. Smart Link と Track のコラボレーション

Smart Link は、中間デバイスまたはネットワークパス上で障害（たとえば、単方向リンク、誤接続、およびパケット損失）が発生したときや障害が復旧したとき、リンク状態を検出できません。リンク状態を監視するために Smart Link のポートは、リンク検出プロトコルを使用する必要があります。障害が検出/復旧すると、リンク検出プロトコルは、リンクを切り替えるために Smart Link に通知します。

Smart link は track エントリを使用してリンク検出プロトコルとのコラボレーションを行います。リンク検出は CFD(Connectivity Fault Detection)の CC(Continuity Check)機能のみサポートしています。CFD は検出 VLAN と検出ポートを使用して、故障検出イベントの smart link グループメンバポートに通知します。ポートは、所属する Smart Link グループの制御 VLAN が検出した VLAN に一致するときのみ、連続してチェックに応答します。track エントリ、CFD の CC 機能の詳細は、セクション 9 *高可用性 オペレーションマニュアルの “Track”、“CFD”* を参照してください。

5.2. 制限とガイドライン

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とき、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。

5.3. 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 • (オプション設定項目) Smart Link と track のコラボレーションの設定
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

5.4. Smart Link装置の設定:

5.4.1. 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することができます。
- 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と RRPP を無効にしてください。

5.4.2. Smart Link グループのプロテクト VLAN の設定

I. 設定要件

プロテクト VLAN を設定する前に、MST region、VLAN-インスタンスマッピングの設定を行ってください。MST region の詳細はセクション 3 *アクセス オペレーションマニュアル*の"*STP*"を参照してください。

II. 設定手順

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 グループのプロテクト VLAN を設定する	**protected-vlan reference-instance** *instance-id-list*	—

メモ ：

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。

5.4.3. Smart Link グループのメンバポートの設定

I. 制限とガイドライン

Smart Link グループのメンバポートを smart link group view あるいは 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。

II. smart link group view でのメンバポートの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. 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

III. interface view でのメンバポートの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. Layer 2 Ethernet interface view または aggregate interface view に移行する	**interface** *interface-type interface-number*	—
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

5.4.4. Smart link グループの Preemption モードの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. smart link group view に移行する	**smart-link group** *group-id*	—
3. Preemption モードを有効にする	**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、Preemptionモードを有効にした後にのみ適用されます。

5.4.5. Flush メッセージの送信の有効化

I. 制限とガイドライン

- 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。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. smart link group view に移行する	**smart-link group** *group-id*	—
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 VLAN1は制御VLANです。

5.4.6. Smart と Track のコラボレーションの設定

I. Smart Link と Track のコラボレーションの設定

リンク検出を行うため、Track エントリを通して、CFD の CC 機能と Smart link のコラボレーションを行います。

II. 設定要件

ポートで Smart link と Track 間のコラボレーションの設定を行う前に、ポートを指定した Smart link グループに追加されていることを確認してください。

III. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. 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 Smart Link と CFD の CC 機能とのコラボレーションを設定する	**port smart-link group** *group-id* **track** *track-entry-number*	デフォルト：設定なし。

5.5. Flushメッセージを受信する関連装置の有効化

I. 制限とガイドライン

- 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。

II. 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ときに転送状態にない場合、ポートは flush メッセージを破棄します。

III. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. 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

5.6. 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** }
Flushメッセージの統計情報を削除する	**reset smart-link statistics**

5.7. Smart Linkの設定例

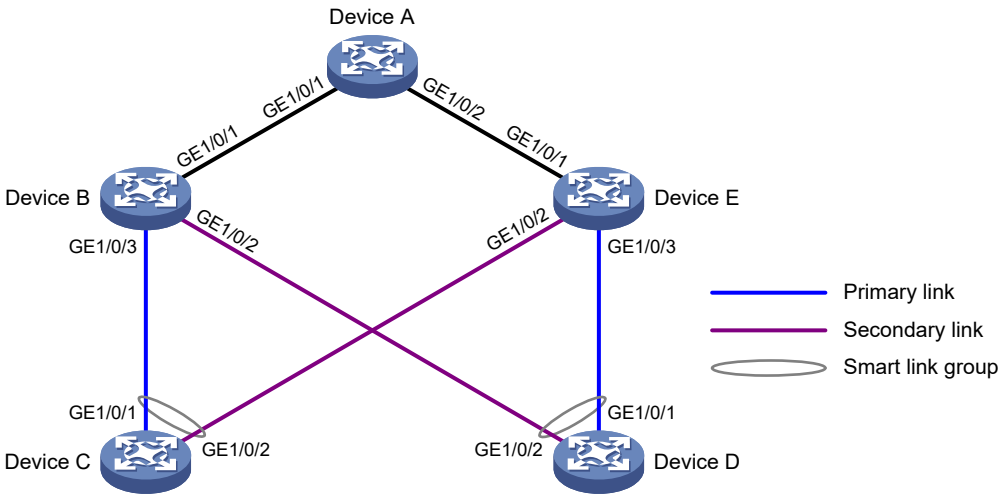
5.7.1. 単一 Smart Link グループの設定例

I. ネットワーク要件

図 5-2 に示すように設定します。

- 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 VLAN1～30 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 5-2 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

VLAN を MSTI1 にマッピングします。

[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

ポート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設定します。

[DeviceC-GigabitEthernet1/0/1] port link-type trunk

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、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 VLAN10 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。

VLAN1～30 を作成します。

<DeviceD> system-view

[DeviceD] vlan 1 to 30

VLAN を MSTI1 にマッピングします。

[DeviceD] stp region-configuration

[DeviceD-mst-region] instance 1 vlan 1 to 30

MST region 設定を動作させます。

[DeviceD-mst-region] active region-configuration

[DeviceD-mst-region] quit

GigabitEthernet 1/0/1 をシャットダウンします。

[DeviceD] interface gigabitethernet 1/0/1

[DeviceD-GigabitEthernet1/0/1] shutdown

ポートでスパニングツリー機能を無効にします。

[DeviceD-GigabitEthernet1/0/1] undo stp enable

トランクポートとして設定します。

[DeviceD-GigabitEthernet1/0/1] port link-type trunk

ポートを VLAN1～30 に割り当てます。

[DeviceD-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30

[DeviceD-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。

[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 VLAN 20 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ます。

[DeviceB] interface gigabitethernet 1/0/1

[DeviceB-GigabitEthernet1/0/1] port link-type trunk

ポートを VLAN 1～VLAN 30 に割り当てます。

[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30

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-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ます。

[DeviceB] interface gigabitethernet 1/0/2

[DeviceB-GigabitEthernet1/0/2] port link-type trunk

ポートを VLAN 1～VLAN 30 に割り当てます。

[DeviceB-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30

ポートでスパニングツリー機能を無効にします。

[DeviceB-GigabitEthernet1/0/2] undo stp enable

flush メッセージの受信を有効にし、VLAN 20 を受信制御 VLAN として設定します。

[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ます。

[DeviceB] interface gigabitethernet 1/0/3

[DeviceB-GigabitEthernet1/0/3] port link-type trunk

ポートを VLAN 1～VLAN 30 に割り当てます。

[DeviceB-GigabitEthernet1/0/3] port trunk permit vlan 1 to 30

ポートでスパニングツリー機能を無効にします。

[DeviceB-GigabitEthernet1/0/3] undo stp enable

flush メッセージの受信を有効にし、VLAN 10 を受信制御 VLAN として設定します。

[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ます。

[DeviceE] interface gigabitethernet 1/0/1

[DeviceE-GigabitEthernet1/0/1] port link-type trunk

ポートを VLAN 1～VLAN 30 に割り当てます。

[DeviceE-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30

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。

[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ます。

[DeviceE] interface gigabitethernet 1/0/2

[DeviceE-GigabitEthernet1/0/2] port link-type trunk

ポートを VLAN 1～VLAN 30 に割り当てます。

[DeviceE-GigabitEthernet1/0/2] port trunk permit vlan 1 to 30

ポートでスパニングツリー機能を無効にします。

[DeviceE-GigabitEthernet1/0/2] undo stp enable

flush メッセージの受信を有効にし、VLAN 10 を受信制御 VLAN として設定します。

[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ます。

[DeviceE] interface gigabitethernet 1/0/3

[DeviceE-GigabitEthernet1/0/3] port link-type trunk

ポートを VLAN 1～VLAN 30 に割り当てます。

[DeviceE-GigabitEthernet1/0/3] port trunk permit vlan 1 to 30

ポートでスパニングツリー機能を無効にします。

[DeviceE-GigabitEthernet1/0/3] undo stp enable

flush メッセージの受信を有効にし、VLAN 20 を受信制御 VLAN として設定します。

[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 をトランクポートとして設定します。

[DeviceA] interface gigabitethernet 1/0/1

[DeviceA-GigabitEthernet1/0/1] port link-type trunk

ポートを VLAN 1～VLAN 30 に割り当てます。

[DeviceA-GigabitEthernet1/0/1] port trunk permit vlan 1 to 30

flush メッセージの受信を有効にし、VLAN10、VLAN 20 を受信制御 VLAN として設定します。

[DeviceA-GigabitEthernet1/0/1] smart-link flush enable control-vlan 10 20

[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 control-vlan 10 20

[DeviceA-GigabitEthernet1/0/2] quit

III. 設定の確認

Device C 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 2012/04/21
  GE1/0/2                 SECONDARY STANDBY  1               16:37:20 2012/04/21
```

Device B が受信した 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 2012/04/21
Device ID of the last flush packet                  : 000f-e23d-5af0
Control VLAN of the last flush packet               : 10
```

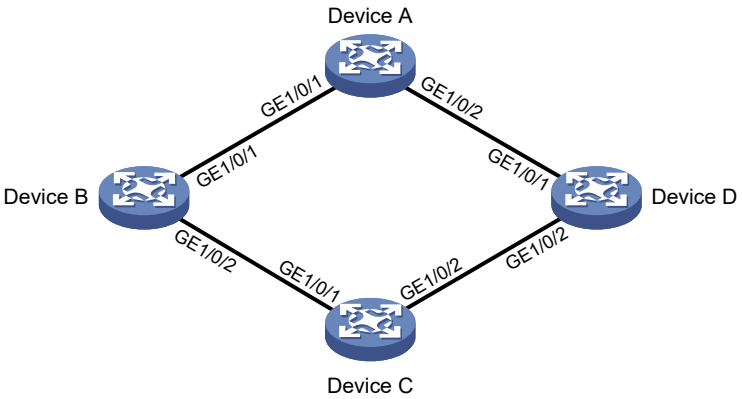
5.7.2. 複数 Smart Link グループのロードバランスの設定例

I. ネットワーク要件

図 5-3 に示すように設定します。

- 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ロードバランスを実装します。VLAN1～100 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 5-3 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。

   <DeviceC> system-view

   [DeviceC] vlan 1 to 200

   # VLAN 1～ 100 を MSTI 1 にマッピングし、VLAN 101～200 を MSTI 2 にマッピングします。

   [DeviceC] stp region-configuration

   [DeviceC-mst-region] instance 1 vlan 1 to 100

   [DeviceC-mst-region] instance 2 vlan 101 to 200

   # MST region 設定をアクティブにします。

   [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
ポート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設定します。
[DeviceC-GigabitEthernet1/0/1] port link-type trunk
ポートを VLAN 1～VLAN 200 に割り当てます。
[DeviceC-GigabitEthernet1/0/1] port trunk permit vlan 1 to 200
[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 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 Preemption モードを有効にし、flush メッセージの送信を有効にし、送信制御 VLAN として VLAN10 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 Preemption モードを有効にし、flush メッセージの送信を有効にし、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ます。

[DeviceB] interface gigabitethernet 1/0/1

[DeviceB-GigabitEthernet1/0/1] port link-type trunk

ポートを VLAN 1～VLAN 200 に割り当てます。

[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 1 to 200

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。

[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ます。

[DeviceB] interface gigabitethernet 1/0/2

[DeviceB-GigabitEthernet1/0/2] port link-type trunk

ポートを VLAN 1～VLAN 200 に割り当てます。

[DeviceB-GigabitEthernet1/0/2] port trunk permit vlan 1 to 200

ポートでスパニングツリー機能を無効にします。

[DeviceB-GigabitEthernet1/0/2] undo stp enable

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。

[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ます。

[DeviceD] interface gigabitethernet 1/0/1

[DeviceD-GigabitEthernet1/0/1] port link-type trunk

ポートを VLAN 1～VLAN 200 に割り当てます。

[DeviceD-GigabitEthernet1/0/1] port trunk permit vlan 1 to 200

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。

[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ます。

[DeviceD] interface gigabitethernet 1/0/2

[DeviceD-GigabitEthernet1/0/2] port link-type trunk

ポートを VLAN 1～VLAN 200 に割り当てます。

[DeviceD-GigabitEthernet1/0/2] port trunk permit vlan 1 to 200

ポートでスパニングツリー機能を無効にします。

[DeviceD-GigabitEthernet1/0/2] undo stp enable

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。

[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 をトランクポートとして設定します。

[DeviceA] interface gigabitethernet 1/0/1

[DeviceA-GigabitEthernet1/0/1] port link-type trunk

ポートを VLAN 1～VLAN 200 に割り当てます。

[DeviceA-GigabitEthernet1/0/1] port trunk permit vlan 1 to 200

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-GigabitEthernet1/0/1] smart-link flush enable control-vlan 10 110

[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 200

[DeviceA-GigabitEthernet1/0/2] smart-link flush enable control-vlan 10 110

[DeviceA-GigabitEthernet1/0/2] quit

III. 設定の確認

Device C で 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 2012/04/21
  GE1/0/2                 SECONDARY STANDBY  1               16:37:20 2012/04/21

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 2012/04/21
  GE1/0/1                 SECONDARY STANDBY  1               16:37:20 2012/04/21
```

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 2012/04/21
 Device ID of the last flush packet                  : 000f-e23d-5af0
 Control VLAN of the last flush packet               : 10
```

5.7.3. Smart Link と Track のコラボレーション設定例

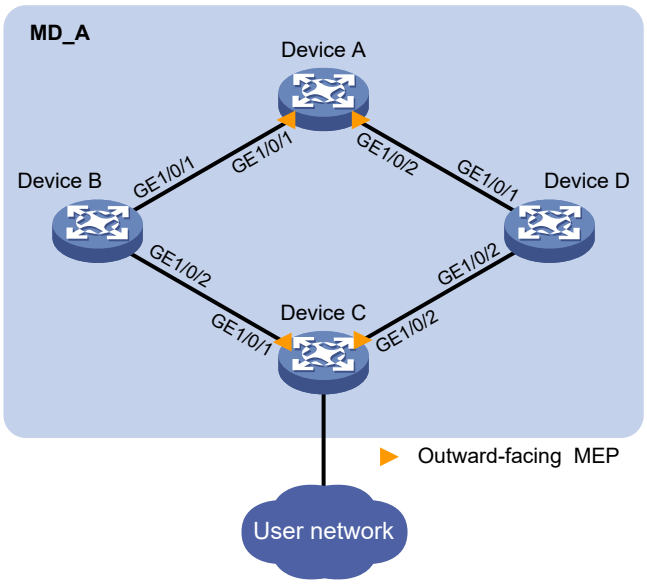
I. ネットワーク要件

図 5-4 に示すように設定します。

- Device A、Device B、Device C、Device D は、レベル 5 のメンテナンスドメイン（MD）**MD_A** を形式しています。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 200 のトラフィックは、Device B および Device D によって、2 重に Device A にアップリンクされています。
- 以下の要件に合うように track エントリを通して Smart Link と CFD の CC 機能間のコラボレーションを設定します。
  - Smart Link のための CFD の CC 機能を設定すると、GigabitEthernet 1/0/1（Smart Link グループ 1 の primary ポート）を介した Device C により、VLAN 1～VLAN 100 のトラフィックが Device A にアップリンクされます。
  - GigabitEthernet 1/0/2（Smart Link グループ 2 の primary ポート）を介した Device C により、VLAN101～200 のトラフィックが Device A にアップリンクされます。
  - Device C と Device A の間のリンクに障害が発生した場合、トラフィックが急激にそれぞれの Smart Link グループの secondary ポートに切り替えられます。障害がクリアされると、primary ポートに戻ります。

CFD の詳細は、セクション 9 *高可用性 オペレーションマニュアル*の"*CFD*"を参照してください。

図 5-4 ネットワーク図



II. 設定手順

1. 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 をトランクポートとして設定します。

   [DeviceA] interface gigabitethernet 1/0/1

   [DeviceA-GigabitEthernet1/0/1] port link-type trunk

   # ポートを VLAN 1～VLAN 200 に割り当てます。

   [DeviceA-GigabitEthernet1/0/1] port trunk permit vlan 1 to 200

   # 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-GigabitEthernet1/0/1] smart-link flush enable control-vlan 10 110

   [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 200

   [DeviceA-GigabitEthernet1/0/2] smart-link flush enable control-vlan 10 110

   [DeviceA-GigabitEthernet1/0/2] quit

   # CFD を有効にし、レベル 5 の **MD_A** を作成します。

   [DeviceA] cfd enable

   [DeviceA] cfd md MD_A level 5

MD_A に MA 名が VLAN ID に対応した MA を作成し、VLAN10 として動作するよう設定します。MD と MA にサービスインスタンス 1 を作成します。

[DeviceA] cfd service-instance 1 ma-id vlan-based md MD_A vlan 10

サービスインスタンス 1 に MEP リストを作成し、出力方向の MEP 1002 を作成し、有効にします。GigabitEthernet 1/0/1 のサービスインスタンス 1 で CCM 送信を有効にします。

[DeviceA] cfd meplist 1001 1002 service-instance 1

[DeviceA] interface gigabitethernet 1/0/1

[DeviceA-GigabitEthernet1/0/1] cfd mep 1002 service-instance 1 outbound

[DeviceA-GigabitEthernet1/0/1] cfd cc service-instance 1 mep 1002 enable

[DeviceA-GigabitEthernet1/0/1] quit

MD_A に MA 名が VLAN ID に対応した MA を作成し、VLAN110 として動作するよう設定します。MD と MA にサービスインスタンス 2 を作成します。

[DeviceA] cfd service-instance 2 ma-id vlan-based md MD_A vlan 110

サービスインスタンス 2 に MEP リストを作成し、出力方向の MEP 1002 を作成し有効にします。GigabitEthernet 1/0/2 のサービスインスタンス 2 で CCM 送信を有効にします。

[DeviceA] cfd meplist 2001 2002 service-instance 2

[DeviceA] interface gigabitethernet 1/0/2

[DeviceA-GigabitEthernet1/0/2] cfd mep 2002 service-instance 2 outbound

[DeviceA-GigabitEthernet1/0/2] cfd cc service-instance 2 mep 2002 enable

[DeviceA-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ます。

[DeviceB] interface gigabitethernet 1/0/1

[DeviceB-GigabitEthernet1/0/1] port link-type trunk

ポートを VLAN 1～VLAN 200 に割り当てます。

[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 1 to 200

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。

[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ます。

[DeviceB] interface gigabitethernet 1/0/2

[DeviceB-GigabitEthernet1/0/2] port link-type trunk

ポートを VLAN 1～VLAN 200 に割り当てます。

[DeviceB-GigabitEthernet1/0/2] port trunk permit vlan 1 to 200

ポートでスパニングツリー機能を無効にします。

[DeviceB-GigabitEthernet1/0/2] undo stp enable

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。

[DeviceB-GigabitEthernet1/0/2] smart-link flush enable control-vlan 10 110

[DeviceB-GigabitEthernet1/0/2] quit

3. Device C を設定します。

VLAN 1～VLAN 200 を作成します。

<DeviceC> system-view

[DeviceC] vlan 1 to 200

VLAN 1～100 を MSTI 1 に、VLAN 101～200 を MSTI 2 にマッピングします。

[DeviceC] stp region-configuration

[DeviceC-mst-region] instance 1 vlan 1 to 100

[DeviceC-mst-region] instance 2 vlan 101 to 200

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

ポート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

ポートをトランクポートとして設定します。

[DeviceC-GigabitEthernet1/0/1] port link-type trunk

ポートを VLAN 1～VLAN 200 に割り当てます。

[DeviceC-GigabitEthernet1/0/1] port trunk permit vlan 1 to 200

[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 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 Preemption モードを有効にし、flush メッセージの送信を有効にし、送信制御 VLAN として VLAN10 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 Preemption モードを有効にし、flush メッセージの送信を有効にし、送信制御 VLAN として VLAN110 を設定します。

[DeviceC-smlk-group2] preemption mode role

[DeviceC-smlk-group2] flush enable control-vlan 110

[DeviceC-smlk-group2] quit

CFD を有効にし、レベル 5 の **MD_A** を作成します。

[DeviceC] cfd enable

[DeviceC] cfd md MD_A level 5

MD_A に MA 名が VLAN ID に対応した MA を作成し、VLAN10 として動作するよう設定します。MD と MA にサービスインスタンス 1 を作成します。

[DeviceC] cfd service-instance 1 ma-id vlan-based md MD_A vlan 10

サービスインスタンス 1 に MEP リストを作成し、出力方向の MEP 1001 を作成し有効にします。GigabitEthernet 1/0/1 のサービスインスタンス 1 で CCM 送信を有効にします。

[DeviceC] cfd meplist 1001 1002 service-instance 1

[DeviceC] interface gigabitethernet 1/0/1

[DeviceC-GigabitEthernet1/0/1] cfd mep 1001 service-instance 1 outbound

[DeviceC-GigabitEthernet1/0/1] cfd cc service-instance 1 mep 1001 enable

[DeviceC-GigabitEthernet1/0/1] quit

MD_A に MA 名が VLAN ID に対応した MA を作成し、VLAN110 として動作するよう設定します。MD と MA にサービスインスタンス 2 を作成します。

[DeviceC] cfd service-instance 2 ma-id vlan-based md MD_A vlan 110

サービスインスタンス 2 に MEP リストを作成し、出力方向の MEP 2001 を作成し有効にします。GigabitEthernet 1/0/2 のサービスインスタンス 2 で CCM 送信を有効にします。

[DeviceC] cfd meplist 2001 2002 service-instance 2

[DeviceC] interface gigabitethernet 1/0/2

[DeviceC-GigabitEthernet1/0/2] cfd mep 2001 service-instance 2 outbound

[DeviceC-GigabitEthernet1/0/2] cfd cc service-instance 2 mep 2001 enable

[DeviceC-GigabitEthernet1/0/2] quit

サービスインスタンス 1 に MEP 1001 の CFD CC 機能に関連した track エントリ 1 を作成します。

[DeviceC] track 1 cfd cc service-instance 1 mep 1001

Smart Link グループ 1 の primary ポート GigabitEthernet 1/0/1 と track エントリ 1 を通した CFD の CC 機能とのコラボレーションを設定し、ポートをアップにします。

[DeviceC] interface gigabitethernet 1/0/1

[DeviceC-GigabitEthernet1/0/1] port smart-link group 1 track 1

[DeviceC-GigabitEthernet1/0/1] undo shutdown

[DeviceC-GigabitEthernet1/0/1] quit

サービスインスタンス 2 に MEP 2001 の CFD CC 機能に関連した track エントリ 2 を作成します。

[DeviceC] track 2 cfd cc service-instance 2 mep 2001

Smart Link グループ 2 の primary ポート GigabitEthernet 1/0/2 と track エントリ 2 を通した CFD の CC 機能とのコラボレーションを設定し、ポートをアップにします。

[DeviceC] interface gigabitethernet 1/0/2

[DeviceC-GigabitEthernet1/0/2] port smart-link group 2 track 2

[DeviceC-GigabitEthernet1/0/2] undo shutdown

[DeviceC-GigabitEthernet1/0/2] quit

4. 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ます。

[DeviceD] interface gigabitethernet 1/0/1

[DeviceD-GigabitEthernet1/0/1] port link-type trunk

ポートを VLAN 1～VLAN 200 に割り当てます。

[DeviceD-GigabitEthernet1/0/1] port trunk permit vlan 1 to 200

flush メッセージの受信を有効にし、VLAN 10 と VLAN110 を受信制御 VLAN として設定します。

[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ます。

[DeviceD] interface gigabitethernet 1/0/2

[DeviceD-GigabitEthernet1/0/2] port link-type trunk

ポートを VLAN 1～VLAN 200 に割り当てます。

[DeviceD-GigabitEthernet1/0/2] port trunk permit vlan 1 to 200

ポートでスパニングツリー機能を無効にします。

[DeviceD-GigabitEthernet1/0/2] undo stp enable

flush メッセージの受信を有効にし、VLAN 10 と VLAN110 を受信制御 VLAN として設定します。

[DeviceD-GigabitEthernet1/0/2] smart-link flush enable control-vlan 10 110

[DeviceD-GigabitEthernet1/0/2] quit

III. 設定の確認

Device A と Device B 間の光ファイバに障害が発生したと仮定します。Device C の Smart Link グループ設定を表示します。

[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   DOWN    5               16:45:20 2012/04/21
  GE1/0/2                 SECONDARY ACTIVE  1               16:37:20 2012/04/21

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 2012/04/21
  GE1/0/1                 SECONDARY STANDBY 1               16:37:20 2012/04/21
```

出力結果は Smart Link グループ 1 の primary ポート GigabitEthernet 1/0/1 がエラーし、secondary ポート GigabitEthernet 1/0/2 が転送ステートで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 **9-x-x** です。

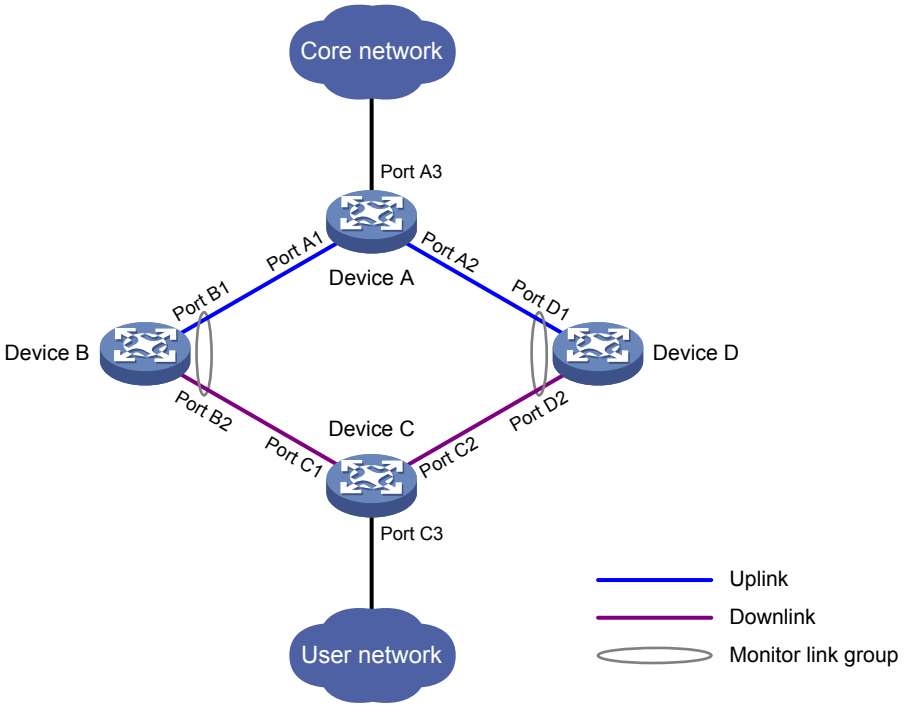
6 章 Monitor Link……6-1
6.1. 概要……6-1
6.2. 制限とガイドライン……6-2
6.3. Monitor Link 設定作業リスト……6-2
6.4. Monitor Link グループの作成……6-2
6.5. Monitor Link グループメンバインタフェースの設定……6-2
6.5.1. 制限とガイドライン……6-2
6.5.2. monitor link group view での Monitor Link グループのメンバインタフェースの設定……6-3
6.5.3. interface view での Monitor Link グループのメンバインタフェースの設定……6-3
6.6. Monitor Link の表示と維持……6-3
6.7. Monitor Link の設定例……6-3

6章 Monitor Link

6.1. 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とき、下流のデバイスが別のリンクに接続を変更します。

図 6-1 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。
- 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。

図 6-1 に示すように、

- Device B の Port B1 と Port B2 が Monitor Link グループとなります。Port B1 はアップリンクインタフェースです。Port B2 はダウンリンクインタフェースです。
- Device D の Port D1 と Port D2 が別の Monitor Link グループとなります。Port D1 はアップリンクインタフェースです。Port D2 は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 グループがアップリンクインタフェースを含んでいない、あるいはすべてのアップリンクインタフェースがダウンしているとき、Monitor Link グループはダウンとなります。このとき、すべてのアップリンクインタフェースを強制的に同時にダウンさせます。アップリンクインタフェースが UP

になると、Monitor Link グループは UP になり、すべてのダウンリンクインタフェースを UP にさせます。

6.2. 制限とガイドライン

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。

6.3. Monitor Link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

6.4. 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**	—
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*	—

6.5. Monitor Linkグループメンバインタフェースの設定

6.5.1. 制限とガイドライン

- 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。
- ダウンリンクインタフェースで予期せずダウン/アップ状態が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 グループのダウンリンクインタフェースとしてアグリゲーショングループの Selected ポートを設定した場合、Monitor Link グループのアップリンクインタフェースとしてアグリゲーショングループの Unselected ポートを設定しないでください。
- 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。
- 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。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。

6.5.2. monitor link group view での Monitor Link グループのメンバインタフェースの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. monitor link group view に移行する	**monitor-link group** *group-id*	—
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

6.5.3. interface view での Monitor Link グループのメンバインタフェースの設定

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. 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

6.6. 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** }

6.7. Monitor Linkの設定例

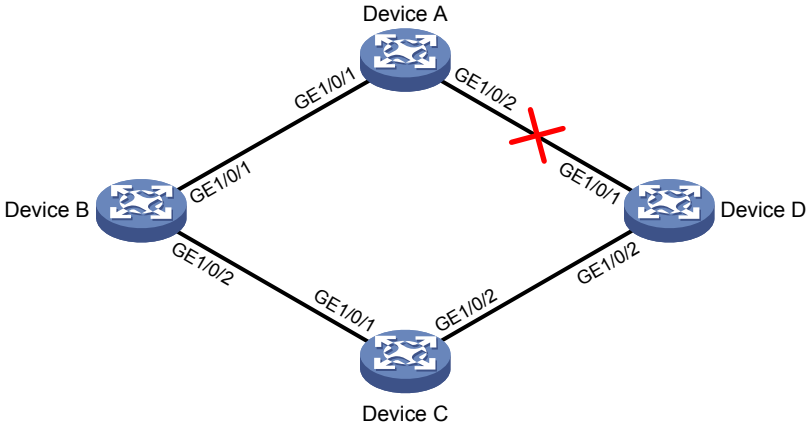
I. ネットワーク要件

図 6-2 に示すように設定します。

- 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 はリンク障害を検出し、Smart Link グループ内でリンクの切り替えを行います。

Smart Link の詳細はセクション 9 *高可用性 オペレーションマニュアル*の"*Smart Link*"を参照してください。

図 6-2 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

トランクポートとして 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 がダウンしたとき、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 2012/4/21
  Last-down-time    : 16:37:20 2012/4/21
  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 2012/4/21
  Last-down-time   : 16:38:26 2012/4/21
  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 **9-x-x** です。

7 章 BFD 7-1
7.1. 概要 7-1
7.1.1. BFD セッションの確立と終了 7-1
7.1.2. シングル Hop 検出とマルチ Hop 検出 7-1
7.1.3. BFD セッションモードと動作モード 7-1
7.1.4. サポート機能 7-2
7.1.5. プロトコルと標準 7-3
7.2. 制限とガイドライン 7-3
7.3. エコーパケットモードの設定 7-3
7.4. コントロールパケットモードの設定 7-4
7.4.1. 制限とガイドライン 7-4
7.4.2. シングル Hop 検出のコントロールパケットモードの設定 7-4
7.4.3. マルチ Hop 検出のコントロールパケットモードの設定 7-5
7.5. BFD の SNMP 通知の有効化 7-6
7.6. BFD の表示と維持 7-6

7章 BFD

7.1. 概要

双方向フォワーディング検出（BFD）は、汎用性を有し、標準的で、中規模ネットワークに向き、プロトコルに依存しない高速な障害検出メカニズムを提供します。BFD では、通信障害検出するため、IP での接続状態を監視・検出することができます。これにより、素早く障害対策を実施でき、ネットワークの可用性を高め、サービスの継続性を確保することができます。

BFD は、ルーティングプロトコルとして位置づけられる上位層プロトコルのための 2 つのデバイス間の双方向の転送パスの障害を均一かつ迅速に検出することができます。BFD は、ミリ秒単位での検出結果の提供ができますが、上位層プロトコルによって使用される hello メカニズムは、リンク障害を検出するのに数秒を必要とします。

7.1.1. BFD セッションの確立と終了

BFD はネイバ発見メカニズムを提供しません。BFD を提供するプロトコル群は、セッションを確立する必要のあるルータの BFD に通知します。ネイバとの確立を行った後、上位プロトコルは、宛先アドレス、送信元アドレスが含まれるネイバ情報を BFD に通知します。BFD は BFD セッションを確立するため、ネイバ情報を使用します。

BFD がリンク障害を検出したとき、以下の処理を行います。

1. BFD はネイバセッションをクリアし、障害が発生しているプロトコルに通知します。
2. プロトコルはリンクの隣接関係を終了します。
3. バックアップリンクが有効である場合、プロトコルは通信を行うためバックアップリンクを使用します。

7.1.2. シングル Hop 検出とマルチ Hop 検出

BFD はシングル Hop 検出とマルチ Hop 検出の双方を使用することができます。

- **シングル Hop 検出**－2 つの直接に接続されたシステムの間の IP 接続性を検出します。
- **マルチ Hop 検出**－2 つのシステムの間のどのようなパスでも検出します。 これらのパスは複数の Hop を持ち、重複する可能性があります。

7.1.3. BFD セッションモードと動作モード

BFD セッションはエコーパケットとコントロールパケットを使用します。

I. エコーパケットモード

エコーパケットはポート番号 3785 で UDP パケットにカプセル化されています。

リンクのローカルエンドが BFD セッションを確立して、リンクの状態を監視するためのエコーパケットを送信します。ピアエンドは BFD セッションを確立せず、パケットを発信側に戻すために転送

するのみ行います。ローカルエンドが検出時間以内にピアからエコーパケットを受信しない場合、セッションがダウンしたと認識します。

エコーモードでは、BFD はシングル Hop 検出のみをサポートし、BFD セッションは動作モードとは無関係となります。

Ⅱ. コントロールパケットモード

コントロールパケットはシングル Hop 検出用にポート番号 3784 で UDP パケットにカプセル化されています。マルチ Hop 検出用にポート番号 4784 で UDP パケットにカプセル化されています。

リンクの両端がリンク状態を監視するために BFD コントロールパケットを交換します。

BFD セッションが確立される前に、BFD には 2 つの動作モード（Active、Passive）があります。

- **Active モード**ーピアから BFD コントロールパケットを受信したかどうかに関係なく、BFD コントロールパケットを自発的に送信します。
- **Passive モード**ーピアから BFD コントロールパケットを受信するまで BFD コントロールパケットを送信しません。

少なくとも 1 つの装置は BFD セッションを確立するために Active モードで動作する必要があります。

BFD セッションが確立された後、両端で BFD の動作モードのいずれかを動作させる必要があります。

- **Asynchronous モード**ー装置が互いに定期的に BFD コントロールパケットを送信します。BFD は指定した時間内に BFD コントロールパケットを受信しない場合、セッションがダウンしたとみなします。
- **Demand モード**–装置は定期的に BFD コントロールパケットを送信します。片端が Asynchronous モードである場合（デフォルト）、片端は BFD コントロールパケットの送信を停止します。片端が Demand モードである場合、両端は BFD コントロールパケットの送信を停止します。別のシステムに接続していることを明示する必要がある場合、システムはネゴシエートした送信間隔で Poll(P)ビットがセットされた BFD コントロールパケットを送信します。検出時間内に応答がない場合、セッションがダウンしたとみなします。接続していると認識した場合、次のコマンドが送信されるまで BFD コントロールパケットを送信しません。

7.1.4. サポート機能

機能	参照
スタティックルーティング	セクション5 *ルーティングプロトコル オペレーションマニュアル*を参照してください。
IPv6スタティックルーティング	セクション5 *ルーティングプロトコル オペレーションマニュアル*を参照してください。
Track	セクション9 *高可用性 オペレーションマニュアル*の"*Track*"を参照してください。
リンクアグリゲーション	セクション10 *高可用性 オペレーションマニュアル*の"*Track*"を参照してください。

7.1.5. プロトコルと標準

- RFC 5880, *Bidirectional Forwarding Detection (BFD)*
- RFC 5881, *Bidirectional Forwarding Detection (BFD) for IPv4 and IPv6 (Single Hop)*
- RFC 5882, *Generic Application of Bidirectional Forwarding Detection (BFD)*
- RFC 5883, *Bidirectional Forwarding Detection (BFD) for Multihop Paths*
- RFC 7130, *Bidirectional Forwarding Detection (BFD) on Link Aggregation Group (LAG) Interfaces*

7.2. 制限とガイドライン

- デフォルトで装置は BFD Version 1 で動作します。BFD Version 0 と互換性があります。コマンドで BFD の Version を 0 に変更することはできません。ピアの装置が BFD Version 0 で動作しているとき、ローカル装置は自動で BFD Version 0 に切り替わります。
- BFD セッションが確立した後、両端で BFD 関連の以下のようなパラメータを取り決めます。最小受信間隔、セッションモード、パケット認証です。両端は現在のセッションに影響を及ぼすことなく、取り決めたパラメータを使用します。
- 異なる IRF メンバ装置のアグリゲートインタフェースのメンバポートでは、BFD セッションの切り替わりが頻繁に発生する可能性があります。ます BFD パケットを送受信するマスタ装置が取り外されたあるいは、再起動したとき、メンバ装置がすぐさま切り替わらない可能性があります。たとえば、メンバ装置が短い検出時間あるいは BFD セッションが多い場合、メンバ装置が切り替わりません。

7.3. エコーパケットモードの設定

I. 設定手順

操作		コマンド	補足
1. system view に移行する		**system-view**	—
2. エコーパケットの送信元 IP アドレスを設定する		**bfd echo-source-ip** *ip-address*	デフォルト：設定なし 送信元IPアドレスは、ローカルインターフェースのIPアドレスと同一のネットワークにすることができません。 そうでないと、大量のICMPリダイレクトパケットが、ピアから送信され、ネットワークの輻輳が生じる可能性があります。
3. (オプション設	1. interface view に移行する	**interface** *interface-type interface-number*	—

操作		コマンド	補足
定項目）エコーパケットモードのパラメータを設定する	2. エコーパケットの最小受信間隔を設定する	**bfd min-echo-receive-interval** *value*	デフォルト：400ミリ秒
	3. シングル Hop 検出時間の乗数を設定する	**bfd detect-multiplier** *value*	デフォルト：5

7.4. コントロールパケットモードの設定

7.4.1. 制限とガイドライン

上位レイヤプロトコルが BFD をサポートするように設定した後、装置は自動でコントロールパケットモードの BFD セッションを作成します。以下の処理を行う必要はありません。

BFD Version0 は以下のコマンドをサポートしていません。

- **bfd session init-mode**
- **bfd authentication-mode**
- **bfd demand enable**
- **bfd echo enable**

7.4.2. シングル Hop 検出のコントロールパケットモードの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. BFD セッションを確立するモードを指定する	**bfd session init-mode** { **active** | **passive** }	デフォルト：active BFD MADのセッションを確立する場合、activeモードにする必要があります。
3. interface view に移行する	**interface** *interface-type interface-number*	—
4. （オプション設定項目）シングル Hop コントロールパケットの認証モードを設定する	**bfd authentication-mode** { **md5** | **sha1** | **simple** } *key-id* { **cipher** *cipher-string* | **plain** *plain-string* }	デフォルト：認証なし
5. Demand モードを有効にする	**bfd demand enable**	デフォルト：Asynchronous モード

操作	コマンド	補足
6. （オプション設定項目）エコーパケットモードを有効にする	**bfd echo enable**	デフォルト：無効 コントロールパケットが送信され、セッションがUPになる間に、エコーパケットモードを有効にした場合、リンク接続を検出し、コントロールパケットの受信レートを減らすため、定期的にエコーパケットを送信します。
7. シングル Hop コントロールパケットを転送する最小間隔を設定する	**bfd min-transmit-interval** *value*	デフォルト：400ミリ秒
8. シングル Hop コントロールパケットを受信する最小間隔を設定する	**bfd min-receive-interval** *value*	デフォルト：400ミリ秒
9. シングル Hop 検出時間の乗数を設定する	**bfd detect-multiplier** *value*	デフォルト：5

7.4.3. マルチ Hop 検出のコントロールパケットモードの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. BFD セッションを確立するモードを指定する	**bfd session init-mode** { **active** | **passive** }	デフォルト：active
3. シングル Hop コントロールパケットの認証モードを設定する	**bfd multi-hop authentication-mode** { **md5** | **sha1** | **simple** } *key-id* { **cipher** *cipher-string* | **plain** *plain-string* }	デフォルト：認証なし
4. マルチ Hop BFD コントロールパケットの宛先ポート番号を設定する	**bfd multi-hop destination-port** *port-number*	デフォルト： 4784
5. マルチ Hop 検出時間の乗数を設定する	**bfd multi-hop detect-multiplier** *value*	デフォルト： 5
6. マルチ Hop コントロールパケットを受信する最小間隔を設定する	**bfd multi-hop min-receive-interval** *value*	デフォルト：400ミリ秒
7. マルチ Hop コントロールパケットを送信する最小間隔を設定する	**bfd multi-hop min-transmit-interval** *value*	デフォルト：400ミリ秒

7.5. BFDのSNMP通知の有効化

I. BFD の SNMP 通知

BFD の SNMP 通知を有効にした場合、装置は NMS に重要なイベントを通知します。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 通知の詳細は、セクション 10 *システム管理 オペレーションマニュアル*の"*SNMP*"を参照してください。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. BFD の SNMP 通知を有効にする	**snmp-agent trap enable bfd**	デフォルト：有効

7.6. BFD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
BFDセッション情報を表示する	**display bfd session** [**discriminator** *value* | **verbose**]
BFDセッション統計情報を削除する	**reset bfd session statistics**

目次

このセクションのページは **9-x-x** です。

8 章 Track 8-1
8.1. 概要 8-1
8.1.1. コラボレーションメカニズム 8-1
8.1.2. サポート検出モジュール 8-2
8.1.3. サポートアプリケーションモジュール 8-2
8.2. 制限とガイドライン 8-2
8.3. コラボレーションアプリケーション例 8-2
8.4. Track 設定作業リスト 8-3
8.5. Track モジュールと検出モジュールの関連づけ 8-3
8.5.1. Track と NQA の関連づけ 8-3
8.5.2. Track と BFD の関連づけ 8-4
8.5.3. Track とインタフェース管理モジュールの関連づけ 8-5
8.6. 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 8-5
8.6.1. 設定要件 8-6
8.6.2. Track とスタティックルーティングの関連づけ 8-6
8.6.3. Track と Smart link の関連づけ 8-7
8.7. Track の表示と維持 8-8
8.8. Track 設定例 8-8
8.8.1. スタティックルーティング-Track-NQA コラボレーション設定例 8-8
8.8.2. スタティックルーティング-Track-BFD コラボレーション設定例 8-13

8章 Track

8.1. 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。

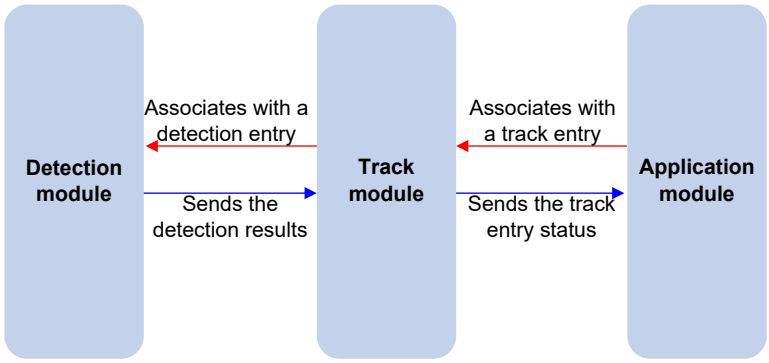
8.1.1. コラボレーションメカニズム

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 8-1 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とき、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 8-1 Track モジュールを介したコラボレーション



I. 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。結果に依存して、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。

II. 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。

8.1.2. 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
- BFD
- インタフェース管理モジュール

8.1.3. 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。

- スタティックルーティング
- Smart Link

8.2. 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とき、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とき、通信が失敗することを防ぎます。たとえば、VRRP グループでマスタは Track モジュールを通してアップリンクインタフェースを監視します。Track モジュールはマスタに優先度を下げるように通知します。高い優先度を持つバックアップがマスタとなります。故障したアップリンクインタフェースが回復したとき、Track モジュールは元のマスタに優先度を戻し、トラフィックを転送するように通知します。もしアップリンクが回復していない場合、転送は失敗します。

8.3. コラボレーションアプリケーション例

以下に NQA、Track、スタティック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 のスタティックルートを設定します。ネクストホップが到達可能なとき、スタティックルートは有効です。もしネクストホップが到達不可能となったとき、スタティックルートは無効となります。このため、NQA、Track、スタティック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 が到達可能であるとき、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とき、Track エントリは Negative 状態となります。

3. スタティックルートに Track エントリを関連づけます。
   - Track エントリが Positive 状態になったとき、スタティックルートが有効となります。
   - Track エントリが Negative 状態になったとき、スタティックルートが無効となります。

8.4. 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 BFD の関連づけ • Track とインタフェース管理モジュールの関連づけ
(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 とスタティックルーティングの関連づけ • Track と Smart Link の関連づけ

8.5. Trackモジュールと検出モジュールの関連づけ

8.5.1. 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、セクション 10 *システム管理 オペレーションマニュアル*の"*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**	—
2. Track エントリを生成し、NQA リアクションエントリと関連づけを行う	**track** *track-entry-number* **nqa entry** *admin-name operation-tag* **reaction** *item-number*	—

8.5.2. Track と BFD の関連づけ

I. Track と BFD の関連づけ

Track エントリはエコーモード BFD と関連づけることができます。Track エントリはエコーモード BFD セッションのみと関連づけることができます。BFD の詳細はセクション 9 *高可用性 オペレーションマニュアル*の"*BFD*"を参照してください。

Track エントリが BFD に関連づけられているとき、以下のように動作します。

- BFD がリンク故障を検出したとき、リンク故障を Track エントリに通知します。Track モジュールは Track エントリの状態を Negative にします。
- BFD がリンクの正常動作を検出したとき、Track モジュールは Track エントリの状態を Positive にします。

II. 制限とガイドライン

BFD セッションのローカルあるいはリモートアドレスとして VRRP グループの仮想 IP アドレスを設定しないでください。

III. 設定要件

Track と BFD を関連づける前に、BFD エコーパケットの送信元 IP アドレスを設定してください。詳細はセクション 9 *高可用性 オペレーションマニュアル*の"*BFD*"を参照してください。

IV. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. Track エントリを生成し、BFD セッションと関連づけを行う	**track** *track-entry-number* **bfd echo interface** *interface-type interface-number* **remote ip** *remote-ip* **local ip** *local-ip* [**delay** { **negative** *negative-time* | **positive** *positive-time* } *]	—

8.5.3. Track とインタフェース管理モジュールの関連づけ

I. Track とインタフェース管理モジュールの関連づけ

インタフェース管理モジュールは、インタフェースの物理的な状態やネットワーク層のプロトコルの状態を監視します。インタフェース管理モジュールは、Track エントリに関連づけられている場合、次のように機能します。

- インタフェースのリンクまたはネットワーク層のプロトコル状態がアップになると、インタフェース管理モジュールは、状態の変更を Track モジュールに通知し、Track モジュールは Track エントリの状態を Positive に変更します。
- インタフェースのリンクまたはネットワーク層のプロトコルの状態がダウンになると、インタフェース管理モジュールは、状態の変更を Track モジュールに通知し、Track モジュールは Track エントリの状態を Negative に変更します。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. Track をインタフェース管理モジュールと関連づける	• インタフェースのリンク（物理的状態）を監視するためにインタフェース管理モジュールと関連づける: **track** *track-entry-number* **interface** *interface-type interface-number* [**delay** { **negative** *negative-time* | **positive** *positive-time* } *] • インタフェースのネットワークプロトコル状態を監視するためにインタフェース管理モジュールと関連づける: **track** *track-entry-number* **interface** *interface-type interface-number* **protocol** { **ipv4** | **ipv6** } [**delay** { **negative** *negative-time* | **positive** *positive-time* } *]	—

8.6. 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。

8.6.1. 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。

8.6.2. Track とスタティックルーティングの関連づけ

I. Track とスタティックルーティングの関連づけ

スタティックルートは手動でルートを設定します。スタティックルートについての詳細は、セクション 5 *ルーティングプロトコル オペレーションマニュアル*の”*スタティックルーティング*”を参照してください。

スタティックルートの欠点は、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、スタティックルートのバックアップをする別のルートを設定します。スタティックが到達可能であるとき、パケットはスタティックルートを通して転送されます。スタティックルートが到達不可能であるとき、パケットはバックアップルートを通して転送されます。

リアルタイムでスタティックルートの到達可能性をチェックする場合、Track とスタティックルート間の関連づけを行います。

スタティックルートを設定するときに、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、スタティックルート、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 エントリの状態でスタティック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。
  - スタティックルートのネクストホップが到達可能です。
  - 設定されたスタティックルートが有効です。
- Track エントリの状態が Negative の場合、以下の状況となります。
  - スタティックルートのネクストホップが到達不可能です。
  - 設定されたスタティックルートが無効です。
- Track エントリの状態が NotReady の場合、以下の状況となります。
  - スタティックルートのネクストホップの到達可能性が不明です。
  - スタティックルートが有効です。

II. 制限とガイドライン

スタティックルート、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 用に同一のスタティック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。

スタティックルートのルートを復旧させる場合、関連する Track エントリはスタティック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**	—
2. ネクストホップの到達可能性をチェックするためにスタティックルーティングと Track エントリを関連づける	**ip route-static** *dest-address* { *mask-length* | *mask* } { *interface-type interface-number* [*next-hop-address*] | *next-hop-address* [**bfd control-packet bfd-source** *ip-address* | **permanent** | **track** *track-entry-number*] } [**preference** *preference*] [**tag** *tag-value*] [**description** *text*]	デフォルト：設定なし

8.6.3. Track と Smart link の関連づけ

I. Track と Smart link の関連づけ

Smart Link は、中間デバイスまたはネットワークパス上で障害（たとえば、単方向リンク、誤接続、およびパケット損失）が発生したときや障害が復旧したとき、リンク状態を検出できません。また故障が解決したときも検出することができません。リンク状態を監視するために Smart Link のポートは、リンク検出プロトコルを使用する必要があります。障害が検出あるいは復旧すると、リンク検出プロトコルは、リンクを切り替えるために Smart Link に通知します。

Smart Link グループメンバポートで Smart Link と Track 間のコラボレーションを設定することができます。Smart Link は、ポートのリンク状態を検出するため、Track エントリを通して CFD の CC 機能とコラボレーションを行います。

- Track エントリが Positive 状態の場合、リンクは通常状態です。Smart Link は Smart Link グループのリンクの切り替えを行いません。
- Track エントリが Negative 状態の場合、リンクは故障状態です。Smart Link は Smart Link グループに設定されたリンクの preemption モードとポート役割に従い、リンクの切り替えを行うかどうか決定します。
- Track エントリが NotReady 状態の場合、ポートの状態は変更しません。

Smart link の詳細はセクション 9 *高可用性 オペレーションマニュアル*の”*Smart link*”を参照してください。

II. 制限とガイドライン

Smart Link とコラボレーションに使用される Track エントリは CFD の CC 機能と関連付けられている必要があります。

III. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. 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. ポートの Smart Link と Track のコラボレーションを設定する	**port smart-link group** *group-id* **track** *track-entry-number*	デフォルト：設定なし

8.7. 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**]

8.8. Track設定例

8.8.1. スタティックルーティング-Track-NQA コラボレーション設定例

I. ネットワーク要件

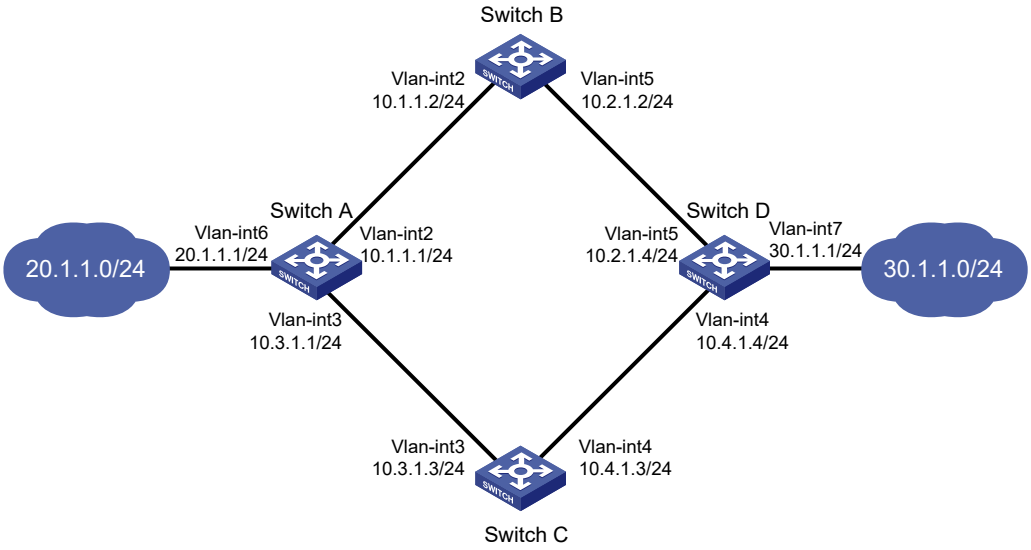
図 8-2 に示すように設定します。

- Switch A はサブネット 20.1.1.0/24 内の Host のデフォルトゲートウェイです。
- Switch D はサブネット 30.1.1.0/24 内の Host のデフォルトゲートウェイです。
- 2 つのサブネット内の Host はスタティックルートを通して互いに通信します。

ネットワークの信頼性を保証するため、ルートのバックアップを設定し、以下のように Switch A と Switch D のスタティックルーティング-Track-NQA コラボレーションを設定します。

- Switch A 上で、高い優先度、ネクストホップが Switch B、宛先が 30.1.1.0/24 のスタティックルートを割り当てます。このルートがマスタールートです。ネクストホップが Switch C、宛先が 30.1.1.0/24 へのスタティックルートはバックアップルートとして動作します。Switch A は、Switch C を通して 30.1.1.0/24 にパケットを転送します。
- Switch D 上で、高い優先度、ネクストホップが Switch B、宛先が 20.1.1.0/24 のスタティックルートを割り当てます。このルートがマスタールートです。ネクストホップが Switch C、宛先が 20.1.1.0/24 へのスタティックルートはバックアップルートとして動作します。マスタールートが到達不能であるとき、バックアップルートが適用されます。Switch D は、Switch C を通して 20.1.1.0/24 にパケットを転送します。

図 8-2 ネットワーク図



II. 設定手順

1. VLAN を作成し、対応するポートを割り当てます。図 8-2 に示すように各 VLAN インタフェースの IP アドレスを割り当てます。(詳細は省略します)
2. Switch A を設定します。

   # ネクストホップのアドレスを 10.1.1.2、デフォルトの優先度を 60 のスタティックルート 30.1.1.0/24 を設定します。このスタティックルートを Track エントリ 1 に関連づけます。

   <SwitchA> system-view

   [SwitchA] ip route-static 30.1.1.0 24 10.1.1.2 track 1

   # ネクストホップのアドレスが 10.3.1.3、優先度を 80 のスタティックルート 30.1.1.0/24 を設定します。

   [SwitchA] ip route-static 30.1.1.0 24 10.3.1.3 preference 80

   # ネクストホップのアドレスが 10.1.1.2 のスタティックルート 10.2.1.4 を設定します。

   [SwitchA] ip route-static 10.2.1.4 24 10.1.1.2

   # 管理者 **admin**、オペレータタグ **test** の NQA オペレーションを作成します。

   [SwitchA] nqa entry admin test

   # オペレーションタイプを ICMP エコータイプとして設定します。

   [SwitchA-nqa-admin-test] type icmp-echo

   # 宛先アドレスを 10.2.1.4 に設定します。

   [SwitchA-nqa-admin-test-icmp-echo] destination ip 10.2.1.4

   # ネクストホップのアドレスを 10.1.1.2 に設定します。

   [SwitchA-nqa-admin-test-icmp-echo] next-hop ip 10.1.1.2

   # 100 ミリ秒の間隔で繰り返す ICMP エコーオペレーションを設定します。

   [SwitchA-nqa-admin-test-icmp-echo] frequency 100

   # リアクションエントリ 1 を設定し、Track モジュールのトリガーを 5 回連続して失敗するように指定します。

[SwitchA-nqa-admin-test-icmp-echo] reaction 1 checked-element probe-fail threshold-type consecutive 5 action-type trigger-only

[SwitchA-nqa-admin-test-icmp-echo] quit

NQA オペレーションを開始します。

[SwitchA] nqa schedule admin test start-time now lifetime forever

Track エントリ 1 を設定し、NQA オペレーションのリアクションエントリ 1 に関連づけます。

[SwitchA] track 1 nqa entry admin test reaction 1

3. Switch B を設定します。

ネクストホップのアドレスが 10.2.1.4、宛先が 30.1.1.0/24 のスタティックルートを設定します。

<SwitchB> system-view

[SwitchB] ip route-static 30.1.1.0 24 10.2.1.4

ネクストホップのアドレスが 10.1.1.1、宛先が 20.1.1.0/24 のスタティックルートを設定します。

[SwitchB] ip route-static 20.1.1.0 24 10.1.1.1

4. Switch C を設定します。

ネクストホップのアドレスが 10.4.1.4、宛先が 30.1.1.0/24 のスタティックルートを設定します。

<SwitchC> system-view

[SwitchC] ip route-static 30.1.1.0 24 10.4.1.4

ネクストホップのアドレスが 10.3.1.1、宛先が 20.1.1.0/24 のスタティックルートを設定します。

[SwitchC] ip route-static 20.1.1.0 24 10.3.1.1

5. Switch D を設定します。

ネクストホップのアドレスが 10.2.1.2、宛先が 20.1.1.0/24 のスタティックルートを設定し、デフォルトの優先度を 60 に設定します。このスタティックルートを Track エントリ 1 に割り当てます。

<SwitchD> system-view

[SwitchD] ip route-static 20.1.1.0 24 10.2.1.2 track 1

ネクストホップのアドレスが 10.4.1.3、宛先が 20.1.1.0/24 のスタティックルートを設定し、デフォルトの優先度を 80 に設定します。

[SwitchD] ip route-static 20.1.1.0 24 10.4.1.3 preference 80

ネクストホップのアドレスが 10.2.1.2、宛先が 10.1.1.1/24 のスタティックルートを設定します。

[SwitchD] ip route-static 10.1.1.1 24 10.2.1.2

管理者 **admin**、オペレータタグ **test** の NQA オペレーションを作成します。

[SwitchD] nqa entry admin test

テストタイプを ICMP エコータイプとして設定します。

[SwitchD-nqa-admin-test] type icmp-echo

オペレーションの宛先 IP アドレスを 10.1.1.1 に設定します。

[SwitchD-nqa-admin-test-icmp-echo] destination ip 10.1.1.1

ネクストホップアドレスを 10.2.1.2 に設定します。

[SwitchD-nqa-admin-test-icmp-echo] next-hop ip 10.2.1.2

ICMP エコーオペレーションのテスト間隔を 100ms に設定します。

[SwitchD-nqa-admin-test-icmp-echo] frequency 100

リアクションエントリ 1 を設定し、Track モジュールのトリガーを 5 回連続して失敗するように指定します。

[SwitchD-nqa-admin-test-icmp-echo] reaction 1 checked-element probe-fail threshold-type consecutive 5 action-type trigger-only

[SwitchD-nqa-admin-test-icmp-echo] quit

NQA オペレーションを開始します。

[SwitchD] nqa schedule admin test start-time now lifetime forever

Track エントリ 1 を設定し、NQA オペレーションのリアクションエントリ 1 に関連づけます。

[SwitchD] track 1 nqa entry admin test reaction 1

III. 設定の確認

Switch A の Track エントリの情報を表示します。

[SwitchA] display track all

```
Track ID: 1
  State: Positive
  Duration: 0 days 0 hours 0 minutes 32 seconds
  Notification delay: Positive 0, Negative 0 (in seconds)
  Tracked object:
    NQA entry: admin test
    Reaction: 1
    Remote IP/URL:--
    Local IP:--
    Interface:--
```

出力は、Track エントリの状態が Positive で、NQA オペレーションが成功し、マスタールートが有効であることを示します。

Switch A のルーティングテーブルを表示します。

[SwitchA] display ip routing-table

```
Destinations : 10       Routes : 10

Destination/Mask    Proto   Pre  Cost         NextHop         Interface
10.1.1.0/24         Direct  0    0            10.1.1.1        Vlan2
10.1.1.1/32         Direct  0    0            127.0.0.1       InLoop0
10.2.1.0/24         Static  60   0            10.1.1.2        Vlan2
10.3.1.0/24         Direct  0    0            10.3.1.1        Vlan3
10.3.1.1/32         Direct  0    0            127.0.0.1       InLoop0
20.1.1.0/24         Direct  0    0            20.1.1.1        Vlan6
20.1.1.1/32         Direct  0    0            127.0.0.1       InLoop0
30.1.1.0/24         Static  60   0            10.1.1.2        Vlan2
127.0.0.0/8         Direct  0    0            127.0.0.1       InLoop0
```

```
127.0.0.1/32        Direct 0    0           127.0.0.1       InLoop0
```

出力では、Switch A は Switch B を通して 30.1.1.0/24 にパケットを転送しています。

Switch B で VLAN インタフェース 2 の IP アドレスを削除します。

<SwitchB> system-view

[SwitchB] interface vlan-interface 2

[SwitchB-Vlan-interface2] undo ip address

Switch A の Track エントリの情報を表示します。

[SwitchA] display track all

```
Track ID: 1
  State: Negative
  Duration: 0 days 0 hours 0 minutes 32 seconds
  Notification delay: Positive 0, Negative 0 (in seconds)
  Tracked object:
    NQA entry: admin test
    Reaction: 1
    Remote IP/URL:--
    Local IP:--
    Interface:--
```

出力では、Track エントリの状態が Negative で、NQA オペレーションが失敗し、マスタールートが無効であることを示します。

Switch A のルーティングテーブルを表示します。

[SwitchA] display ip routing-table

```
Destinations : 10       Routes : 10

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
10.1.1.0/24         Direct 0    0            10.1.1.1        Vlan2
10.1.1.1/32         Direct 0    0            127.0.0.1       InLoop0
10.2.1.0/24         Static 60   0            10.1.1.2        Vlan2
10.3.1.0/24         Direct 0    0            10.3.1.1        Vlan3
10.3.1.1/32         Direct 0    0            127.0.0.1       InLoop0
20.1.1.0/24         Direct 0    0            20.1.1.1        Vlan6
20.1.1.1/32         Direct 0    0            127.0.0.1       InLoop0
30.1.1.0/24         Static 80   0            10.3.1.3        Vlan3
127.0.0.0/8         Direct 0    0            127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0            127.0.0.1       InLoop0
```

出力では、Switch A は Switch C を通して 30.1.1.0/24 にパケットを転送しています。バックアップルートが適用されています。

マスタが故障したとき、20.1.1.0/24 内の Host が 30.1.1.0/24 内の Host と通信できることを確認してください。

[SwitchA] ping -a 20.1.1.1 30.1.1.1

```
Ping 30.1.1.1: 56  data bytes, press CTRL_C to break
```

```
Reply from 30.1.1.1: bytes=56 Sequence=1 ttl=254 time=2 ms
Reply from 30.1.1.1: bytes=56 Sequence=2 ttl=254 time=1 ms
Reply from 30.1.1.1: bytes=56 Sequence=3 ttl=254 time=1 ms
Reply from 30.1.1.1: bytes=56 Sequence=4 ttl=254 time=2 ms
Reply from 30.1.1.1: bytes=56 Sequence=5 ttl=254 time=1 ms

--- Ping statistics for 30.1.1.1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.00% packet loss
round-trip min/avg/max/std-dev = 1/1/2/1 ms
```

マスタが故障したとき、30.1.1.0/24 内の Host が 20.1.1.0/24 内の Host と通信できることを確認してください。

[SwitchB] ping -a 30.1.1.1 20.1.1.1

```
Ping 20.1.1.1: 56  data bytes, press CTRL_C to break
Reply from 20.1.1.1: bytes=56 Sequence=1 ttl=254 time=2 ms
Reply from 20.1.1.1: bytes=56 Sequence=2 ttl=254 time=1 ms
Reply from 20.1.1.1: bytes=56 Sequence=3 ttl=254 time=1 ms
Reply from 20.1.1.1: bytes=56 Sequence=4 ttl=254 time=1 ms
Reply from 20.1.1.1: bytes=56 Sequence=5 ttl=254 time=1 ms

--- Ping statistics for 20.1.1.1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.00% packet loss
round-trip min/avg/max/std-dev = 1/1/2/1 ms
```

8.8.2. スタティックルーティング-Track-BFD コラボレーション設定例

I. ネットワーク要件

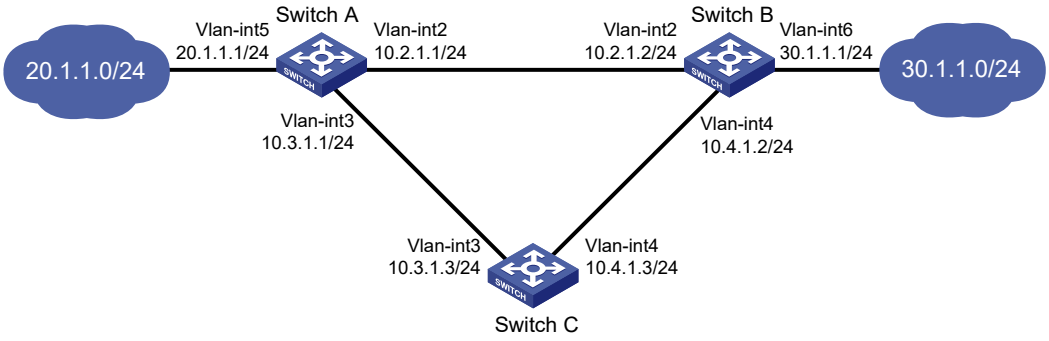
図 8-3 に示すように設定します。

- Switch A はサブネット 20.1.1.0/24 内の Host のデフォルトゲートウェイです。
- Switch D はサブネット 30.1.1.0/24 内の Host のデフォルトゲートウェイです。
- 2 つのサブネット内の Host はスタティックルートを通して互いに通信します。

ネットワークの信頼性を保証するため、ルートのバックアップを設定し、以下のように Switch A と Switch B のスタティックルーティング-Track-BFD コラボレーションを設定します。

- Switch A 上で、高い優先度、ネクストホップが Switch B、宛先が 30.1.1.0/24 のスタティックルートを割り当てます。このルートがマスタールートです。ネクストホップが Switch C、宛先が 30.1.1.0/24 へのスタティックルートはバックアップルートとして動作します。マスタールートが故障したとき、バックアップルートを適用するため、BFD が早急にルートの故障を検出します。
- Switch B 上で、高い優先度、ネクストホップが Switch A、宛先が 20.1.1.0/24 のスタティックルートを割り当てます。このルートがマスタールートです。ネクストホップが Switch C、宛先が 20.1.1.0/24 へのスタティックルートはバックアップルートとして動作します。マスタールートが故障したとき、バックアップルートを適用するため、BFD が早急にルートの故障を検出します。

図 8-3 ネットワーク図



II. 設定手順

1. VLAN を作成し、対応するポートを割り当てます。図 8-3 に示すように各 VLAN インタフェースの IP アドレスを割り当てます。(詳細は省略します)
2. Switch A を設定します。

   # ネクストホップのアドレスを 10.2.1.2、デフォルトの優先度を 60 のスタティックルート 30.1.1.0/24 を設定します。このスタティックルートを Track エントリ 1 に関連づけます。

   <SwitchA> system-view

   [SwitchA] ip route-static 30.1.1.0 24 10.2.1.2 track 1

   # ネクストホップのアドレスを 10.3.1.3、優先度を 80 のスタティックルート 30.1.1.0/24 を設定します。

   [SwitchA] ip route-static 30.1.1.0 24 10.3.1.3 preference 80

   # BFD エコーパケットの送信元 IP アドレスを 10.10.10.10 に設定します。

   [SwitchA] bfd echo-source-ip 10.10.10.10

   # Track エントリ 1 を設定し、Switch A と Switch B 間が通信可能かどうか確認するため、BFD セッションに関連づけます。

   [SwitchA] track 1 bfd echo interface vlan-interface 2 remote ip 10.2.1.2 local ip 10.2.1.1
3. Switch B を設定します。

   # ネクストホップのアドレスを 10.2.1.1、デフォルトの優先度を 60 のスタティックルート 20.1.1.0/24 を設定します。このスタティックルートを Track エントリ 1 に関連づけます。

   <SwitchB> system-view

   [SwitchB] ip route-static 20.1.1.0 24 10.2.1.1 track 1

   # ネクストホップのアドレスを 10.4.1.3、優先度を 80 のスタティックルート 20.1.1.0/24 を設定します。

   [SwitchB] ip route-static 20.1.1.0 24 10.4.1.3 preference 80

   # BFD エコーパケットの送信元 IP アドレスを 1.1.1.1 に設定します。

   [SwitchB] bfd echo-source-ip 1.1.1.1

   # Track エントリ 1 を設定し、Switch A と Switch B 間が通信可能かどうか確認するため、BFD セッションに関連づけます。

   [SwitchB] track 1 bfd echo interface vlan-interface 2 remote ip 10.2.1.1 local ip 10.2.1.2
4. Switch C を設定します。

   # ネクストホップのアドレスを 10.4.1.2、スタティックルート 30.1.1.0/24 を設定します。

<SwitchC> system-view

[SwitchC] ip route-static 30.1.1.0 24 10.4.1.2

ネクストホップのアドレスを 10.3.1.1、スタティックルート 20.1.1.0/24 を設定します。

[SwitchB] ip route-static 20.1.1.0 24 10.3.1.1

III. 設定の確認

Switch A の Track エントリの情報を表示します。

[SwitchA] display track all

```
Track ID: 1
  State: Positive
  Duration: 0 days 0 hours 0 minutes 32 seconds
  Notification delay: Positive 0, Negative 0 (in seconds)
  Tracked object:
    BFD session mode: Echo
    Outgoing interface: Vlan-interface2
    Remote IP: 10.2.1.2
    Local IP: 10.2.1.1
```

出力は、Track エントリの状態が Positive で、ネクストホップ 10.2.1.2 が到達可能であることを示します。

Switch A のルーティングテーブルを表示します。

[SwitchA] display ip routing-table

```
Destinations : 9        Routes : 9

Destination/Mask    Proto   Pre  Cost         NextHop         Interface
10.2.1.0/24         Direct  0    0            10.2.1.1        Vlan2
10.2.1.1/32         Direct  0    0            127.0.0.1       InLoop0
10.3.1.0/24         Direct  0    0            10.3.1.1        Vlan3
10.3.1.1/32         Direct  0    0            127.0.0.1       InLoop0
20.1.1.0/24         Direct  0    0            20.1.1.1        Vlan5
20.1.1.1/32         Direct  0    0            127.0.0.1       InLoop0
30.1.1.0/24         Static  60   0            10.2.1.2        Vlan2
127.0.0.0/8         Direct  0    0            127.0.0.1       InLoop0
127.0.0.1/32        Direct  0    0            127.0.0.1       InLoop0
```

出力では、Switch A は Switch B を通して 30.1.1.0/24 にパケットを転送しています。マスタールートが適用されています。

Switch B の VLAN インタフェース 2 の IP アドレスを削除します。

<SwitchB> system-view

[SwitchB] interface vlan-interface 2

[SwitchB-Vlan-interface2] undo ip address

Switch A の Track エントリの情報を表示します。

[SwitchA] display track all

```
Track ID: 1
```

```
  State: Negative
  Duration: 0 days 0 hours 0 minutes 32 seconds
  Notification delay: Positive 0, Negative 0 (in seconds)
  Tracked object:
    BFD session mode: Echo
    Outgoing interface: Vlan-interface2
    VPN instance name: --
    Remote IP: 10.2.1.2
    Local IP: 10.2.1.1
```

出力は、Track エントリの状態が Negative で、ネクストホップ 10.2.1.2 が到達不可能であることを示します。

Switch A のルーティングテーブルを表示します。

[SwitchA] display ip routing-table

```
Destinations : 9        Routes : 9

Destination/Mask    Proto   Pre  Cost         NextHop         Interface
10.2.1.0/24         Direct  0    0            10.2.1.1        Vlan2
10.2.1.1/32         Direct  0    0            127.0.0.1       InLoop0
10.3.1.0/24         Direct  0    0            10.3.1.1        Vlan3
10.3.1.1/32         Direct  0    0            127.0.0.1       InLoop0
20.1.1.0/24         Direct  0    0            20.1.1.1        Vlan5
20.1.1.1/32         Direct  0    0            127.0.0.1       InLoop0
30.1.1.0/24         Static  80   0            10.3.1.3        Vlan3
127.0.0.0/8         Direct  0    0            127.0.0.1       InLoop0
127.0.0.1/32        Direct  0    0            127.0.0.1       InLoop0
```

出力では、Switch A は Switch C を通して 30.1.1.0/24 にパケットを転送しています。バックアップルートが適用されています。

マスタが故障したとき、20.1.1.0/24 内の Host が 30.1.1.0/24 内の Host と通信できることを確認してください。

[SwitchA] ping -a 20.1.1.1 30.1.1.1

```
Ping 30.1.1.1: 56  data bytes, press CTRL_C to break
Reply from 30.1.1.1: bytes=56 Sequence=1 ttl=254 time=2 ms
Reply from 30.1.1.1: bytes=56 Sequence=2 ttl=254 time=1 ms
Reply from 30.1.1.1: bytes=56 Sequence=3 ttl=254 time=1 ms
Reply from 30.1.1.1: bytes=56 Sequence=4 ttl=254 time=2 ms
Reply from 30.1.1.1: bytes=56 Sequence=5 ttl=254 time=1 ms

--- Ping statistics for 30.1.1.1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.00% packet loss
round-trip min/avg/max/std-dev = 1/1/2/1 ms
```

マスタが故障したとき、30.1.1.0/24 内の Host が 20.1.1.0/24 内の Host と通信できることを確認してください。

[SwitchB] ping -a 30.1.1.1 20.1.1.1

```
Ping 20.1.1.1: 56  data bytes, press CTRL_C to break
Reply from 20.1.1.1: bytes=56 Sequence=1 ttl=254 time=2 ms
Reply from 20.1.1.1: bytes=56 Sequence=2 ttl=254 time=1 ms
Reply from 20.1.1.1: bytes=56 Sequence=3 ttl=254 time=1 ms
Reply from 20.1.1.1: bytes=56 Sequence=4 ttl=254 time=1 ms
Reply from 20.1.1.1: bytes=56 Sequence=5 ttl=254 time=1 ms

--- Ping statistics for 20.1.1.1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.00% packet loss
round-trip min/avg/max/std-dev = 1/1/2/1 ms
```

QX-S5300G シリーズ Ethernet スイッチ

オペレーションマニュアル

10. 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-NQA

03-NTP

04-SNMP

05-RMON

06-NETCONF

07-NETCONF サポートオペレーション

08-プロセスモニタリングとメンテナンス

09-ポートミラーリング

10-トラフィックミラーリング

11-sFlow

12-Information Center

13-NetMeister

目次

このセクションのページは **10-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 について 1-1
1.1.2. ping コマンドを使用したネットワークの接続試験 1-1
1.1.3. ping 設定例 1-1
1.2. Tracert 1-3
1.2.1. 概要 1-3
1.2.2. 設定要件 1-4
1.2.3. 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
1.2.4. Tracert 設定例 1-5
1.3. システムのデバッグ 1-6
1.3.1. システムのデバッグについて 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、システムのデバッグ情報について記載します。

1.1. Ping

1.1.1. Ping について

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。

1.1.2. 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。

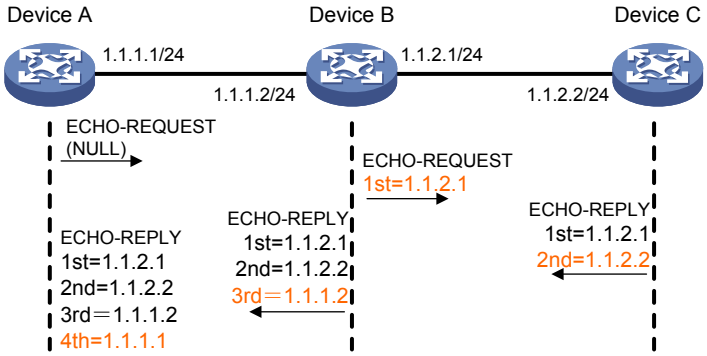
操作	コマンド
指定したアドレスに到達可能かどうかを確認する	低速ネットワークで**ping**コマンドを使用するとき、タイムアウトタイマの値を大きな値に設定してください。(コマンドの**-t**キーワードで示されます) IPv4ネットワーク: **ping** [**ip**] [**-a** *source-ip* | **-c** *count* | **-f** | **-h** *ttl* | **-i** *interface-type interface-number* | **-m** *interval* | **-n** | **-p** *pad* | **-q** | **-r** | **-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** | **-vpn-instance** *vpn-instance-name*] * *host*

1.1.3. 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. Procedure

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。

<DeviceA> ping 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=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、以下の情報を示します。

- Device A は 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はありません。
- ルートが到達可能であることを示します。

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。

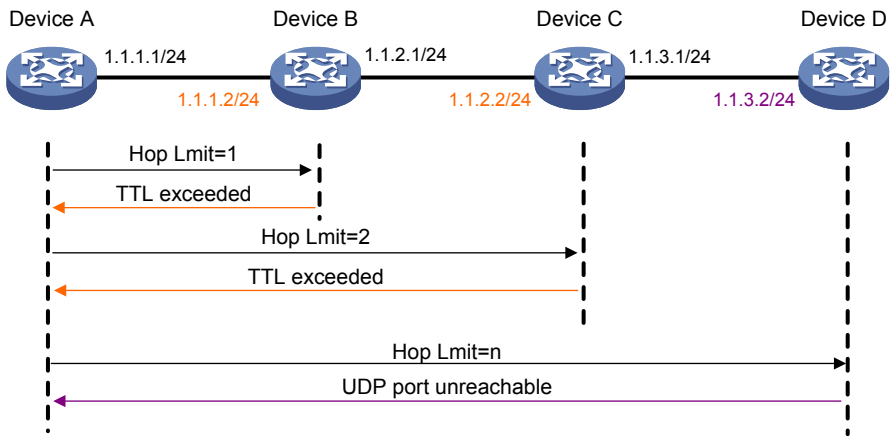
1. 送信元（Device A）は RR オプションが空で ICMP エコーリクエストを宛先（Device C）に対して送信します。
2. 中間デバイス（Device B）は ICMP エコーリクエストの RR オプションに出力インタフェースの IP アドレス（1.1.2.1）を追加し、転送します。
3. リクエストを受信した宛先デバイスはリクエストの RR オプションをコピーし、RR オプションに出力インタフェースの IP アドレス（1.1.2.2）を追加します。ICMP エコーリプライを送信します。
4. 中間デバイスは ICMP エコーリプライの RR オプションに出力インタフェースの IP 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デバイスは 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 から Device C の詳細な情報を取得します。

1.2. Tracert

1.2.1. 概要

Tracert(traceroute とも呼ばれます)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 デバイスの 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 はデバイスの 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. 送信元デバイス（Device A）が宛先デバイス（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 デバイス）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、送信元デバイスは最初のレイヤ 3 デバイスのアドレス（1.1.1.2）を受信します。
3. 送信元デバイスが宛先のデバイスに 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、これで送信元デバイスは 2 番目のレイヤ 3 デバイスのアドレス（1.1.2.2）を取得します。
5. このプロセスは、最終宛先のデバイス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. 送信元デバイスが到達不能 ICMP エラーメッセージを受信したとき、宛先に届いたことを認識し、宛先デバイス（1.1.1.2、1.1.2.2、1.1.3.2）に到達するまでのレイヤ 3 デバイスの IP アドレスを取得することができます。

1.2.2. 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：

- 中間デバイス(送信元デバイスと宛先デバイスの間のデバイス)で ICMP タイムアウトパケットの送信を有効にします。もし中間デバイスが QX シリーズの場合、デバイスで **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、Chapter 4 *Layer 3 - IP Services Command References* の"*IP performance optimization commands*"を参照してください。
- 中間デバイス(送信元デバイスと宛先デバイスの間のデバイス)で ICMP 宛先到達不能パケットの送信を有効にします。もし中間デバイスが QX シリーズの場合、デバイスで **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、Chapter 4 *Layer 3 - IP Services Command References* の"*IP performance optimization commands*"を参照してください。

IPv6 ネットワーク：

- 中間デバイス(送信元デバイスと宛先デバイスの間のデバイス)で ICMPv6 タイムアウトパケットの送信を有効にします。もし中間デバイスが QX シリーズの場合、デバイスで **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、Chapter 4 *Layer 3 - IP Services Command References* の"*IPv6 basics commands*"を参照してください。
- 中間デバイス(送信元デバイスと宛先デバイスの間のデバイス)で ICMPv6 宛先到達不能パケットの送信を有効にします。もし中間デバイスが QX シリーズの場合、デバイスで **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、Chapter 4 *Layer 3 - IP Services Command References* の"*IPv6 basics commands*"を参照してください。

1.2.3. 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* | -**vpn-instance** *vpn-instance-name* | -**w** *timeout*] * *host*

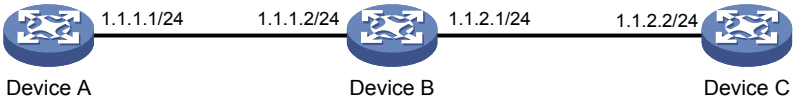
1.2.4. Tracert 設定例

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

図 1-3 に示すように Device に IP アドレスを設定します。

1. Device A でスタティック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

2. ping コマンドを使用して 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。

3. tracert コマンドを使用して、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

Device A で **tracert** コマンドを実行します。

<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>
```

4. 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. 4. の問題を解決するため、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 の接続を確認します。

1.3. システムのデバッグ

1.3.1. システムのデバッグについて

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。

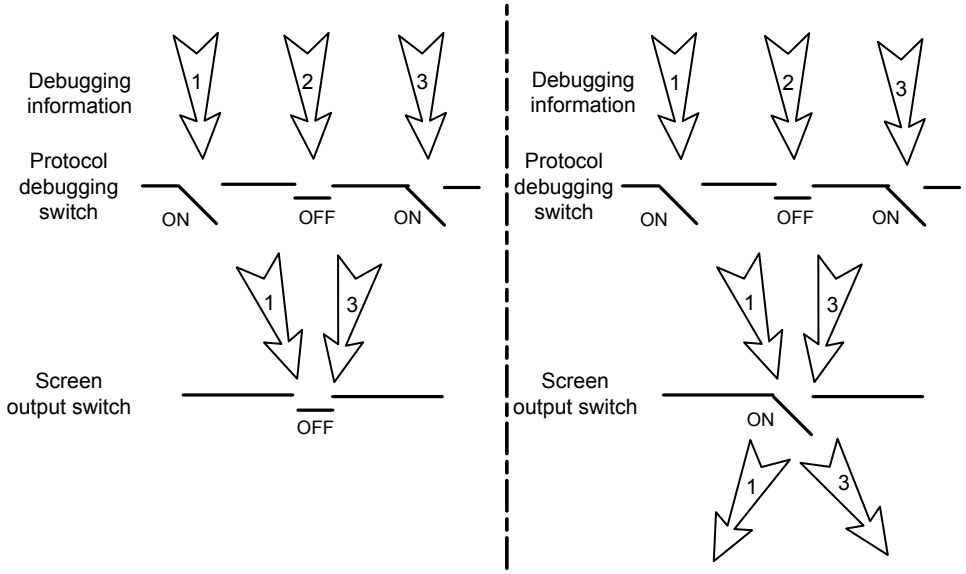
次のスイッチがデバッグ情報の表示を制御します。:

- **プロトコルデバッグスイッチ** ― プロトコル特有のデバッグ情報を制御します。
- **出力画面スイッチ** ― 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、Chapter 11 *Network Management and Monitoring Command References* の "*Information center*"を参照してください。

図 1-4 に示すように、プロトコ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。デバイスは、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とき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、セクション 11 *システム管理 オペレーションマニュアル*の"*Information center*"を参照してください。

図 1-4 プロトコ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

I. 制限とガイドライン

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。

II. 設定手順

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 **10-x-x** です。

2 章 NQA 2-1
2.1. NQA について 2-1
2.1.1. NQA オペレーティングメカニズム 2-1
2.1.2. コラボレーション 2-1
2.1.3. しきい値監視機能 2-2
2.2. NQA 設定作業リスト 2-3
2.3. NQA サーバの設定 2-3
2.4. NQA クライアントの有効化 2-4
2.5. NQA クライアントの NQA テストの設定 2-4
2.5.1. NQA テストの設定作業リスト 2-4
2.5.2. ICMP エコーテストの設定 2-5
2.5.3. DHCP テストの設定 2-6
2.5.4. DNS テストの設定 2-7
2.5.5. FTP テストの設定 2-8
2.5.6. HTTP テストの設定 2-9
2.5.7. UDP ジッタテストの設定 2-10
2.5.8. SNMP テストの設定 2-12
2.5.9. TCP テストの設定 2-12
2.5.10. UDP エコーテストの設定 2-13
2.5.11. 音声テストの設定 2-14
2.5.12. DLSw テストの設定 2-17
2.5.13. NQA テストのオプションパラメータの設定 2-17
2.5.14. コラボレーション機能の設定 2-18
2.5.15. しきい値監視機能の設定 2-19
2.5.16. NQA 統計情報収集機能の設定 2-20
2.5.17. NQA 履歴記録保存の設定 2-21
2.5.18. NQA クライアントにおける NQA テストのスケジューリング 2-22
2.6. NQA の表示と維持 2-22
2.7. NQA 設定例 2-23
2.7.1. ICMP エコーテスト設定例 2-23
2.7.2. DHCP テスト設定例 2-25
2.7.3. DNS テスト設定例 2-26
2.7.4. FTP テスト設定例 2-27
2.7.5. HTTP テスト設定例 2-29
2.7.6. UDP ジッタテスト設定例 2-30
2.7.7. SNMP テスト設定例 2-33
2.7.8. TCP テスト設定例 2-35
2.7.9. UDP エコーテスト設定例 2-36
2.7.10. 音声テスト設定例 2-38
2.7.11. DLSw テスト設定例 2-40
2.7.12. NQA コラボレーション設定例 2-42

2章 NQA

2.1. NQAについて

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。

2.1.1. NQA オペレーティングメカニズム

NQA オペレーションには、実行方法を定義するためのオペレーションタイプ、宛先 IP アドレス、ポート番号などのパラメータのセットが含まれます。各 NQA オペレーションは、管理者名とオペレーションタグの組み合わせによって識別されます。NQA クライアントは、スケジュールされた期間でオペレーションを実行するように設定できます。

図 2-1 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 2-1 ネットワーク図

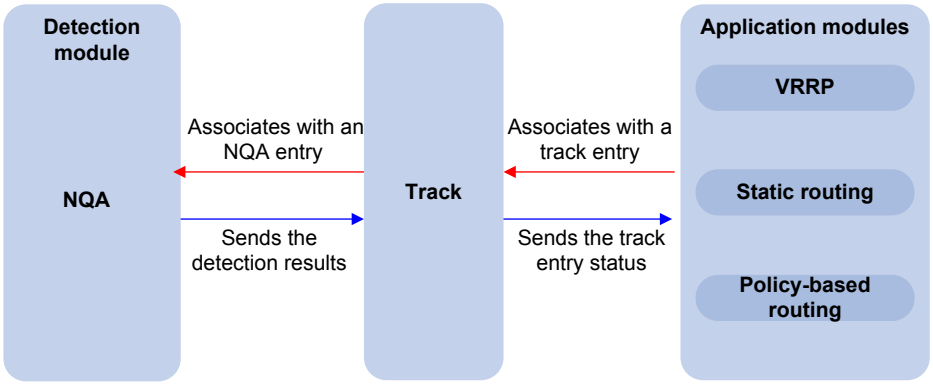


2.1.2. コラボレーション

NQA は、アプリケーションモジュールがあらかじめ定義されたアクションを実行できるようにするため、アプリケーションモジュールの状態あるいは性能が変更されたことを通知できるようにトラックモジュールとコラボレーションを行います。

NQA と Track のコラボレーションは以下のアプリケーションモジュールで有効です。

- スタティックルーティング
- Smart Link



以下に、コラボレーションを使用して、192.168.0.88 のスタティックルートの動作をモニタする方法を示します。

1. NQA は 192.168.0.88 の到達可能性をモニタします。
2. 192.168.0.88 が到達不可能となったとき、NQA はその変化をトラックモジュールに通知します。
3. トラックモジュールは、スタティックルーティングモジュールに状態の変化を通知します。
4. スタティックルーティングモジュールはスタティックルートを無効にします。

コラボレーションについての詳細は、セクション 9 *高可用性 オペレーションマニュアル*の"*Track*"を参照してください。

2.1.3. しきい値監視機能

しきい値監視機能は、NQA オペレーションの測定基準が指定されたしきい値を越えたとき、NQA クライアントがあらかじめ決められたアクションを行うことを有効にします。

表 2-1 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 2-1 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
周期時間	UDPジッタ、音声テスト
1方向のジッタ(送信元から宛先、あるいは宛先から送信元)	UDPジッタ、音声テスト
1方向の遅延(送信元から宛先、あるいは宛先から送信元)	UDPジッタ、音声テスト

監視対象	サポートするテストタイプ
ICPIF(Calculated Planning Impairment Factor)(詳細は*セクション10 システム管理 オペレーションマニュアルの"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*セクション10 システム管理 オペレーションマニュアルの"NQA"の"音声テストの設定"*を参照してください。)	音声テスト

2.2. 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です。
(必須設定項目) NQAクライアントの有効化	―
(必須設定項目) NQAテストの設定 NQAクライアントのNQAテストの設定	―

2.3. NQAサーバの設定

I. 制限とガイドライン

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。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. NQA サーバを有効にする	**nqa server enable**	デフォルト：無効

操作	コマンド	補足
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* [**vpn-instance** *vpn-instance-name*] [**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* [**vpn-instance** *vpn-instance-name*] [**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

2.4. 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**	―
2. NQA クライアントを有効にする	**nqa agent enable**	デフォルト：有効

2.5. NQAクライアントのNQAテストの設定

2.5.1. 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つを実行してください。 • 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

作業リスト
(オプション設定項目) コラボレーション機能の設定
(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

2.5.2. ICMP エコーテストの設定

I. ICMP エコーテスト

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。

ICMP エコーテストは IPv6 ネットワークを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 Chapter 11 *Network Management and Monitoring Command References* の "*Ping, tracert, and system debugging commands*"を参照してください。

II. 設定手順

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 IP 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) 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 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。
6. (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
7. (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
8. (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：00102030405060708(16進数表示)

2.5.3. DHCP テストの設定

I. DHCP テスト

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 テストを完了したとき、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。

II. 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 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 出力インタフェースのIPアドレスは送信元IPアドレスとして使われます。 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クライアントは送信元IPアドレスを、DHCPサーバに送信するDHCP要求のgiaddrフィールドに追加します。 詳細はセクション4 *IPサービス オペレーションマニュアル*の"*DHCPリレー*"を参照してください。

2.5.4. DNS テストの設定

I. DNS テスト

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。

II. 設定手順

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**	―

操作	コマンド	補足
4. DNS パケットの宛先 IP 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

2.5.5. FTP テストの設定

I. FTP テスト

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。

II. 制限とガイドライン

filename コマンドが設定され、**put** オペレーションが行われるとき、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。

III. 設定手順

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. 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
5. 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
6. (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 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。

操作	コマンド	補足
7. 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。
8. 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 以下のどちら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とき、ファイル名が必要です。
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ときに必要です。

2.5.6. HTTP テストの設定

I. HTTP テスト

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。

HTTP テストは以下のオペレーションタイプがあります。

- **Get**—HTTP サーバから Web ページのようなデータを取得します。
- **Post**—プロセスを行う HTTP サーバにデータを送信します。

HTTP テストは 1 回のテストごとに指定されたタイプのテストを行います。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. 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 以下のどちら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

操作	コマンド	補足
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. HTTP バージョンを指定する	**version** { **v1.0** | **v1.1** }	デフォルト：HTTP 1.0
8. 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) 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 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。

2.5.7. UDP ジッタテストの設定

I. UDP ジッタテスト

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、Chapter 11 *Network Management and Monitoring Command References* の "*NQA commands*"の"*NQA server commands*"を参照してください。

II. 制限とガイドライン

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。

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。

III. 設定手順

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 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IP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。
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を行っているポート番号と同一です。
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：設定なし 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) 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
9. (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** *packet-interval*	デフォルト：20ミリ秒
10. (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** *packet-timeout*	デフォルト：3000ミリ秒
11. (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

操作	コマンド	補足
12. (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)

2.5.8. SNMP テストの設定

I. SNMP テスト

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。

SNMP テストは 1 回のテストごとに、SNMP エージェントに SNMPv1、SNMPv2c、SNMPv3 パケットをそれぞれ 1 つずつ送信します。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. 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 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) 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 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. (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

2.5.9. TCP テストの設定

I. TCP テスト

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、セクション 10 *システム管理 オペレーションマニュアル*の"*NQA*"の"*NQA サーバの設定*"を参照してください。

TCP テストは 1 回のテストごとに TCP 接続を確立します。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. 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**	―
4. TCP 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IP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。
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。
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 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。

2.5.10. UDP エコーテストの設定

I. UDP エコーテスト

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、Chapter 11 *Network Management and Monitoring Command References* の"*NQA commands*"の"*NQA server commands*"を参照してください。

UDP エコーテストは 1 回のテストごとに UDP パケットを宛先デバイスに送信します。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. 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**	―
4. UDP 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IP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。
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。
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：設定なし 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。
7. (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
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に入る文字列を指定する	**data-fill** *string*	デフォルト：00010203040506070809(16進数表示

2.5.11. 音声テストの設定

I. 音声テスト

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、Chapter 11 *Network Management and Monitoring Command References* の "*NQA commands*"の"*NQA server commands*"を参照してください。

II. 制限とガイドライン

音声テストでポート番号 1～1023 で行わないでください。1～1023 を使用した場合、このポートに該当するサービスが動作しなくなります。

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。

III. 設定手順

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IP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。

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。
6. (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：設定なし 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。
7. (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
8. 基本的な音声テストのパラメータを設定する	• コーデックタイプを指定する：**codec-type** { **g711a** | **g711u** | **g729a** } • 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*	コーデックタイプのデフォルト：G.711 A-law アドバンテージファクタのデフォルト：0
9. 音声テストのプローブパラメータを設定する	• 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* • 音声パケットを送信する間隔を設定する：**probe packet-interval** *packet-interval* • 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** *packet-timeout*	UDPパケット数のデフォルト：1000 送信間隔のデフォルト：20ミリ秒 受信待ち時間のデフォルト：5000ミリ秒
10. ペイロードのパラメータを指定する	• 音声パケットのペイロードサイズを指定する：**data-size** *size* • 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*	ペイロードサイズのデフォルト：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。 使われる文字列のデフォルト：00010203040506070809(16進数表示)

2.5.12. DLSw テストの設定

I. DLSw テスト

DLSw テストは DLSw 装置の応答時間を測定します。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. 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：設定なし 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。

2.5.13. NQA テストのオプションパラメータの設定

I. 制限とガイドライン

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。

II. 設定手順

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. 説明を設定する	**description** *text*	デフォルト：設定なし

操作	コマンド	補足
4. 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。
5. 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。
6. 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。
7. 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。
8. 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
9. 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。
10. VPN インスタンスが実行される場所を指定する	**vpn-instance** *vpn-instance-name*	デフォルト：パブリックネットワークで実行されます。

2.5.14. コラボレーション機能の設定

I. コラボレーション機能

コラボレーションは、NQA テストのリアクションエントリをトラックエントリと関連付けることで行うことができます。リアクションエントリは NQA テストを監視します。連続した検出失敗回数がしきい値に達した場合、設定された動作が行われます。

II. 制限とガイドライン

コラボレーション機能は以下のタイプでは利用できません。

- UDP ジッタテスト
- 音声テスト

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 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. リアクションエントリを設定する	**reaction** *item-number* **checked-element probe-fail threshold-type consecutive** *consecutive-occurrences* **action-type trigger-only**	デフォルト：設定なし 存在するリアクションエントリを修正することはできません。
4. system view に戻る	**quit**	―
5. トラックと NQA を関連付ける	セクション9 *高可用性 オペレーションマニュアル*の "*Track*"を参照してください。	―
6. トラックとアプリケーションモジュールを関連付ける	セクション9 *高可用性 オペレーションマニュアル*の "*Track*"を参照してください。	―

2.5.15. しきい値監視機能の設定

I. しきい値監視

この機能は NQA テストの動作状態を監視することができます。

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です。

以下のアクションをサポートします。

- **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、NMS にトラップを送信します。

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、Chapter 11 *Network Management and Monitoring Command References* の"*SNMP commands*"を参照してください。

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、トリガー動作を設定します。

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。

II. 設定手順

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. 指定状況下になったとき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** *cumulate-probe-failures* | **test-complete** | **test-failure** *cumulate-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。
4. 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* | **average** | **consecutive** *consecutive-occurrences* } **threshold-value** *upper-threshold lower-threshold* **[action-type { none | trap-only }]**	DNSテストは、**none**のアクションのみサポートしています。

2.5.16. NQA 統計情報収集機能の設定

I. NQA 統計情報の収集

NQA は指定した期間内に完了したテストの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。

統計情報グループの数が最大数になったとき、NQA クライアントは、新しい統計情報を保存するために、もっとも古い統計情報グループから削除します。

指定した期間に到達したとき、統計情報グループは自動で削除されます。

II. 制限とガイドライン

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。NQA テストを 1 回のみ動作するように設定する場合、**frequency** コマンドを使用し、テスト間隔を 0 に設定してください。

III. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. 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. (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
4. (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とき、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。
5. (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ときに、統計グループは削除されます。

2.5.17. NQA 履歴記録保存の設定

I. NQA 履歴記録の保存

NQA クライアントが NQA 履歴記録を保存することを可能にします。NQA 履歴記録を表示するには、**display nqa history** コマンドを使用します。

II. 制限とガイドライン

NQA 履歴記録保存機能は以下のタイプでは利用できません。

- UDP ジッタテスト
- 音声テスト

III. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. 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 テストの履歴記録の保存を有効にする	**history-record enable**	デフォルト：無効

操作	コマンド	補足
4. (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とき記録が削除されます。
5. (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 もし最大数を超過した場合、一番古い履歴が削除されます。

2.5.18. NQA クライアントにおける NQA テストのスケジューリング

I. 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 テストは即座に開始します。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。

II. 制限とガイドライン

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。

III. 設定手順

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**]

2.6. 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*]

操作	コマンド
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 status**

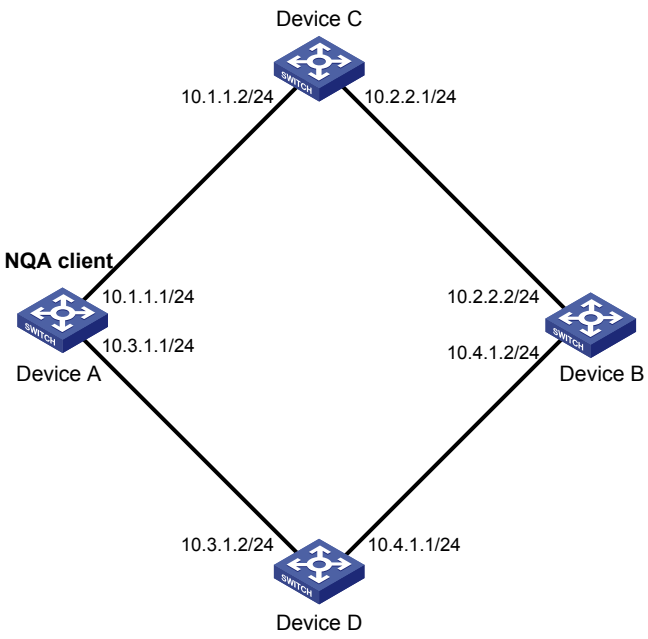
2.7. NQA設定例

2.7.1. ICMP エコーテスト設定例

I. ネットワーク要件

図 2-2 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 2-2 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 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 と指定します。

[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 履歴記録を保存するように設定します。

[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
```

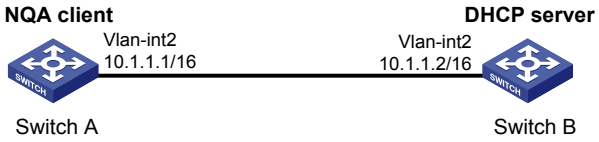
出力では、Device A からのパケットが Device C を通して Device B に送信できることを示しています。NQA テスト中のパケットロスはありません。最小、最大、平均ラウンドトリップ時間はそれぞれ、2、5、3ms です。

2.7.2. DHCP テスト設定例

I. ネットワーク要件

図 2-3 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 2-3 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。

2.7.3. DNS テスト設定例

I. ネットワーク要件

図 2-4 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 2-4 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。

2.7.4. FTP テスト設定例

I. ネットワーク要件

図 2-5 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 2-5 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。

2.7.5. HTTP テスト設定例

I. ネットワーク要件

図 2-6 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 2-6 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。

2.7.6. UDP ジッタテスト設定例

I. ネットワーク要件

図 2-7 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 2-7 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

宛先 IP アドレス 10.2.2.2、宛先ポート 9000 を設定します。

[DeviceA-nqa-admin-test1-udp-jitter] destination ip 10.2.2.2

[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
  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: 2011-05-29 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
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
```

2.7.7. SNMP テスト設定例

I. ネットワーク要件

図 2-8 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 2-8 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。

SNMPv1、SNMPvc2、SNMPv3 のバージョンを設定します。

<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。

2.7.8. TCP テスト設定例

I. ネットワーク要件

図 2-9 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 2-9 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、宛先ポート番号を 9000 に設定します。

[DeviceA-nqa-admin-test1-tcp] destination ip 10.2.2.2

[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。

2.7.9. UDP エコーテスト設定例

I. ネットワーク要件

図 2-10 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 2-10 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 アドレスとして 10.2.2.2、宛先ポート番号として 8000 を設定します。

[DeviceA-nqa-admin-test1-udp-echo] destination ip 10.2.2.2

[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。

2.7.10. 音声テスト設定例

I. ネットワーク要件

図 2-11 に示すように、Device A と Device B 間のジッタ、MOS、ICPIF をテストするため音声テストを設定します。

図 2-11 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、宛先ポート番号を 9000 に設定します。

[DeviceA-nqa-admin-test1-voice] destination ip 10.2.2.2

[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
  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: 2011-06-13 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
  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
```

2.7.11. DLSw テスト設定例

I. ネットワーク要件

図 2-12 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 2-12 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
```

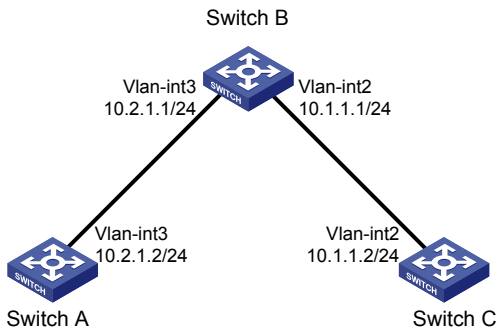
出力では、DLSw 装置の応答時間が 19 ミリ秒であることを示します。

2.7.12. NQA コラボレーション設定例

I. ネットワーク要件

図 2-13 に示すように、Switch B を Switch A のネクストホップとするように Switch C にスタティックルートを設定します。スタティックルートの状態を監視するため、スタティックルート、トラックエントリ、ICMP エコーテストを関連付けます。

図 2-13 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. Switch A でユニキャストスタティックルートを設定し、スタティックルートとトラックエントリ 1 を関連付けます。

<SwitchA> system-view

[SwitchA] ip route-static 10.1.1.2 24 10.2.1.1 track 1

3. Switch A で ICMP エコーテストを設定します。

管理者名 admin、オペレーションタグが test1 の NQA テストを作成します。

[SwitchA] nqa entry admin test1

NQA テストタイプとして ICMP エコーを設定します。

[SwitchA-nqa-admin-test1] type icmp-echo

宛先 IP アドレスとして 10.2.1.1 を設定します。

[SwitchA-nqa-admin-test1-icmp-echo] destination ip 10.2.1.1

1000 ミリ秒の間隔でテストを繰り返すように設定します。

[SwitchA-nqa-admin-test1-icmp-echo] frequency 100

リアクションエントリ 1 を作成します。テストの連続失敗回数が 5 回になったとき、コラボレーションが発生します。

[SwitchA-nqa-admin-test1-icmp-echo] reaction 1 checked-element probe-fail threshold-type consecutive 5 action-type trigger-only

[SwitchA-nqa-admin-test1-icmp-echo] quit

ICMP テストを開始します。

[SwitchA] nqa schedule admin test1 start-time now lifetime forever

4. Switch A でトラックエントリ 1 を作成し、NQA テスト(admin-test1)のリアクションエントリ 1 と関連付けます。

[SwitchA] track 1 nqa entry admin test1 reaction 1

III. 設定の確認

Switch A ですべてのトラックエントリを表示します。

[SwitchA] display track all

```
Track ID: 1
  State: Positive
  Duration: 0 days 0 hours 0 minutes 0 seconds
  Notification delay: Positive 0, Negative 0 (in seconds)
  Tracked object:
    NQA entry: admin test1
    Reaction: 1
```

Switch A のルーティングテーブルのアクティブルートの概要情報を表示します。

[SwitchA] display ip routing-table

```
Destinations : 13        Routes : 13

Destination/Mask    Proto   Pre  Cost         NextHop         Interface
0.0.0.0/32          Direct  0    0            127.0.0.1       InLoop0
10.1.1.0/24         Static  60   0            10.2.1.1        Vlan3
10.2.1.0/24         Direct  0    0            10.2.1.2        Vlan3
10.2.1.0/32         Direct  0    0            10.2.1.2        Vlan3
10.2.1.2/32         Direct  0    0            127.0.0.1       InLoop0
10.2.1.255/32       Direct  0    0            10.2.1.2        Vlan3
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
```

出力では、ネクストホップ 10.2.1.1 のスタティックルートがアクティブで、トラックエントリの状態が positive であることを示します。

Switch B の VLAN インタフェース 3 の IP アドレスを削除します。

<SwitchB> system-view

[SwitchB] interface vlan-interface 3

[SwitchB-Vlan-interface3] undo ip address

Switch A ですべてのトラックエントリを表示します。

[SwitchA] display track all

```
Track ID: 1
```

```
  State: Negative
  Duration: 0 days 0 hours 0 minutes 0 seconds
  Notification delay: Positive 0, Negative 0 (in seconds)
  Tracked object:
    NQA entry: admin test1
    Reaction: 1
```

Switch A のルーティングテーブルのアクティブルートの概要情報を表示します。

[SwitchA] display ip routing-table

```
Destinations : 12        Routes : 12

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
0.0.0.0/32          Direct 0    0            127.0.0.1       InLoop0
10.2.1.0/24         Direct 0    0            10.2.1.2        Vlan3
10.2.1.0/32         Direct 0    0            10.2.1.2        Vlan3
10.2.1.2/32         Direct 0    0            127.0.0.1       InLoop0
10.2.1.255/32       Direct 0    0            10.2.1.2        Vlan3
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
```

出力では、スタティックルートがなく、トラックエントリの状態が negative であることを示します。

目次

このセクションのページは **10-x-x** です。

3 章 NTP 3-1
3.1. 概要 3-1
3.1.1. NTP アプリケーションシナリオ 3-1
3.1.2. NTP の動作 3-1
3.1.3. NTP アーキテクチャ 3-2
3.1.4. 運用モード 3-3
3.1.5. NTP セキュリティ 3-5
3.1.6. プロトコルと標準 3-6
3.2. 設定要件とガイドライン 3-7
3.3. 設定作業リスト 3-7
3.4. NTP サービスの有効化 3-8
3.5. NTP 運用モードの設定 3-8
3.5.1. NTP クライアント/サーバモードの設定 3-8
3.5.2. NTP シンメトリックアクティブ/パッシブモードの設定 3-9
3.5.3. NTP ブロードキャストモードの設定 3-9
3.5.4. NTP マルチキャストモードの設定 3-10
3.6. 参照ソース用ローカルクロックの設定 3-11
3.7. NTP サービスアクセス制御権の設定 3-12
3.8. NTP 認証の設定 3-12
3.8.1. クライアント/サーバモードの NTP 認証の設定 3-12
3.8.2. 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 3-14
3.8.3. ブロードキャストモードの NTP 認証の設定 3-16
3.8.4. マルチキャストモードの NTP 認証の設定 3-18
3.9. NTP オプションパラメータの設定 3-20
3.9.1. NTP メッセージの送信元インタフェースの設定 3-20
3.9.2. インタフェースでの NTP メッセージ受信の無効化 3-21
3.9.3. ダイナミックアソシエーションの最大数の設定 3-21
3.9.4. NTP パケットの DSCP 値の設定 3-22
3.10. NTP の表示と維持 3-22
3.11. NTP 設定例 3-23
3.11.1. NTP クライアント/サーバモードの設定例 3-23
3.11.2. NTP シンメトリックアクティブ/パッシブモードの設定例 3-24
3.11.3. NTP ブロードキャストモードの設定例 3-26
3.11.4. NTP マルチキャストモードの設定例 3-28
3.11.5. NTP 認証を使用したクライアント/サーバモードの設定例 3-31
3.11.6. NTP 認証を使用したブロードキャストモードの設定例 3-33

3章 NTP

3.1. 概要

NTP(Network Time Protocol)を使用して、あるいはシステムクロックを変更することで、ネットワークで動作させる前に、信頼されたシステムクロックと同期を取ります。

NTP は UDP の上位プロトコルで、UDP ポート 123 を使用します。

3.1.1. NTP アプリケーションシナリオ

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を含む、さまざまなアプリケーションは正確なシステムクロックが必要となります。

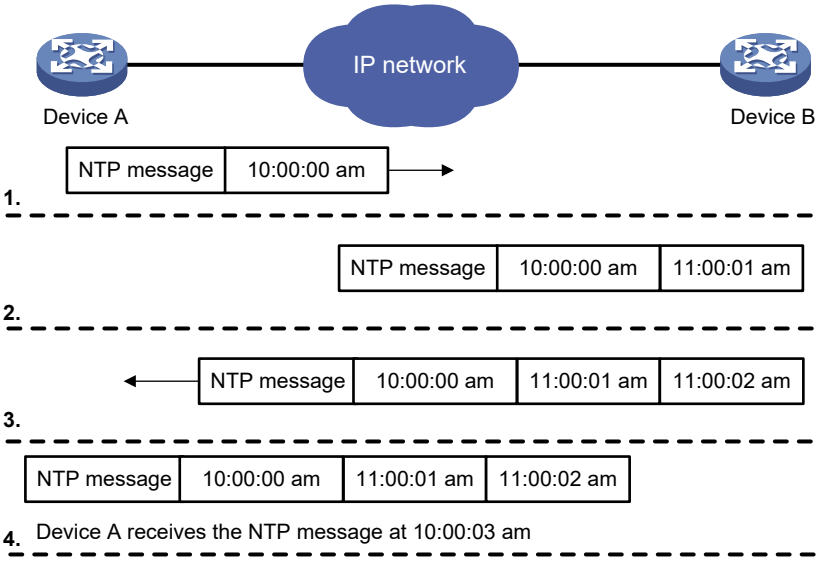
NTP はネットワーク装置間のシステムクロックを動的に同期させるため、一般的に大規模ネットワークで使用されます。手動でシステムクロックを設定するよりも、高い時間の精度が保証されます。小規模ネットワークでは高い精度のシステムクロックは必要としませんが、装置のシステムクロックを 1 台ずつ変更することで、装置間でシステムクロックを同期させ続けることができます。

3.1.2. NTP の動作

図 3-1 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 3-1 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 から発信されるとき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 から発信されるときに、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とき、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

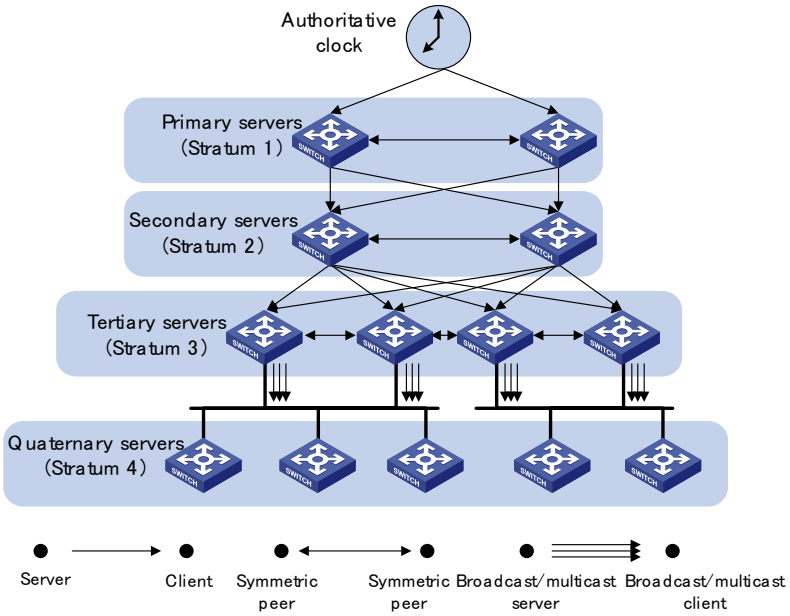
これらのパラメータにもとづき、Device A の時計を Device B の時計に同期することができます。

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。

3.1.3. 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 3-2 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 3-2 NTP アーキテクチャ



一般的に 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。各サーバの精度は、最上位レベル(プライマリサーバ)に割り当てられた stratum のレベルは 1 で、階層化された下のレベル(セカンダリサーバ)に割り当てられた stratum のレベルは 2、そして下の階層に下がるにつれて stratum のレベルの値が大きくなります。NTP は、いくつの NTP ホップ数がプライマリ時刻サーバと装置が離れているかを記述するのに stratum を使用します。stratum レベル 2 の NTP サーバは stratum レベル 1 のサーバなどから時間を取得することができます。

時間の精度と有効性を保証するため、装置が複数の NTP サーバを指定することができます。装置は、stratum のようなパラメータをもとにして最適なソースを選択します。クロックの選択の詳細は、関連するプロトコルと標準を参照してください。

もしネットワークの装置が最も権威のあるサーバに同期することができない場合、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することができます。ネットワークのほかの装置と同期させるため、その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。

3.1.4. 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

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。

表 3-1 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 3-2 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。もし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 3-2 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。

モード	作業処理	原則	アプリケーションシナリオ
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とき、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 3-2 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。
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。

3.1.5. 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、本装置では 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 アクセス制御

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、ローカル装置がピアの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。

装置は NTP 要求を以下のように処理します。

- アクセス制御権が設定されていない場合、**peer** はローカル装置とピアの装置に与えられます。
- ピアの装置の 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、最も制限の少ないアクセス制御権がピ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の ACL が一つも作成されていない場合、**peer** が与えられます。
- アクセス制御権のための ACL に条件が設定されていない場合、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とき、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。もしパスしないとき、メッセージを廃棄します。この機能は、認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 3-3 NTP 認証

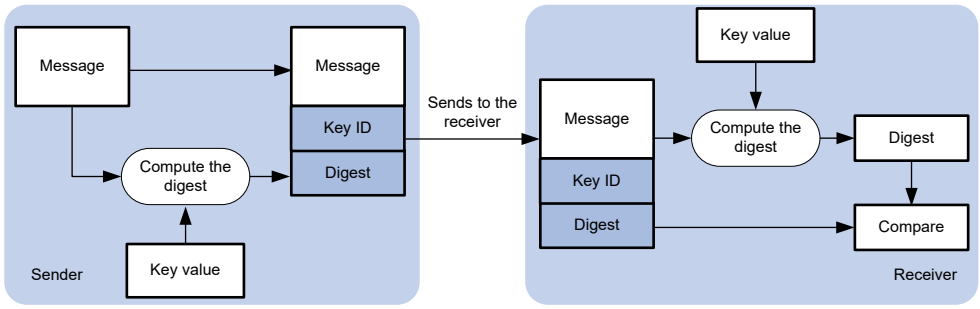


図 3-3 に示すように NTP 認証は以下のように動作します。

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、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 Receiver はメッセージのキーID によってキーを確認し、ダイジェストを計算するため、MD5 アルゴリズムを使用します。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と比較します。もし同一である場合、Receiver はメッセージを受信し、異なる場合メッセージを廃棄します。

3.1.6. 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*

3.2. 設定要件とガイドライン

以下の設定要件とガイドラインに従って NTP を設定してください。

- 同一装置で NTP と SNTP を同時に設定することはできません。
- NTP は VLAN インタフェースでのみサポートします。
- アグリゲートメンバポートで NTP を設定することはできません。
- NTP サービスと SNTP サービスは同時に有効にすることができません。NTP サービスあるいは SNTP サービスのどちらか一方のみ、有効にすることができます。
- クロック同期の精度を保証するため、複数の参照先を指定することを推奨しません。複数の参照先を指定した場合、頻繁にクロックが変更するか、同期の失敗が発生する可能性があります。
- NTP としてクロックを設定する場合、**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、Chapter 1 *Fundamentals Command References* の”*Device management commands*”を参照してください。

3.3. 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) NTP運用モードの設定 • NTP クライアント/サーバモードの設定 • NTP シンメトリックアクティブ/パッシブモードの設定 • NTP ブロードキャストモードの設定 • NTP マルチキャストモードの設定
(オプション設定項目) 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) アクセス制御権の設定
(オプション設定項目) NTP認証の設定 • クライアント/サーバモードの NTP 認証の設定 • 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 • ブロードキャストモードの NTP 認証の設定 • マルチキャストモードの 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 • NTP メッセージの送信元インタフェースの • インタフェースでの NTP メッセージ受信の無効 • ダイナミックアソシエーションの最大数の • NTP パケットの DSCP 値の

3.4. NTPサービスの有効化

I. 制限とガイドライン

NTP サービスと SNTP サービスは同時に有効にすることができません。NTP サービスを有効にする前に SNTP サービスが無効であることを確認してください。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. NTP サービスを有効にする	**ntp-service enable**	デフォルト：無効

3.5. NTP運用モードの設定

3.5.1. NTP クライアント/サーバモードの設定

I. 制限とガイドライン

装置がクライアント/サーバモードで動作するとき、クライアントの IP アドレスを指定します。

NTP クライアントを設定するとき、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。

II. 設定手順

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

3.5.2. NTP シンメトリックアクティブ/パッシブモードの設定

I. 制限とガイドライン

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とき、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。

NTP シンメトリックアクティブピアを設定するとき、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。

II. 設定手順

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* } [**vpn-instance** *vpn-instance-name*] [**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

3.5.3. NTP ブロードキャストモードの設定

I. 制限とガイドライン

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。

II. 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**	―

操作	コマンド	補足
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。

III. ブロードキャストサーバの設定

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送信するインタフェースに移行します。
3. NTP ブロードキャストサーバモードで動作するように装置を設定する	**ntp-service broadcast-server** [**authentication-keyid** *keyid* | **version** *number*|**version** *number*] *	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。

3.5.4. NTP マルチキャストモードの設定

I. 制限とガイドライン

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。

II. 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。

III. マルチキャストサーバの設定

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送信するインタフェースに移行します。
3. NTP マルチキャストサーバモードで動作するように装置を設定する	**ntp-service multicast-server** [*ip-address*] [**authentication-keyid** *keyid* | **ttl** *ttl-number*| **version** *number*] *	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送信します。

3.6. 参照ソース用ローカルクロックの設定

I. 参照ソース用ローカルクロック設定

参照ソースとしてローカルクロックを設定することを可能にします。

II. 制限とガイドライン

参照ソースとしてローカルクロックを設定した後、ローカルクロックは、同期化され、ネットワークのほかの装置に同期化するため、タイムサーバとして動作することができます。もしローカルクロックが正確でない場合、タイムエラーが発生します。

メモ ：

ntp-service refclock-master コマンドを有効にすることで QX を NTP マスタとして稼働させることが可能になります。しかし QX を NTP マスタとして運用した場合、うるう秒の挿入等が行われた際の情報を得ることができず、時刻のずれが発生します。また、装置内部の時計精度についても、一般的な PC 等と同様であるため、時計精度による時刻ずれも発生します。

信頼できる NTP サーバから時刻の取得を行い、同期して運用することを推奨します。

III. 設定要件

この機能を設定する前に、ローカルシステム時間を正しい値に設定してください。

IV. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. 参照ソース用ローカルクロックを設定する	**ntp-service refclock-master** [*ip-address*] [*stratum*]	デフォルト：設定なし

3.7. NTPサービスアクセス制御権の設定

I. 設定要件

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 Chapter 7 *ACL and QoS Command References* の”*ACL commands*”を参照してください。

ACL の詳細はセクション 7 *ACL and QoS オペレーションマニュアル*の“*ACL*”を参照してください。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
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** *acl-number*	デフォルト：peer

3.8. NTP認証の設定

3.8.1. クライアント/サーバモードの NTP 認証の設定

I. 制限とガイドライン

NTP 認証を保証する場合、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。

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 3-2 に示します。(ー は相違がないことを示します)

表 3-2 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。

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	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	―	―	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	―	―	―	―	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。

II. クライアントの NTP 認証の設定

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** } *value*	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* } [**vpn-instance** *vpn-instance-name*] **authentication-keyid** *keyid*	―

III. サーバの NTP 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. 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** } *value*	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

3.8.2. 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

I. 制限とガイドライン

NTP 認証を保証する場合、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。

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 3-3 に示します。(ー は相違がないことを示します)

表 3-3 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。

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	
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。
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。
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	―	―	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	―	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	―	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。

II. アクティブピアの NTP 認証の設定

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** } *value*	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** { *peer-name* | *ip-address* } [**vpn-instance** *vpn-instance-name*] **authentication-keyid** *keyid*	―

III. パッシブピアの NTP 認証の設定

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** } *value*	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

3.8.3. ブロードキャストモードの NTP 認証の設定

I. 制限とガイドライン

NTP 認証を保証する場合、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。

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 3-4 に示します。(― は相違がないことを示します)

表 3-4 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。

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	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	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	Yes	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。
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。
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。

II. ブロードキャストクライアントの NTP 認証の設定

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** } *value*	デフォルト：設定なし

操作	コマンド	補足
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

III. ブロードキャストサーバの NTP 認証の設定

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** } *value*	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. interface view に移行する	**interface** *interface-type interface-number*	―
6. ブロードキャストサーバとキーを関連づける	**ntp-service broadcast-server authentication-keyid** *keyid*	デフォルト：設定なし

3.8.4. マルチキャストモードの NTP 認証の設定

I. 制限とガイドライン

NTP 認証を保証する場合、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 とキーの値は同一にする必要があります。

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 3-5 に示します。(― は相違がないことを示します)

表 3-5 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。

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	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	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	Yes	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。
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。
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。

II. マルチキャストクライアントの NTP 認証の設定

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

操作	コマンド	補足
3. NTP 認証キーを設定する	**ntp-service authentication-keyid** *keyid* **authentication-mode md5** { **cipher** | **simple** } *value*	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

III. マルチキャストサーバの NTP 認証の設定

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 認証を有効にする	**ntp-service authentication-keyid** *keyid* **authentication-mode md5** { **cipher** | **simple** } *value*	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. interface view に移行する	**interface** *interface-type interface-number*	―
6. マルチキャストサーバとキーを関連づける	**ntp-service multicast-server** [*ip-address*] **authentication-keyid** *keyid*	デフォルト：設定なし

3.9. 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。

3.9.1. NTP メッセージの送信元インタフェースの設定

I. 制限とガイドライン

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とき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、**ntp-service unicast-server** コマンドあるいは **ntp-service unicast-peer** コマンドで指定したインタフェースは NTP メッセージの送信元インタフェースとして動作します。

ntp-service broadcast-server コマンドあるいは **ntp-service multicast-server** コマンドが設定された場合、ブロードキャスト NTP メッセージあるいはマルチキャスト NTP メッセージの送信元インタフェースは、それぞれのコマンドで設定したインタフェースです。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. NTP メッセージの送信元インタフェースを指定する	**ntp-service source** *interface-type interface-number*	デフォルト：設定なし

3.9.2. インタフェースでの NTP メッセージ受信の無効化

I. インタフェースでの NTP メッセージ受信の無効化

NTP が有効なとき、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。

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. 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

3.9.3. ダイナミックアソシエーションの最大数の設定

I. ダイナミックアソシエーションの最大数の設定

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使用することを防ぐためにダイナミックアソシエーションの数を制限することができます。

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。

II. 制限とガイドライン

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。

III. 設定手順

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

3.9.4. NTP パケットの DSCP 値の設定

I. 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。

II. 設定手順

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

3.10. 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**]

操作	コマンド
NTPサービスステータスの情報を表示する	**display ntp-service status**
装置とNTPサーバ間のネットワーク情報(経路)を表示する	**display ntp-service trace**

3.11. NTP設定例

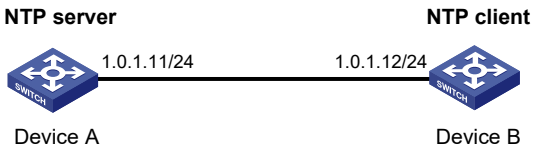
3.11.1. NTP クライアント/サーバモードの設定例

I. ネットワーク要件

図 3-4 に示すように設定します。

- 参照ソースとして Device A の stratum レベル 2 のローカルクロックを設定します。
- クライアントモードで動作するように Device B を設定し、Device B の NTP サーバとして Device A を設定します。

図 3-4 ネットワーク図



II. 設定手順

1. 図 3-4 に示すように各インタフェースの IP アドレスを設定し、Switch A、Switch B が互いに通信できることを確認します。(詳細は省略します)
2. Device A を設定します。

NTP サービスを有効にします。

<DeviceA> system-view

[DeviceA] ntp-service enable

参照ソースとして stratum レベル 2 のローカルクロックを指定します。

[DeviceA] ntp-service refclock-master 2

3. 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 minpoll 6

III. 設定の確認

Device B が Device A に同期しており、Device B の stratum レベルが 3、Device A の stratum レベル 2 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^-10
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
**************************************************************************
[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
```

3.11.2. 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 3-5 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。
- クライアントモードで動作するように Device B を設定し、Device B の NTP サーバとして Device A を指定します。

図 3-5 ネットワーク図



II. 設定手順

1. 図 3-5 に示すように各インタフェースの IP アドレスを設定し、Switch A、Switch B が互いに通信できることを確認します。(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

3. Device A を設定します。

NTP サービスを有効にします。

<DeviceA> system-view

[DeviceA] ntp-service enable

参照ソースとして stratum レベル 2 のローカルクロックを設定します。

[DeviceA] ntp-service refclock-master 2

シンメトリックパッシブピアとして Device B を設定します。

[DeviceA] ntp-service unicast-peer 3.0.1.32

III. 設定の確認

Device B が Device A に同期していることを確認します。

[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^-17
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
```

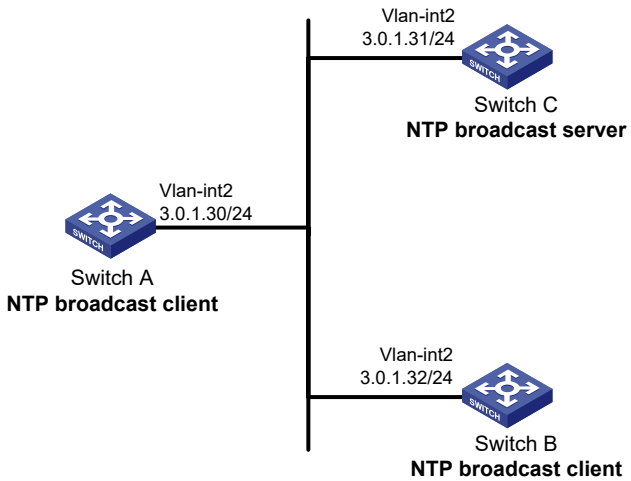
3.11.3. NTP ブロードキャストモードの設定例

I. ネットワーク要件

図 3-6 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、複数の装置間でクロックの同期を行います。

- 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 を通してブロードキャストメッセージを受信します。

図 3-6 ネットワーク図



II. 設定手順

1. 図 3-6 に示すように各インタフェースの IP アドレスを設定し、Switch A、Switch B、Switch C が互いに通信できることを確認します。(詳細は省略します)
2. Switch C を設定します。

NTP サービスを有効にします。

<SwitchC> system-view

[SwitchC] ntp-service enable

参照ソースとして stratum レベル 2 のローカルクロックを設定します。

[SwitchC] ntp-service refclock-master 2

ブロードキャストサーバモードで動作するように Switch C 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送信します。

[SwitchC] interface vlan-interface 2

[SwitchC-Vlan-interface2] ntp-service broadcast-server

3. 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

4. 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

Switch A が Switch C に同期しており、Switch A の stratum レベルが 3、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^-10
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。

[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
```

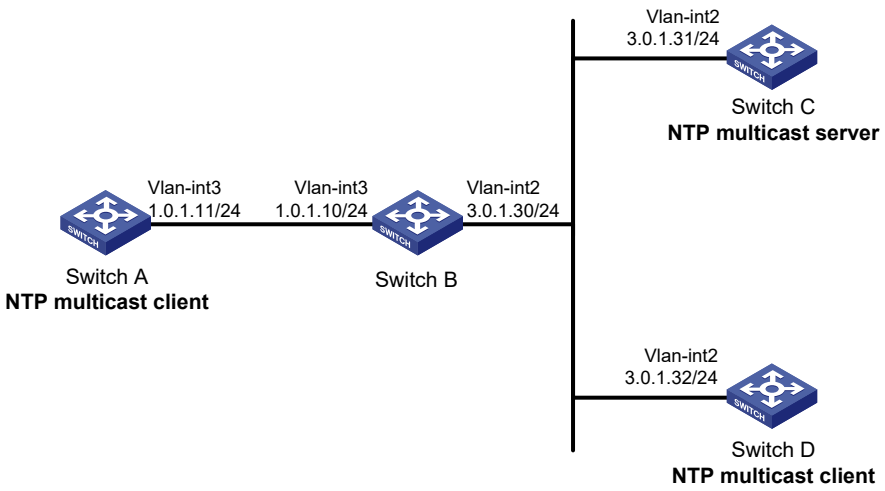
3.11.4. NTP マルチキャストモードの設定例

I. ネットワーク要件

図 3-7 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、複数の装置間でクロックの同期を行います。

- 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。

図 3-7 ネットワーク図



II. 設定手順

この例では、Switch B が IPv4 マルチキャストルーティングをサポートしている必要があります。

1. 図 3-7 に示すように各インタフェースの IP アドレスを設定し、Switch A、Switch B、Switch C、Switch D が互いに通信できることを確認します。(詳細は省略します)
2. Switch C を設定します。

NTP サービスを有効にします。

<SwitchC> system-view

[SwitchC] ntp-service enable

参照ソースとして stratum レベル 2 のローカルクロックを設定します。

[SwitchC] ntp-service refclock-master 2

マルチキャストサーバモードで動作するように Switch C 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。

[SwitchC] interface vlan-interface 2

[SwitchC-Vlan-interface2] ntp-service multicast-server

3. 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

4. 設定の確認

Switch D と Switch C は同一サブネットにあるため、Switch D は以下ができます。

- Switch D は Switch C からマルチキャスト機能を有効にしない状態で Switch C からマルチキャストメッセージを受信できます。
- Switch C と同期することができます。

Switch D が Switch C に同期しており、Device D の stratum レベルが 3、Device C の stratum レベル 2 であることを確認します。

[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^-10
 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。

[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
```

5. Switch B を設定します。

Switch A と Switch C は異なるサブネットにあるため、Switch A が Switch C からマルチキャストメッセージを受信する前に、Switch B でマルチキャスト機能を有効にする必要があります。

IP マルチキャストルーティング、IGMP を有効にします。

<SwitchB> system-view

[SwitchB] multicast routing

[SwitchB-mrib] quit

[SwitchB] interface vlan-interface 2

[SwitchB-Vlan-interface2] pim sm

[SwitchB-Vlan-interface2] quit

[SwitchB] vlan 3

[SwitchB-vlan3] port gigabitethernet 1/0/1

[SwitchB-vlan3] quit

[SwitchB] interface vlan-interface 3

[SwitchB-Vlan-interface3] igmp enable

[SwitchB-Vlan-interface3] igmp static-group 224.0.1.1

[SwitchB-Vlan-interface3] quit

[SwitchB] igmp-snooping

[SwitchB-igmp-snooping] quit

[SwitchB] interface gigabitethernet 1/0/1

[SwitchB- GigabitEthernet1/0/1] igmp-snooping static-group 224.0.1.1 vlan 3

6. 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送信します。

[SwitchA] interface vlan-interface 3

[SwitchA-Vlan-interface3] ntp-service multicast-client

III. 設定の確認

Switch A が Switch C に同期しており、Switch A の stratum レベルが 3、Switch C の stratum レベルが 2 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^-10
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。

[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
```

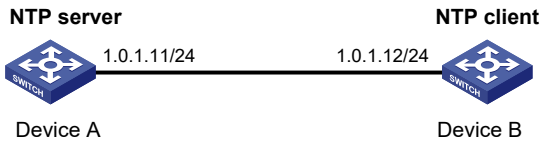
3.11.5. NTP 認証を使用したクライアント/サーバモードの設定例

I. ネットワーク要件

図 3-8 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 3-8 ネットワーク図



II. 設定手順

1. 図 3-8 に示すように各インタフェースの IP アドレスを設定し、Device A、Device B が互いに通信できることを確認します。(詳細は省略します)
2. Device A を設定します。

NTP サービスを有効にします。

<DeviceA> system-view

[DeviceA] ntp-service enable

参照ソースとして stratum レベル 2 のローカルクロックを指定します。

[DeviceA] ntp-service refclock-master 2

3. 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

認証キーを設定し、プレーンテキストでキーを入力します。

[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。

4. Device A で NTP 認証を設定します。

NTP 認証を有効にします。

[DeviceA] ntp-service authentication enable

認証キーを設定し、プレーンテキストでキーを入力します。

[DeviceA] 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。

[DeviceA] ntp-service reliable authentication-keyid 42

III. 設定の確認

Device B が Device A に同期しており、Device B の stratum レベルが 3、Device A の stratum レベルが 2 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^-10
 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
**************************************************************************
 [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
```

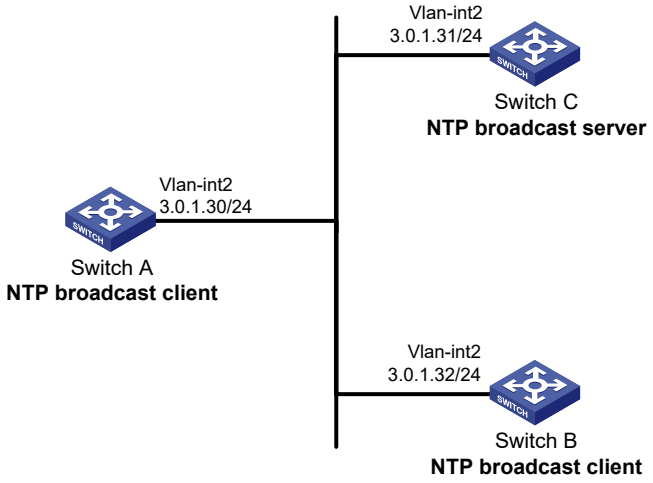
3.11.6. NTP 認証を使用したブロードキャストモードの設定例

I. ネットワーク要件

図 3-9 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、複数の装置間でクロックの同期を行います。Switch A と Switch B は参照ソースを認証します。

- 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 3-9 ネットワーク図



II. 設定手順

1. 図 3-9 に示すように各インタフェースの IP アドレスを設定し、Switch A、Switch B、Switch C、Switch D が互いに通信できることを確認します。(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。認証キーの 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

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。認証キーの 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

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

4. Switch C を設定します。

NTP サービスを有効にします。

<SwitchC> system-view

[SwitchC] ntp-service enable

参照ソースとして stratum レベル 3 のローカルクロックを指定します。

[SwitchC] ntp-service refclock-master 3

ブロードキャストサーバモードで動作するように Switch C 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送信します。

[SwitchC] interface vlan-interface 2

[SwitchC-Vlan-interface2] ntp-service broadcast-server

[SwitchC-Vlan-interface2] quit

5. 設定の確認。

NTP 認証は Switch A と Switch B で有効となっていますが、Switch C では有効でないため、Switch A と Switch B は Switch C とローカルクロックを同期化することができません。Switch B の NTP サービスステータスを表示します。

[SwitchB-Vlan-interface2] display ntp-service status

```
Clock status: unsynchronized
Clock stratum: 16
Reference clock ID: none
```

6. Switch C で NTP 認証を設定します。

Switch C で NTP 認証を有効にします。認証キーの 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。

[SwitchC] ntp-service authentication enable

[SwitchC] ntp-service authentication-keyid 88 authentication-mode md5 simple 123456

[SwitchC] ntp-service reliable authentication-keyid 88

NTP ブロードキャストサーバとして Switch C を指定し、Switch C を認証キー88 に関連づけます。

[SwitchC] interface vlan-interface 2

[SwitchC-Vlan-interface2] ntp-service broadcast-server authentication-keyid 88

III. 設定の確認

Switch C で NTP 認証を有効にした後、Switch A と Switch B は Switch C にローカルクロックを同期化することができます。

Switch B が Switch C に同期しており、Switch B の stratum レベルが 4、Switch C の stratum レベルが 3 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^-10
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。

[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 **10-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 操作 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. 設定作業リスト 4-3
4.3. SNMP エージェントの有効化 4-3
4.4. SNMP バージョンの有効化 4-4
4.5. SNMP の基本パラメータの設定 4-4
4.6. SNMPv1 / SNMPv2c コミュニティの設定 4-6
4.6.1. SNMPv1 / SNMPv2c コミュニティの設定 4-6
4.6.2. 制限とガイドライン 4-6
4.6.3. コミュニティ名による SNMPv1/v2c コミュニティの設定 4-6
4.6.4. SNMPv1/v2c ユーザ作成による SNMPv1/v2c コミュニティの設定 4-6
4.7. SNMPv3 グループとユーザ 4-7
4.7.1. 制限とガイドライン 4-7
4.7.2. SNMPv3 グループとユーザの設定 4-7
4.8. SNMP 通知の設定 4-8
4.8.1. SNMP 通知について 4-8
4.8.2. SNMP notification の有効化 4-8
4.8.3. SNMP notification の送信先の設定 4-9
4.9. SNMP ロギングの設定 4-11
4.10. SNMP alive トラップの有効化と送信間隔の設定 4-11
4.11. SNMP の表示と維持 4-12
4.12. SNMP の設定例 4-12
4.12.1. SNMPv1/SNMPv2c の設定例 4-13
4.12.2. SNMPv3 の設定例 4-14

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。

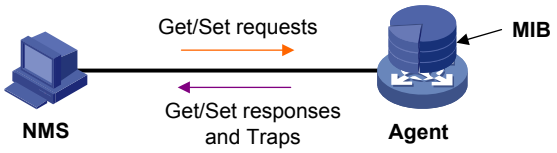
SNMP を使用することで、装置の状態のモニタリング、トラブルシューティング、コリジョンの統計情報やほかの情報の管理を行うため、ネットワーク管理者が、装置の情報を確認し、設定することができます。

4.1.1. SNMP の構造

SNMP は以下の機能で構成されています。

- **SNMP マネージャ**— NMS（network management system）上で動作し、ネットワーク内の SNMP が有効な装置をモニタし、管理します。
- **SNMP エージェント**—管理装置上で動作し、NMS からの要求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 NMS に Trap を送信します。
- **Management Information Base (MIB)**— SNMP マネージャが読み取り、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。

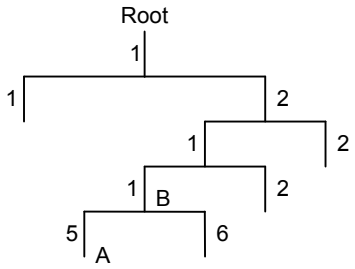
図 4-1 NMS、エージェント、MIB の関係



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 操作

SNMP は以下の基本的な操作を提供します。

- **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**—認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）— 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。

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。

もし同じ 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。

4.2. 設定作業リスト

作業リスト
(必須設定項目) SNMPエージェントの有効化
(必須設定項目) SNMPバージョンの有効化
SNMPの基本パラメータの設定 • （オプション設定項目）SNMP の共通パラメータの設定 • SNMPv1 / SNMPv2c コミュニティの設定 • SNMPv3 グループとユーザの設定
(オプション設定項目) SNMP通知の設定
(オプション設定項目) SNMPロギングの設定
(オプション設定項目) SNMP aliveトラップの有効化と送信間隔の設定

4.3. SNMPエージェントの有効化

I. 制限とガイドライン

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。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. SNMP エージェントを有効にする	**snmp-agent**	デフォルト：無効

4.4. SNMPバージョンの有効化

I. 制限とガイドライン

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。

II. 設定手順

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

同じ設定を複数回割り当てた場合、最後の設定が適用されます。

4.5. SNMPの基本パラメータの設定

I. 制限とガイドライン

SNMP エンジン ID は、SNMP 管理ネットワーク内の装置を固有に識別します。通信の問題を回避するために、SNMP 管理ネットワーク内でローカル SNMP エンジン ID が固有であることを確認します。デフォルトでは、装置に固有の SNMP エンジン ID が割り当てられます。

SNMPv3 ユーザが設定されている場合、必要に応じてローカル SNMP エンジン ID を変更します。この変更によって、設定した SNMPv3 ユーザ名と暗号化された鍵を無効にすることができます。

II. 設定手順

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

操作	コマンド	補足
3. (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。MIB view はデフォルトで、4つのサブツリーを除き16個の固有の MIB viewのレコードを作成することができます。
4. (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
5. (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
6. (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 MIBノードの情報を含む要求と応答のパケットサイズが、エージェントで処理できる最大パケットサイズを超過した場合、NMSからの処理は失敗します。NMSがエージェントにアクセスするため、エージェントが処理できるパケットサイズより大きい値を設定してください。
7. (オプション設定項目) SNMP 応答の DSCP を設定する	**snmp-agent packet response dscp** *dscp-value*	デフォルト：0

4.6. SNMPv1 / SNMPv2c コミュニティの設定

4.6.1. SNMPv1 / SNMPv2c コミュニティの設定

コミュニティ名を使用するか SNMPv1 または SNMPv2c ユーザを作成することにより、SNMPv1 または SNMPv2c コミュニティを作成できます。SNMPv1 または SNMPv2c ユーザを作成すると、コミュニティ名としてユーザ名を使用して自動的にコミュニティが作成されます。

4.6.2. 制限とガイドライン

NMB とエージェントで使用するコミュニティ名が同一にしていることを確認してください。

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。

4.6.3. コミュニティ名による SNMPv1/v2c コミュニティの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. 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** *acl-number* | **acl ipv6** *ipv6-acl-number*] *	デフォルト：設定なし

4.6.4. SNMPv1/v2c ユーザ作成による SNMPv1/v2c コミュニティの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. SNMP グループを作成する。	**snmp-agent group** { **v1** | **v2c** } *group-name* [**read-view** *view-name*] [**write-view** *view-name*] [**notify-view** *view-name*] [**acl** *ipv4-acl-number* | **acl ipv6** *ipv6-acl-number*] *	デフォルト：設定なし

操作	コマンド	補足
3. SNMP グループにユーザを追加する。	**snmp-agent usm-user** { **v1** | **v2c** } *user-name group-name* [**acl** *ipv4-acl-number* | **acl ipv6** *ipv6-acl-number*] *	コミュニティ名としてユーザーネームを使って、システムは自動的にSNMPコミュニティを作成します。

4.7. SNMPv3グループとユーザ

4.7.1. 制限とガイドライン

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	なし	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。

4.7.2. SNMPv3 グループとユーザの設定

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. SNMPv3 グループを作成する	**snmp-agent group v3** *group-name* [**authentication** | **privacy**] [**read-view** *view-name*] [**write-view** *view-name*] [**notify-view** *view-name*] [**acl** *ipv4-acl-number* | **acl ipv6** *ipv6-acl-number* }] *	デフォルト：設定なし
3. (オプション設定項目) プレーン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* }	―
4. 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* | **acl ipv6** *ipv6-acl-number*] *	**cipher**キーワードが指定されると、*auth-password*と*priv-password*は暗号キーとして使用されます。

4.8. SNMP通知の設定

4.8.1. SNMP 通知について

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。

4.8.2. SNMP notification の有効化

I. 制限とガイドライン

必要なときのみ SNMP 通知を有効にしてください。SNMP 通知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ときに SNMP 通知を送信させるためには下記の設定をする必要があります。

- **snmp-agent trap enable standard** [**linkdown** | **linkup**] * コマンドをグローバルで設定し、linkUp/linkDown 通知を有効にします。
- **enable snmp trap updown** コマンドをインタフェースで設定し、linkUp/linkDown 通知を有効にします。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. グローバルに SNMP 通知を有効にする。	**snmp-agent trap enable** [**configuration** | *protocol* | **standard** [**authentication** | **coldstart** | **linkdown** | **linkup** | **warmstart**] * | **system**]	デフォルト：**configuration**、**standard**、**system**の通知がグローバルで有効です。 ほかのSNMP通知はモジュールに依存します。
3. interface view に移行する。	**interface** *interface-type interface-number*	―
4. リンク状態変化の通知を有効にする	**enable snmp trap updown**	デフォルト：有効

4.8.3. SNMP notification の送信先の設定

I. SNMP notification の送信先の設定

ホストに trap あるいは inform する通知を送信する 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 を受信したとき、NMS は trap を受信するとき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。

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とき、SNMP エージェントはキューに通知をバッファします。キューのサイズと通知の保持時間(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。通知は保持時間が満了したとき削除されます。通知のキューが一杯になったとき、最も古い通知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 通知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。

II. SNMP トラップの送信先の設定

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	**snmp-agent target-host trap address udp-domain** { *ipv4-address* | **ipv6** *ipv6-address* } [**udp-port** *port-number*] [**dscp** *dscp-value*] **params securityname** *security-string* [**v1** | **v2c** | **v3** [**authentication** | **privacy**]]	デフォルト：設定なし

操作	コマンド	補足
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 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。

III. SNMP inform の送信先の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. 宛先ホストを設定する	**snmp-agent target-host inform address udp-domain** { *ipv4-address* | **ipv6** *ipv6-address* } [**udp-port** *port-number*] **params securityname** *security-string* { **v2c** | **v3** [**authentication** | **privacy**] }	デフォルト：設定なし SNMPv2c/SNMPv3のみ、informパケットをサポートします。
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 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。

IV. SNMP notification の共通パラメータの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. (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。
3. (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
4. (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

4.9. SNMPロギングの設定

I. SNMP ロギング

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**— MS に SNMP 通知を送信した後、エージェントをロギングします。
- **SNMP 認証失敗**— エージェントの認証に失敗する時に、エージェントは関連情報をロギングします。

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。

II. 制限とガイドライン

必要なときのみ 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。

III. 設定手順

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 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

4.10. SNMP aliveトラップの有効化と送信間隔の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. alive トラップを有効にし送信間隔を設定する	**snmp-agent trap periodical-interval** *interval*	デフォルト：無効

> 🕮 メモ:
>
> **undo snmp-agent trap periodical-interval** コマンドを実行すると、トラップ送信間隔が 60 秒に設定されます。デフォルト値に戻す場合は、**snmp-agent trap periodical-interval 0** コマンドを実行してください。

4.11. 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
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**]
SNMPグループ情報を表示する	**display snmp-agent group** [*group-name*]
ローカルエンジンIDを表示する	**display snmp-agent local-engineid**
MIB view情報を表示する	**display snmp-agent mib-view** [**exclude** | **include** | **viewname** *view-name*]
SNMPエージェント統計情報を表示する	**display snmp-agent statistics**
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**] *
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* | **username** *user-name* | **group** *group-name*] *

4.12. SNMPの設定例

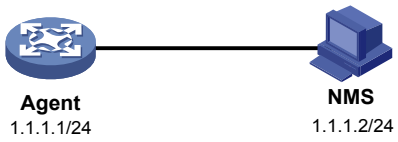
SNMPv1 の設定手順は SNMPv2c 設定手順と同一です。この設定例は SNMPv1 を使用します。

4.12.1. SNMPv1/SNMPv2c の設定例

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
```

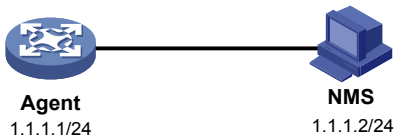
4.12.2. SNMPv3 の設定例

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ときに認証を行います。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. SNMPv3 の設定

1. 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)

   # NMS（SNMPv3 グループ名 managev3group）を作成し、アクセス権限を設定します。

   <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 read-write access をアサインします。MIB-view に test view の system node (OID: 1.3.6.1.2.1.1)と interfaces node (OID:1.3.6.1.2.1.2)配下のオブジェクトを含めます。

[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、認証アルゴリズムに SHA-1、認証キーに 123456TESTauth&!、暗号化アルゴリズムに AES、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

#エージェントへの通知を有効にします。トラップ宛先として 1.1.1.2 の NMS を指定し、ユーザーネームとして VACMtest を指定します。

[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 を選択します。
   - SNMPv3 ユーザ VACMtest を作成します。
   - 認証と暗号化を有効にします。認証アルゴリズムに SHA-1 を選択し、認証キーに 123456TESTauth&!、暗号化アルゴリズムに AES、プライバシーキー123456TESTencr&!を設定します。
   - 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

sysName ノードのための値を Sysname に設定すると、操作は成功します。

インタフェースの Linkup/Down をすると、NMS は linkUP(OID：1.3.6.1.6.3.1.1.5.4)または linkDown(OID：1.3.6.1.6.3.1.1.5.3)を通知します。

目次

このセクションのページは **10-x-x** です。

5 章 RMON 5-1
5.1. 概要 5-1
5.1.1. RMON の動作メカニズム 5-1
5.1.2. RMON グループ 5-1
5.1.3. 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
5.1.4. 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 統計機能について 5-4
5.2.2. RMON Ethernet 統計エントリの作成 5-4
5.2.3. RMON 履歴管理エントリの作成 5-4
5.3. RMON アラーム機能の設定 5-5
5.4. RMON の表示と維持 5-6
5.5. RMON の設定例 5-7
5.5.1. Ethernet 統計グループの設定例 5-7
5.5.2. 履歴グループの設定例 5-8
5.5.3. アラーム機能の設定例 5-9

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の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。

5.1.1. RMON の動作メカニズム

RMON はイーサネットポートのために周期的または継続的にトラフィック統計値を収集し、装置上の MIB オブジェクトの値を監視することができます。統計情報がアラームのしきい値を超えたとき、管理対象の装置は、自動的にイベントを記録するか、通知を NMS に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、さまざまなイベントを通知します。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通知します。

5.1.2. 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。NEC は標準のアラームグループを拡張したプライベートアラームもサポートしています。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 Ethernet 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。

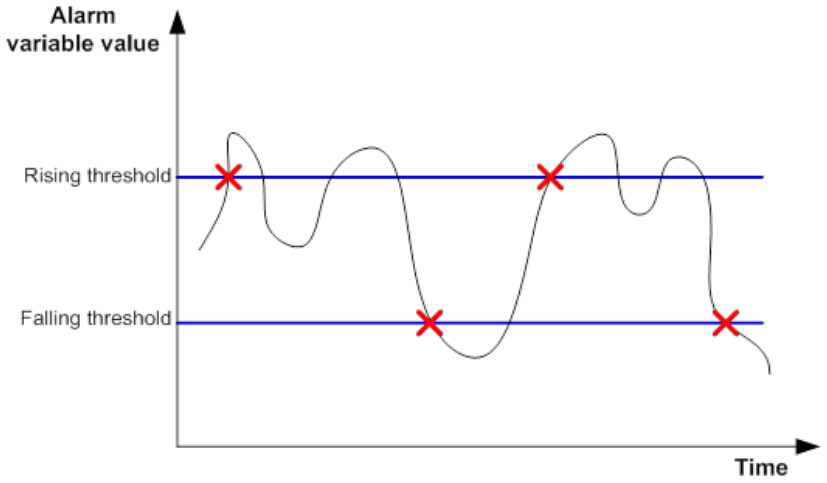
- **Log**—イベントログテーブル内のイベント情報（発生したイベント時間、イベントの内容を含みます）をロギングします。管理装置は、SNMP Get 操作によってログを収集することができます。
- **Trap**—イベントが発生したとき、NMS に SNMP 通知を送信します。
- **Log-Trap**—イベントログテーブルのイベント情報をロギングし、イベントが発生したときに、SNMP 通知を送信します。
- **None**—処理を行いません。

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。例えば、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 上限と下限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開始します。
    - 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開始します。

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。

5.1.3. 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。

5.1.4. 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

5.2.1. RMON 統計機能について

RMON 統計機能は Ethernet 統計グループと履歴グループによって実装されます。統計機能はレイヤ 2 Ethernet インタフェースとレイヤ 3 Ethernet インタフェースでのみ有効です。

Ethernet 統計グループは Ethernet 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。

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。

5.2.2. RMON Ethernet 統計エントリの作成

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 統計情報エントリを作成する	**rmon statistics** *entry-number* [**owner** *text*]	デフォルト：設定なし

5.2.3. RMON 履歴管理エントリの作成

I. 制限とガイドライン

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異なる必要があります。

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。

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*	―

操作	コマンド	補足
3. RMON 履歴管理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

5.3. RMONアラーム機能の設定

I. 制限とガイドライン

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。

- 新しいエントリのパラメータは、既に存在するエントリと同じにすることはできません。
- エントリ数を最大にしないでください。

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

II. 設定要件

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 に通知するために SNMP エージェントを設定してください。

III. 設定手順

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

操作	コマンド	補足
2. (オプション設定項目)RMON 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. RMON アラームエントリを作成する	• アラーム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。

5.4. 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アラームエントリを表示する	**display rmon alarm** [*entry-number*]

操作	コマンド
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*]
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統計情報を表示する	**display rmon statistics** [*interface-type interface-number*]

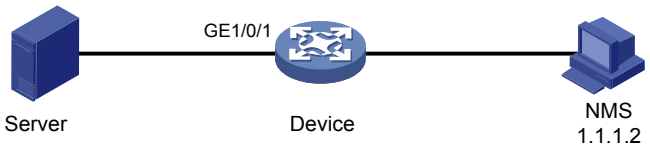
5.5. RMONの設定例

5.5.1. Ethernet 統計グループの設定例

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 Ethernet 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

III. 設定の確認

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
```

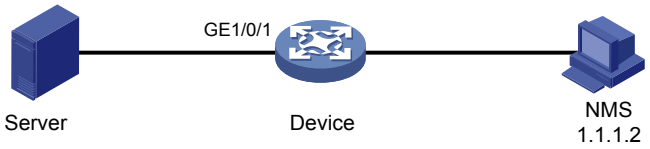
SNMP を通して NMS からトラフィックの統計情報を取得します。(詳細は省略します)

5.5.2. 履歴グループの設定例

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

III. 設定の確認

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
```

SNMP を通して NMS から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)

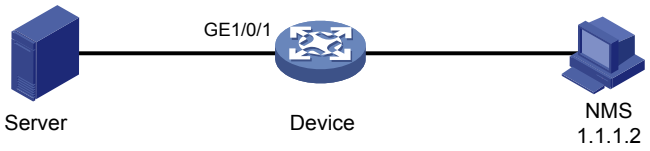
5.5.3. アラーム機能の設定例

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 で RMON Ethernet 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 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 Ethernet統計情報エントリインデックスです。

III. 設定の確認

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
```

NMS でアラームイベントを収集します。(詳細は省略します)

Device でイベントが発生するとき、アラームイベントメッセージが表示されます。

目次

このセクションのページは **10-x-x** です。

6 章 NETCONF 6-1
6.1. 概要 6-1
6.1.1. NETCONF の構成 6-1
6.1.2. NETCONF メッセージフォーマット 6-2
6.1.3. NETCONF の使用方法 6-3
6.1.4. プロトコルと標準 6-4
6.2. NETCONF 設定作業リスト 6-4
6.3. NETCONF セッションの確立 6-5
6.3.1. 制限とガイドライン 6-5
6.3.2. NETCONF セッション属性の設定 6-5
6.3.3. NETCONF over SOAP セッションの確立 6-6
6.3.4. NETCONF over SSH セッションの確立 6-6
6.3.5. NETCONF over Telnet あるいは NETCONF over console セッションの確立 6-7
6.3.6. capability の交換 6-8
6.4. デバイス設定情報の取得 6-8
6.4.1. 制限とガイドライン 6-8
6.4.2. デバイス設定と状態情報の取得 6-9
6.4.3. デフォルト以外の設定の取得 6-11
6.4.4. NETCONF 情報の取得 6-12
6.4.5. YANG ファイルコンテンツの取得 6-12
6.4.6. NETCONF セッション情報の取得 6-13
6.4.7. インタフェーステーブルのデータエントリの取得例 6-14
6.4.8. デフォルト以外の構成データの取得例 6-15
6.4.9. シスログ設定データの取得例 6-16
6.4.10. NETCONF セッション情報の取得例 6-17
6.5. データのフィルタリング 6-18
6.5.1. 概要 6-18
6.5.2. 制限とガイドライン 6-19
6.5.3. テーブルベースのフィルタリング 6-19
6.5.4. 列ベースのフィルタリング 6-19
6.5.5. 正規表現と一致するデータのフィルタリング 6-22
6.5.6. 条件付き一致によるデータのフィルタリング 6-23
6.6. 稼働中の設定のロック、ロック解除 6-25
6.6.1. 設定のロック、ロック解除 6-25
6.6.2. 制限とガイドライン 6-25
6.6.3. 稼働中の設定のロック 6-25
6.6.4. 稼働中の設定のロック解除 6-25
6.6.5. 稼働中の設定のロック例 6-26
6.7. 設定の変更 6-27
6.7.1. <edit-config>オペレーション 6-27
6.7.2. 設定手順 6-27
6.7.3. 設定の変更例 6-28
6.8. 稼働中の設定の保存 6-29

6.8.1. <save>オペレーション ····· 6-29
6.8.2. 制限とガイドライン ····· 6-29
6.8.3. 設定手順 ····· 6-29
6.8.4. 稼働中の設定の保存例 ····· 6-30
6.9. 設定の読み込み ····· 6-31
6.9.1. <load>オペレーション ····· 6-31
6.9.2. 設定とガイドライン ····· 6-31
6.9.3. 設定手順 ····· 6-31
6.10. 設定のロールバック ····· 6-32
6.10.1. 制限とガイドライン ····· 6-32
6.10.2. 設定ファイルにもとづいた設定のロールバック ····· 6-32
6.10.3. ロールバックポイントにもとづいた設定のロールバック ····· 6-32
6.11. NETCONF による CLI オペレーションの実行 ····· 6-37
6.11.1. NETCONF による CLI オペレーション ····· 6-37
6.11.2. 制限とガイドライン ····· 6-37
6.11.3. 設定手順 ····· 6-37
6.11.4. CLI オペレーションの実行例 ····· 6-38
6.12. イベントの登録 ····· 6-39
6.12.1. イベントの登録 ····· 6-39
6.12.2. 制限とガイドライン ····· 6-39
6.12.3. シスログイベントの登録 ····· 6-39
6.12.4. NETCONF によってモニタされるイベントの登録 ····· 6-40
6.12.5. モジュールで報告されたイベントの登録 ····· 6-41
6.12.6. シスログイベントの登録例 ····· 6-43
6.13. NETCONF セッションの終了 ····· 6-44
6.13.1. NETCONF セッションの終了 ····· 6-44
6.13.2. 設定手順 ····· 6-44
6.13.3. 別の NETCONF セッションの終了例 ····· 6-44
6.14. CLI への復帰 ····· 6-45

6章 NETCONF

6.1. 概要

NETCONF (Network Configuration Protocol)は、XML ベースの、フィルタリング機能を持ったネットワーク管理プロトコルです。NETCONF は、ネットワークデバイスを管理、運用するためにプログラマブルなメカニズムを提供します。NETCONF を使用して、デバイスのパラメータ設定、パラメータ値や統計情報を取得できます。

NETCONF メッセージでは、それぞれのデータは固定の要素として包含されています。これにより、同じベンダの異なるデバイスにおいて、同一のアクセス方法と結果出力を提供することが可能になります。異なるベンダのデバイスにおいても、NETCONF メッセージの XML マッピングにより、同一の効果を得ることも可能になります。異なるベンダの異なるデバイスにより構築されるネットワーク環境において、デバイスの設定と管理をシンプルで能率的に行うために、NETCONF をベースにした NMS システムを開発するし、デバイスを簡単に効率的な方法で設定、管理を行うことができます。

6.1.1. NETCONF の構成

NETCONF は 4 つのレイヤ(content レイヤ、operations レイヤ、RPC レイヤと transport protocol レイヤ)から構成されます。

表 6-1 NETCONF レイヤと XML レイヤ

NETCONF レイヤ	XML レイヤ	説明
Content	コンフィグレーションデータ、状態と統計情報	Contentレイヤは、コンフィグレーションデータ、状態と統計情報からなる管理オブジェクトを含んでいます。設定可能なデータの詳細はデバイスのNETCONF XML APIを参照してください。
Operations	<get>,<get-config>,<edit-config>…	Operationsレイヤは、XMLでエンコードされたパラメータにより記述されたRPC処理として実行される、基本的なオペレーションセットを定義します。NETCONFの基本動作には、データ取得、コンフィグレーション、ロックとセッション処理があります。デバイスがサポートするオペレーションについては、セクション10 *システム管理 オペレーションマニュアル*の“*NETCONFサポートオペレーション*”を参照してください。
RPC	<rpc>,<rpc-reply>	RPCレイヤは、シンプルでトランスポート層に依存しない、RPCエンコードのフレーミングメカニズムを提供します。<rpc>要素と<rpc-rely>要素は、NETCONFの要求と応答のデータ(operationsレイヤとcontentレイヤ)を囲むために使用されます。
Transport	Console/Telnet/	transport protocolレイヤは、信頼ある、コネクション型の

NETCONF レイヤ	XML レイヤ	説明
protocol	SSH/HTTP/HTTPS/TLS	シリアルデータリンクを提供します。以下のトランスポートレイヤセッションが有効です。 • TELNET、SSH やコンソールポートから CLI にログインし、NETCONF を操作できます。 • HTTP や HTTPS でログインし、NETCONF や NETCONF over SOAP を操作できます。

6.1.2. NETCONF メッセージフォーマット

I. NETCONF

注意:

XML view で NETCONF を操作する際、XML メッセージの最後に終端文字列”]]>]]”を追加する必要があります。終端文字列を追加しないと、デバイスはメッセージを認識できません。本章での例では、終端文字が省略されています。実際の操作には終端文字を追加してください。

すべての NETCONF メッセージは XML ベースであり、RFC4741 に準拠しています。デバイスが受信するすべての NETCONF メッセージは、実際に処理される前に XML スキーマのチェックをパスしなければなりません。もし XML スキーマチェックに失敗すると、デバイスはクライアントにエラーメッセージを送信します。デバイス、オペレーションデータによってサポートされる NETCONF オペレーションの詳細はデバイスの NETCONF XML API を参照してください。

以下の例は、デバイスの全インタフェースの全パラメータを取得する NETCONF メッセージです。

```
<?xml version="1.0" encoding="utf-8"?>
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <get-bulk>
    <filter type="subtree">
      <top xmlns="http://www.nec.com/netconf/data:1.0">
        <Ifmgr>
          <Interfaces>
                 <Interface/>
          </Interfaces>
        </Ifmgr>
      </top>
    </filter>
  </get-bulk>
</rpc>
```

II. NETCONF over SOAP

すべての NETCONF-over-SOAP メッセージは XML ベースで、RFC4741 準拠です。NETCONF メッセージは SOAP（Simple Object Access Protocol）メッセージ中の<BODY>要素で包含されます。また、NETCONF over SOAP メッセージは、以下のルールに従います。

- SOAP メッセージは、SOAP エンベロープの名前空間を使用しなければなりません。
- SOAP メッセージは、SOAP エンコーディングの名前空間を使用しなければなりません。
- SOAP メッセージは、以下の情報を含むことができません。
  - DTD 参照
  - XML 処理命令

以下の例は、デバイスの全インタフェースのすべてのパラメータを取得する NETCONF-over-SOAP メッセージです。

```
<env:Envelope xmlns:env="http://www.w3.org/2003/05/soap-envelope">
  <env:Header>
    <auth:Authentication env:mustUnderstand="1"
xmlns:auth="http://www.nec.com/netconf/base:1.0">
      <auth:AuthInfo>800207F0120020C</auth:AuthInfo>
    </auth:Authentication>
  </env:Header>
  <env:Body>
    <rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
      <get-bulk>
        <filter type="subtree">
          <top xmlns="http://www.nec.com/netconf/data:1.0">
            <Ifmgr>
              <Interfaces>
                <Interface/>
              </Interfaces>
            </Ifmgr>
          </top>
        </filter>
      </get-bulk>
    </rpc>
  </env:Body>
</env:Envelope>
```

6.1.3. NETCONF の使用方法

NETCONF の表 6-2 に示した方法で、デバイスの運用と設定が可能です。

表 6-2 NETCONF のデバイス設定方法

設定ツール	ログイン方法	補足
CLI	• コンソールポート • SSH • Telnet	NETCONFを実行するには、適切なNETCONFメッセージをCLIのXML viewにコピーします。この方法は、開発とテスト目的です。
専用設定ツール	N/A	この方法を使用するには、NETCONF over SOAP を有効にする必要があります。転送を行うため、NETCONFメッセージはSOAPにカプセル化されます。

6.1.4. プロトコルと標準

- RFC 3339, *Date and Time on the Internet: Timestamps*
- RFC 4741, *NETCONF Configuration Protocol*
- RFC 4742, *Using the NETCONF Configuration Protocol over Secure SHell (SSH)*
- RFC 4743, *Using NETCONF over the Simple Object Access Protocol (SOAP)*
- RFC 5277, *NETCONF Event Notifications*
- RFC 5381, *Experience of Implementing NETCONF over SOAP*
- RFC 5539, *NETCONF over Transport Layer Security (TLS)*
- RFC 6241, *Network Configuration Protocol*

6.2. NETCONF設定作業リスト

作業リスト
(必須設定項目) NETCONFセッションの確立 1. （オプション設定項目）NETCONF セッションの属性の設定 2. NETCONF over SOAP セッションの確立 3. NETCONF over SSH セッションの確立 4. NETCONF over Telnet あるいは NETCONF over console セッションの確立 5. capability の交換
（オプション設定項目）デバイス設定情報の取得 • デバイス設定と状態情報の取得 • デフォルト以外の設定の取得 • YANG ファイルコンテンツの取得 • NETCONF セッション情報の取得
（オプション設定項目）データのフィルタリング • テーブルベースのフィルタリング • 列ベースのフィルタリング
（オプション設定項目）稼働中の設定のロック、ロック解除 • 稼働中の設定のロック • 稼働中の設定のロック解除
（オプション設定項目）設定の変更
（オプション設定項目）設定ファイルの管理 • 稼働中の設定の保存 • 設定の読み込み • 設定のロールバック
（オプション設定項目）NETCONFによるCLIオペレーションの実行
（オプション設定項目）イベントの登録 • シスログイベントの登録 • NETCONF によってモニタされるイベントの登録 • モジュールで報告されたイベントの登録

作業リスト
（オプション設定項目）NETCONFセッションの終了
（オプション設定項目）CLIへの復帰

6.3. NETCONFセッションの確立

6.3.1. 制限とガイドライン

NETCONF セッションが確立した後、装置は自動でクライアントに capability を送信します。ほかの NETCONF オペレーションを実行する前に、デバイスにクライアントの capability を送信する必要があります。

NETCONF オペレーションを実行する前に、デバイスで設定あるいは管理しているユーザがいないことを確認してください。複数のユーザが同時に装置を設定あるいは管理した場合、予想外の結果が生じる可能性があります。

デバイスは **aaa session-limit** コマンドで NETCONF セッション数の最大値を設定することができます。もし上限に達すると、新しいユーザはデバイスにアクセスできません。

6.3.2. NETCONF セッション属性の設定

I. NETCONF のネームスペース

NETCONF は以下のタイプのネームスペースをサポートします。

- **共通ネームスペース**–共通ネームスペースはすべてのモジュールで共有されます。パケットのネームスペースは共通のネームスペースを使用します。ネームスペースは<top>エレメントで示します。モジュールは<top>エレメントの下にリストされます。

  例:

```
<rpc message-id="100" xmlns="urn:ietf:Params:xml:ns:netconf:base:1.0">
   <get-bulk>
      <filter type="subtree">
         <top xmlns="http://www.nec.com/netconf/data:1.0">
            <Ifmgr>
               <Interfaces>
               </Interfaces>
            </Ifmgr>
         </top>
      </filter>
   </get-bulk>
</rpc>
```

II. 設定手順

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

手順	コマンド	補足
2. NETCONF ロギングを有効化する	**netconf log source** { { **agent** | **soap** } * } { **protocol-operation** { **all** | { **action** | **config** | **get** | **session** | **set** | **syntax** | **others** } * } | **verbose** }	デフォルトは、NETCONF ロギングが無効です。

6.3.3. NETCONF over SOAP セッションの確立

I. NETCONF over SOAP

カスタムユーザインタフェースを使用して、デバイスへの NETCONF over SOAP セッションを確立し、NETCONF オペレーションを実行できます。NETCONF over SOAP は、NETCONF メッセージを SOAP メッセージにカプセル化し、HTTP または HTTPS 経由で SOAP メッセージを送信します。

II. 制限とガイドライン

認証ドメインを SOAP 要求の< UserName >パラメータに追加できます。 認証ドメインは、現在の要求でのみ有効です。

III. 設定手順

手順	コマンド	補足
1. system view に移行する	**system-view**	―
2. NETCONF over SOAP を有効化する	**netconf soap** { **http** | **https** } **enable**	デフォルトは、NETCONF over SOAPが無効です。
3. カスタムユーザインタフェースを使用して、デバイスで NETCONF over SOAP セッションを確立する		カスタムユーザインタフェースの詳細は、インタフェースのユーザガイドを参照してください。

6.3.4. NETCONF over SSH セッションの確立

I. 制限とガイドライン

NETCONF メッセージのフォーマットが正しいことを確認する場合、メッセージをコピーして貼り付けます。手動でメッセージを入力しないでください。

NETCONF オペレーションを実行している間は、NETCONF メッセージの貼り付けや Enter キーの押下など、ほかのオペレーションを実行しないでください。

デバイスが NETCONF メッセージを識別するためには、各 NETCONF メッセージの最後に終端文字列“**]]>]]>**”を追加する必要があります。 この文書の例は、必ずしもこの終端文字列を持っているわけではありません。 実際のオペレーションには終端文字列を追加してください。

II. 設定要件

NETCONF over SSH セッションを確立する場合、最初に SSH を通してデバイスにログインしてください。

III. 設定手順

操作	コマンド	補足

SSHセッション上でNETCONFを確立する	必要に応じて以下のどちらかのオプションを実行してください。
	• 次のコマンドを順番に実行して、SSH セッション上で NETCONF を確立する
	  ○ **quit**
	  ○ **xml**
	• カスタムユーザインタフェースを使用して、デバイスで NETCONF over SOAP セッションを確立する
		XML viewプロンプトが表示されるとNETCONF over SSHセッションが正常に確立されます。
		カスタムユーザインタフェースの詳細は、インタフェースのユーザガイドを参照してください。

6.3.5. NETCONF over Telnet あるいは NETCONF over console セッションの確立

I. 制限とガイドライン

NETCONF メッセージのフォーマットが正しいことを確認する場合、メッセージをコピーして貼り付けます。手動でメッセージを入力しないでください。

NETCONF オペレーションを実行している間は、NETCONF メッセージの貼り付けや Enter キーの押下など、ほかのオペレーションを実行しないでください。

デバイスが NETCONF メッセージを識別するためには、各 NETCONF メッセージの最後に終端文字列“**]]>]]>**”を追加する必要があります。 この文書の例は、必ずしもこの終端文字列を持っているわけではありません。 実際のオペレーションには終端文字列を追加してください。

II. 設定要件

NETCONF over SSH セッションを確立する場合、最初に Telnet またはコンソールポートを通してデバイスにログインしてください。

III. 設定手順

操作	コマンド	補足
XML viewに移行する	**xml**	user viewで使用可能です。 XML viewプロンプトが表示されると、NETCONF over Telnet あるいはNETCONF over consoleセッションが正常に確立されます。

6.3.6. capability の交換

I. capability の交換

NETCONF セッションが確立されると、デバイスはその機能をクライアントに送信します。 ほかの NETCONF オペレーションを実行する前に、クライアントの機能をデバイスに送信するためにhello メッセージを使用する必要があります。

II. デバイスからクライアントへの Hello メッセージ

```
<?xml version="1.0" encoding="UTF-8"?><hello
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"><capabilities><capability>urn:ietf:pa
rams:netconf:base:1.1</capability><capability>urn:ietf:params:netconf:writable-runnin
g</capability><capability>urn:ietf:params:netconf:capability:notification:1.0</capabi
lity><capability>urn:ietf:params:netconf:capability:validate:1.1</capability><capabil
ity>urn:ietf:params:netconf:capability:interleave:1.0</capability><capability>urn:nec
:params:netconf:capability:nec-netconf-ext:1.0</capability></capabilities><session-id
>1</session-id></hello>]]>]]>
```

<capabilities> エレメントは装置でサポートします。

<session-id> エレメントは NETCONF セッションに割り当てられて固有の ID を保持します。

III. クライアントからデバイスへの Hello メッセージ

デバイスから hello メッセージを受信した後、次の hello メッセージをコピーして、クライアントがサポートする機能をデバイスに通知します。

```
<hello xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <capabilities>
    <capability>
     capability-set
   </capability>
 </capabilities>
</hello>
```

項目	説明
capability-set	クライアントがサポートする一連の機能を指定します。 各ユーザ定義capabilityセットを囲むには、<capability> タグと</capability>タグを使用します。

6.4. デバイス設定情報の取得

6.4.1. 制限とガイドライン

<get>、<get-bulk>、<get-config>、<get-bulk-config> オペレーションを行う間、NETCONF はクライアントにデータを送信する前に取得したデータにある認識できない文字列を(?)に置き換えます。

<get><netconf-state/></get>オペレーションは、データのフィルタリングをサポートしていません。NETCONF オペレーションの詳細はデバイスの NETCONF XML API を参照してください。

6.4.2. デバイス設定と状態情報の取得

次の NETCONF オペレーションを使用して、デバイス設定と状態情報を取得できます。

- **<get> オペレーション**–指定した条件に一致するすべてのデバイス設定と状態情報を取得します。
- **<get-bulk> オペレーション**–指定したインデックスのあるデータエントリの隣にあるデータエントリからデータエントリを取得します。1 つのデータ入力には、デバイス設定エントリと状態情報エントリが含まれます。 返される出力にはインデックス情報は含まれません。

<get>メッセージと<get-bulk>メッセージは、次のフォーマットを共有します。

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <getoperation>
    <filter>
      <top xmlns="http://www.nec.com/netconf/data:1.0">
          Specify the module, submodule, table name, and column name
      </top>
    </filter>
  </getoperation>
</rpc>
```

項目	説明
getoperation	オペレーション名です。 **get**、**get-bulk**があります。
filter	モジュール名、サブモジュール名、テーブル名、列名などのフィルタ条件を指定します。 • モジュール名を指定すると、指定したモジュールのデータが取得されます。 モジュール名を指定しない場合、操作はすべてのモジュールのデータを取得します。 • サブモジュール名を指定すると、指定したサブモジュールのデータが取得されます。 サブモジュール名を指定しない場合、操作はすべてのサブモジュールのデータを取得します。 • テーブル名を指定すると、指定したテーブルのデータが取得されます。 テーブル名を指定しない場合、操作はすべてのテーブルのデータを取得します。 • インデックス列のみを指定した場合、操作はすべての列のデータを取得します。 索引列およびその他の列を指定すると、その索引列と指定した列のデータが取得されます。

<get-bulk>メッセージは、**count** 属性と **index** 属性を保持できます。

項目	説明
index	インデックスを指定します。 この項目を指定しない場合、インデックス値はデフォルト1で始まります。
count	データエントリの数を指定します。 **count**属性は、次のルールに準拠しています。

項目	説明

	• **count** 属性はモジュールノードおよびテーブルノードに配置できます。 ほかのノードでは、解決できません。
	• **count** 属性がモジュールノードに配置されると、子孫ノードに **count** 属性が含まれていない場合、子孫ノードはこの count 属性を継承します。
	• <get-bulk>操作は、次のいずれかの条件が発生した場合に、指定したインデックスのあるデータエントリから始まる残りのデータエントリをすべて取得します。
	  ○ **count** 属性は指定しません。
	  ○ 一致するデータエントリの数が **count** 属性の値よりも小さいです。

次の<get-bulk>メッセージの例では、**count** 属性と **index** 属性を指定します。

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"
xmlns:xc="http://www.nec.com/netconf/base:1.0">
  <get-bulk>
    <filter type="subtree">
      <top xmlns="http://www.nec.com/netconf/data:1.0"
xmlns:base="http://www.nec.com/netconf/base:1.0">
        <Syslog>
          <Logs xc:count="5">
            <Log>
              <Index>10</Index>
            </Log>
          </Logs>
        </Syslog>
      </top>
    </filter>
  </get-bulk>
</rpc>
```

インタフェース情報を取得する場合、デバイスは、<IfIndex>要素の整数値がインタフェース名またはインデックスを表すかどうかを識別できません。問題を解決するには、**valetype** 属性を使用して値タイプを指定できます。

valtype 属性には、次の値があります。

値	説明
name	<IfIndex> エレメントは名前を持っています。
index	<IfIndex> エレメントはインデックスを持っています。
auto	デフォルトです。 デバイスは、インタフェースの名前として <IfIndex>要素の値を使用します。 一致しない場合、デバイスは、インタフェースのインデックスとして値を使用します。

次の例では、<IfIndex>エレメントの index-type 値を指定します。

```
<rpc xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <getoperation>
```

```
    <filter>
      <top xmlns="http://www.nec.com/netconf/config:1.0"
xmlns:base="http://www.nec.com/netconf/base:1.0">
       <VLAN>
        <TrunkInterfaces>
          <Interface>
            <IfIndex base:valuetype="index">1</IfIndex>
          </Interface>
        </TrunkInterfaces>
       </VLAN>
      </top>
    </filter >
  </getoperation>
</rpc>
```

<get> あるいは < get-bulk> オペレーションが成功した場合、デバイスは取得したデータを次のフォーマットで返します。

```
<?xml version="1.0"?>
 <rpc-reply message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <data>
     Device state and configuration data
  </data>
</rpc-reply>
```

6.4.3. デフォルト以外の設定の取得

<get-config> および <get-bulk-config> オペレーションは、デフォルト以外のすべての設定を取得するために使用されます。<get-config>、<get-bulk-config>メッセージには、データをフィルタするための<filter>エレメントを含めることができます。

<get-config>および<get-bulk-config>メッセージは類似しています。<get-config>メッセージの例を次に示します。

```
<?xml version="1.0"?>
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <get-config>
    <source>
      <running/>
    </source>
    <filter>
      <top xmlns="http://www.nec.com/netconf/config:1.0">
          Specify the module name, submodule name, table name, and column name
      </top>
    </filter>
  </get-config>
</rpc>
```

<get-config>または<get-bulk-config>オペレーションが成功すると、デバイスは取得したデータを次のフォーマットで返します。

```
<?xml version="1.0"?>
```

```
<rpc-reply message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <data>
    Data matching the specified filter
  </data>
</rpc-reply>
```

6.4.4. NETCONF 情報の取得

NETCONF 情報を取得するには<get><netconf-state/></get>メッセージを使用します。

#次のテキストをクライアントにコピーし、NETCONF 情報を取得します。

```
<?xml version="1.0" encoding="UTF-8"?>
  <rpc message-id="m-641" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
    <get>
      <filter type='subtree'>
        <netconf-state xmlns='urn:ietf:params:xml:ns:yang:ietf-netconf-monitoring'>
            <getType/>
        </netconf-state>
      </filter>
    </get>
  </rpc>
```

getType の値を指定しない場合、取得オペレーションはすべての NETCONF 情報を取得します。

getType の値は、次のいずれかのオペレーション指定できます。

操作	説明
capabilities	デバイス機能を取得します。
datastores	デバイスからデータベースを取得します。
schemas	デバイスからYANGファイル名のリストを取得します。
sessions	デバイスからセッション情報を取得します。
statistics	NETCONF統計情報を取得します。

<get><netconf-state/></get>オペレーションが成功すると、デバイスは次のフォーマットで応答を返します。

```
<?xml version="1.0"?>
 <rpc-reply message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <data>
     Retrieved NETCONF information
  </data>
</rpc-reply>
```

6.4.5. YANG ファイルコンテンツの取得

YANG ファイルは、デバイスがサポートする NETCONF オペレーションを保存します。ユーザは、YANG ファイルのコンテンツを取得および分析することによって、サポートされるオペレーションを知ることができます。

YANG ファイルはデバイスソフトウェアに統合され、*yang_identifier@yang_version.yang* のフォーマットで名前が付けられます。**dir** コマンドを実行して YANG ファイル名を表示することはできません。YANG ファイル名の取得方法についてはセクション 10 *システム管理 オペレーションマニュアル*の“*NETCONF*”の“*NETCONF 情報の取得*”を参照してください。

#次のテキストをクライアントにコピーして、**syslog-data@2017-01-01.yang** という名前の YANG ファイルを取得します。

```
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <get-schema xmlns='urn:ietf:params:xml:ns:yang:ietf-netconf-monitoring'>
    <identifier>syslog-data</identifier>
    <version>2017-01-01</version>
    <format>yang</format>
  </get-schema>
</rpc>
```

<get-schema>オペレーションが成功すると、デバイスは次のオペレーションで応答を返します。

```
<?xml version="1.0"?>
<rpc-reply message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <data>
     Content of the specified YANG file
  </data>
</rpc-reply>
```

6.4.6. NETCONF セッション情報の取得

<get-sessions>オペレーションを使用して、デバイスの NETCONF セッション情報を取得します。

#次のメッセージをクライアントにコピーして、デバイスから NETCONF セッション情報を取得します。

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <get-sessions/>
</rpc>
```

<get-sessions> オペレーションが成功すると、デバイスは次のフォーマットで応答を返します。

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <get-sessions>
    <Session>
      <SessionID>Configuration session ID</SessionID>
      <Line>Line information</Line>
      <UserName>Name of the user creating the session</UserName>
      <Since>Time when the session was created</Since>
      <LockHeld>Whether the session holds a lock</LockHeld>
    </Session>
  </get-sessions>
</rpc-reply>
```

6.4.7. インタフェーステーブルのデータエントリの取得例

I. ネットワーク要件

インタフェーステーブルのデータエントリを取得します。

II. 設定手順

XML view に移行します。

```
<Switch> xml
```

#クライアントでサポートされている NETCONF 機能のデバイスに通知します。

```
<hello xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <capabilities>
    <capability>urn:ietf:params:netconf:base:1.0</capability>
  </capabilities>
</hello>
```

#インタフェーステーブルのデータエントリを取得します。

```
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"
xmlns:web="urn:ietf:params:xml:ns:netconf:base:1.0">
  <get-bulk>
    <filter type="subtree">
      <top xmlns="http://www.nec.com/netconf/data:1.0"
xmlns:web="http://www.nec.com/netconf/base:1.0">
        <Ifmgr>
          <Interfaces web:count="1">
          </Interfaces>
        </Ifmgr>
      </top>
    </filter>
  </get-bulk>
</rpc>
```

III. 設定の確認

クライアントが次のテキストを受信すると、<get-bulk>オペレーションが成功します。

```
<rpc-reply xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"
xmlns:web="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="100">
  <data>
    <top xmlns="http://www.nec.com/netconf/data:1.0">
      <Ifmgr>
        <Interfaces>
          <Interface>
            <IfIndex>3</IfIndex>
            <Name>GigabitEthernet1/0/2</Name>
            <AbbreviatedName>GE1/0/2</AbbreviatedName>
            <PortIndex>3</PortIndex>
            <ifTypeExt>22</ifTypeExt>
            <ifType>6</ifType>
            <Description>GigabitEthernet1/0/2 Interface</Description>
```

```
            <AdminStatus>2</AdminStatus>
            <OperStatus>2</OperStatus>
            <ConfigSpeed>0</ConfigSpeed>
            <ActualSpeed>100000</ActualSpeed>
            <ConfigDuplex>3</ConfigDuplex>
            <ActualDuplex>1</ActualDuplex>
          </Interface>
        </Interfaces>
      </Ifmgr>
    </top>
  </data>
</rpc-reply>
```

6.4.8. デフォルト以外の構成データの取得例

I. ネットワーク要件

デフォルト以外の設定データをすべて取得します。

II. 設定手順

XML view に移行します。

```
<Switch> xml
```

#クライアントでサポートされている NETCONF 機能のデバイスに通知します。

```
<hello xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <capabilities>
    <capability>
           urn:ietf:params:netconf:base:1.0
    </capability>
  </capabilities>
</hello>
```

#デフォルト以外のすべての構成データを取得します。

```
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <get-config>
    <source>
      <running/>
    </source>
  </get-config>
</rpc>
```

III. 設定の確認

クライアントが次のテキストを受信すると、<get-config>オペレーションが成功します。

```
<rpc-reply xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"
xmlns:web="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="100">
    <data>
        <top xmlns="http://www.nec.com/netconf/config:1.0">
            <Ifmgr>
                <Interfaces>
```

```
                    <Interface>
                        <IfIndex>1307</IfIndex>
                        <Shutdown>1</Shutdown>
                    </Interface>
                    <Interface>
                        <IfIndex>1308</IfIndex>
                        <Shutdown>1</Shutdown>
                    </Interface>
                    <Interface>
                        <IfIndex>1309</IfIndex>
                        <Shutdown>1</Shutdown>
                    </Interface>
                    <Interface>
                        <IfIndex>1311</IfIndex>
                            <VlanType>2</VlanType>
                    </Interface>
                    <Interface>
                        <IfIndex>1313</IfIndex>
                            <VlanType>2</VlanType>
                    </Interface>
                </Interfaces>
            </Ifmgr>
            <Syslog>
                <LogBuffer>
                    <BufferSize>120</BufferSize>
                </LogBuffer>
            </Syslog>
            <System>
                <Device>
                    <SysName>Sysname</SysName>
                    <TimeZone>
                        <Zone>+11:44</Zone>
                        <ZoneName>beijing</ZoneName>
                    </TimeZone>
                </Device>
            </System>
        </top>
    </data>
</rpc-reply>
```

6.4.9. シスログ設定データの取得例

I. ネットワーク要件

シスログモジュールの構成データを取得します。

II. 設定手順

XML view に移行します。

```
<Switch> xml
```

#クライアントでサポートされている NETCONF 機能のデバイスに通知します。

```
<hello xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <capabilities>
    <capability>
           urn:ietf:params:netconf:base:1.0
    </capability>
  </capabilities>
</hello>
```

シスログモジュールの構成データを取得します。

```
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <get-config>
    <source>
      <running/>
    </source>
    <filter type="subtree">
      <top xmlns="http://www.nec.com/netconf/config:1.0">
        <Syslog/>
      </top>
    </filter>
  </get-config>
</rpc>
```

III. 設定の確認

クライアントが次のテキストを受信すると、<get-config>オペレーションが成功します。

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="100">
    <data>
        <top xmlns="http://www.nec.com/netconf/config:1.0">
            <Syslog>
                    <LogBuffer>
                        <BufferSize>120</BufferSize>
                    </LogBuffer>
            </Syslog>
        </top>
    </data>
</rpc-reply>
```

6.4.10. NETCONF セッション情報の取得例

I. ネットワーク要件

NETCONF セッション情報を取得します。

II. 設定手順

XML view に移行します。

```
<Switch> xml
```

#次のメッセージをクライアントにコピーして、デバイスとの機能を交換します。

```
<hello xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <capabilities>
    <capability>
           urn:ietf:params:netconf:base:1.0
    </capability>
  </capabilities>
</hello>
```

次のメッセージをクライアントにコピーして、デバイス上の現在の NETCONF セッション情報を取得します。

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <get-sessions/>
</rpc>
```

III. 設定の確認

クライアントが次のメッセージを受信すると、オペレーションは正常に実行されます。

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="100">
    <get-sessions>
        <Session>
            <SessionID>1</SessionID>
            <Line>vty0</Line>
            <UserName></UserName>
            <Since>2017-01-07T00:24:57</Since>
            <LockHeld>false</LockHeld>
        </Session>
    </get-sessions>
</rpc-reply>
```

出力には、次の情報が表示されます。

- 既存の NETCONF セッションのセッション ID は 1 です。
- ログインユーザタイプは vty0 です。
- ログイン時間は 2017-01-07T00:24:57 です。
- ユーザは設定のロックを保持しません。

6.5. データのフィルタリング

6.5.1. 概要

フィルタを定義して、<get>、<get-bulk>、<get-config>、または<get-bulk-config>オペレーションを実行するときにフィルタを設定できます。 データのフィルタリングには次のタイプがあります。

- **表ベースのフィルタリング**－テーブル情報をフィルタします。
- **列ベースのフィルタリング**－単一列の情報をフィルタします。

6.5.2. 制限とガイドライン

テーブルベースのフィルタリングを有効にするには、列ベースのフィルタリングを行う前にテーブルベースのフィルタリングを設定する必要があります。

6.5.3. テーブルベースのフィルタリング

I. テーブルベースのフィルタリング

ネームスペースは **http://www.nec.com/netconf/base:1.0** です。属性名は **filter** です。テーブルベースの一致のサポートについては、NETCONF XML API リファレンスを参照してください。

#次のテキストをクライアントにコピーして、IP アドレス 1.1.1.0 と、IPv4 ルーティングテーブルからのマスク長 24 を持つ最長データを取得します。

```
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"
xmlns:nec="http://www.nec.com/netconf/base:1.0">
  <get>
    <filter type="subtree">
      <top xmlns="http://www.nec.com/netconf/data:1.0">
        <Route>
         <Ipv4Routes>
           <RouteEntry nec:filter="IP 1.1.1.0 MaskLen 24 longer"/>
         </Ipv4Routes>
        </Route>
      </top>
    </filter>
  </get>
</rpc>
```

II. 制限とガイドライン

テーブルベースのフィルタリングを使用するには、**filter** 行属性の一致条件を指定します。

6.5.4. 列ベースのフィルタリング

I. 列ベースのフィルタリング

列ベースのフィルタリングには、完全一致フィルタリング、正規表現一致フィルタリング、条件付き一致フィルタが含まれます。完全一致フィルタリングは優先順位がもっとも高く、条件付き一致フィルタリングはもっとも優先順位が低くなります。複数のフィルタ条件を指定すると、優先順位がもっとも高いものが有効になります。

II. 完全一致フィルタリング

完全一致フィルタを実装するために、XML メッセージでエレメント値を指定できます。 複数のエレメント値を指定すると、指定したすべての値に一致するデータが戻されます。

#次のテキストをクライアントにコピーして、UP 状態のすべてのインタフェースの設定データを取得します。

```
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <get>
```

```
    <filter type="subtree">
      <top xmlns="http://www.nec.com/netconf/data:1.0">
        <Ifmgr>
          <Interfaces>
            <Interface>
              <AdminStatus>1</AdminStatus>
            </Interface>
          </Interfaces>
        </Ifmgr>
      </top>
    </filter>
  </get>
</rpc>
```

完全一致フィルタを実装する行の現在のテーブルの列名と同じ属性名を指定することもできます。この属性名に一致する設定データのみが戻されます。上記エレメント値ベースの完全一致フィルタリングと同等の XML メッセージを以下に示します。

```
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <get>
    <filter type="subtree">
      <top
xmlns="http://www.nec.com/netconf/data:1.0"xmlns:data="http://www.nec.com/netconf/dat
a:1.0">
        <Ifmgr>
          <Interfaces>
            <Interface data:AdminStatus="1"/>
          </Interfaces>
        </Ifmgr>
      </top>
    </filter>
  </get>
</rpc>
```

上記の例では、エレメント値ベースの完全一致フィルタリングと属性名ベースの完全一致フィルタリングの両方が、すべてのインタフェースの同じインデックスおよび列情報をアップ状態で取得できることを示しています。

III. 正規表現マッチングフィルタリング

文字による複雑なデータフィルタリングを実装するには、特定の要素に対して **regExp** 属性を追加します。

サポートされるデータ型には、整数、日付と時刻、文字列、IPv4 アドレス、IPv4 マスク、IPv6 アドレス、MAC アドレス、OID、およびタイムゾーンがあります。

#次のテキストをクライアントにコピーし、インタフェースの説明を取得します。すべての文字が A～Z の大文字である必要があります。

```
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"
xmlns:nec="http://www.nec.com/netconf/base:1.0">
  <get-config>
    <source>
      <running/>
```

```
    </source>
    <filter type="subtree">
      <top xmlns="http://www.nec.com/netconf/config:1.0">
        <Ifmgr>
          <Interfaces>
            <Interface>
              <Description nec:regExp="^[A-Z]*$"/>
            </Interface>
          </Interfaces>
        </Ifmgr>
      </top>
    </filter>
  </get-config>
</rpc>
```

IV. 条件付き一致フィルタリング

数字と文字列で複雑なデータフィルタリングを実装するには、特定の要素に **match** 属性を追加できます。表 6-3 に条件付き一致演算子を示します。

表 6-3 条件付き一致演算子

操作	演算子	備考
More than	match="more:*value*"	指定した値より大きい値です。 サポートされるデータ型には、日付、数字、文字列があります。
Less than	match="less:*value*"	指定した値未満の値です。 サポートされるデータ型には、日付、数字、文字列があります。
Not less than	match="notLess:*value*"	指定した値以上の値です。 サポートされるデータ型には、日付、数字、文字列があります。
Not more than	match="notMore:*value*"	指定された値以下の値です。 サポートされるデータ型には、日付、数字、文字列があります。
Equal	match="equal:*value*"	指定した値に等しい値です。 サポートされるデータ型には、日付、数字、文字列、OID、およびBOOLがあります。
Not equal	match="notEqual:*value*"	指定した値と等しくない値です。 サポートされるデータ型には、日付、数字、文字列、OID、およびBOOLがあります。
Include	match="include:*string*"	指定された文字列を含みます。 サポートされるデータ型には文字列のみが含まれます。
Not include	match="exclude:*string*"	指定された文字列を除外します。 サポートされるデータ型には文字列のみが含まれます。
Start with	match="startWith:*string*"	指定した文字列で開始します。 サポートされるデータ型には、文字列とOIDが含まれます。
End with	match="endWith:*string*"	指定した文字列で終了します。 サポートされるデータ型には文字列のみが含まれます。

#次のテキストをクライアントにコピーして、CPU 使用率が 50%以上のエンティティに関する拡張情報を取得します。

```
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"
xmlns:nec="http://www.nec.com/netconf/base:1.0">
  <get>
    <filter type="subtree">
      <top xmlns="http://www.nec.com/netconf/data:1.0">
        <Device>
          <ExtPhysicalEntities>
            <Entity>
              <CpuUsage nec:match="more:50"></CpuUsage>
            </Entity>
          </ExtPhysicalEntities>
        </Device>
      </top>
    </filter>
  </get>
</rpc>
```

6.5.5. 正規表現と一致するデータのフィルタリング

I. ネットワーク要件

Ifmgr モジュールの下の Interfaces テーブルの **Description** 列の **Gigabit** を含むすべてのデータを取得します。

II. 設定手順

XML view に移行します。

```
<Switch> xml
```

#クライアントでサポートされている NETCONF 機能のデバイスに通知します。

```
<hello xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <capabilities>
    <capability>
           urn:ietf:params:netconf:base:1.0
    </capability>
  </capabilities>
</hello>
```

Ifmgr モジュールの下の Interfaces テーブルの **Description** 列の **Gigabit** を含むすべてのデータを取得します。

```
<?xml version="1.0"?>
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"
xmlns:nec="http://www.nec.com/netconf/base:1.0">
  <get>
    <filter type="subtree">
      <top xmlns="http://www.nec.com/netconf/data:1.0">
        <Ifmgr>
          <Interfaces>
```

```
            <Interface>
              <Description nec:regExp="(Gigabit)+"/>
            </Interface>
          </Interfaces>
        </Ifmgr>
      </top>
    </filter>
  </get>
</rpc>
```

III. 設定の確認

クライアントが次のテキストを受信すると、オペレーションは成功します。

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"
xmlns:nec="http://www.nec.com/netconf/base:1.0" message-id="100">
    <data>
        <top xmlns="http://www.nec.com/netconf/data:1.0">
            <Ifmgr>
                <Interfaces>
                    <Interface>
                        <IfIndex>2681</IfIndex>
                        <Description>GigabitEthernet1/0/1 Interface</Description>
                    </Interface>
                    <Interface>
                        <IfIndex>2685</IfIndex>
                        <Description>GigabitEthernet1/0/2 Interface</Description>
                    </Interface>
                    <Interface>
                        <IfIndex>2689</IfIndex>
                        <Description>GigabitEthernet1/0/3 Interface</Description>
                    </Interface>
                 <Interface>
            </Ifmgr>
        </top>
    </data>
</rpc-reply>
```

6.5.6. 条件付き一致によるデータのフィルタリング

I. ネットワーク要件

Ifmgr モジュールの下の Interfaces テーブルで、ifindx 値が 5000 以上の **Name** 列のデータを取得します。

II. 設定手順

XML view に移行します。

```
<Switch> xml
```

#クライアントでサポートされている NETCONF 機能のデバイスに通知します。

```
<hello xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <capabilities>
    <capability>
           urn:ietf:params:netconf:base:1.0
    </capability>
  </capabilities>
</hello>
```

#Ifmgr モジュールの下の Interfaces テーブルで ifindx 値が 5000 以上の **Name** 列のデータを取得します。

```
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"
xmlns:nec="http://www.nec.com/netconf/base:1.0">
  <get>
    <filter type="subtree">
      <top xmlns="http://www.nec.com/netconf/data:1.0">
        <Ifmgr>
          <Interfaces>
            <Interface>
              <IfIndex nec:match="notLess:5000"/>
              <Name/>
            </Interface>
          </Interfaces>
        </Ifmgr>
      </top>
    </filter>
  </get>
</rpc>
```

III. 設定の確認

クライアントが次のテキストを受信すると、オペレーションは成功します。

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"
xmlns:nec="http://www.nec.com/netconf/base:1.0" message-id="100">
    <data>
        <top xmlns="http://www.nec.com/netconf/data:1.0">
            <Ifmgr>
                <Interfaces>
                    <Interface>
                        <IfIndex>7241</IfIndex>
                        <Name>NULL0</Name>
                    </Interface>
                </Interfaces>
            </Ifmgr>
        </top>
    </data>
</rpc-reply>
```

6.6. 稼働中の設定のロック、ロック解除

6.6.1. 設定のロック、ロック解除

CLI、NETCONF、SNMP などのデバイスを設定するには、複数の方法があります。 デバイスの設定、管理、またはトラブルシューティングを行う前に、ほかのユーザがデバイス設定を変更できないように設定をロックできます。構成をロックすると、設定を変更したり、設定をロック解除するために<edit-config>オペレーションを実行できます。ほかのユーザは設定のみを読み込むことができます。

NETCONF セッションを閉じると、システムは設定をロック解除します。 設定を手動でロック解除することもできます。

6.6.2. 制限とガイドライン

<lock>オペレーションは、デバイスの稼働中の設定をロックします。特定のモジュールの設定をロックするために使用することはできません。

6.6.3. 稼働中の設定のロック

稼働中の設定をロックするには、次のテキストをクライアントにコピーします。

```
<?xml version="1.0" encoding="UTF-8"?>
  <rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
    <lock>
      <target>
        <running/>
      </target>
    </lock>
  </rpc>
```

<lock>オペレーションが成功すると、デバイスは次のフォーマットで応答を返します。

```
<?xml version="1.0" encoding="UTF-8"?>
  <rpc-reply message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
     <ok/>
</rpc-reply>
```

6.6.4. 稼働中の設定のロック解除

#次のテキストをクライアントにコピーして、稼働中の設定をロック解除します。

```
<?xml version="1.0" encoding="UTF-8"?>
  <rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
    <unlock>
      <target>
        <running/>
      </target>
```

```
    </unlock>
  </rpc>
```

<unlock> オペレーションが成功すると、デバイスは次のフォーマットで応答を返します。:

```
<?xml version="1.0" encoding="UTF-8"?>
    <rpc-reply message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
      <ok/>
</rpc-reply>
```

6.6.5. 稼働中の設定のロック例

I. ネットワーク要件

デバイス構成をロックして、ほかのユーザがデバイス設定を変更できないようにします。

II. 設定手順

XML view に移行します。

```
<Switch> xml
```

#クライアントでサポートされている NETCONF 機能のデバイスに通知します。

```
<hello xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
    <capabilities>
        <capability>
            urn:ietf:params:netconf:base:1.0
        </capability>
    </capabilities>
</hello>
```

設定をロックします。

```
<?xml version="1.0" encoding="UTF-8"?>
  <rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
    <lock>
      <target>
        <running/>
      </target>
    </lock>
  </rpc>
```

III. 設定の確認

クライアントが次の応答を受信すると、<lock>オペレーションが成功します。

```
<?xml version="1.0" encoding="UTF-8"?>
    <rpc-reply message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
      <ok/>
</rpc-reply>
```

別のクライアントがロック要求を送信すると、デバイスは次の応答を返します。

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
<rpc-error>
  <error-type>protocol</error-type>
```

```
  <error-tag>lock-denied</error-tag>
  <error-severity>error</error-severity>
  <error-message xml:lang="en"> Lock failed because the NETCONF lock is held by another
session.</error-message>
  <error-info>
    <session-id>1</session-id>
  </error-info>
  </rpc-error>
</rpc-reply>
```

出力は、<lock>オペレーションが失敗したことを示します。 セッション ID 1 のクライアントはロックを保持しています。

6.7. 設定の変更

6.7.1. <edit-config>オペレーション

<edit-config>オペレーションは、merge、create、replace、remove、delete、default-operation、error-option、test-option、incremental 属性をサポートします。デバイスがサポートするオペレーションについては、セクション 10 *システム管理 オペレーションマニュアル*の“*NETCONF サポートオペレーション*”を参照してください。

6.7.2. 設定手順

次のテキストをクライアントにコピーして、<edit-config>オペレーションを実行します。

```
<?xml version="1.0"?>
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <edit-config>
    <target><running></running></target>
<error-option>
   error-option
</error-option>
    <config>
      <top xmlns="http://www.nec.com/netconf/config:1.0">
        Specify the module name, submodule name, table name, and column name
      </top>
    </config>
  </edit-config>
</rpc>
```

<error-option>エレメントはオペレーション中に発生するエラーに応じて実行されるアクションを示します。以下に値を示します。

値	説明
stop-on-error	<edit-config>オペレーションを停止します。
continue-on-error	<edit-config>オペレーションを継続します。

値	説明
rollback-on-error	<edit-config>オペレーションが実行される前に設定をロールバックします。 デフォルトでデバイスが設定をロールバックする間、<edit-config>オペレーションは実行することができません。 ロールバック時間がクライアントの待ち時間を超過した場合、クライアントは<edit-config>オペレーションが失敗したと認識し、オペレーションを再度実行します。前回のロールバックが完了していないため、オペレーションは別のロールバックを開始します。このプロセスが繰り返される場合、CPUとメモリリソースが使い果たされ、デバイスが再起動します。 設定のロールバックを行う間、<edit-config>オペレーションを実行できるようにするためには**DisableEditConfigWhenRollback**属性の値を**false**に変更します。

<edit-config> オペレーションが成功すると、デバイスは次のフォーマットで応答を返します。

```
<?xml version="1.0">
<rpc-reply message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <ok/>
</rpc-reply>
```

<get>>オペレーションを実行し、現在のエレメントの値が<edit-config>オペレーションを通して実行された値と同一であることを確認します。

6.7.3. 設定の変更例

I. ネットワーク要件

シスログモジュールのログバッファを 512 に変更します。

II. 設定手順

XML view に移行します。

```
<Switch> xml
```

クライアントでサポートされている NETCONF 機能のデバイスに通知します。

```
<hello xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <capabilities>
    <capability>urn:ietf:params:netconf:base:1.0</capability>
  </capabilities>
</hello>
```

シスログモジュールのログバッファを 512 に変更します。

```
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"
xmlns:web="urn:ietf:params:xml:ns:netconf:base:1.0">
  <edit-config>
    <target>
      <running/>
    </target>
```

```
    <config>
      <top xmlns="http://www.nec.com/netconf/config:1.0" web:operation="merge">
        <Syslog>
          <LogBuffer>
            <BufferSize>512</BufferSize>
          </LogBuffer>
        </Syslog>
      </top>
    </config>
  </edit-config>
</rpc>
```

III. 設定の確認

クライアントが以下のテキストを受信した場合、<edit-config> オペレーションが成功します。

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
    <ok/>
</rpc-reply>
```

6.8. 稼働中の設定の保存

6.8.1. <save>オペレーション

<save>オペレーションは稼働中の設定を設定ファイルに保存し、次回に起動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ファイルを指定します。

6.8.2. 制限とガイドライン

<save>オペレーションはリソースを集中的に使用します。システムリソースが大量に占有されている場合、このオペレーションを実行しないでください。

6.8.3. 設定手順

次のテキストをクライアントにコピーします。

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <save OverWrite="false">
    <file>Configuration file name</file>
  </save>
</rpc>
```

項目	説明
file	名前で設定ファイル.cfgを指定します。名前は記憶媒体の名前から始まる必要があります。 ファイル列を指定する場合、ファイル名が必要です。

項目	説明
	デバイスはテキストとバイナリ形式の設定ファイルの両方に保存することができます。 • 指定された.cfg ファイルが存在しない場合、稼働中の設定ファイルを保存するため、デバイスはバイナリ形式の設定ファイルを作成します。 • ファイル列を指定しない場合、デバイスは稼働中の設定ファイルをテキスト形式とバイナリ形式の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に保存します。
OverWrite	ファイルが既に存在する場合､指定したファイルに上書きするかどうかを指定します。以下の値を使用できます。 • **true**–ファイルを上書きします。 • **false**–ファイルを上書きしません。稼働中のコンフィグレーションは保存することができません。システムはエラーメッセージを表示します。 デフォルトは**true**です。

<save> オペレーションが成功すると、デバイスは次のフォーマットで応答を返します。

```
<?xml version="1.0" encoding="UTF-8"?>
    <rpc-reply message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
      <ok/>
</rpc-reply>
```

6.8.4. 稼働中の設定の保存例

I. ネットワーク要件

稼働中の設定を **config.cfg** に保存します。

II. 設定手順

XML view に移行します。

```
<Switch> xml
```

クライアントでサポートされている NETCONF 機能のデバイスに通知します。

```
<hello xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <capabilities>
    <capability>
           urn:ietf:params:netconf:base:1.0
    </capability>
  </capabilities>
</hello>
```

デバイスの稼働中の設定を **config.cfg** に保存します。

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <save>
    <file>config.cfg</file>
  </save>
</rpc>
```

III. 設定の確認

クライアントが次の応答を受信すると、<save>オペレーションは成功します。

```
<?xml version="1.0" encoding="UTF-8"?>
    <rpc-reply message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
      <ok/>
</rpc-reply>
```

6.9. 設定の読み込み

6.9.1. <load>オペレーション

<load>オペレーションは、設定ファイルから稼働中の設定に次のように設定をマージします。

- 稼働中の設定に存在しない設定を読み込みます。
- 稼働中の設定に存在する設定を上書きします。

6.9.2. 設定とガイドライン

<load>オペレーションを実行するとき、以下の制限とガイドラインに従ってください。

- <load>オペレーションはリソースを集中的に使用します。システムリソースが大量に占有されている場合、このオペレーションを実行しないでください。
- コンフィグレーション成ファイル内の設定によっては、既存の設定と競合する場合があります。ファイルの設定を適用するには、既存の競合する設定を削除し、設定ファイルを読み込みます。

6.9.3. 設定手順

次のテキストをクライアントにコピーして、デバイスの設定ファイルを読み込みます。

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <load>
    <file>Configuration file name</file>
  </load>
</rpc>
```

設定ファイル名は、記憶媒体名で開始する必要があります。.cfg 拡張子を指定します。

<load>オペレーションが成功すると、デバイスは次のフォーマットで応答を返します。

```
<?xml version="1.0" encoding="UTF-8"?>
    <rpc-reply message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
      <ok/>
</rpc-reply>
```

6.10. 設定のロールバック

6.10.1. 制限とガイドライン

<rollback>オペレーションはリソースを集中的に使用します。システムリソースが大量に占有されている場合、このオペレーションを実行しないでください。

デフォルトでは、デバイスが設定をロールバック中に<edit-config>オペレーションを実行できません。設定のロールバック中に<edit-config>オペレーションを実行できるようにするには、**DisableEditConfigWhenRollback** 属性の値を **false** に変更する<action>オペレーションを実行します。

6.10.2. 設定ファイルにもとづいた設定のロールバック

次のテキストをクライアントにコピーして、稼働中の設定を設定ファイルの設定にロールバックします。

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <rollback>
    <file>Specify the configuration file name</file>
  </rollback>
</rpc>
```

<rollback> オペレーションが成功すると、デバイスは次のフォーマットで応答を返します。

```
<?xml version="1.0" encoding="UTF-8"?>
    <rpc-reply message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
      <ok/>
</rpc-reply>
```

6.10.3. ロールバックポイントにもとづいた設定のロールバック

I. ロールバックポイントにもとづいた設定のロールバック

ロールバックポイントにもとづいて稼働中の設定をロールバックするには、次のいずれかの状況が発生します。

- NETCONF クライアントがロールバック要求を送信します。
- NETCONF セッションアイドル時間がロールバックアイドルタイムアウト時間より長いです。
- NETCONF クライアントがデバイスから予期せず切断されました。

II. 制限とガイドライン

複数のユーザが同時にデバイスを設定する場合があります。ほかのユーザが稼働中の設定を変更することを防ぐため、設定をロールバックする前に、システムをロックしてからシステムをロックしてください。

III. 設定手順

1. 稼働中の設定をロックします。詳細はセクション 10 *システム管理 オペレーションマニュアル* の“*NETCONF*”の“*稼働中の設定のロック、ロック解除*”を参照してください。
2. ロールバックポイントにもとづいて設定のロールバックを有効にします。

   # 次のテキストをクライアントにコピーして<save-point>/<begin>オペレーションを実行します。

```
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
      <save-point>
        <begin>
          <confirm-timeout>100</confirm-timeout>
       </begin>
      </save-point>
</rpc>
```

項目	説明
confirm-timeout	ロールバックアイドルタイムアウト時間を指定します。設定範囲は1～65535秒です。デフォルトは600秒です。このアイテムはオプションです。

   <save-point/begin>オペレーションが成功すると、デバイスは次のフォーマットで応答を返します。

```
<rpc-reply message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <data>
    <save-point>
       <commit>
          <commit-id>1</commit-id>
       </commit>
    </save-point>
  </data>
</rpc-reply>
```

3. 稼働中の設定を変更します。詳細はセクション 10 *システム管理 オペレーションマニュアル* “*NETCONF*”の“*設定の変更*”を参照してください。
4. ロールバックポイントをマークします。

   システムは最大 50 のロールバックポイントをサポートしています。 制限に達した場合は、<save-point>/<commit>オペレーションの **force** 属性を指定して、もっとも初期のロールバックポイントを上書きします。

   # 次のテキストをクライアントにコピーして<save-point>/<commit>オペレーションを実行します。

```
  <save-point>
    <commit>
      <label>SUPPORT VLAN<label>
      <comment>vlan 1 to 100 and interfaces. Each vlan used for different custom as
fllows: ……</comment>
     </commit>
  </save-point>
</rpc>
```

   <label> および<comment>エレメントはオプションです。

<save-point>/<commit> オペレーションが成功すると、デバイスは次のフォーマットで応答を返します。:

```
<rpc-reply message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <data>
    <save-point>
       <commit>
          <commit-id>2</commit-id>
       </commit>
    </save-point>
  </data>
</rpc-reply>
```

5. ロールバックポイントの設定の記録を取得します。

次のテキストは、<save point/get-commits>要求のメッセージフォーマットを示します。

```
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <save-point>
    <get-commits>
      <commit-id/>
      <commit-index/>
      <commit-label/>
    </get-commits>
  </save-point>
</rpc>
```

指定したロールバックポイントの設定の記録を取得する場合、<commit-id/>、<commit-index/>、<commit-label/>エレメントを指定します。エレメントが指定されていない場合、オペレーションはすべてのロールバックポイント設定の記録を取得します。

#次のテキストをクライアントにコピーして<save-point>/<get-commits>オペレーションを実行します。

```
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <save-point>
    <get-commits>
      <commit-label>SUPPORT VLAN</commit-label>
    </get-commits>
  </save-point>
</rpc>
```

<save-point/get-commits> オペレーションが成功すると、デバイスは次のフォーマットで応答を返します。

```
<rpc-reply message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
   <data>
      <save-point>
         <commit-information>
           <CommitID>2</CommitID>
           <TimeStamp>Sun Jan 1 11:30:28 2017</TimeStamp>
           <UserName>test</UserName>
           <Label>SUPPORT VLAN</Label>
         </commit-information>
    </save-point>
  </data>
</rpc-reply>
```

6. ロールバックポイントに対応する設定データを取得します。

次のテキストは、<save-point>/<get-commit-information>要求のメッセージフォーマットを示します。

```
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <save-point>
    <get-commit-information>
       <commit-information>
         <commit-id/>
         <commit-index/>
         <commit-label/>
      </commit-information>
      <compare-information>
         <commit-id/>
         <commit-index/>
         <commit-label/>
      </compare-information
    </get-commit-information>
  </save-point>
</rpc>
```

<commit-id/>、<commit-index/>、<commit-label/>のいずれかのエレメントを指定します。<compare-information>エレメントはオプションです。

項目	説明
commit-id	ロールバックポイントを固有に識別します。
commit-index	最近設定された50のロールバックポイントを指定します。 値が0の場合、もっとも最後に設定されたロールポイントです。49がもっとも古く設定されたロールポイントを示します。
commit-label	ロールバックポイントの固有のラベルを指定します。
get-commit-information	もっとも最後に設定されたロールバックポイントに対応する設定データを取得します。

次のテキストをクライアントにコピーして<save-point>/<get-commit-information>オペレーションを実行します。

```
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <save-point>
    <get-commit-information>
               <commit-information>
                  <commit-label>SUPPORT VLAN</commit-label>
               </commit-information>
    </get-commit-information>
  </save-point>
</rpc>
```

<save-point/get-commit-information> オペレーションが成功すると、デバイスは次のフォーマットで応答を返します。

```
<rpc-reply message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
   <data>
```

```
      <save-point>
         <commit-information>
            <content>
               …
               interface vlan 1
               …
            </content>
         </commit-information>
      </save-point>
   </data>
</rpc-reply>
```

7. ロールバックポイントにもとづいて設定をロールバックします。

   構成は、NETCONF セッションアイドルタイマが満了したときに、最後に設定されたロールバックポイントにもとづいて自動的にロールバックすることもできます。

   # 次のテキストをクライアントにコピーして<save-point>/<rollback>オペレーションを実行します。

```
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <save-point>
    <rollback>
      <commit-id/>
      <commit-index/>
      <commit-label/>
    </rollback>
  </save-point>
</rpc>
```

   <commit-id/>、<commit-index/>、<commit-label/>のいずれかのエレメントを指定します。エレメントが指定されていない場合、オペレーションは最後に構成されたロールバックポイントにもとづいて設定をロールバックします。

項目	説明
commit-id	ロールバックポイントを固有に識別します。
commit-index	最近設定された50のロールバックポイントを指定します。 値が0の場合、もっとも最後に設定されたロールポイントです。49がもっとも古く設定されたロールポイントを示します。
commit-label	ロールバックポイントの固有のラベルを指定します。

   <save-point/rollback> オペレーションが成功すると、デバイスは次のフォーマットで応答を返します。

```
<rpc-reply message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <ok></ok>
</rpc-reply>
```

8. ロールバックの設定を終了します。

   # 次のテキストをクライアントにコピーして<save-point>/<end>オペレーションを実行します。

```
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <save-point>
    <end/>
  </save-point>
</rpc>
```

<save-point/end> オペレーションが成功すると、デバイスは次のフォーマットで応答を返します。:

```
<rpc-reply message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
   <ok/>
</rpc-reply>
```

9. 設定をロック解除します。詳細はセクション 10 *システム管理 オペレーションマニュアル*の“*NETCONF*”の“*稼働中の設定のロック、ロック解除*”を参照してください。

6.11. NETCONFによるCLIオペレーションの実行

6.11.1. NETCONF による CLI オペレーション

デバイスを設定するために、XML メッセージにコマンドラインを含めることができます。

6.11.2. 制限とガイドライン

NETCONF を介した CLI オペレーションはリソースを集中的に使用します。次のタスクを実行しないことを推奨します。

- 複数のコマンド行を 1 つの XML メッセージに含めます。
- ほかのユーザが NETCONF の CLI オペレーションを実行している場合、NETCONF を使用して CLI オペレーションを実行します。

6.11.3. 設定手順

次のテキストをクライアントにコピーしてコマンドを実行します。

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <CLI>
    <Execution>
      Commands
    </Execution>
  </CLI>
</rpc>
```

<Execution>エレメントには、1 行に 1 つのコマンドを持つ複数のコマンドを含めることができます。

CLI オペレーションが成功すると、デバイスは次のフォーマットで応答を返します。:

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <CLI>
```

```
    <Execution>
      <![CDATA[Responses to the commands]]>
    </Execution>
  </CLI>
</rpc-reply>
```

6.11.4. CLI オペレーションの実行例

I. ネットワーク要件

デバイスに **display vlan** コマンドを送信します。

II. 設定手順

XML view に移行します。

<Switch> xml

#クライアントでサポートされている NETCONF 機能のデバイスに通知します。

```
<hello xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <capabilities>
    <capability>
           urn:ietf:params:netconf:base:1.0
    </capability>
  </capabilities>
</hello>
```

次のテキストをクライアントにコピーして、**display vlan** コマンドを実行します。

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <CLI>
    <Execution>
         display vlan
    </Execution>
  </CLI>
</rpc>
```

III. 設定の確認

クライアントが次のテキストを受信すると、オペレーションは成功します。

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <CLI>
    <Execution><![CDATA[
<Switch>display vlan
 Total VLANs: 1
 The VLANs include:
 1(default)
   ]]>
   </Execution>
  </CLI>
</rpc-reply>
```

6.12. イベントの登録

6.12.1. イベントの登録

デバイスでイベントが発生すると、デバイスはイベントに関する情報をイベントに登録している NETCONF クライアントに送信します。

6.12.2. 制限とガイドライン

登録は、現在のセッションでのみ有効です。 セッションが終了するとキャンセルされます。

登録するイベントストリームを指定しない場合、デバイスはシスログイベント通知を NETCONF クライアントに送信します。

6.12.3. シスログイベントの登録

次のメッセージをクライアントにコピーして、登録を完了します。

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <create-subscription  xmlns="urn:ietf:params:xml:ns:netconf:notification:1.0">
    <stream>NETCONF</stream>
      <filter>
        <event xmlns="http://www.nec.com/netconf/event:1.0">
          <Code>code</Code>
            <Group>group</Group>
              <Severity>severity</Severity>
        </event>
      </filter>
      <startTime>start-time</startTime>
      <stopTime>stop-time</stopTime>
   </create-subscription>
</rpc>
```

項目	説明
stream	イベントストリームを指定します。シスログイベントストリームの名前は**NETCONF**です。
event	イベントを指定します。登録できるイベントについては、デバイスのシステムログメッセージを参照してください。
code	ログメッセージの記号シンボルを指定します。
group	ログメッセージのモジュール名を指定します。
severity	ログメッセージのseverityレベルを指定します。
start-time	登録の開始時間を指定します。
stop-time	登録の終了時間を指定します。

登録が成功すると、デバイスは次のフォーマットで応答を返します。

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply message-id="100" xmlns:netconf="urn:ietf:params:xml:ns:netconf:base:1.0">
    <ok/>
</rpc-reply>
```

登録が失敗した場合、デバイスは次のフォーマットでエラーメッセージを返します。

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
<rpc-error>
   <error-type>error-type</error-type>
   <error-tag>error-tag</error-tag>
   <error-severity>error-severity</error-severity>
   <error-message xml:lang="en">error-message</error-message>
</rpc-error>
</rpc-reply>
```

エラーメッセージの詳細については、RFC4741 を参照してください。

6.12.4. NETCONF によってモニタされるイベントの登録

この節の説明に従ってイベントを登録すると、NETCONF は定期的に登録されたイベントをポーリングし、登録条件に一致するイベントを NETCONF クライアントに送信します。

次のメッセージをクライアントにコピーして、登録を完了します。

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
<create-subscription xmlns='urn:ietf:params:xml:ns:netconf:notification:1.0'>
  <stream>NETCONF_MONITOR_EXTENSION</stream>
  <filter>
    <NetconfMonitor xmlns='http://www.nec.com/netconf/monitor:1.0'>
      <XPath>XPath</XPath>
      <Interval>interval</Interval>
      <ColumnConditions>
        <ColumnCondition>
          <ColumnName>ColumnName</ColumnName>
          <ColumnValue>ColumnValue</ColumnValue>
          <ColumnCondition>ColumnCondition</ColumnCondition>
        </ColumnCondition>
      </ColumnConditions>
      <MustIncludeResultColumns>
        <ColumnName>columnName</ColumnName>
      </MustIncludeResultColumns>
    </NetconfMonitor>
  </filter>
<startTime>start-time</startTime>
<stopTime>stop-time</stopTime>
</create-subscription>
```

```
</rpc>
```

項目	説明
stream	イベントストリームを指定します。イベントストリームの名前は**NETCONF_MONITOR_EXTENSION**です。
NetconfMonitor	イベントのフィルタ情報を指定します。
XPath	*ModuleName*[/*SubmoduleName*]/*TableName* のフォーマットでイベントのパスを指定します。
interval	登録条件に一致するイベントを取得するためのNETCONFの間隔を指定します。設定範囲は1~4294967秒です。 デフォルトは300秒です。
ColumnName	列名を[*GroupName*.]*ColumnName*のフォーマットで指定します。
ColumnValue	基準値を指定します。
ColumnCondition	オペレータを指定します。 • **more** • **less** • **notLess** • **notMore** • **equal** • **notEqual** • **include** • **exclude** • **startWith** • **endWith** 基準値のタイプに従ってオペレータを選択します。
start-time	登録の開始時間を指定します。
stop-time	登録の終了時間を指定します。

サブスクリプションが成功すると、デバイスは次のフォーマットで応答を返します。

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply message-id="100" xmlns:netconf="urn:ietf:params:xml:ns:netconf:base:1.0">
    <ok/>
</rpc-reply>
```

6.12.5. モジュールで報告されたイベントの登録

この節の説明に従ってイベントを登録すると、指定されたモジュールは登録されたイベントをNETCONF に報告します。 NETCONF は、イベントを NETCONF クライアントに送信します。

次のメッセージをクライアントにコピーして、登録を完了します。

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"
xmlns:xs="http://www.nec.com/netconf/base:1.0">
<create-subscription xmlns="urn:ietf:params:xml:ns:netconf:notification:1.0">
```

```
<stream>XXX_STREAM</stream>
   <filter type="subtree">
<event xmlns="http://www.nec.com/netconf/event:1.0/xxx-features-list-name:1.0">
       <ColumnName xs:condition="Condition">value</ColumnName>
</event>
</filter>
<startTime>start-time</startTime>
<stopTime>stop-time</stopTime>
</create-subscription>
</rpc>
```

属性	説明
stream	イベントストリームを指定します。
event	イベント名を指定します。 イベントストリームには、複数のイベントが含まれます。 イベントはイベントストリームと同じネームスペースを使用します。
ColumnName	列の名前を指定します。
ColumnCondition	オペレータを指定します。 • **more** • **less** • **notLess** • **notMore** • **equal** • **notEqual** • **include** • **exclude** • **startWith** • **endWith** 基準値のタイプに従ってオペレータを選択します。
value	列の基準値を指定します。
start-time	登録の開始時間を指定します。
stop-time	登録の終了時間を指定します。

サブスクリプションが成功すると、デバイスは次のフォーマットで応答を返します。

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply message-id="100" xmlns:netconf="urn:ietf:params:xml:ns:netconf:base:1.0">
    <ok/>
</rpc-reply>
```

6.12.6. シスログイベントの登録例

I. ネットワーク要件

時間制限なしでシスログイベントを登録するようにクライアントを設定します。登録が正常に終了すると、デバイスとクライアント間のセッションが終了する前に、デバイス上のすべてのイベントがクライアントに送信されます。

II. 設定手順

XML view に移行します。

```
<Switch> xml
```

#クライアントでサポートされている NETCONF 機能のデバイスに通知します。

```
<hello xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <capabilities>
    <capability>
            urn:ietf:params:netconf:base:1.0
    </capability>
  </capabilities>
</hello>
```

時間制限なしのシスログイベントを登録します。

```
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <create-subscription xmlns="urn:ietf:params:xml:ns:netconf:notification:1.0">
    <stream>NETCONF</stream>
  </create-subscription>
</rpc>
```

III. 設定の確認

#クライアントが次の応答を受信した場合、登録は正常に終了します。

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="100">
    <ok/>
</rpc-reply>
```

#別のクライアント(192.168.100.130)がデバイスにログインすると、デバイスは、すべてのイベントを登録しているクライアントに通知を送信します。

```
<?xml version="1.0" encoding="UTF-8"?>
<notification xmlns="urn:ietf:params:xml:ns:netconf:notification:1.0">
    <eventTime>2011-01-04T12:30:52</eventTime>
    <event xmlns="http://www.nec.com/netconf/event:1.0">
        <Group>SHELL</Group>
        <Code>SHELL_LOGIN</Code>
        <Slot>1</Slot>
        <Severity>Notification</Severity>
        <context>VTY logged in from 192.168.100.130.</context>
    </event>
</notification>
```

6.13. NETCONFセッションの終了

6.13.1. NETCONF セッションの終了

NETCONF を使用すると、1 つのクライアントがほかのクライアントの NETCONF セッションを終了できます。 セッションが終了したクライアントは、user view に戻ります。

6.13.2. 設定手順

#次のメッセージをクライアントにコピーし、NETCONF セッションを終了します。

```
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <kill-session>
    <session-id>
      Specified session-ID
    </session-id>
  </kill-session>
</rpc>
```

<kill-session> オペレーションが成功すると、デバイスは次のフォーマットで応答を返します。:

```
<?xml version="1.0" encoding="UTF-8"?>
    <rpc-reply message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
      <ok/>
</rpc-reply>
```

6.13.3. 別の NETCONF セッションの終了例

I. ネットワーク要件

セッション ID 1 のユーザはセッション ID 2 のセッションを終了します。

II. 設定手順

XML view に移行します。

```
<Switch> xml
```

クライアントでサポートされている NETCONF 機能のデバイスに通知します。

```
<hello xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <capabilities>
    <capability>
           urn:ietf:params:netconf:base:1.0
    </capability>
  </capabilities>
</hello>
```

セッション ID 2 でセッションを終了します。

```
<rpc message-id="100"xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <kill-session>
    <session-id>2</session-id>
```

```
  </kill-session>
</rpc>
```

III. 設定の確認

クライアントが次のテキストを受信すると、セッション ID 2 の NETCONF セッションが終了し、セッション ID 2 のクライアントが XML view から user view に戻ります。

```
<?xml version="1.0" encoding="UTF-8"?>
  <rpc-reply message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
    <ok/>
</rpc-reply>
```

6.14. CLIへの復帰

I. 制限とガイドライン

XML view から CLI に戻る前に、デバイスとクライアント間の capability の交換を最初に完了する必要があります。

II. 設定手順

次のテキストをクライアントにコピーして、XML view から CLI に戻ります。

```
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
   <close-session/>
</rpc>
```

デバイスが close-session 要求を受信すると、次の応答を送信し、CLI の user view に戻ります。

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
   <ok/>
</rpc-reply>
```

目次

このセクションのページは **10-x-x** です。

7 章 NETCONF サポートオペレーション 7-1
7.1. NETCONF サポートオペレーション 7-1
7.1.1. action 7-1
7.1.2. CLI 7-1
7.1.3. close-session 7-2
7.1.4. edit-config: create 7-2
7.1.5. edit-config: delete 7-3
7.1.6. edit-config: merge 7-3
7.1.7. edit-config: remove 7-4
7.1.8. edit-config: replace 7-4
7.1.9. edit-config: test-option 7-4
7.1.10. edit-config: default-operation 7-5
7.1.11. edit-config: error-option 7-6
7.1.12. edit-config: incremental 7-7
7.1.13. get 7-8
7.1.14. get-bulk 7-8
7.1.15. get-bulk-config 7-9
7.1.16. get-config 7-9
7.1.17. get-sessions 7-10
7.1.18. kill-session 7-10
7.1.19. load 7-10
7.1.20. lock 7-11
7.1.21. rollback 7-11
7.1.22. save 7-11
7.1.23. unlock 7-12

7章 NETCONF サポートオペレーション

この章では、Comware7 で使用可能な NETCONF オペレーションについて説明します。

7.1. NETCONFサポートオペレーション

7.1.1. action

説明

このオペレーションは、デフォルト以外の設定 (リセットアクションなど) のアクションを実行します。

XML 設定例

すべてのインタフェースの統計情報をクリアします。

```
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <action>
    <top xmlns="http://www.nec.com/netconf/action:1.0">
      <Ifmgr>
            <ClearAllIfStatistics>
                <Clear>
                </Clear>
        </ClearAllIfStatistics>
      </Ifmgr>
    </top>
  </action>
</rpc>
```

7.1.2. CLI

説明

このオペレーションは CLI コマンドを実行します。

request メッセージは、<CLI>エレメント内のコマンドを囲みます。応答メッセージは、<CLI>エレメント内のコマンド出力を囲みます。

次のエレメント内を使用してコマンドを実行できます。

- **Execution**—user view でコマンドを実行します。
- **Configuration**— system view でコマンドを実行します。system view の下位の view でコマンドを実行する場合、最初に<Configuration>エレメントを使用して view を移行します。

  このエレメントを使用するには、**exec-use-channel** 属性を含め、属性の値を指定します。

  - **false**ーチャンネルを使用せずにコマンドを実行します。

- **true**ー一時チャネルを使用してコマンドを実行します。チャンネルは実行後自動的に閉じます。
- **persist**ーセッションの永続チャネルを使用してコマンドを実行します。

  永続チャネルを使用するには、まず<Open-channel>オペレーションを実行して永続チャネルを開きます。 そうしないと、システムは自動的に永続チャネルを開きます。

  永続チャネルを使用した後、<Close-channel>オペレーションを実行してチャネルを閉じ、system view に戻ります。 <Open-channel>オペレーションを実行しないと、システムは view 内に留まり、view 内の後続のコマンドを実行します。

NETCONF セッションは、1 つの永続チャネルのみをサポートしますが、複数の一時チャネルをサポートします。

NETCONF は対話型コマンドの実行をサポートしていません。

user view を終了するためにチャネルを使用して **quit** コマンドを実行することはできません。

XML 設定例

#チャネルを使用せずに、system view で **display this** コマンドを実行します。

```
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <CLI>
     <Configuration exec-use-channel="false">display this</Configuration>
  </CLI>
</rpc>
```

7.1.3. close-session

説明

このオペレーションは、現在の NETCONF セッションを終了し、設定のロックを解除し、セッションで使用されるリソース(例えばメモリ)を解放します。 このオペレーションの後、XML view を終了します。

XML 設定例

現在の NETCONF セッションを終了します。

```
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
<close-session/>
</rpc>
```

7.1.4. edit-config: create

説明

このオペレーションにより、ターゲット設定アイテムが作成されます。

<edit-config>オペレーションで **create** 属性を使用するには、ターゲット設定アイテムを指定する必要があります。

- テーブルがターゲット設定項目の作成をサポートしており、項目が存在しない場合は、項目が作成され、項目が設定されます。
- 指定されたアイテムがすでに存在する場合は、データが存在するエラーメッセージが返されます。

XML 設定例

#バッファサイズを 120 に設定します。

```
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"
xmlns:xc="urn:ietf:params:xml:ns:netconf:base:1.0">
  <edit-config>
    <target>
      <running/>
    </target>
    <config>
      <top xmlns="http://www.nec.com/netconf/config:1.0">
        <Syslog xmlns="http://www.nec.com/netconf/config:1.0" xc:operation="create">
           <LogBuffer>
             <BufferSize>120</BufferSize>
          </LogBuffer>
        </Syslog>
      </top>
    </config>
  </edit-config>
</rpc>
```

7.1.5. edit-config: delete

説明

このオペレーションにより、指定された設定が削除されます。

- 指定したターゲットにテーブルインデックスのみがある場合は、指定したターゲットのすべての設定が削除され、ターゲット自体が削除されます。
- 指定したターゲットにテーブルインデックスおよび設定データがある場合、このターゲットの指定された設定データが削除されます。
- 指定したターゲットが存在しない場合は、ターゲットが存在しないことを示すエラーメッセージが戻されます。

XML 設定例

構文は、**create** 属性を持つ edit-config メッセージと同じです。**create** オペレーションから **delete** にオペレーション属性を変更します。

7.1.6. edit-config: merge

説明

このオペレーションは、ターゲット設定アイテムを稼働中の設定にコミットします。

<edit-config>オペレーションで **merge** 属性を使用するには、ターゲット設定アイテム(特定のレベルで)を指定する必要があります。

- 指定したアイテムが存在する場合、オペレーションはアイテムの設定を直接更新します。
- 指定した項目が存在しない場合は、オペレーションは項目を作成し、項目を設定します。
- 指定したアイテムが存在しない場合は、作成することができず、エラーメッセージが返されます。

XML 設定例

構文は、**create** 属性を持つ edit-config メッセージと同じです。**create** オペレーションから **merge** オペレーション属性を変更します。

7.1.7. edit-config: remove

説明

このオペレーションにより、指定された設定が削除されます。

- 指定したターゲットにテーブルインデックスのみがある場合は、指定したターゲットのすべての設定が削除され、ターゲット自体が削除されます。
- 指定したターゲットにテーブルインデックスおよび設定データがある場合、このターゲットの指定された設定データが削除されます。
- 指定したターゲットが存在しない場合、または XML メッセージがターゲットを指定しない場合、成功メッセージが返されます。

XML 設定例

構文は、**create** 属性を持つ edit-config メッセージと同じです。**create** オペレーションから **remove** オペレーション属性を変更します。

7.1.8. edit-config: replace

説明

このオペレーションは、指定された設定を置き換えます。

- 指定されたターゲットが存在する場合、オペレーションは、メッセージ内の設定にターゲットの設定を置き換えます。
- 指定されたターゲットが存在しないが、作成可能な場合、オペレーションはターゲットを作成してから設定を適用します。
- 指定したターゲットが存在せず、作成できない場合は、オペレーションは実行されず、invalid-value エラーメッセージが返されます。

XML 設定例

構文は、**create** 属性を持つ edit-config メッセージと同じです。**create** オペレーションから **replace** にオペレーション属性を変更します。

7.1.9. edit-config: test-option

説明

このオペレーションは、<edit-configure>オペレーションで設定アイテムをコミットするかどうかを決定します。<test-option>エレメントには、次のいずれかの値があります。

- **test-then set**ー構文チェックを実行し、項目がチェックにパスした場合に項目をコミットします。項目がチェックに失敗すると、項目はコミットされません。 これはデフォルトの test-option 値です。
- **set**ー構文チェックを実行せずにアイテムをコミットします。

- **test only**ー構文チェックのみを実行します。 アイテムがチェックを通過すると、成功メッセージが返されます。 それ以外の場合は、エラーメッセージが返されます。

XML 設定例

#インタフェースの設定をテストします。

```
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <edit-config>
    <target>
      <running/>
    </target>
    <test-option>test-only</test-option>
    <config xmlns:xc="urn:ietf:params:xml:ns:netconf:base:1.0">
      <top xmlns="http://www.nec.com/netconf/config:1.0">
        <Ifmgr xc:operation="merge">
          <Interfaces>
            <Interface>
              <IfIndex>262</IfIndex>
              <Description>222</Description>
                <ConfigSpeed>2</ConfigSpeed>
                <ConfigDuplex>1</ConfigDuplex>
               </Interface>
          </Interfaces>
        </Ifmgr>
      </top>
    </config>
  </edit-config>
</rpc>
```

7.1.10. edit-config: default-operation

説明

このオペレーションは、デフォルトのオペレーション方式を使用して、デバイスの稼働中の設定を変更します。

NETCONF は、**merge**、**create**、**delete**、**replace** のオペレーション属性のいずれかを使用して設定を変更します。edit-config メッセージのオペレーション属性を指定しない場合、NETCONF はデフォルトオペレーション方式を使用します。<default-operation>エレメントの値の設定は、1 回だけ有効になります。 <edit-config>メッセージのオペレーション属性またはデフォルトオペレーション方式を指定しない場合、**merge** は常に適用されます。

<default-operation>エレメントには次の値があります。

- **merge**ー<default-operation>エレメントのデフォルト値です。
- **replace**ーオペレーション属性が指定されておらず、デフォルトオペレーション方式が replace として指定されている場合に使用される値です。
- **none**ーオペレーション属性が指定されておらず、デフォルトのオペレーション方式が none として指定されている場合に使用される値です。 この値を指定した場合、<edit-config>オペレーションは設定を発行するのではなく、スキーマの検証にのみ使用されます。 スキーマ検

証がパスすると、正常なメッセージが返されます。 それ以外の場合は、エラーメッセージが返されます。

XML 設定例

スキーマ検証のために空のオペレーションを発行します。

```
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <edit-config>
    <target>
      <running/>
    </target>
    <default-operation>none</default-operation>
    <config xmlns:xc="urn:ietf:params:xml:ns:netconf:base:1.0">
      <top xmlns="http://www.nec.com/netconf/config:1.0">
        <Ifmgr>
          <Interfaces>
            <Interface>
              <IfIndex>262</IfIndex>
              <Description>222222</Description>
            </Interface>
          </Interfaces>
        </Ifmgr>
      </top>
    </config>
  </edit-config>
</rpc>
```

7.1.11. edit-config: error-option

説明

このオペレーションは、設定エラーの場合に実行するアクションを決定します。

<エラーオプション>エレメントには次の値があります。

- **stop-on-error**－オペレーションを停止し、エラーメッセージを返します。 デフォルトの error-option 値です。
- **continue on error**－オペレーションを続行し、エラーメッセージを返します。
- **rollback on error**－設定をロールバックします。

XML 設定例

#<error-option>エレメント値を **continue-on-error** として 2 つのインタフェースの設定を発行します。

```
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <edit-config>
    <target>
      <running/>
    </target>   <error-option>continue-on-error</error-option>
    <config xmlns:xc="urn:ietf:params:xml:ns:netconf:base:1.0">
      <top xmlns="http://www.nec.com/netconf/config:1.0">
```

```
        <Ifmgr xc:operation="merge">
          <Interfaces>
            <Interface>
              <IfIndex>262</IfIndex>
              <Description>222</Description>
                <ConfigSpeed>1024</ConfigSpeed>
                <ConfigDuplex>1</ConfigDuplex>
            </Interface>
            <Interface>
              <IfIndex>263</IfIndex>
              <Description>333</Description>
                <ConfigSpeed>1024</ConfigSpeed>
                <ConfigDuplex>1</ConfigDuplex>
            </Interface>
          </Interfaces>
        </Ifmgr>
      </top>
    </config>
  </edit-config>
</rpc>
```

7.1.12. edit-config: incremental

説明

このオペレーションでは、元のデータに影響を与えずに、設定データを列に追加します。

incremental 属性は、vlan permit リスト列などのリスト列に適用されます。

<replace>オペレーションを除く<edit-config>オペレーションの **incremental** 属性を使用できます。

incremental 属性のサポートはモジュールによって異なります。 詳細は、NETCONF XML API ドキュメントを参照してください。

XML 設定例

#VLAN 1～VLAN 10 をタグなし VLAN 12～VLAN 15 までのタグなし VLAN リストに追加します。

```
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"
xmlns:nec="http://www.nec.com/netconf/base:1.0">
  <edit-config>
    <target>
      <running/>
    </target>
    <config xmlns:xc="urn:ietf:params:xml:ns:netconf:base:1.0">
      <top xmlns="http://www.nec.com/netconf/config:1.0">
        <VLAN xc:operation="merge">
          <HybridInterfaces>
            <Interface>
              <IfIndex>262</IfIndex>
              <UntaggedVlanList  nec: incremental="true">1-10</UntaggedVlanList>
               </Interface>
```

```
          </HybridInterfaces>
        </VLAN>
      </top>
    </config>
  </edit-config>
</rpc>
```

7.1.13. get

説明

このオペレーションは、デバイス設定と状態情報を取得します。

XML 設定例

シスログモジュールのデバイス設定と状態情報を取得します。

```
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"
xmlns:xc="http://www.nec.com/netconf/base:1.0">
  <get>
    <filter type="subtree">
      <top xmlns="http://www.nec.com/netconf/data:1.0">
        <Syslog>
        </Syslog>
      </top>
    </filter>
  </get>
</rpc>
```

7.1.14. get-bulk

説明

このオペレーションでは、指定されたインデックスの次のインデックスのデータエントリからデータエントリ(デバイス設定と状態情報を含む)を取得します。

XML 設定例

#すべてのインタフェースのデバイス設定と状態情報を取得します。

```
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <get-bulk>
    <filter type="subtree">
      <top xmlns="http://www.nec.com/netconf/data:1.0">
        <Ifmgr>
          <Interfaces xc:count="5" xmlns:xc="http://www.nec.com/netconf/base:1.0">
            <Interface/>
          </Interfaces>
        </Ifmgr>
      </top>
    </filter>
```

```
  </get-bulk>
</rpc>
```

7.1.15. get-bulk-config

説明

このオペレーションでは、指定されたインデックスの次のインデックスのデータエントリからデフォルトでない設定データエントリを取得します。

XML 設定例

#すべてのインタフェースに対してデフォルト以外の設定を取得します。

```
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <get-bulk-config>
    <source>
      <running/>
    </source>
    <filter type="subtree">
      <top xmlns="http://www.nec.com/netconf/config:1.0">
        <Ifmgr>
        </Ifmgr>
      </top>
    </filter>
  </get-bulk-config>
</rpc>
```

7.1.16. get-config

説明

このオペレーションは、デフォルト以外の設定データを取得します。デフォルト以外の設定データが存在しない場合、デバイスは空のデータを持つ応答を返します。

XML 設定例

#インタフェーステーブルのデフォルト以外の設定データを取得します。

```
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"
xmlns:xc="http://www.nec.com/netconf/base:1.0">
  <get-config>
    <source>
      <running/>
    </source>
    <filter type="subtree">
      <top xmlns="http://www.nec.com/netconf/config:1.0">
        <Ifmgr>
           <Interfaces>
              <Interface/>
            </Interfaces>
        </Ifmgr>
      </top>
```

```
    </filter>
  </get-config>
</rpc>
```

7.1.17. get-sessions

説明

このオペレーションは、システム内のすべての NETCONF セッションに関する情報を取得します。特定の NETCONF セッションに関する情報を取得するためのセッション ID を指定することはできません。

XML 設定例

#システム内のすべての NETCONF セッションに関する情報を取得します。

```
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
<get-sessions/>
</rpc>
```

7.1.18. kill-session

説明

このオペレーションは、別のユーザの NETCONF セッションを終了します。このオペレーションは、現在のユーザの NETCONF セッションを終了できません。

XML 設定例

#セッション ID 1 の NETCONF セッションを終了します。

```
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <kill-session>
    <session-id>1</session-id>
  </kill-session>
</rpc>
```

7.1.19. load

説明

このオペレーションにより設定がロードされます。 デバイスが<load>オペレーションを終了すると、指定されたファイルの設定がデバイスの実行中の設定にマージされます。

XML 設定例

#ファイル a1.cfg 内の設定をデバイスの稼働中の設定にマージします。

```
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <load>
    <file>a1.cfg</file>
  </load>
</rpc>
```

7.1.20. lock

説明

このオペレーションにより設定がロックされます。 設定がロックされた後は、<edit-config>オペレーションを実行できません。 その他のオペレーションは許可されます。

ユーザが設定をロックすると、他のユーザは NETCONF や CLI や SNMP などのその他の設定方法を使用してデバイスを設定できません。

XML 設定例

設定をロックします。

```
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
 <lock>
    <target>
        <running/>
    </target>
</lock>
</rpc>
```

7.1.21. rollback

説明

このオペレーションにより、設定がロールバックされます。 そのためには、<file>エレメントに設定ファイルを指定する必要があります。 デバイスが<rollback>オペレーションを終了すると、現在のデバイス設定は、指定された設定ファイル内の設定に完全に置き換えられます。

XML 設定例

稼働中の設定をファイル 1A.cfg の設定にロールバックします。

```
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <rollback>
    <file>1A.cfg</file>
  </rollback>
</rpc>
```

7.1.22. save

説明

このオペレーションにより、稼働中の設定が保存されます。 <file>エレメントを使用して、設定を保存するファイルを指定できます。テキストにファイル列が含まれていない場合、稼働中のコンフィギュレーションは自動的に次回に起動するメインのコンフィギュレーションファイルに保存されます。

OverWrite 属性は、指定したファイルがすでに存在する場合に、稼働中の設定が元の設定ファイルを上書きするかどうかを決定します。

Binary-only 属性は、稼働中の設定をバイナリ設定ファイルにのみ保存するかどうかを決定します。

XML 設定例

稼働中の設定をファイル **test.cfg** に保存します。

```
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <save OverWrite="false" Binary-only="true">
    <file>test.cfg</file>
  </save>
</rpc>
```

7.1.23. unlock

説明

このオペレーションによって設定がロック解除され、他のユーザがデバイスを設定できます。

NETCONF セッションを終了すると、設定が自動的にロック解除されます。

XML 設定例

設定をロック解除します。

```
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
<unlock>
    <target>
        <running/>
    </target>
</unlock>
</rpc>
```

目次

このセクションのページは **10-x-x** です。

8 章 プロセスモニタリングとメンテナンス 8-1
8.1. 概要 8-1
8.2. プロセスの表示と維持 8-1
8.3. ユーザプロセスの表示と維持 8-1

8章 プロセスモニタリングとメンテナンス

8.1. 概要

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。

8.2. 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ます。

操作	コマンド
メモリ使用率を表示する	**display memory** [**summary**] [**slot** *slot-number* [**cpu** *cpu-number*]]

8.3. 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
例外プロセスに関する情報を表示する	**display exception context** [**count** *value*] [**slot** *slot-number* [**cpu** *cpu-number*]]
コアファイルディレクトリを表示する	**display exception filepath** [**slot** *slot-number* [**cpu** *cpu-number*]]
例外発生時に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** } { **job** *job-id* | **name** *process-name* }
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*
例外プロセスに関する情報をクリアする	**reset exception context** [**slot** *slot-number* [**cpu** *cpu-number*]]

目次

このセクションのページは **10-x-x** です。

9 章 ポートミラーリング 9-1
9.1. 概要 9-1
9.1.1. 用語 9-1
9.1.2. ポートミラーリングの分類 9-2
9.1.3. ローカルポートミラーリング 9-2
9.1.4. レイヤ 2 リモートポートミラーリング 9-3
9.2. 制限とガイドライン 9-4
9.3. ローカルポートミラーリングの設定 9-5
9.3.1. 制限とガイドライン 9-5
9.3.2. ローカルポートミラーリングの設定作業リスト 9-5
9.3.3. ローカルミラーリンググループの作成 9-5
9.3.4. ソースポートの設定 9-5
9.3.5. モニタポートの設定 9-6
9.4. 複数モニタポートのローカルミラーリングの設定 9-7
9.5. レイヤ 2 リモートポートミラーリングの設定 9-8
9.5.1. 制限とガイドライン 9-8
9.5.2. 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 9-9
9.5.3. 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 9-9
9.5.4. リモートデスティネーショングループの作成 9-10
9.5.5. モニタポートの設定 9-10
9.5.6. リモートプローブ VLAN の設定 9-11
9.5.7. リモートプローブ VLAN へのモニタポートの割り当て 9-11
9.5.8. リモートソースグループの作成 9-12
9.5.9. ミラーリングソースの設定 9-12
9.5.10. リフレクタポートの設定 9-13
9.5.11. 出力ポートの設定 9-13
9.6. ポートミラーリングの表示と維持 9-14
9.7. ポートミラーリングの設定例 9-15
9.7.1. ローカルポートミラーリングの設定例 9-15
9.7.2. 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 9-16
9.7.3. 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例 9-17
9.7.4. 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 9-20

9章 ポートミラーリング

9.1. 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、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。

9.1.1. 用語

ポートミラーリングの設定では以下の用語が使用されます。

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。

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デバイスに接続するポートにコピーされます。コピーはミラードパケットと呼ばれます。

II. ソースデバイス

ミラーリングソースが存在するデバイスは”送信元デバイス”あるいは”ソースデバイス”と呼ばれます。

III. ミラーリングデスティネーション

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ミラーリングソースをモニタするとき、複数のパケットをコピーする可能性があります。たとえば、以下の状況が存在するとき、2 つのパケットのコピーはポート A で受信されます。

- ポート A は同一デバイス上のポート B とポート C 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 B からポート C へ転送されます。

IV. デスティネーションデバイス

モニタポートが存在するデバイスは"宛先デバイス"あるいは”デスティネーションデバイス”と呼ばれます。

V. 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。

- **Inbound**–受信パケットをコピーします。
- **Outbound**–送信パケットをコピーします。
- **Bidirectional**–送受信パケットをコピーします。

VI. 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はローカルミラーリンググループ、リモートソースグループ、リモート宛先グループを含みます。

VII. 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 はミラーリングパケットを宛先デバイスに送信するための専用 VLAN です。

リフレクタポートと出力ポートのどちらも、送信元デバイス上に存在し、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。

ポートミラーリングをおこなう装置において、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。

9.1.2. ポートミラーリングの分類

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**–送信元デバイスはデータ監視機器に直接接続します。送信元デバイスデスティネーションデバイスの働きもおこない、ミラーパケットを直接データ監視機器に転送します。
- **リモートポートミラーリング**–送信元デバイスはデータ監視機器に直接接続しません。送信元デバイスはミラーパケットを宛先デバイスに送り、そのパケットをデータ監視機器に転送します。

送信元デバイスと宛先デバイスが同じレイヤ 2 ネットワークの上にそんざいするため、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。

9.1.3. ローカルポートミラーリング

図 9-1 ローカルポートミラーリングの実行

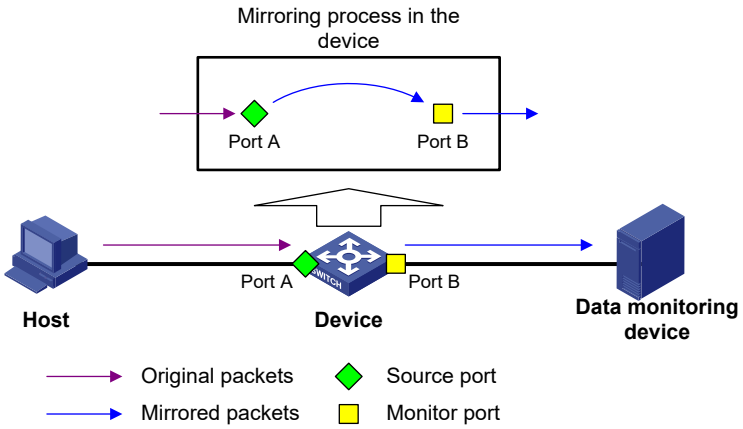


図 9-2 に示すように、ソースポート(Port A)とモニタポート(Port B)は同じデバイス上にあります。Port A のパケットは Port B にコピーされ、解析を行うためデータ監視機器に転送されます。

9.1.4. レイヤ 2 リモートポートミラーリング

レイヤ 2 リモートポートミラーリングにおいて、ミラーリングソースとミラーリング宛先は別のデバイス上に配置され、別のミラーリンググループに属します。

リモートソースグループあるいはリモート宛先グループはそれぞれミラーリングソースあるいはミラーリングデスティネーションを含むミラーリンググループです。送信元デバイスと宛先デバイスの間のデバイスは、中間デバイスです。

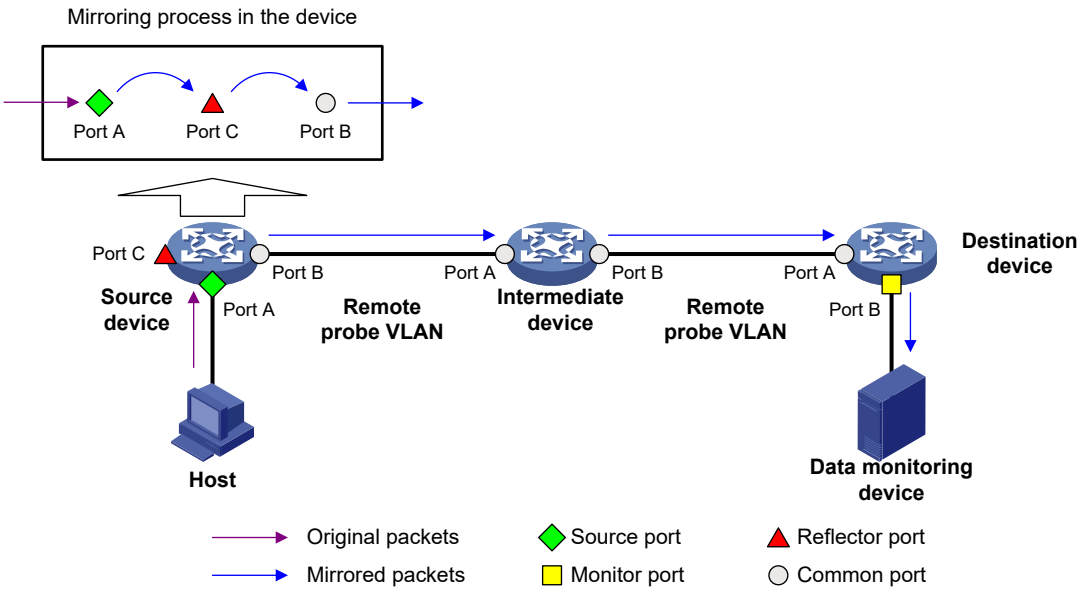
レイヤ 2 リモートポートミラーリングにはリフレクタポートまたは出力ポートを使用します。

I. リフレクタポートを使用したミラーリング

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は以下のフローによって動作します。

1. 送信元デバイスはリフレクタポートにミラーリングソース上で受信したコピーします。
2. リフレクタポートはリモートプローブ VLAN にミラーパケットをブロードキャスト転送します。
3. 中間デバイスはリモートプローブ VLAN を通してミラーパケットを宛先デバイスに送ります。
4. ミラーパケットを受信するとすぐに、宛先デバイスはミラーパケットの ID がリモートプローブ VLAN ID と同じであるかを決定します。2 つの VLAN ID が一致しているならば、宛先デバイスはモニタポートを通してミラーパケットをデータ監視機器に転送します。

図 9-2 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



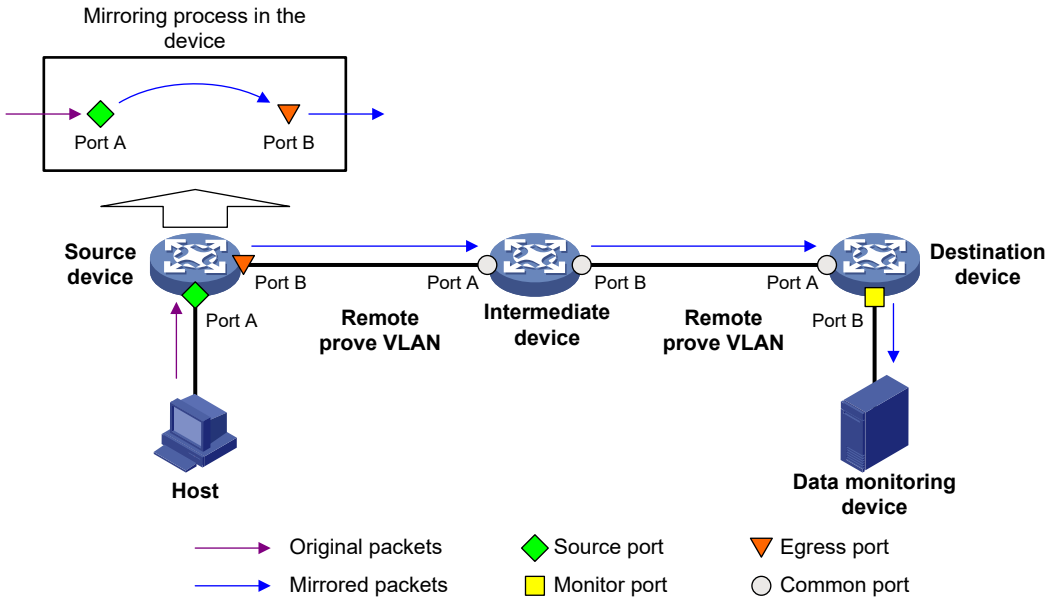
II. 出力ポートを使用したミラーリング

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は以下のフローによって動作します。

1. 送信元デバイスは出力ポートにミラーリングソース上で受信したコピーします。
2. 出力ポートはミラーパケットを中間デバイスに転送します。
3. 中間デバイスはリモートプローブ VLAN においてミラーパケットをフラッディングし、ミラーパケットを宛先デバイスに送ります。

4. ミラーパケットを受信するとすぐに、宛先デバイスはミラーパケットの ID がリモートプローブ VLAN ID と同じであるかを決定します。2 つの VLAN ID が一致しているならば、宛先デバイスはモニタポートを通してミラーパケットをデータ監視機器に転送します。

図 9-3 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



9.2. 制限とガイドライン

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は、複数のモニタポートによってローカルポートミラーリングを実施するために使われることができます。

リフレクタポートを使用する場合、リフレクタポートはリモートプローブ VLAN においてミラーパケットをブロードキャスト転送します。

リモートプローブ VLAN を複数のポートを割り当てることによって、複数のモニタポートでパケットを監視することができます。

出力ポートを使用した場合はこのようなローカルポートミラーリングを実施することができません。

受信トラフィックのミラーリングでは、オリジナルパケットの VLAN タグはミラーパケットにコピーされます。

送信トラフィックのミラーリングでは、ミラーパケットは出力インタフェースの VLAN タグを持ちます。

9.3. ローカルポートミラーリングの設定

9.3.1. 制限とガイドライン

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ときのみ動作します。

リンクアグリゲーションインタフェースはミラーリンググループのモニタポートにすることはできません。

9.3.2. ローカル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) ローカルミラーリンググループの作成
(必須設定項目) ソースポートの設定
(必須設定項目) モニタポートの設定

9.3.3. 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

9.3.4. ソースポートの設定

I. 制限とガイドライン

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。

- 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。
- 1 つのポートは 1 つのミラーリンググループのソースポートとしてのみ使用できます。
- 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設定できません。

II. ソースポートの設定

- 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**	―

操作	コマンド	補足
2. 指定したローカルミラーリング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

- 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*	―
3. 指定したローカルミラーリンググループのソースポートを設定する	**mirroring-group** *group-id* **mirroring-port { both | inbound | outbound }**	デフォルト：設定なし

9.3.5. モニタポートの設定

I. 制限とガイドライン

モニタポートで STP 機能を有効にしないでください。

モニタポートは、ミラーされたトラフィックのみを転送するために使用してください。

II. 設定手順

- 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

- 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*	―
3. 指定したローカルミラーリンググループの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

9.4. 複数モニタポートのローカルミラーリングの設定

I. 複数モニタポートのローカルミラーリング

リモートプローブVLAN を通して複数のローカルモニタポートにミラーされたパケットをブロードキャストするため、以下の作業を行います。

1. リモートソースグループを装置に設定します。
2. リモートソースグループのためにミラーリングソースとリフレクタポートを設定します。
3. VLAN をリモートプローブ VLAN として指定し、データ監視装置と接続しているポートに VLAN に割り当ててください。

この設定では、ミラーリングソースで受信したパケットをリフレクタポートにコピーし、リモートプローブ VLAN 内のパケットをブロードキャストすることにより、リモートプローブ VLAN のメンバポートからデータ監視装置にパケットを送信します

II. 制限とガイドライン制限とガイドライン

デバイス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とき、工場出荷状態の設定に戻ります。リフレクタポートで他の機能を設定しないでください。

ポートミラーリングを正常に動作させるため、リモートプローブ VLAN にソースポートを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。NEC では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ことを推奨します。VLAN インタフェースを作成あるいは他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 が削除されたとき、リモートミラーリンググループは無効になります。

III. 設定手順

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

操作	コマンド	補足
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 での設定: **mirroring-group** *group-id* **mirroring-port** *mirroring-port-list* { **both** | **inbound** | **outbound** } • interface view での設定: ○ interface view に移行する: **interface** *interface-type interface-number* ○ 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** } ○ 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** *reflector-port*	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*	デフォルト : VLAN1のみが存在します(システムデフォルトVLAN)
6. VLAN にモニタポートを割り当てる	**port** *interface-list*	デフォルト：設定なし
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

9.5. レイヤ2リモートポートミラーリングの設定

9.5.1. 制限とガイドライン

トラフィックミラーリングを保証するために、宛先デバイス、中間デバイス、送信元デバイスの順に機器を設定してください。

中間デバイスがある場合、送信元デバイス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。

リモートデスティネーションデバイスにミラーパケットが到達するために、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。

ソースポートの双方向通信を監視するために、送信元デバイス、中間デバイス、宛先デバイスの上のリモートプローブ VLAN において MAC アドレス学習を無効にしてください。

リンクアグリゲーションインタフェースのメンバポートはレイヤ 2 リモートポートミラーリングのためのモニタポートとしてとして設定されることができません。

9.5.2. 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) デスティネーションデバイスの設定 • リモートデスティネーショングループの作成 • モニタポートの設定 • モートプローブ VLAN の設定 • 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) ソースデバイスの設定 • リモートソースグループの作成 • ミラーリングソースの設定 • リフレクタポートの設定 • リモートプローブ VLAN の設定

9.5.3. 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) デスティネーションデバイスの設定 • リモートデスティネーショングループの作成 • モニタポートの設定 • リモートプローブ VLAN の設定 • 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) ソースデバイスの設定 • リモートソースグループの作成 • ミラーリングソースの設定 • 出力ポートの設定 • リモートプローブ VLAN の設定

9.5.4. リモートデスティネーショングループの作成

I. 制限とガイドライン

宛先デバイスでのみ、設定をしてください。

II. 設定手順

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

9.5.5. モニタポートの設定

I. 制限とガイドライン

宛先デバイスでのみ、設定をしてください。

モニタポートで STP 機能を有効にしないで下さい。

モニタポートは、ミラーされたトラフィックのみを転送するために使用してください。

1 つのミラーリンググループは 1 つのモニタポートのみ持つことができます。

リンクアグリゲーションインタフェースはミラーリンググループのモニタポートにすることはできません。

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. 指定したミラーリング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

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の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

9.5.6. リモートプローブ VLAN の設定

I. 制限とガイドライン

送信元デバイスと宛先デバイスの両方で設定をしてください。

既存のスタティック VLAN のみをリモートプローブ VLAN として設定することができます。

リモートプローブ VLAN を設定されている VLAN は、ミラーリングのみの VLAN として使用してください。

送信元デバイスと宛先デバイスで、リモートグループのリモートプローブ VLAN が同一になるように設定してください。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. 指定したミラーリング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

9.5.7. リモートプローブ VLAN へのモニタポートの割り当て

I. 制限とガイドライン

宛先デバイスでのみ、設定をしてください。

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. リモートプローブ VLAN をポートに割り当てる	• 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* { **tagged** | **untagged** }	デフォルト：**port access vlan 1**

9.5.8. リモートソースグループの作成

I. 制限とガイドライン

送信元デバイスでのみ、設定をしてください。

II. 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

9.5.9. ミラーリングソースの設定

I. 制限とガイドライン

送信元デバイスでのみ、設定をしてください。

リモートソースグループのソースポートを設定するとき、以下の制限とガイドラインに従ってください。

- リモートソースグループのソースポートにリモートソース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。
- ソースポートとして動作させるポートは 1 つのミラーリンググループのみで使用してください。
- 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。

II. ソースポートの設定

- 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. 指定したミラーリング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

- 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のソースポートを設定する	**mirroring-group** *group-id* **mirroring-port** { **both** | **inbound** | **outbound** }	デフォルト：設定なし

9.5.10. リフレクタポートの設定

I. 制限とガイドライン

送信元デバイスでのみ、設定をしてください。

デバイス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とき、工場出荷状態の設定に戻ります。リフレクタポートで他の機能を設定しないでください。

リモートソースグループは、1 つのリフレクタポートのみサポートしています。

II. system view でのリフレクタポートの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. 指定したミラーリング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

III. interface view でのリフレクタポートの設定

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のリフレクタポートを設定する	**mirroring-group** *group-id* **reflector-port**	デフォルト：設定なし

9.5.11. 出力ポートの設定

I. 制限とガイドライン

送信元デバイスでのみこの設定をしてください。

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

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。

1 つのミラーリンググループに 1 つの出力ポートのみ設定できます。

II. system view での出力ポートの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. 指定したミラーリング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
3. interface view に移行する	**interface** *interface-type interface-number*	―
4. リモートプローブ VLAN を出力ポートに割り当てる	• 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* { **tagged** | **untagged** }	デフォルト：**port access vlan 1**

III. interface view での出力ポートの設定

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の出力ポートを設定する	**mirroring-group** *group-id* **monitor-egress**	デフォルト：設定なし

9.6. 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** }

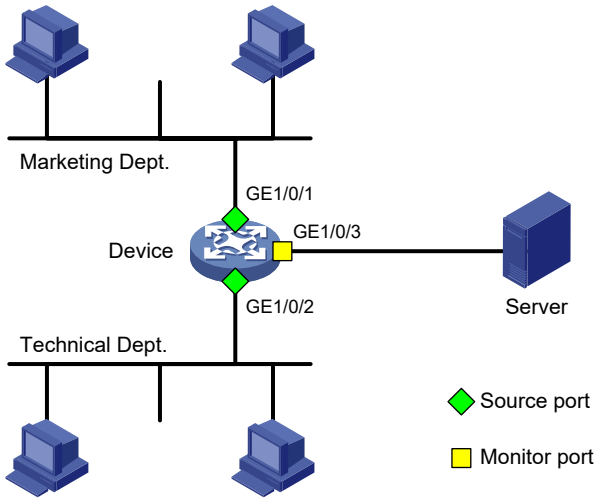
9.7. ポートミラーリングの設定例

9.7.1. 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 9-4 に示すように、marketing department と technical department の双方向のパケットをモニタするため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 9-4 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 と 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 で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情報を表示します。

[Device] display mirroring-group all

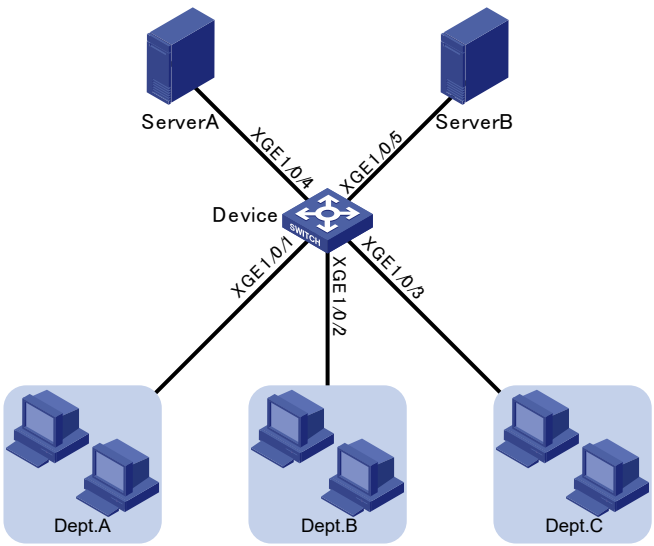
```
Mirroring group 1:
    Type: Local
    Status: Active
    Mirroring port:
        GigabitEthernet1/0/1  Both
        GigabitEthernet1/0/2  Both
    Monitor port: GigabitEthernet1/0/3
```

9.7.2. 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 9-5 に示すように、2 つのデータモニタリングデバイス(Server A、Server B)が 3 つの部門の双方向のトラフィックを監視できるように、ポートミラーリングを設定します。

図 9-5 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

#リモートソースミラーリンググループのソースポートとして Ten-GigabitEthernet 1/0/1 から Ten-GigabitEthernet 1/0/3 を設定します。

[Device] mirroring-group 1 mirroring-port Ten-GigabitEthernet1/0/1 to Ten-GigabitEthernet1/0/3 both

#未使用ポート（例：Ten-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 Ten-GigabitEthernet1/0/6

```
This operation may delete all settings made on the interface. Continue? [Y/N]:y
```

VLAN10 を作成し、Ten-GigabitEthernet 1/0/4 と Ten-GigabitEthernet 1/0/5 を VLAN10 に割り当てます。

[Device] vlan 10

[Device-vlan10] port Ten-GigabitEthernet1/0/4 to Ten-GigabitEthernet1/0/5

[Device-vlan10] quit

#リモートソースモニタリンググループ 1 のリモートプローブ VLAN として VLAN 10 を設定します。

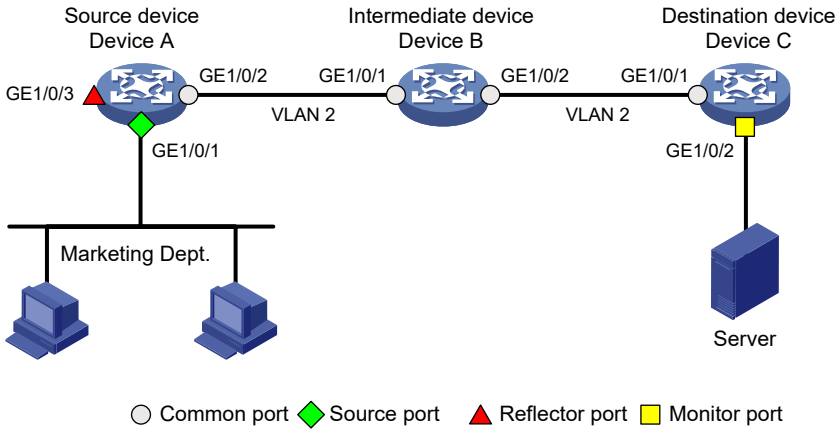
[Device] mirroring-group 1 remote-probe vlan 10

9.7.3. 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例

I. ネットワーク要件

図 9-6 に示すように、2 つの部門の双方向のトラフィックを監視できるように、レイヤ 2 リモートポートミラーリングを設定します。

図 9-6 ネットワーク図



II. 設定手順

1. Device C(宛先デバイス)を設定します。

   # VLAN 2 を作成します。

   <DeviceC> system-view

   [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

GigabitEthernet 1/0/1 をトランクポートに設定し、VLAN 2 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 2

[DeviceC-GigabitEthernet1/0/1] quit

リモートデスティネーショングループを作成します。

[DeviceC] mirroring-group 2 remote-destination

ミラーリンググループ 2 にリモートプローブ VLAN 2 を設定します。

[DeviceC] mirroring-group 2 remote-probe vlan 2

ミラーリンググループ 2 のモニタポートを GigabitEthernet 1/0/2 に設定します。

[DeviceC] interface gigabitethernet 1/0/2

[DeviceC-GigabitEthernet1/0/2] mirroring-group 2 monitor-port

GigabitEthernet 1/0/2 で STP 機能を無効にします。

[DeviceC-GigabitEthernet1/0/2] undo stp enable

GigabitEthernet 1/0/2 に VLAN 2 を割り当てます。

[DeviceC-GigabitEthernet1/0/2] port access vlan 2

[DeviceC-GigabitEthernet1/0/2] quit

2. Device B (中間デバイス) 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

GigabitEthernet 1/0/1 をトランクポートに設定し、VLAN 2 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 2

[DeviceB-GigabitEthernet1/0/1] quit

Configure GigabitEthernet 1/0/2 をトランクポートに設定し、VLAN 2 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 2

[DeviceB-GigabitEthernet1/0/2] quit

3. Device A (送信元デバイス) 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 1 を作成し、リモートプローブ 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 1 のソースポートとして GigabitEthernet 1/0/1 を割り当てます。

[DeviceA] mirroring-group 1 mirroring-port gigabitethernet 1/0/1 both

ミラーリンググループ 1 のリフレクタポートとして GigabitEthernet 1/0/3 を割り当てます。

[DeviceA] mirroring-group 1 reflector-port gigabitethernet 1/0/3

This operation may delete all settings made on the interface. Continue? [Y/N]: y

GigabitEthernet 1/0/2 をトランクポートに設定し、VLAN 2 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 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

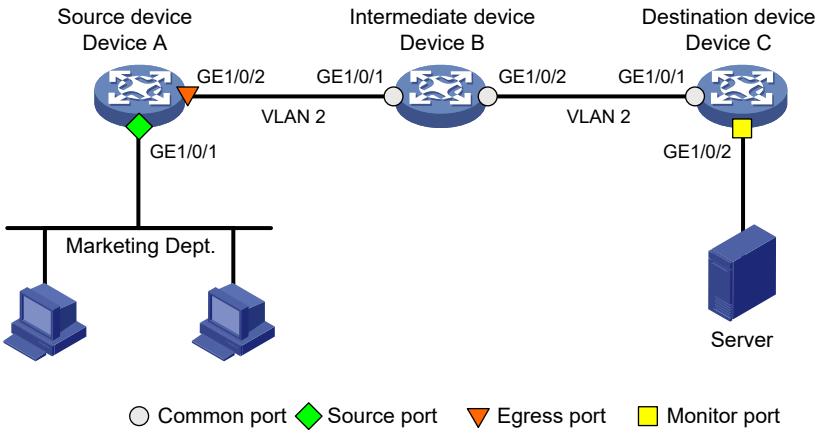
```
Mirroring group 1:
    Type: Remote source
    Status: Active
    Mirroring port:
        GigabitEthernet1/0/1  Both
    Reflector port: GigabitEthernet1/0/3
    Remote probe VLAN: 2
```

9.7.4. 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

I. ネットワーク要件

図 9-7 に示すように、2 つの部門の双方向のトラフィックを監視できるように、レイヤ 2 リモートポートミラーリングを設定します。

図 9-7 ネットワーク図



II. 設定手順

1. Device C(宛先デバイス)を設定します。

   # VLAN 2 を作成します。

   <DeviceC> system-view

   [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

   # GigabitEthernet 1/0/1 をトランクポートに設定し、VLAN 2 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 2

   [DeviceC-GigabitEthernet1/0/1] quit

   # リモートデスティネーショングループを作成します。

   [DeviceC] mirroring-group 2 remote-destination

   # ミラーリンググループ 2 にリモートプローブ VLAN 2 を設定します。

   [DeviceC] mirroring-group 2 remote-probe vlan 2

   # ミラーリンググループ 2 のモニタポートを GigabitEthernet 1/0/2 に設定します。

   [DeviceC] interface gigabitethernet 1/0/2

[DeviceC-GigabitEthernet1/0/2] mirroring-group 2 monitor-port

GigabitEthernet 1/0/2 で STP 機能を無効にします。

[DeviceC-GigabitEthernet1/0/2] undo stp enable

GigabitEthernet 1/0/2 に VLAN 2 を割り当てます。

[DeviceC-GigabitEthernet1/0/2] port access vlan 2

[DeviceC-GigabitEthernet1/0/2] quit

2. Device B (中間デバイス)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

GigabitEthernet 1/0/1 をトランクポートに設定し、VLAN 2 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 2

[DeviceB-GigabitEthernet1/0/1] quit

Configure GigabitEthernet 1/0/2 をトランクポートに設定し、VLAN 2 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 2

[DeviceB-GigabitEthernet1/0/2] quit

3. Device A (送信元デバイス)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 1 を作成し、リモートプローブ 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 1 のソースポートとして GigabitEthernet 1/0/1 を割り当てます。

[DeviceA] mirroring-group 1 mirroring-port gigabitethernet 1/0/1 both

ミラーリンググループ 1 の出力ポートとして GigabitEthernet 1/0/2 を割り当てます。

[DeviceA] mirroring-group 1 monitor-egress gigabitethernet 1/0/2

GigabitEthernet 1/0/2 をトランクポートに設定し、VLAN 2 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 2

GigabitEthernet 1/0/2 で STP 機能を無効にします。

[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
```

目次

このセクションのページは **10-x-x** です。

10 章 トラフィックミラーリング……10-1
10.1. 概要……10-1
10.2. 制限とガイドライン……10-1
10.3. トラフィックミラーリングの設定作業リスト……10-1
10.4. 一致条件の設定……10-2
10.5. トラフィック動作の設定……10-2
10.6. QoS ポリシーの設定……10-2
10.7. QoS ポリシーの適用……10-3
10.7.1. インタフェースへの QoS ポリシーの適用……10-3
10.7.2. VLAN への QoS ポリシーの適用……10-3
10.7.3. グローバルへの QoS ポリシーの適用……10-4
10.8. トラフィックミラーリングの設定例……10-4
10.8.1. トラフィックミラーリングの設定例……10-4

10章　トラフィックミラーリング

10.1. 概要

トラフィックミラーリングは、パケットの監視と解析を行うために、指定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**—データをモニタする装置に接続する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デバイス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セクション 7 *ACL and QoS オペレーションマニュアル*の”*QoS ポリシー*”を参照してください。

10.2. 制限とガイドライン

mirror-to コマンドを除いたコマンドの詳細は、Chapter 7 *ACL and QoS Command References* の "*QoS policy commands*"を参照してください。

10.3. 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

10.4. 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**	―
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. 一致条件を作成する	**if-match** *match-criteria*	デフォルト：設定なし
4. （オプション設定項目）一致条件の設定を表示する	**display traffic classifier**	すべてのviewで実行可能です。

10.5. 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**	―
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*	―
3. トラフィック動作を作成する	**mirror-to interface** *interface-type interface-number*	デフォルト：設定なし トラフィック動作は1つのインタフェースのみに設定することができます。トラフィック動作の設定を複数行った場合、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。

10.6. 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**	―
2. QoS ポリシーを設定し qos policy view に移行する	**qos policy** *policy-name*	デフォルト：設定なし

操作	コマンド	補足
3. QoS ポリシーに一致条件とトラフィック動作を紐付ける	**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。

10.7. QoSポリシーの適用

10.7.1. インタフェースへの QoS ポリシーの適用

I. 制限とガイドライン

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の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。

インタフェースの入力方向のトラフィックの為に、インタフェースに 1 つのポリシーを適用することができます。出力方向のトラフィックをインタフェースにおいてミラーすることはできません。

装置は、リンクアグリゲーションインタフェースの出力方向のミラーリングをサポートしていません。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. interface view に移行する	**interface** *interface-type interface-number*	―
3. インタフェースにポリシーを追加する	**qos apply policy** *policy-name* **inbound**	デフォルト：設定なし
4. （オプション設定項目）インタフェースに追加された QoS ポリシーの設定を表示する	**display qos policy interface**	すべてのviewで実行可能です。

10.7.2. VLAN への QoS ポリシーの適用

I. 制限とガイドライン

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。

VLAN に関連した全てのポートの入力方向のトラフィックの為に、VLAN に 1 つのポリシーを適用することができます。VLAN において出力方向のトラフィックをミラーすることはできません。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. VLAN にポリシーを追加する	**qos vlan-policy** *policy-name* **vlan** *vlan-id-list* **inbound**	デフォルト：設定なし
3. （オプション設定項目）VLAN に追加された QoS ポリシーの設定を表示する	**display qos vlan-policy**	すべてのviewで実行可能です。

10.7.3. グローバルへの QoS ポリシーの適用

I. 制限とガイドライン

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。

全てのポートの入力方向のトラフィックの為に、グローバルに 1 つのポリシーを適用することができます。出力方向のトラフィックをミラーすることはできません。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. グローバルにポリシーを追加する	**qos apply policy** *policy-name* **global inbound**	デフォルト：設定なし
3. （オプション設定項目）グローバルに追加された QoS ポリシーの設定を表示する	**display qos policy global**	すべてのviewで実行可能です。

10.8. トラフィックミラーリングの設定例

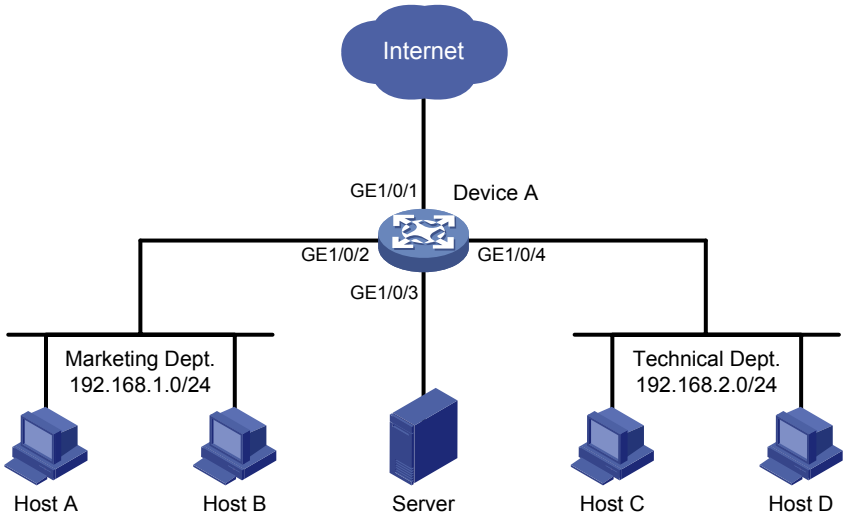
10.8.1. トラフィックミラーリングの設定例

I. ネットワーク要件

図 10-1 に示すように、サーバがトラフィックを監視することができるように設定します。

- Technical department がインターネットに送信するすべてのトラフィックを監視します。
- Technical department が平日の 8:00 から 18:00 までに Marketing department に送信する IP トラフィックを監視します。

図 10-1 ネットワーク図



II. 設定手順

時間範囲 work を作成します。work の就業時間は平日の 8:00 から 18:00 までです。

<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と Marketing department にアクセスできるよう 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 を関連付けます。

[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

III. 設定の確認

サーバは以下のトラフィックを監視することができます。

- Technical department がインターネットに送信するすべてのトラフィック
- Technical department が平日の勤務時間の間に Marketing Department に送る IP トラフィック

（詳細は省略します。）

目次

このセクションのページは **10-x-x** です。

11 章 sFlow……11-1
11.1. 概要……11-1
11.2. プロトコルと標準……11-1
11.3. 基本 sFlow 情報の設定……11-2
11.4. フローサンプリングの設定……11-2
11.5. カウンタサンプリングの設定……11-3
11.6. sFlow の表示と維持……11-3
11.7. sFlow の設定例……11-4
11.7.1. sFlow の設定例……11-4
11.8. sFlow のトラブルシューティング……11-5
11.8.1. リモート sFlow コレクタが sFlow パケットを受信できない……11-5

11章 sFlow

11.1. 概要

sFlow (sampled Flow) は、トラフィック監視技術です。

図 11-1 に示すように、sFlow システムは、装置に組み込まれた sFlow エージェントとリモートの sFlow コレクタから構成されます。sFlow エージェントはトラフィック統計情報と sFlow が有効なインタフェースからのパケットを収集し、sFlow パケットにカプセル化します。sFlow パケットバッファが一杯になった時、または sFlow パケットのエージタイム(1 秒固定)が終了した時、sFlow エージェントは以下の作業を行います。

- UDP データグラムに sFlow パケットをカプセル化します。
- 指定された sFlow コレクタに UDP データグラムを送信します。

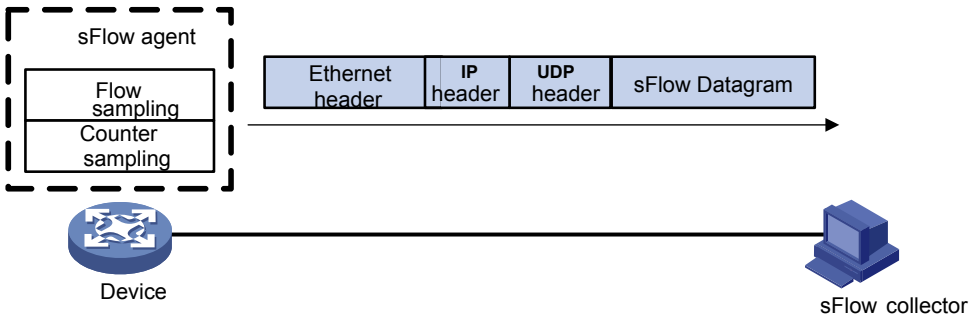
sFlow コレクタは sFlow パケットを分析し、結果を表示します。1 つの sFlow コレクタは複数の sFlow エージェントをモニタすることができます。

sFlow には、以下の 2 つのサンプリングメカニズムがあります。

- **フローサンプリング**—パケットの内容情報を取得します。
- **カウンタサンプリング**—インタフェーストラフィック統計情報を取得します。

sFlow はフローサンプリングとカウンタサンプリングを同時に使用することが可能です。

図 11-1 sFlow システム



11.2. プロトコルと標準

- RFC 3176, *InMon Corporation's sFlow: A Method for Monitoring Traffic in Switched and Routed Networks*
- sFlow.org, *sFlow Version 5*

11.3. 基本sFlow情報の設定

I. 制限とガイドライン

sFlow エージェントの IP アドレスを手動で設定することを推奨します。装置は sFlow エージェントのアドレスを定期的にチェックします。sFlow エージェントに IP アドレスを未設定の場合、装置は自動的に sFlow エージェントに IPv4 アドレスを選択しますが、IPv4 アドレスを設定ファイルに保存しません。

sFlow エージェントの IP アドレスは装置上で 1 つのみ設定できます。新しく設定した IP アドレスは、古い IP アドレスを上書きします。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. sFlow エージェントの IP アドレスを設定する	**sflow agent** { **ip** *ipv4-address* | **ipv6** *ipv6-address* }	デフォルト：設定なし
3. sFlow コレクタ情報を設定する	**sflow collector** *collector-id* [**vpn-instance** *vpn-instance-name*] { **ip** *ipv4-address* | **ipv6** *ipv6-address* } [**port** *port-number* | **datagram-size** *size* | **time-out** *seconds* | **description** *string*] *	デフォルト：設定なし
4. sFlow パケットの送信元 IP アドレスを指定する	**sflow source** { **ip** *ipv4-address* | **ipv6** *ipv6-address* } *	デフォルト：ルーティングによって送信元IPアドレスが決まります。

11.4. フローサンプリングの設定

I. フローサンプリング

Ethernet インタフェースでフローサンプリングの設定をします。インタフェースの sFlow エージェントは、以下の作業を行います。

1. 設定されたパラメータによってインタフェースのパケットをサンプリングします。
2. sFlow パケットにカプセル化します。
3. UDP パケットに sFlow パケットをカプセル化し、指定された sFlow コレクタに UDP パケットを送信します。

II. 設定手順

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

操作	コマンド	補足
2. Ethernet interface view に移行する	**interface** *interface-type interface-number*	―
3. (オプション設定項目) フローサンプリングモードを設定する	**sflow sampling-mode random**	デフォルト：random
4. フローサンプリングを有効にし、パケットのサンプリング間隔を指定する	**sflow sampling-rate** *rate*	デフォルト：設定なし 設定値を8192以上の2のn乗の値とすることを推奨します。(例:32768)
5. (オプション設定項目) パケット毎にコピーできるサンプルパケットの最大コピー長を設定する(パケットヘッダから数えます)	**sflow flow max-header** *length*	デフォルト：128バイト デフォルトにすることを推奨します。
6. sFlow コレクタを指定する	**sflow flow collector** *collector-id*	デフォルト：指定なし

11.5. カウンタサンプリングの設定

I. カウンタサンプリング

Ethernet インタフェースでカウンタサンプリングの設定をします。sFlow エージェントは以下の作業を行います。

1. sFlow エージェントは周期的にインタフェースのカウンタ情報を収集します。
2. sFlow パケットにカウンタ情報をカプセル化します。
3. UDP パケットに sFlow パケットをカプセル化し、指定された sFlow コレクタに UDP パケットを送信します。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Ethernet interface view に移行する	**interface** *interface-type interface-number*	―
3. カウンタサンプリングを有効にし、パケットのサンプリング間隔を指定する	**sflow counter interval** *interval*	デフォルト：無効
4. sFlow コレクタを指定する	**sflow counter collector** *collector-id*	デフォルト：指定なし

11.6. sFlow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
sFlow設定を表示する	**display sflow**

11.7. sFlowの設定例

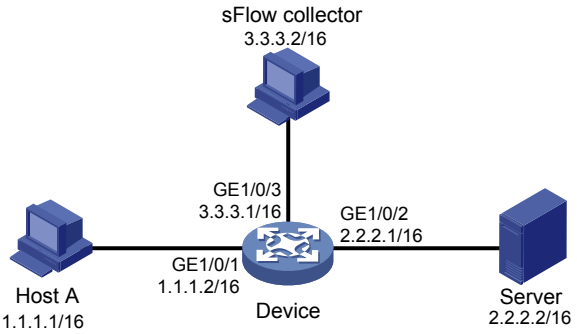
11.7.1. sFlow の設定例

I. ネットワーク要件

図 11-2 に示すように以下の設定を行います。

- Device は、ポートのトラフィックを監視するため Device の GigabitEthernet 1/0/1 で、ランダムモードによるフローサンプリングとカウンタサンプリングを設定します。
- Device は、sFlow コレクタに GigabitEthernet 1/0/3 を通して監視した情報を送信します。

図 11-2 ネットワーク図



II. 設定手順

1. 図 11-2 に示すように、インタフェースの IP アドレス、サブネットマスクを設定します。(詳細は省略します)
2. sFlow エージェントを設定し、sFlow コレクタの情報を設定します。

   # sFlow エージェントの IP アドレスを設定します。

   <Device> system-view

   [Device] sflow agent ip 3.3.3.1

   # sFlow コレクタの情報を設定します。sFlow コレクタの ID を 1、IP アドレスを 3.3.3.2、ポート番号を 6343(デフォルト)、説明を netserver に設定します。

   [Device] sflow collector 1 ip 3.3.3.2 description netserver
3. カウンタサンプリングを設定します。

   # カウンタサンプリングを有効にし、GigabitEthernet 1/0/1 のサンプリング間隔を 120 秒に設定します。

   [Device] interface gigabitethernet 1/0/1

   [Device-GigabitEthernet1/0/1] sflow counter interval 120

   # カウンタサンプリングの sFlow コレクタ 1 を指定します。

[Device-GigabitEthernet1/0/1] sflow counter collector 1

4. フローサンプリングを設定します。

フローサンプリングを有効にし、モードを random、サンプリング間隔を 32768 に設定します。

[Device-GigabitEthernet1/0/1] sflow sampling-mode random

[Device-GigabitEthernet1/0/1] sflow sampling-rate 32768

フローサンプリングの sFlow コレクタ 1 を指定します。

[Device-GigabitEthernet1/0/1] sflow flow collector 1

III. 設定の確認

- sFlow が有効な GigabitEthernet 1/0/1 がアクティブです。
- カウンタサンプリング間隔が 120 秒です。
- フローサンプリング間隔が 32768(32768 パケットに 1 パケット)です。

[Device-GigabitEthernet1/0/1] display sflow

```
sFlow datagram version: 5
Global information:
Agent IP: 3.3.3.1(CLI)
Source address:
Collector information:
ID    IP              Port  Aging      Size VPN-instance Description
1     3.3.3.2         6343  N/A        1400              netserver
Port information:
Interface      CID   Interval(s) FID   MaxHLen Rate     Mode      Status
GE1/0/1        1     120         1     128     32768    Random    Active
```

11.8. sFlowのトラブルシューティング

11.8.1. リモート sFlow コレクタが sFlow パケットを受信できない

I. 症状

リモート sFlow コレクタが sFlow パケットを受信できません。

II. 分析

問題の原因は以下のものが考えられます。

- sFlow コレクタが指定されていません。
- sFlow がインタフェースで設定されていません。
- sFlow エージェントで指定された sFlow コレクタの IP アドレスが、リモート sFlow コレクタの IP アドレスと異なります。
- sFlow パケットが送信されるレイヤ 3 インタフェースの IP アドレスが設定されていません。

- IP アドレスが設定されているが、送信元 IP アドレスの UDP データグラムが sFlow コレクタに送信できません。
- 装置と sFlow コレクタ間の物理的なリンクが故障しています。
- sFlow コレクタが存在しない VPN に結合しています。
- sFlow パケット長が以下の 2 つの値の合計よりも小さい。
  - sFlow パケットヘッダ長
  - パケット毎にフローサンプリングがコピーできるバイト数

III. 解決策

問題を解決する場合、以下を行ってください。

1. **display sflow** コマンドを使用し、sFlow が正しく設定されていることを確認してください。
2. sFlow コレクタと通信する装置に正しい IP アドレスが設定されていることを確認してください。
3. 装置と sFlow コレクタ間の物理的なリンクがアップしていることを確認してください。
4. 結合する VPN が既存であることを確認してください。
5. sFlow パケット長が以下の 2 つの値の合計よりも大きいことを確認してください。
   - sFlow パケットヘッダ長
   - パケット毎にフローサンプリングがコピーできるバイト数(デフォルトの値を推奨します。

目次

このセクションのページは **10-x-x** です。

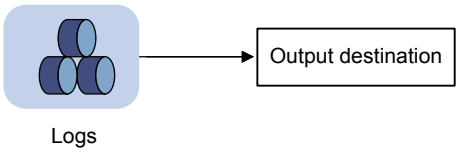
12 章 information center ····· 12-1
12.1. 概要 ····· 12-1
12.1.1. Log タイプ ····· 12-1
12.1.2. ログレベル ····· 12-1
12.1.3. ログの出力先 ····· 12-2
12.1.4. デフォルトの出力ルール ····· 12-2
12.1.5. Diagnostic ログのデフォルト出力ルール ····· 12-2
12.1.6. hidden ログのデフォルト出力ルール ····· 12-3
12.1.7. ログのフォーマット ····· 12-3
12.2. Information center の設定作業リスト ····· 12-5
12.2.1. 一般的なログの管理 ····· 12-5
12.2.2. Hidden ログの管理 ····· 12-6
12.2.3. diagnostic ログの管理 ····· 12-6
12.3. information center の有効化 ····· 12-6
12.4. さまざまな宛先へのログ出力 ····· 12-7
12.4.1. コンソールへのログ出力 ····· 12-7
12.4.2. モニタ端末へのログ出力 ····· 12-7
12.4.3. ログホストへのログ出力 ····· 12-8
12.4.4. ログバッファへのログ出力 ····· 12-9
12.4.5. ログファイルへのログ保存 ····· 12-9
12.5. ログの最小記録期間の設定 ····· 12-10
12.6. 情報の同期出力設定 ····· 12-11
12.7. ログの抑制設定 ····· 12-11
12.7.1. インタフェースでのリンクアップ/ダウンログの無効設定 ····· 12-11
12.8. Information Center の SNMP 通知の有効化 ····· 12-12
12.9. information center の表示と維持 ····· 12-12
12.10. Information center の設定例 ····· 12-13
12.10.1. コンソールへのログ出力の設定例 ····· 12-13
12.10.2. UNIX ログホストへのログ出力の設定例 ····· 12-13
12.10.3. Linux ログホストへのログ出力の設定例 ····· 12-15

12章 information center

12.1. 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。

図 12-1 Information center 図



12.1.1. Log 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。

12.1.2. ログレベル

ログは重要度により 0 から 7 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 から 6 までの重要度のログが出力されます。

表 12-1 Log レベル

重要度 (Severity)	レベル	説明
0	Emergency	システムが使用できません。たとえば、システムの認可が終了しました。
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 (Severity)	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。

12.1.3. 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。

12.1.4. デフォルトの出力ルール

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 12-2 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	Debug
モニタ端末	サポートされるすべてのモジュール	無効	Debug
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

12.1.5. 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 12-3 Diagnostic ログの出力ルール

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	Debug

12.1.6. 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 12-4 Hidden ログの出力ルール

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

12.1.7. ログのフォーマット

I. 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 12-5 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 12-5 Log 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 2016 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 2016 Sysname %%10 SHELL/5/SHELL_LOGIN: -DevIP=1.1.1.1; VTY logged in from 192.168.1.26

II. ログのフィールド説明

表 12-6 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リングするのに使用します • **level** は重要度(Severity)の範囲で 0 から 7 です。
Timestamp	ログが作成されたとき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。
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。
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	ログの送信元を示します。IRFスタックメンバIDとログの送信者のIPアドレスを含みます。
Content	ログの内容が記載されます。

表 12-7 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	ミリ秒
設定コマンド	**info-center timestamp loghost**	**info-center timestamp**

表 12-8 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。
date	ログホストに出力されるログの現在日時と時間です。フォーマットはmmm dd hh:mm:ss yyyです。あるいはほかの宛先に出力されるログの現在日時と時間です。フォーマットはMMM DD hh:mm:ss:xxx YYYY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 2003は**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(l): User ftp (192.168.1.23) has logged in successfully. 2003-05-30T06:42:44は**iso**フォーマットのタイムスタンプです。
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	年を除いた現在時間と時間です。フォーマットはMMM DD hh:mm:ss:xxx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。

12.2. Information centerの設定作業リスト

12.2.1. 一般的なログの管理

作業リスト
information centerの有効化

作業リスト
さまざまな宛先へのログ出力 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 • ログファイルへのログの保存
(オプション設定項目) ログの最小記録期間の設定
(オプション設定項目) 情報の同期出力設定
(オプション設定項目) ログの抑制設定 • インタフェースでのリンクアップ/ダウンログの無効設定
(オプション設定項目) Information CenterのSNMP通知の有効化

12.2.2. Hidden ログの管理

作業リスト
information centerの有効化
さまざまな宛先へのログ出力 以下の少なくとも1つの作業を実行します。 • 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 • ログファイルへのログの保存
(オプション設定項目) ログの最小記録期間の設定

12.2.3. diagnostic ログの管理

作業リスト
information centerの有効化

12.3. information centerの有効化

I. information center の有効化

information center を有効にした後、ログを出力することができます。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Information Center を有効にする	**info-center enable**	デフォルト：有効

12.4. さまざまな宛先へのログ出力

12.4.1. コンソールへのログ出力

I. 制限とガイドライン

terminal monitor、**terminal debugging**、**terminal logging** コマンドは装置に接続されているモニタ端末上でのみ機能します。新しい接続が行なわれた場合、新しいモニタ端末はデフォルト状態です。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. 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** { **deny** | **level** *severity* }	デフォルト出力ルールについての詳細は、セクション10 *システム管理 オペレーションマニュアルの”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。
3. (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**
4. user view に戻る	**quit**	―
5. 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。
6. 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
7. (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)

12.4.2. モニタ端末へのログ出力

I. モニタ端末

モニタ端末は、AUX、VTY、TTY を通して機器にログインする端末です。

II. 制限とガイドライン

terminal monitor、**terminal debugging**、**terminal logging** コマンドは装置に接続されているモニタ端末上でのみ機能します。新しい接続が行なわれた場合、新しいモニタ端末はデフォルト状態です。

III. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. 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** } **monitor** { **deny** | **level** *severity* }	デフォルト出力ルールについての詳細は、セクション10 *システム管理 オペレーションマニュアル*の”*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。
3. (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**
4. user view に戻る	**quit**	―
5. 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。
6. 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
7. (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)

12.4.3. ログホストへのログ出力

I. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. 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 } loghost { deny | level** *severity* **}**	デフォルト出力ルールについての詳細は、セクション10 *システム管理 オペレーションマニュアル*の”*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。
3. (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。
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 loghost { date | iso | no-year-date | none }**	デフォルト：**date**

操作	コマンド	補足
5. 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** { *ipv4-address* | **ipv6** *ipv6-address* } [**port** *port-number*] [**facility** *local-number*]	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。

12.4.4. ログバッファへのログ出力

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. ログバッファの出力ルールを設定する	**info-center source { *module-name* | default } logbuffer { deny | level** *severity* **}**	デフォルト出力ルールについての詳細は、セクション10 *システム管理 オペレーションマニュアルの”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。
3. (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**
4. 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
5. (オプション設定項目) ログバッファに保存できるバッファサイズの最大数を設定する	**info-center logbuffer size** *buffersize*	デフォルト：512

12.4.5. ログファイルへのログ保存

I. ログファイルへのログの保存

ログをログファイルに保存する前にログファイルバッファと呼ばれる一時バッファに出力します。ログファイルバッファをログバッファと混同しないでください。それはログの出力先と独立しています。

システムは指定された間隔(デフォルトで 24 時間)でログバッファのログをログファイルに保存します。また手動で保存することができます。ログファイルバッファにログを保存した後、システムはログファイルバッファをクリアします。

装置は 1 つのログファイルのみをサポートし、必要な時に自動生成されます。ログファイルが容量に達すると、システムは最初のログに新しいログを上書きします。

ポイント:

ログファイルを作成するため、定期的に装置の記憶媒体に空き容量があることを確認してください。ログファイルを作成できない場合、ログはログファイルに保存できません。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. ログファイル機能を有効にする	**info-center logfile enable**	デフォルト：有効
3. (オプション設定項目) ログファイルの最大記憶容量を設定する	**info-center logfile size-quota** *size*	デフォルト：10MB ログファイルの動作を正常に行うため、1MB～10MBのサイズに設定してください。
4. (オプション設定項目) ログファイルを保存するディレクトリを指定する	**info-center logfile directory** *dir-name*	デフォルト：flash:/logfile IRFスタックの再起動やマスタ/メンバの切り替えで設定は消去されます。
5. ログファイルにログファイルバッファのログを保存する	• アプローチ 1：ログファイルを記録する間隔を設定する **info-center logfile frequency** *freq-sec* • アプローチ 2：手動でログファイルを記録する **logfile save**	デフォルト：ログファイルを記録する間隔は86400秒です。 すべてのviewで**logfile save**コマンドを実行できます。

メモ:

info-center logfile frequency コマンドでログファイルをセーブする周期を著しく短くした場合、フラッシュメモリの書き込み可能回数の超過や、装置動作に影響を与える恐れがあります。

したがって、通常はデフォルト値での使用を推奨します。

12.5. ログの最小記録期間の設定

I. 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とき、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。

II. 設定手順

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

12.6. 情報の同期出力設定

I. 情報の同期出力

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。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. 情報の同期出力を設定する	**info-center synchronous**	デフォルト：無効

12.7. ログの抑制設定

12.7.1. インタフェースでのリンクアップ/ダウンログの無効設定

I. インタフェースでのリンクアップ/ダウンログの無効設定

デフォルトでは、インタフェースのリンク状態が変わるとき、装置のすべてのインタフェースはアップ/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。

- 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。

インタフェースの状態監視のために、正常時はデフォルト設定で使用することを推奨します。

II. 設定手順

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

操作	コマンド	補足
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とき、リンクアップ/ダウンのログ情報を生成します。

12.8. Information CenterのSNMP通知の有効化

I. システムログの SNMP 通知の有効化

snmp-agent trap enable syslog コマンドを有効にすると、装置は syslog メッセージによる SNMP 通知の送信を有効にします。装置は SNMP 通知をカプセル化し、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 通知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、セクション 10 *システム管理 オペレーションマニュアル*の“*SNMP*”を参照してください。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. Information Center の SNMP 通知を有効にする	**snmp-agent trap enable syslog**	デフォルト：無効

12.9. 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
各出力先の情報を表示する	**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**

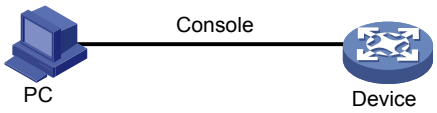
12.10. Information centerの設定例

12.10.1. 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 12-2 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

不要な情報のログ出力を防ぐため、出力ルールを設定する前に、すべてのモジュールから指定した宛先（この例ではコンソール）にログ情報の出力を無効にします。

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とき、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。

12.10.2. 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 12-3 ネットワーク図



II. 設定手順

設定を行う前に、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

   不要な情報のログ出力を防ぐため、出力ルールを設定する前に、すべてのモジュールから指定した宛先（この例ではログホスト）にログ情報の出力を無効にします。

   # 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。

   以下の設定は Solaris で行ったものです。ほかの UNIX システムの設定は同様に行います。

   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 を編集するとき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。

```
# 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。

12.10.3. 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 12-4 ネットワーク図



II. 設定手順

設定を行う前に、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

不要な情報のログ出力を防ぐため、出力ルールを設定する前に、すべてのモジュールから指定した宛先（この例ではログホスト）にログ情報の出力を無効にします。

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。

以下の設定は Solaris で行ったものです。ほかの UNIX システムの設定は同様に行います。

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
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** を編集するとき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** の使用を再開します。

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 **10-x-x** です。

13 章 NetMeister 13-1
13.1. 概要 13-1
13.1.1. NetMeister の利用 13-1
13.1.2. 設定手段について 13-3
13.2. 設定作業リスト 13-4
13.2.1. 手動設定による NetMeister の利用 13-5
13.3. NetMeister の表示と維持 13-8
13.3.1. ゼロタッチプロビジョニング機能による NetMeister の利用 13-9
13.4. NetMeister による管理 13-17
13.4.1. タブ一覧 13-17
13.5. NetMeister の設定例 13-18

13章 NetMeister

🕮 **メモ:**

本機能は Version 7.2.15 を含む以降のソフトウェアから子機モードでの NetMeister への接続をサポートし、Version7.4.35 を含む以降のソフトウェアから親機モードでの NetMeister の接続をサポートしています。
IRF スタックでの NetMeister 利用は、Version7.4.30 を含む以降のソフトウェアからサポートしています。IRF スタックで利用する場合、MAC アドレスが Master 選定によって変化しないように **irf mac-address persistent always** コマンドを設定してください。また、IRF 分裂によって同一 MAC の装置が複数登録されないように MAD 機能を利用して下さい。

13.1. 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 の詳細、運用については、以下の URL を参照してください。

https://www.necplatforms.co.jp/product/netmeister/

13.1.1. NetMeister の利用

NetMeister を利用する場合、あらかじめ NetMeister のサイトで「ユーザーアカウント登録」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。

子機モードの機器を NetMeister によって管理する場合、図 13-1 に示すように、親機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。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。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 上で管理されます。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)

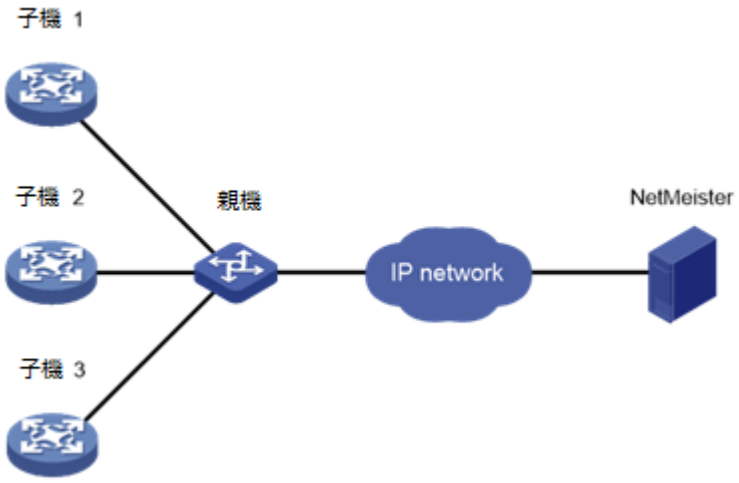


図 13-1 NetMeister の利用環境

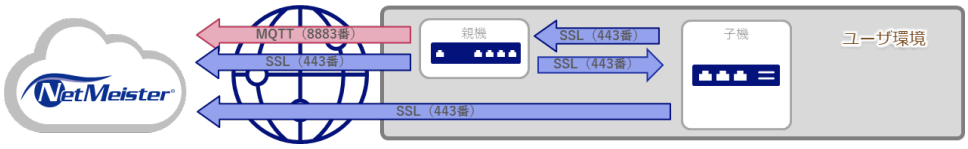


図 13-2 NetMeister への通信イメージ

Version 7.2.23 を含む以降のソフトウェアでは、図 13-2 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。

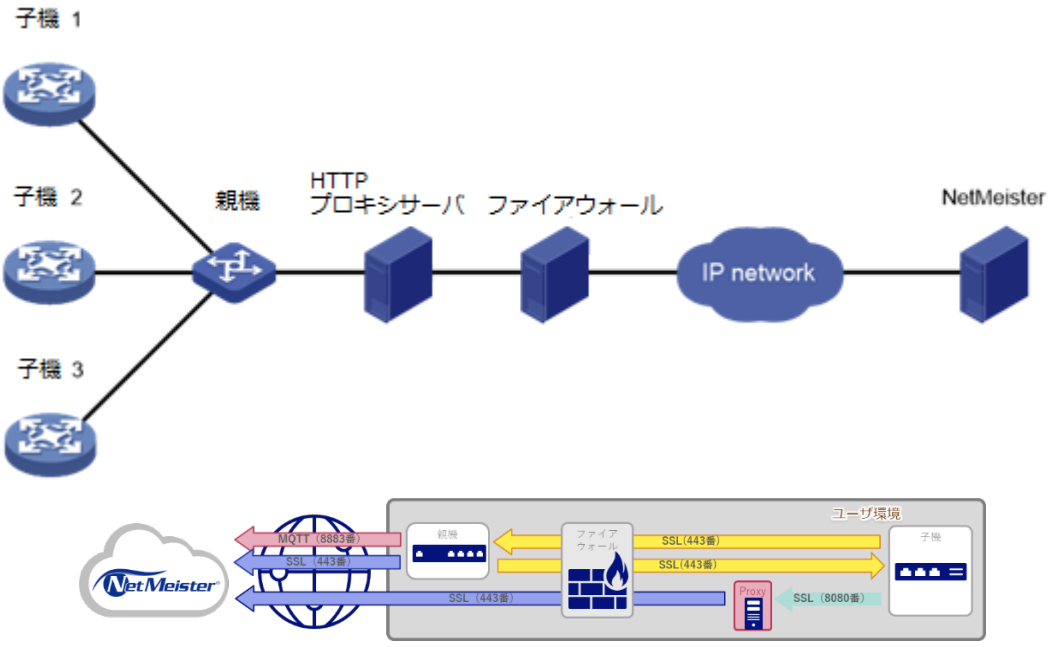


図 13-3 プロキシサーバを用いた NetMeister の通信イメージ

メモ:

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。

13.1.2. 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。

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。

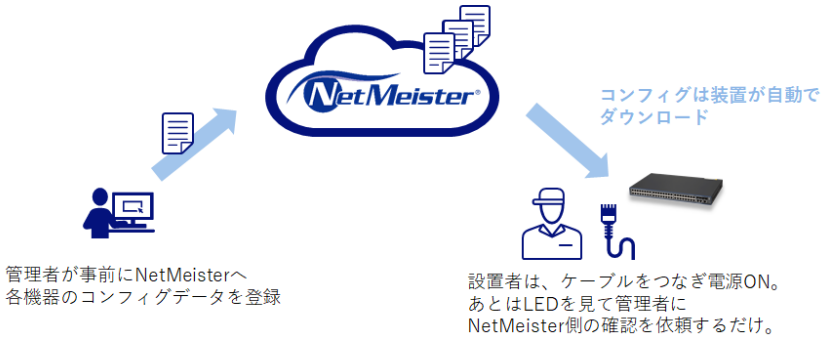


図 13-4 ゼロタッチプロビジョニングのイメージ

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。

13.2. 設定作業リスト

作業リスト
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

作業リスト
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 • (オプション設定項目) イベントログの送信無効の設定 • (オプション設定項目)注意レベルの NM アラームの送信有効の設定 • (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 • (オプション設定項目) イベントログの送信無効の設定 • (オプション設定項目)注意レベルの NM アラームの送信有効の設定 • (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

13.2.1. 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**	—

操作	コマンド	補足
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*	—
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**	—
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** *dest-address* { *mask-length* | *mask* } { *interface-type interface-number* [*next-hop-address*] | *next-hop-address* } [**permanent** | **track** *track-entry-number*] [**preference** *preference*] [**tag** *tag-value*] [**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. (必須設定項目) 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. (オプション設定項目) イベントログの送信を無効にする。	**undo netmeister event log enable**	デフォルト：V7.4.37以降のソフトウェアからイベントログを送信します。
9. (オプション設定項目) イベントログ(syslog)の送信を無効にする。	**undo netmeister event syslog enable**	デフォルト：V7.4.48以降のソフトウェアからsyslogを送信します。
10. (オプション設定項目) 注意レベルの NM アラームの送信を有効にする。	**netmeister alarm enable notice**	デフォルト：無効 V7.4.37以降のソフトウェアからサポート。
11. 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

操作	コマンド	補足
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. (オプション設定項目) イベントログの送信を無効にする。	**undo netmeister event log enable**	デフォルト：V7.4.37以降のソフトウェアからイベントログを送信します。
7. (オプション設定項目) イベントログ(syslog)の送信を無効にする。	**undo netmeister event syslog enable**	デフォルト：V7.4.48以降のソフトウェアからsyslogを送信します。
8. (オプション設定項目) 注意レベルの NM アラームの送信を有効にする。	**netmeister alarm enable notice**	デフォルト：無効 V7.4.37以降のソフトウェアからサポート
9. (オプション設定項目) NGN 閉域網経由の NetMeister 接続の有効化	**netmeister ngn enable**	デフォルト：無効 v7.4.48以降のソフトウェアからサポート。
10. NetMeister 機能の有効化	**netmeister enable**	デフォルト：無効

🕮 **メモ:**
netmeister proxy コマンドは Version 7.2.23 を含む以降のソフトウェアからサポートしています。
QX を NGN 閉域網経由で NetMeister に接続するためには、NGN 閉域網コントロール子機収容に対応し、NGN 閉域網経由で NetMeister に接続している IX-R(親機)が必要です。また、QX を NGN 閉域網経由で NetMeister に接続するために、proxy サーバ指定(netmeister proxy)を、IX-R に設定されている子機接続用 HTTP プロキシアドレス設定(tunnel nm-child-ngn-proxy)のアドレス、ポート番号に合わせて設定する必要があります。

13.3. 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**

13.3.1. 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 7.4.30 を含む以降のソフトウェアからサポートしています。

IV. 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) 親機の設定

子機(QX)でゼロタッチプロビジョニング機能を利用する場合、子機がインターネット上の NetMeister と接続を行うために、親機に DHPC サーバ及び「ゼロタッチプロビジョニング子機対応」の設定をしてください。設定方法は親機のマニュアル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。
- ゼロタッチプロビジョニング子機対応：子機がゼロタッチプロビジョニングを利用する場合に親機で設定をしてください。

🕮 **メモ:**

親機が 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親機と同様の 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。

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。

V. 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。

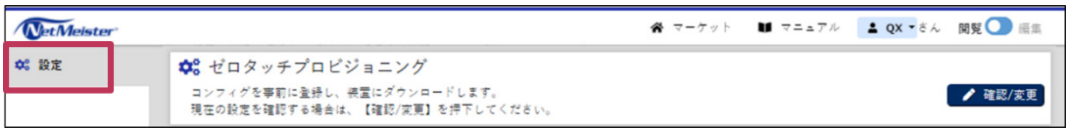


図 13-5 設定メニューの表示

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 13-6 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 13-7 コンフィグ登録画面

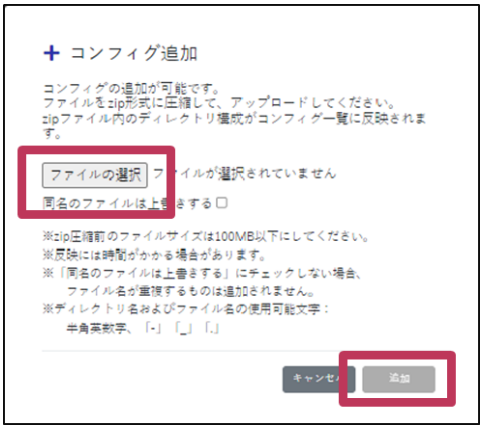


図 13-8 コンフィグの選択

🕮 **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。

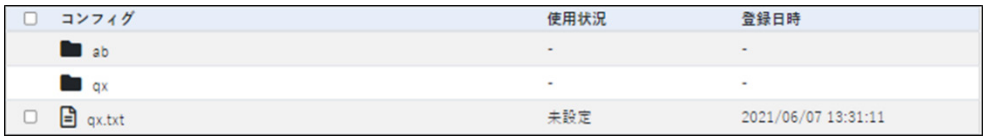


図 13-9 コンフィグ登録後の表示

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。

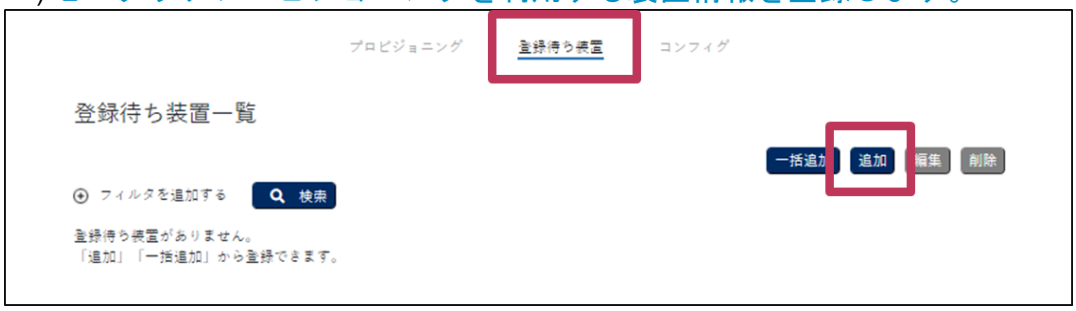


図 13-10 登録待ち装置設定画面



図 13-11 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 13-12 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 13-13 プロビジョニングの設定画面

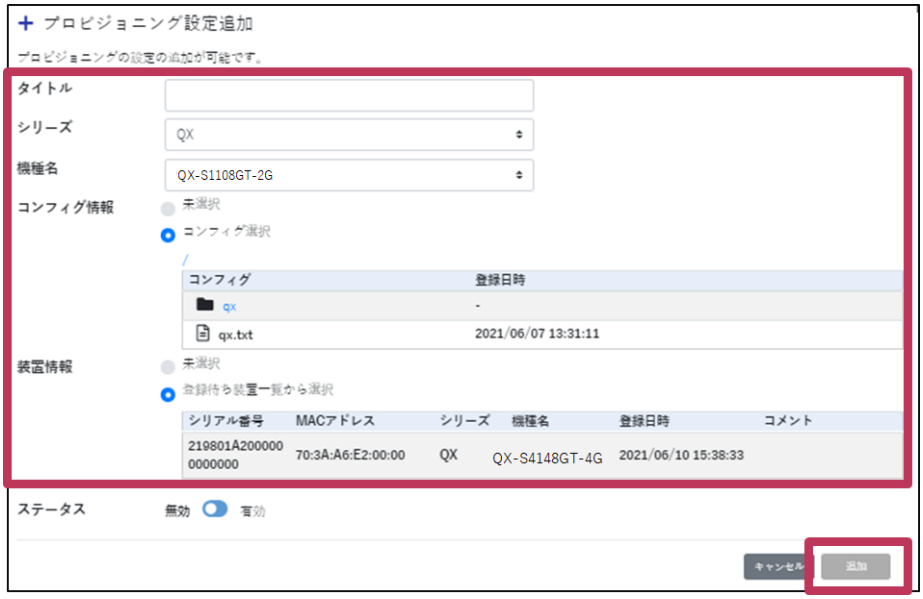


図 13-14 装置とコンフィグの選択

🕮 **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。

VI. 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 13-15 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 13-16 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 13-1 QX-S5300G 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 13-17 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 13-18 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。

VII. 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。

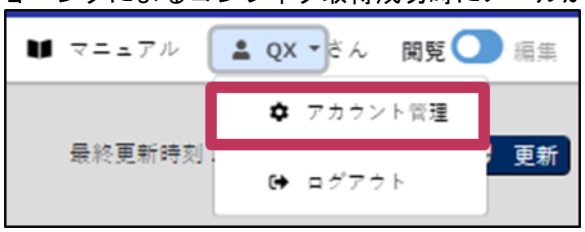


図 13-19 アカウント管理



図 13-20 通知の設定

13.4. NetMeisterによる管理

Netmeister の操作、及び、対応機能に関しては、以下の URL より NetMeister が提供する操作ガイドをご確認ください。

https://www.necplatforms.co.jp/product/netmeister/

13.4.1. 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、NetMeister prime の利用によって表示、利用可能になる機能もあります。詳細は NetMeister が提供する操作ガイドをご確認ください。

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。
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。 オプション装置は対象外です。
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。オプション装置は対象外です。
ログ	V7.4.37 を含む以降のソフトウェアで表示されます。 NetMeister から定期的に装置情報を取得し、NetMeister に保存できます。装置ごとに、時間帯を指定できます。オプション装置は対象外です。
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。 オプション装置は対象外です。

タブ名	説明
ポート状態	物理インタフェースの情報を表示します。 オプション装置は対象外です。

13.5. NetMeisterの設定例

I. ネットワーク要件

図 13-21 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「ユーザーアカウント登録」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(bbb)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できる設定を行い、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。

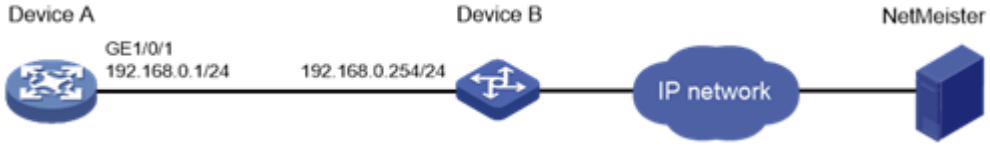


図 13-21 ネットワーク図

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. 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(bbb)を設定します。

   [DeviceA] netmeister account aaa password simple bbb

   # 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

QX-S5300G シリーズ Ethernet スイッチ

オペレーションマニュアル

11. 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 **11-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/
11-1-10

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]

[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]
[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]

[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]
[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 ｩ 2003 Sun 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 <wsanchez@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

Networks Associates 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]

[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]
[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]

[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]

[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.

[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]
[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]
[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]

[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]

[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]

[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]

[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

[rpcapd 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.

[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]
//
//
/// \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
