Future X Communications

FXC3524 Management Guide

2007年5月 Ver.1.0

FXC株式会社

本マニュアルについて

- 本マニュアルでは、FXC3524 の各種設定およびシステムの監視手順について説明します。本製品の設定および監視は、RS-232C シリアルポートまたは、イーサネットポートに設定、監視用の端末接続して、CLI （コマンドラインインタフェース）または Web ブラウザで行います。
- 本マニュアルに記載している機能は、ファームウェアバージョン 4.86i 以降の製品に対応しています。

目次

1. 本書について

1.1 リリースノート

本書は、レイヤ 3 10/100Mbps ルーティングスイッチ FXC3524 の取扱説明書です。

1.2 対象読者

本書は、次の読者を対象としています。

- ネットワークエンジニア
- ネットワーク管理者
- ネットワークの基礎知識をお持ちの方

1.3 表記法

本書は、次の表記法に従って記載しています。

1.3.1 コマンドの表記法

表記方法	内容
太字	コマンドラインのキーワードは太字で記載しています。
斜体	コマンドの引数は斜体で記載しています。
[ ]	角かっこ [ ] で囲んでいる項目（キーワードまたは引数）は、省略可能です。
{x | y | ...}	選択肢は大かっこ { } で囲み、それぞれ垂直線で区切って記載しています。1 つ選択できます。
[x | y | ...]	選択肢は角かっこ [ ] で囲み、それぞれ垂直線で区切って記載しています。選択しないか、または 1 つ選択します。

1.3.2 GUI の表記法

表記方法	内容
< >	ボタン名は山かっこ < > で囲んで記載しています。例：<OK> ボタンをクリックします。
[ ]	ウィンドウ名、メニュー項目、データテーブル、およびフィールド名は山かっこ [ ] で囲んで記載しています。例：[New User] ウィンドウをポップアップします。
/	メニュー階層は、スラッシュで区切って記載しています。例：[File/Create/Folder]

1.3.3 注意

本書では、重要な注意事項を、太字で強調しています。

[注意]　操作中、特に注意する点です。

（白紙）

2. 製品概要

2.1 FXC3524 の概要

10/100Mbps レイヤ 3 ルーティングスイッチ FXC3524 はボックス型、レイヤ 2/ レイヤ 3 でワイヤスピードを実現するイーサネットスイッチで、多くのレイヤから構成される小中規模のエンタープライズネットワーク、IP 網で接続されているメトロポリタンエリアネットワーク（MAN）、また、住宅地のイーサネットに利用できます。

本機は次のサービスをサポートしています。

- インターネットへのブロードバンドアクセス
- MAN、エンタープライズ / キャンパスネットワーク
- マルチキャストサービス、マルチキャストルーティング、音声・映像のマルチキャスト配信サービス

2.2 各機能の詳細

機能	解説
VLAN	IEEE 802.1Q 標準の VLAN に準拠 GVRP（GARP VLAN Registration Protocol）をサポート
STP	STP（Spanning Tree Protocol）をサポート
フローコントロール	IEEE 802.3x フローコントロール（Full-Duplex） バックプレッシャーフローコントロール（Half-Duplex）
Broadcast Suppression	Broadcast Suppression をサポート
マルチキャスト	IGMP スヌーピング（Internet Group Management Protocol Snooping） IGMP（Internet Group Management Protocol） PIM-SM（Protocol-Independent Multicast-Sparse Mode）
IP ルーティング	IP Static ルーティング RIP（Routing Information Protocol）v1/v2 OSPF（Open Shortest Path First）
DHCP	DHCP（Dynamic Host Configuration Protocol）リレー DHCP（Dynamic Host Configuration Protocol）サーバ
ポートトランク	ポートトランクをサポート
ミラーリング	ミラーリング（ポートベース /ACL ベース）
QoS（Quality of Service）	トラフィックのクラス分け / 帯域幅制御 / ポートに対する異なるプライオリティキュー / キューイングスケジュール：SP（Strict Priority Queuing）、 WRR（Weighted Round Robin）、および SP+WRR
セキュリティ	マルチレベルでのユーザ管理とパスワードによる保護 IEEE 802.1X 認証 パケットフィルタリング
マネージメントと保守	CLI（Command Line Interface）による設定 / コンソールポートまたは AUX ポートからのローカル設定 / Telnet 経由でのローカル / リモート設定 / SNMP マネージメント（RMON MIB Group1,2,3,9）/ デバッグ情報の出力 /PING
ソフトウェアの読み込みとアップデート	FTP（File Transfer Protocol）または TFTP（Trivial File Transfer Protocol）経由でのソフトウェアの読み込みとアップデートをサポート

3. 本機へのログイン

3.1 本機へのログイン

3.1.1 設定環境のセットアップ（コンソールポート経由）

手順 1：下図のように、コンソールケーブルを使用し、PC（ターミナル）のシリアルポート - 本機のコンソールポートを接続して、ローカルでの設定環境のセットアップをおこないます。

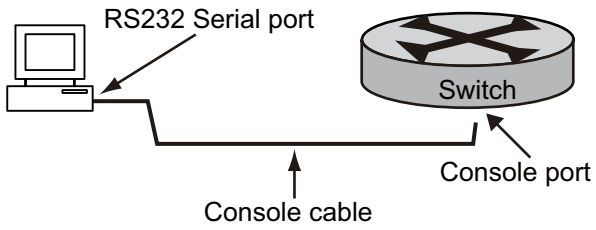


図 1　コンソールポートを介したローカル設定環境のセットアップ

手順 2：PC で、ターミナルエミュレータ（Windows 3.x のターミナル、Windows 9x 以降のハイパーターミナルなど）を起動します。次のように、ターミナルエミュレータの通信パラメータを設定します。

- **通信速度：**9600
- **データビット：**8
- **パリティ：なし**
- **ストップビット：**1
- **フロー制御：なし**
- **ターミナルの種類：**VT100

図 2　新しい接続の設定

図 3　接続ポートの設定

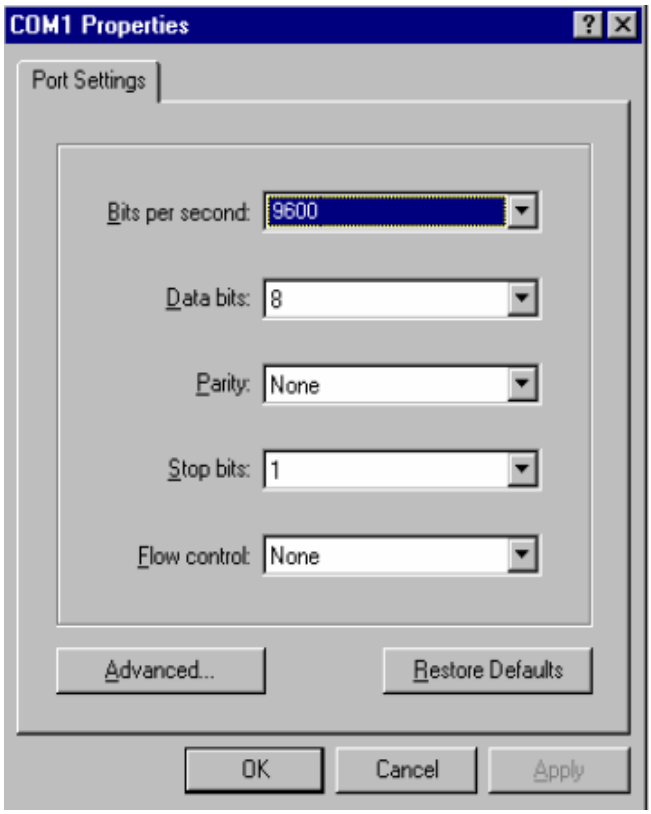


図 4　通信パラメータの設定

手順 3：本機の電源をオンにします。セルフテスト情報が表示され、<Enter> キーを押して switch> のようなコマンドラインプロンプトを表示するよう促します。

手順 4：コマンドを入力し、本機の設定をおこなうか、または動作状態を表示します。「?」を入力すると、クイックヘルプが表示されます。各コマンドの詳細については、以降の説明箇所を参照してください。

3.2 設定環境のセットアップ（Telnet 経由）

3.2.1 Telnet 経由での本機と PC の接続

本機で Telnet 接続を行う前に、まずコンソールポート経由で正しく本機の VLAN インターフェースに IP アドレスを設定し Telnet 接続をおこなうポートを（VLAN 画面のポートコマンドを使用）この VLAN に追加してください。

手順 1：コンソールポート経由で Telnet ユーザの認証をおこない、Telnet にログインします。

手順 2：設定環境をセットアップするには、LAN 経由で PC のイーサネットポートと本機のイーサネットポートを接続します。

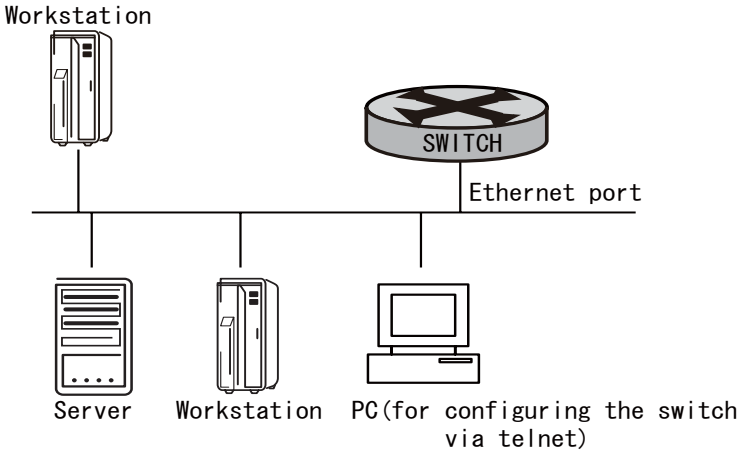


図 5　Telnet 経由での設定環境のセットアップ

手順 3：PC で Telnet を起動し、PC のポートに接続している VLAN の IP アドレスを入力します。

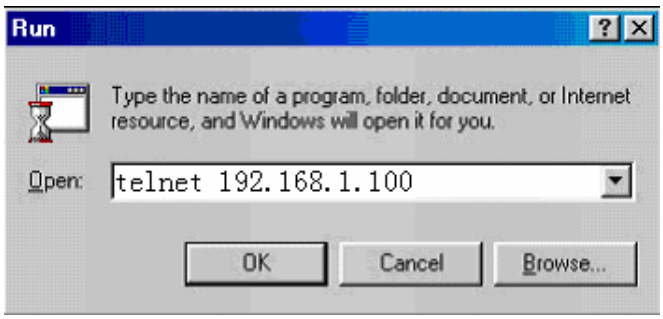


図 6　Telnet の実行

手順 4：ターミナルに「Login:」と表示され、ログインユーザ名とパスワードを要求されます。正しいユーザ名とパスワードを入力すると、コマンドラインプロンプト（switch# など）が表示されます。

手順 5：関連コマンドを使用し、本機の設定や稼動状態の監視をおこないます。? を入力すると、即時にヘルプが表示されます。各コマンドの詳細については、以降の説明箇所を参照してください。

3.2.2 ほかのスイッチから本機への Telnet 経由での接続

スイッチへのログイン後、このスイッチから Telnet 経由で別のスイッチの設定をおこなうことができます。ローカルスイッチが Telnet クライアント、通信先のスイッチが Telnet サーバとして機能します。この 2 台のスイッチが接続しているポートが同じローカルネットワークに所属している場合、両スイッチには同一のネットワークセグメントの IP アドレスを設定する必要があります。

そうでない場合、相互に到達可能な経路を両スイッチに確立しておく必要があります。

下図に示すように、スイッチに Telnet ログインしたあと、もう一台のスイッチに telnet コマンドを実行してログインし、設定をおこないます。

図 7　Telnet クライアントサービスの使用

手順 1：コンソールポート経由で Telnet ユーザの認証をおこない、Telnet サーバ（スイッチ）にログインします。

手順 2：Telnet クライアント（スイッチ）にログインします。ログインプロセスについては、「Telnet 経由での本機と PC の接続」の項の説明を参照してください。

手順 3：Telnet クライアントで次の操作をおこないます。

手順 4：ログインパスワードを入力すると、switch# のようなプロンプトを表示します。

手順 5：関連コマンドを使用し、本機の設定や稼動状態の監視をおこないます。? を入力すると、即時にヘルプが表示されます。各コマンドの詳細については、以降の説明箇所を参照してください。

3.3 設定環境のセットアップ（Web 経由）

本機に組み込んでいる HTTP エージェント機能を使用できます。Web ブラウザを使用し、本機の設定やネットワーク利用状態を監視するための統計情報の表示をおこなうことができます。本機の Web エージェント機能には、一般的な Web ブラウザ（Internet Explorer 5.0 以降、または Netscape Navigator 6.2 以降）を使用し、同一ネットワークに所属するコンピュータからアクセスできます。

Web ブラウザを使用して本機へアクセスする前に、まず以下の実行をおこなうことに注意してください。

（1）アウトバンドのシリアル接続をおこない、有効な IP アドレス、サブネットマスク、デフォルトゲートウェイアドレスを本機に設定します。

（2）ユーザ名とパスワードを入力すると、本機の設定プログラムにアクセスできます。

3.3.1 Web ブラウザインターフェースの構成

Web ブラウザインターフェースにアクセスするには、最初にユーザ名とパスワードを入力する必要があります。管理者はすべてのパラメータの設定情報と統計情報に読み取り / 書き込みの権限があります。初期設定のユーザ名・パスワードは以下です。

ユーザ名：admin

パスワード：password

3.3.2 設定ボタン

設定パラメータにはダイアログボックスかドロップダウンリストがあります。画面で設定項目を変更したら、<Apply> または <Refresh> ボタンをクリックして変更後の設定を必ず確定させます。次の表に、Web 画面での設定ボタンをまとめます。

ボタン	実行内容
<Refresh>	その画面の値を最新の状態に更新します
<Apply>	設定値を適用します
<Delete>	設定値を削除します

3.4 コマンドラインインターフェース

3.4.1 コマンドラインインターフェース

本機は、本機の設定・マネージメントのための一連のコマンドとコマンドラインインターフェースを提供しています。
本機のコマンドラインインターフェースには次の特徴があります。

- コンソールポートまたは AUX ポートからの、ローカル設定をサポート
- Telnet 経由のローカルまたはリモート設定
- 階層形式のコマンド保護により、非認証ユーザからのスイッチへのアクセスを回避。? の入力による、即時のヘルプ表示
- Ping に類するネットワーク検証コマンドにより、ネットワークのすばやいトラブルシューティング
- Telnet コマンドを使用した、他のスイッチへの直接のログインとマネージメント
- FTP サービスにより、ユーザによるファイルのアップロードとダウンロード
- Doskey に類する機能を提供し、ヒストリコマンドを実行可能
- 完全にキーワードが一致しない場合も、コマンドラインインタープリタによる正しいキーワードを検索
- 一意的で明確な場合、完全なキーワードまたはその一部を入力するだけで可能

3.4.2 コマンドライン設定モード

本機のコマンドラインには、次の設定モードがあります。

- 通常の実行モード（Normal EXEC）
- 特権的実行モード（Privileged EXEC）
- グローバル設定モード（Global Configuration）
- VLAN インターフェース設定モード（VLAN Inferface Configuration）
- OSPF 設定モード（OSPF Configuration）

次の表で、各モード別に機能・違い・そのモードへの移行や終了方法について記載します。

コマンド mode	機能	プロンプト	Command to enter	Command to exit
通常の実行モード（Normal EXEC）	動作と統計情報に関する基本的な情報の表示	Switch>	正しいユーザ名とパスワードの入力	exit
管理者モード（Privileged EXEC）	動作と統計情報に関する基本的な情報の表示	Switch#	<enable> および正しいパスワード	Exit により通常の実行モードに戻る
グローバル設定モード（Global configuration）	システムパラメータの設定	Swich(config)#	ユーザ設定モードのユーザで config と入力	Exit を実行。ユーザ設定モードへ戻る
VLAN インターフェース設定モード（VLAN Interface configuration）	VLAN 関連パラメータの設定	Swich(config-if)#	システム設定モードで Interface vint x と入力	Exit を実行。ユーザ設定モードへ戻る
OSPF 設定モード（OSPF configuration）	OSPF パラメータの設定	Swich(config-ospf)#	システム設定モードで Router ospf と入力	Exit を実行。ユーザ設定モードへ戻る

3.4.3 コマンドラインの機能

コマンドラインのオンラインヘルプ

コマンドラインインターフェースでは、次のオンラインヘルプモードを提供しています。

- **完全なヘルプ**
- **部分的なヘルプ**

以下に記載するオンラインヘルプコマンドを使用し、ヘルプ情報を参照できます。

いずれかの設定モードで ? を入力すると、そのモードで有効なすべてのコマンドとその説明を表示します。

```
switch#?
  clear     Clear the screen.
  config    Config system's setting.
  debug     Debugging functions
  download  Download file for software upgrade or load user config.
  exit      Exit current mode and shift to previous mode.
  help      Description of the interactive help system.
  history   Config history command.
  kill      Kill some unexpected things.
  logout    Disconnect from switch and quit.
  no        Negate a command or set its defaults.
  ping      Ping command to test if the net is correct.
  quit      Disconnect from switch and quit.
  reboot    Reboot the switch.
  remove    Remove system configuration.
  sendmsg   Send message to online user.
  show      Show running system information.
  telnet    Telnet to other host or switch.
  terminal  Set terminal line parameters.
  upload    Upload file for software upgrade or upload user config.
  who       Display who is connected to the switch.
  write     Save current running configuration to flash.
```

(1) **コマンドの次にスペースを 1 つあけて、? を入力します。それがキーワードの一部の場合、すべてのキーワードとそれに関する短い説明が表示されます。**

```
swich(config)# port ?
  speed  Set port speed.
  state  Set port state.
  type   Set port type.
```

(2) コマンドの次にスペースを 1 つあけて、? を入力します。それがパラメータの一部の場合、すべてのパラメータとそれに関する短い説明が表示されます。

```
swich(config)# router ?
  hw-sync  Dynamic route synchronize with hardware route table
  ospf     OSPF specific commands
  rip      Set Rip config parameters.

switch(config)# router ospf ?
  <cr>  Just Press <Enter> to Execute command!
```

*<cr> は、この部分にはパラメータが存在しないことを示します。次のコマンド行でこのコマンドを再度表示するため、<Enter> を押すとそのまま実行できます。

(3) 文字 1 つに続けて ? を入力すると、この文字から始まるすべてのコマンドを表示します。

```
switch(config)# a?
  access-list     Set access-list parameters.
  arp             Config system's setting.
  authentication  Config information of authentication.
```

(4) コマンド 1 つに続けて ? を入力すると、そのコマンドの、この文字から始まるすべてのキーワードを表示します。

```
switch# show ve ?
  version  Display SPROS version.
```

(5) コマンドのキーワードの最初の文字をいくつか入力し、<Tab> キーを押します。この文字列に続くキーワードがほかに存在しない場合、特定されたキーワードが自動的に表示されます。

コマンドラインインターフェースの表示に関する特徴

コマンドラインインターフェースには、次の表示に関する特徴があります。

- 利便性に配慮し、説明文やヘルプ情報は英文と中文の両方で表示されます。
- 情報が 1 画面を超えて表示される場合、一時停止機能が働きます。この場合、次の表に示す 3 つの方法から選択できます。

キーまたはコマンド	機能
表示が一時停止した際、<Q> を押す	表示を止め、コマンドを実行
表示が一時停止した際、任意のキーを押す	次画面の情報表示を継続
表示が一時停止した際、<Enter> を押す	次行の情報表示を継続

コマンドラインのヒストリコマンド

コマンドラインインターフェースでは、DosKey に類似する機能を提供しています。
入力されたコマンドは、自動的に保存され、その後いつでも呼び出して実行することができます。

ヒストリコマンドバッファは初期設定では 10 です。つまり、コマンドラインインターフェースは、各ユーザごとに 10 個のヒストリコマンドを保存できます。
操作を次の表に示します。

操作	キー	結果
ヒストリコマンドの表示	history	ユーザが入力したヒストリコマンドを表示
直前のヒストリコマンドの表示	Up cursor key < ↑ > or<Ctrl+P>	存在する場合、直前のヒストリコマンドを表示
次のヒストリコマンドの表示	Down cursor key < ↓ >or <Ctrl+N>	Retrieve the next history 存在する場合、直前のヒストリコマンドを表示

主なコマンドラインエラーメッセージ

入力したコマンドは構文チェックに合格すると、正しく実行できます。それ以外の場合、エラーメッセージが表示されます。次の表に主なエラーメッセージを記載します

エラーメッセージ	原因
Unrecognized command	存在しないコマンド
	存在しないキーワード
	パラメータの種類の誤り
	パラメータの設定値が範囲外
Incomplete command	入力されたコマンドが不完全
Too many parameters	入力されたパラメータが多すぎ
Ambiguous command	入力されたパラメータが特定不能

コマンドラインインターフェースの編集に関する特徴

コマンドラインインターフェースは、基本的なコマンド編集機能を提供しており、複数行の編集もサポートしています。1 つのコマンドは 256 文字以下に制限されています。

以下の表を参照してください。

キー	機能
主なキー	編集用のバッファに空き容量があれば、カーソルの挿入位置から右に動く
Backspace	カーソルを 1 文字逆方向に移動
左矢印キー < ← > または <Ctrl+B>	カーソルを 1 文字逆方向に移動
右矢印キー < 右 > または <Ctrl+F>	カーソルを 1 文字順方向に移動
上矢印キー < ↑ > または <Ctrl+P> 下矢印キー < ↓ > または <Ctrl+N>	直前のヒストリコマンドの表示
<Tab>	<Tab> キーをキーワードが不完全な場合に押すと、システムが部分的なヘルプを実行します。入力されたキーワードがキーワードに特定または一致した場合、システムが補完したキーワードに置き換えられて次の行に表示しますが、特定できない場合または一致しない場合、システムが置き換えをおこなわずに元に入力されたキーワードのまま次の行に表示します。

4. 基本設定

4.1 コンソール接続

CLI プログラムは、2 つの異なるコマンドレベルを提供しており、通常のアクセスレベル（Normal Exec）と特権的なアクセスレベル（Privileged Exec）があります。

Normal Exec レベルで使用可能なコマンドは、Privileged Exec レベルに比べ制限されており、情報の表示と基本的なユーティリティの使用のみ可能です。本機のパラメータをすべて設定する場合、Priviledged Exec レベルで CLI にアクセスする必要があります。いずれの CLI レベルへのアクセスはユーザ名とパスワードで制限されます。

本機には、各レベルに対して初期設定のユーザ名とパスワードがあります。CLI に初期設定のユーザ名とパスワードを使用して Privileged Exec レベルでログインするには、次の手順を実行します。

（1）<Enter> を押し、コンソール接続を開始します。「ユーザアクセスの認証」手続きを開始します。

（2）<Login:> プロンプトで、admin と入力します。

（3）パスワードのプロンプトが表示されたら <Enter> キーを押します（初期パスワードは設定されていません）。

（4）セッションが開始し、CLI は switch> プロンプトを表示して Normal Exec レベルでのアクセスが完了したことを示します。

（5）switch> プロンプトで enable と入力します。

（6）パスワードのプロンプトが表示されたら <Enter> キーを押します（初期パスワードは設定されていません）。

（7）セッションが開始し、CLI は switch# プロンプトを表示して Privileged Exec レベルでのアクセスが完了したことを示します。

4.2 データ転送速度の設定

はじめに Privileged Exec モードに移行し、次の手順でコンソールのデータ転送速度を設定します。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**serial speed** *rate*	コンソールのデータ転送速度を設定します。 速度：19200、2400、38400、9600. （初期設定：9600）
手順 3	**exit**	Privileged Exec モードに戻ります。
手順 4	**show serial**	入力を確認します。
手順 5	**write**	（オプション）設定ファイルに入力を保存します。

4.3 ユーザー名 / パスワードの設定

新しいユーザを作成した際、初期設定のユーザは自動的に削除されます。

はじめに Privileged Exec モードに移行し、次の手順でユーザを作成し、パスワードを設定します。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**user add** *user-name* **login-password** *login-password*	ユーザを作成し、ログインパスワードを設定します。
手順 3	**user login-password** user-name <CR> Input new login password for user abc please. New Password: Confirm Password:	（オプション）ログインパスワードを変更します。
手順 4	**user enable-password** *user-name* <CR> Input new enable password for user abc please. New Password: Confirm Password:	（オプション）有効なパスワードを設定 / 変更します。
手順 5	**user role** *user-name* **{NORMA | ADMIN enable-password** *enable-password* **}**	（オプション）ユーザのアクセスレベルを変更します。
手順 6	**exit**	Privileged Exec モードに戻ります。
手順 7	**user list**	入力を確認します。
手順 8	**write**	（オプション）設定ファイルに入力を保存します。

4.4 システム時計の設定

はじめに Privileged Exec モードに移行し、次の手順でシステム時計を設定します。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**time** *year month date hour:minutes:seconds*	システム時計を設定します。
手順 3	**exit**	Privileged Exec モードに戻ります。
手順 4	**show system configuration**	入力を確認します。
手順 5	**write**	（オプション）設定ファイルに入力を保存します。

4.5 システムサービスの設定

本機は SNMP, Telnet, Web サーバサービスを提供しており、これらの有効 / 無効を設定できます。

はじめに Privileged Exec モードに移行し、次の手順でシステムサービスを設定します。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**service snmp {enable | disable }**	SNMP サービスの有効 / 無効を設定します。
手順 3	**service telnet {enable | disable }**	Telnet サービスの有効 / 無効を設定します。
手順 4	**webserver service {enable | disable}**	Web サーバサービスの有効 / 無効を設定します。 Web サーバサービスを有効に設定すると、 Web ブラウザを介した本機のマネージメントを おこなうことができます。
手順 5	**webserver password reset**	（オプション）Web 用パスワードの変更をおこないます。 (初期設定：Web ログイン用ユーザ名 admin ログインパスワードは password） Web を介してパスワードを変更できます。
手順 6	**exit**	Privileged Exec モードに戻ります。
手順 7	**show services**	入力を確認します。
手順 8	**write**	（オプション）設定ファイルに入力を保存します。

4.6 SNMP の連絡 / 管理者 / 場所の設定

はじめに Privileged Exec モードに移行し、次の手順でシステムの連絡先 / 管理者 / 設置場所情報を設定します。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**system contact** *string*	SNMP で使用するシステムの連絡先情報を設定します。
手順 3	**system name** *string*	SNMP で使用するシステムのシステム名を設定します。
手順 4	**system location** *string*	SNMP で使用するシステムの配置場所情報を設定します。
手順 5	**exit**	Privileged Exec モードに戻ります。
手順 6	**show system config**	入力を確認します。
手順 7	**write**	（オプション）設定ファイルに入力を保存します。

4.7 ファームウェアの管理

ファームウェアは FTP サーバまたは TFTP サーバからダウンロードできます。

新しいファームウェアのダウンロード後、本機が次に起動した際、システムは新しいファームウェアを使用します。

FTP サーバ /TFTP サーバからファームウェアをダウンロードする前に、以下の項目の確認が必要です。

- VLAN インターフェースか AUX ポートに IP アドレスを設定済みであること
- FTP サーバ /TFTP サーバがファームウェアのアップデートをおこなうスイッチと正しく通信できること
- FTP サーバ /TFTP サーバで FTP/TFTP プログラムを実行できること
- FTP サーバにユーザ名とパスワードを正しく設定し、正しいディレクトリを設定済みであること
- TFTP サーバの正しいディレクトリを設定済みであること

はじめに Privileged Exec モードに移行し、次の手順で FTP サーバ /TFTP サーバからファームウェアをダウンロードします。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**down ftp image** *ip-address user-name password filename*	FTP サーバからファームウェアをダウンロードします。
手順 3	**down tftp image** *ip-address filename*	TFTP サーバからファームウェアをダウンロードします。
手順 4	**reboot**	（オプション）システムを再起動します。
手順 5	**exit**	Privileged Exec モードに戻ります。
手順 6	**show version**	入力を確認します。
手順 7	**write**	（オプション）設定ファイルに入力を保存します。

4.8 設定ファイルの管理

設定ファイルは FTP サーバまたは TFTP サーバからアップロード / ダウンロードできます。新しい設定ファイルのダウンロード後、次回起動時からシステムは新しい設定ファイルを使用します。

はじめに Privileged Exec モードに移行し、次の手順で FTP サーバ /TFTP サーバから設定ファイルをアップロード / ダウンロードします。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**upload ftp config** *ip-address user-name password filename*	設定ファイルを FTP サーバにアップロードします。
手順 3	**upload tftp config** *ip-address filename*	設定ファイルを TFTP サーバにアップロードします。
手順 4	**down ftp config** *ip-address user-name password filename*	FTP サーバから設定ファイルをダウンロードします。
手順 5	**down tftp config** *ip-address filename*	TFTP サーバから設定ファイルをダウンロードします。
手順 6	**reboot**	（オプション）システムを再起動します。
手順 7	**exit**	Privileged Exec モードに戻ります。
手順 8	**show version**	入力を確認します。
手順 9	**write**	（オプション）設定ファイルに入力を保存します。

4.9 設定ファイルの保存

write コマンドを使用して、フラッシュメモリに現在の設定情報を保存すると、システムが次回再起動した際、この設定が起動時の設定となります。

はじめに Privileged Exec モードに移行し、次の手順でフラッシュメモリに設定ファイルを保存します。

	コマンド	内容
手順 1	**write**	（オプション）設定ファイルに入力を保存します。

4.10 CPU 使用率の確認

以下のコマンドで、CPU/ **メモリ使用率を確認することが可能です。**

show system statistics

例

```
switch#show system statistics
Memory Usage Statistics: 46%
Current CPU Usage  Statistics: 1%
```

4.11 MAC アドレステーブルの管理

4.11.1 MAC アドレステーブルの登録

下記のコマンドで、MAC **アドレステーブルの学習をポート毎に設定可能です。**
(Global configuration **モード)**

switch(config)#fdb mac_learninig enable/disable port # (1-26)

4.11.2 静的 MAC アドレステーブルの登録

下記のコマンドで、任意の MAC **アドレスの登録が可能です。**
(Global configuration **モード)**

switch(config)#fdb add static ##:##:##:##:##:## vlanID # port #
(# は MAC アドレス、VID、ポート番号)

4.12 システムの復元

remove コマンドを使用すると、システムの再起動後に、起動時の設定を初期設定に戻すことができます。

はじめに Privileged Exec モードに移行し、次の手順でシステムを初期設定に復元します。

	コマンド	内容
手順 1	remove	設定ファイルに入力を保存します。
手順 2	reboot	システムを再起動します。

4.13 システムの再起動

はじめに Privileged Exec モードに移行し、次の手順でシステムを再起動します。

	コマンド	内容
手順 1	reboot	システムを再起動します。

5. 設定

5.1 ポート設定

5.1.1 概要

本機は 10/100/ を 24 ポート、拡張スロットを 2 スロット装備しています。
10/100Mpbs ポートは MDI/MDI-X 自動切替機能をサポートしており、オートネゴシエーションモードでは Half または Full Duplex で稼動可能です。これにより、他のネットワーク機器とネゴシエーションし、最適な Duplex モードと速度を選択できます。

5.1.2 イーサネットポートの設定

イーザネットポートの設定には次の項目があります。

- イーサネットポートの有効 / 無効
- イーサネットポートの属性と速度
- フローコントロールの設定
- ポートブロードキャスト / マルチキャスト /dlf サプレッションの設定
- ポートミラーリングの設定
- レートリミットの設定

ポートの有効 / 無効

ポートの有効 / 無効を設定するには、次のコマンドを使用します。

はじめに Privileged Exec モードに移行し、次の手順でイーサネットポートを有効にします。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**port state** *port-number* **enable**	ポート番号を指定し、有効に設定します。 初期設定：有効
手順 3	**exit**	Privileged Exec モードに戻ります。
手順 4	**show port** *port-number*	入力を確認します。
手順 5	**write**	（オプション）設定ファイルに入力を保存します。

ポートの属性と速度

ポートが同時にパケットの送受信をおこなうには、ポートを Full Duplex に設定します。ポートが一度にパケットの送信または受信をおこなうには、ポートを Half Duplex に設定します。ポートがオートネゴシエーションモードに設定されている場合、本機と接続先ポートは自動的に Duplex モードに関してネゴシエーションをおこないます。イーサネットポートの速度を設定するには次のコマンドを使用します。速度がオートネゴシエーションモードに設定されている場合、本機および接続先のポートは自動的に速度に関してネゴシエーションをおこないます。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**port speed** *portnumber* **{100f|100h|10f|10h|Auto}**	ファーストイーサネットポートの Duplex 属性と速度を設定します。 初期設定：auto（オートネゴシエーションモード）
手順 3	**exit**	Privileged Exec モードに戻ります。
手順 4	**show port** *port-number*	入力を確認します。
手順 5	**write**	（オプション）設定ファイルに入力を保存します。

フローコントロールの設定

本機と接続先のスイッチでフローコントロールを有効に設定すると、本機で輻輳が発生した際、本機から接続先にポーズパケットの送信により輻輳状態であることを通知します。接続先のスイッチがこのメッセージを受信すると、接続先スイッチはポーズパケットを送信し、その逆もあります。この方法で、パケットの損失は効果的に減少されます。イーサネットポートのフローコントロール機能は、次のコマンドを使用し、有効 / 無効に設定できます。

はじめに Privileged Exec モードに移行し、次の手順でイーサネットポートのフローコントロールを有効にします。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**control flow enable**	イーサネットポートのフローコントロールを有効に設定します。
手順 3	**exit**	Privileged Exec モードに戻ります。
手順 4	**show control flow**	入力を確認します。
手順 5	**write**	（オプション）設定ファイルに入力を保存します。

フローコントロールを無効に設定

モード	コマンド
Grobal Configuration	**control flow disable**

ポートブロードキャスト / マルチキャスト /dlf サプレッションの設定

次のコマンドを使用し、ブロードキャスト / マルチキャスト /df トラフィックの制限をおこないます。ブロードキャスト / マルチキャスト /dlf が設定された値を超えた場合、システムは、ブロードキャスト / マルチキャスト /dlf ストームを圧縮し、輻輳を回避し、通常のサービスを確保するために、適切なブロードキャスト / マルチキャスト /dlf パケット数を維持するようあふれたトラフィックを破棄します。パラメータでは、ポートで許可されているブロードキャスト / マルチキャスト /dlf トラフィックの最大のワイヤスピードが採用されます。パケット数が少ないほど、より低速のブロードキャスト / マルチキャスト /dlf トラフィックが許可されます。

はじめに Privileged Exec モードに移行し、次の手順でブロードキャスト / マルチキャスト / dlf サプレッションのイーサネットポートへの設定をおこないます。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**control rate speed** *packets* **broadcast enable multicast enable dlf enable**	ブロードキャスト / マルチキャスト /dlf サプレッションを有効に設定します。packets には、秒あたりのパケット数を設定します。
手順 3	**exit**	Privileged Exec モードに戻ります。
手順 4	**show control rate**	入力を確認します。
手順 5	**write**	（オプション）設定ファイルに入力を保存します。

ポートのブロードキャスト / マルチキャスト /dlf サプレッションを無効に設定

モード	コマンド
Grobal Configuration	**control rate speed** *packets* **broadcast disable multicast disable dlf disable**

ポートミラーリングの設定

ポートミラーリングは、データの解析と観察のため、監視対象のポートのデータを指定したポートに複製します。
本機は、複数ポートを 1 ポートでモニタリングする機能をサポートしていますが、これは、複数ポートのパケットを 1 つのモニタリングポートに複製できるものです。

はじめに Privileged Exec モードでログインし、次の手順でポートミラーリングを設定します。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**mirror mirrored-to** *port-number*	監視をおこなうミラーリングポートを設定しす。
手順 3	**mirror link-group set** *index port-list* **[both | ingress | egress]**	監視対象のポートグループを作成します。 index には監視対象のポートグループ番号を 1 ～ 24 の範囲で指定します。 port-list には、監視対象のポートグループメンバを、01m のようにポート番号に m を付けて指定します。
手順 4	**mirror link-group enable** *index*	ミラーリングを有効に設定します。
手順 5	**exit**	Privileged Exec モードに戻ります。
手順 6	**show mirror all**	入力を確認します。
手順 7	**write**	（オプション）設定ファイルに入力を保存します。

監視対象のポートグループの削除方法

モード	コマンド
Grobal Configuration	**no mirror link-group** *index*

[注意] ミラーリングポートのポート速度が、監視対象のポートの速度よりも遅く設定されている場合、ミラーリングポートでパケットが破棄されます。

- **すべてのミラーリングセッションは、同一のデスティネーションポートで共用してください。**
- **ポートトラフィックを監視する際は、監視対象のポートとミラーリングポートは、同じ VLAN に所属していなくてはなりません。**

レートリミットの設定

この機能は、ネットワーク管理者がインターフェースで送受信されるトラフィックの最大速度を制御できるようにします。レートリミットは、ネットワークのエッジのインターフェースに設定し、スイッチが送受信するトラフィックを制限します。レートリミットの範囲にあるトラフィックは転送されますが、有効なトラフィックの範囲を超えたパケットは破棄されます。

レートリミット機能は各ポートまたはトランクに適用できます。インターフェースにこの機能を設定すると、このインターフェースのトラフィックレートがハードウェアによって、同一か否かの検証のため監視されます。一致しなかったトラフィックは破棄され、一致したトラフィックは何の変更も加えられずにフォワーディングされます。

はじめに Privileged Exec モードに移行し、次の手順でレートリミットを設定します。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**traffic-limit link-group set** *group-id port-list* **ingress** [*ingress-rate* **|** *default*] **[egress [***egress-rate***|***default***]]**	レートリミットグループを作成します。 group-id は帯域幅管理ルール番号で、範囲は 1 ～ 64 です。ingress-rate と egress-rate は帯域幅の制度で、1M/s です。　初期設定：レートリミットなし
手順 3	**traffic-limit link-group enable** *group-id*	レートリミットを有効に設定します。
手順 4	**exit**	Privileged Exec モードに戻ります。
手順 5	**show traffic-limit link-group**	入力を確認します。
手順 6	**write**	（オプション）設定ファイルに入力を保存します。

レートリミットを無効に設定

モード	コマンド
Grobal Configuration	**traffic-limit link-group disable** *group-id*

レートリミットグループを無効に設定

モード	コマンド
Grobal Configuration	**no traffic-limit link-group** *group-id*

5.2 トランク

本節では、トランクグループと IEEE 802.ad のポートトランク（リンクアグリゲーション）の設定方法について記載します。

- トランクグループは複数のポートから構成され、手動で設定するリンクの集約です。
- 動的トランク（IEEE 802.3ad リンクアグリゲーション）は、動的にトランクグループを作成、管理するプロトコルです。

5.2.1 概要

動的トランクは、複数のポートを 1 つに集約して、このメンバポート同士がやり取りする総帯域のバランスを取ることを可能にし、接続の信頼性を拡大します。負荷分散の観点からは、動的トランクは負荷分散ベースの動的トランクでも、非負荷分散ベースの動的トランクでもあります。

機器間の複数のリンクを、1 つの仮想的な集約されたリンクとして作成できます。ポートトランクはボトルネックが存在するネットワークセグメントの帯域を劇的に増やすだけでなく、2 台の機器間のフォールトレランスとしてのリンクの提供もおこないます。1 台に最大 6 つのトランクグループを作成できます。

本機は静的トランクおよび動的な LACP（Link Aggregation Control Protocol）の両方をサポートしています。静的トランクはリンクの両端で手入力により設定する必要があります。一方、LACP に設定されているポートは通信相手の機器の LACP に設定されているポートと、リンクの集約について動的にネゴシエーションをおこなうことができます。静的トランクの一部として設定済みでなければ、本機のポートのいくつでも LACP に設定できます。接続先の機器のポートもまた LACP に設定されていれば、本機と接続先の機器が相互にリンクの集約についてネゴシエーションをおこないます。トランクの特定のリンクが切断すると、待機しているポートがこれに代わり自動的に起動します。

本機は 1 台で最大 6 つのトランクグループをサポートし、また 1 つのトランクグループに最大 8 つのポートを所属させることができます。

また、各トランクポートの負荷バランスを取るようになっているため、トランクに所属する 1 つのポートが切断すると、この負荷を引き継ぐことによって、他のポートが冗長機能を提供します。

ただし、機器間で物理的な接続をおこなう前に、Web インターフェース（WBI）かコマンドラインインターフェース（CLI）を使用して、各機能の両端のトランクを設定する必要があります。

ポートトランクを使用する場合、次のポイントに注意してください。

- ループを回避するため、必ずトランクの設定を行ってから、ネットワークケーブルの装着をしてください。
- 本機は最大 6 トランク、各トランクに最大 8 ポートまで作成できます。
- コネクションの両端のポートはトランクポートとして設定する必要があります。
- トランクの両端のポートは通信モード（速度、フローコントロールなど）、VLAN の割り当て、CoS の設定などに関し、同一の方式で設定している必要があります。

- VLAN から移動、追加または削除をおこなう場合、特定のトランクに所属するポートはすべて全体として処理する必要があります。
- STP、VLAN および IGMP の設定は、トランク全体を対象としてのみ設定できます。

5.2.2 静的トランクの設定

[注意] 異なる種類（ベンダ固有の実装をベース）のスイッチとトランクを作成することはできません。ただし、本機の静的トランクは Cisco EtherChannel と互換性があります。

ネットワークでのループの発生を回避するため、ポートを接続する前に Web インターフェースまたは CLI を用いてトランクを追加し、また、トランクを削除する場合も Web/CLI でトランクを削除してからポートを切断することを忘れないでください。

はじめに Privileged Exec モードに移行し、次の手順でトランクを有効にします。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**channel-group add** *group-number port-list* **[smac | dmac | sdmac | sip | dip |sdip]**	静的トランクを設定します。 group-number の範囲は 1 ～ 6 です。port-list には、トランクメンバを、01m のようにポート番号に m を付けて指定します。
手順 3	**exit**	Privileged Exec モードに戻ります。
手順 4	**show channel-group**	入力を確認します。
手順 5	**write**	（オプション）設定ファイルに入力を保存します。

トランクの削除

モード	コマンド
Grobal Configuration	**channel-group delete** *group-number*

5.2.3 動的トランク（LACP [IEEE 802.3ad]）の設定

本機のソフトウェアは IEEE 802.3ad 標準の動的トランクをサポートしています。この標準は LACP（Link Aggregation Control Protocol）について記載したもので、冗長リンクの両端のポートが手入力による設定なしにポートを自身をトランクリンク（集約リンク）に組み込むメカニズムを規定しています。

スイッチのポートのグループに対し、動的トランクを有効に設定すると、そのポートはリンクのリモート側のポートとネゴシエーションをおこなうことができ、トランクグループの確立をおこないます。

LACP の有効化

初期設定では動的トランクのサポートは無効です。本機にこの機能を有効にするよう設定できます。動的トランクを有効に設定すると、本機のポートは標準の LACPDU（LACP Protocol Data Unit）メッセージを交換することができ、リンクのもう一端のポートとトランクグループ設定のネゴシエーションをおこないます。さらに、本機のポートは自発的に LAPDU メッセージを送信してリンクのもう一端の動的トランクのパートナを探し、LACPDU 交換を実行して正しく設定されたリモートポートと動的トランクのパートナに関しネゴシエーションをおこないます。

はじめに Priviledged Exec モードに移行し、次の手順で LACP（Link Aggregation Control Protocol）を本機で有効に設定します。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**lacp enable**	LACP の有効化をおこないます。
手順 3	**exit**	Privileged Exec モードに戻ります。
手順 4	**show link-aggregation** < *1-6* > **neighbors**	入力を確認します。
手順 5	**write**	（オプション）設定ファイルに入力を保存します。

LACP の無効化

モード	コマンド
Grobal Configuration	**lacp disable**

LACP パラメータの設定

各ポートごとに次の動的トランクのパラメータについて設定できます。

- ポートプライオリティ
- キー

ポートプライオリティ：

ポートプライオリティは、リンクのアクティブ / 待機を決定します。ポートグループが他の機器のポートグループとネゴシエーションをおこないトランクグループを確立しようとした際、最も高いプライオリティを有するポートが初期設定のアクティブポートになります。他の（低いプライオリティを有する）ポートがそのトランクグループで待機状態のポートになります。プライオリティには 0 ～ 65535 を設定できます。値が大きいほどプライオリティが低いことを示します。初期設定値は 128 です。

[注意] このパラメータは現時点のソフトウェアリリースではサポートしていません。ポートグループのプライマリポートが最初にアクティブポートになります。プライマリポートは、トランクグループの有効なポートのなかで最も小さなポート番号のポートです。

キー：

IEEE 802.3ad を有効にしているすべてのポートは、キーを有しています。キーが、ポートがどの潜在的なトランクポートのグループに所属するかを特定します。同じキーを有するポートはキーグループと呼ばれ、同じトランクグループに所属する資格があります。

本機で動的トランクを有効に設定すると、ソフトウェアがデフォルトキーをそのポートに割り当てます。デフォルトキーはポートの 1 です。

機器間でキー値が一致する必要はありません。キーの照合について最低限必要なのは、特定の機器で集約するリンクに所属するすべてのポートが同じキーを有することです。

はじめに Privileged Exec モードに移行し、次の手順で動的トランクのパラメータを設定します。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**interface ethernet <***portnum***> [to <***portnum***>]**	物理ポートの設定モードを入力します。
手順 3	**link-aggregation port-priority <***0-65535***>**	（オプション）ポートグループの各ポートのプライオリティを設定します。値が大きいほど優先順位が低くなります。 範囲：0 ～ 65535 の範囲　　初期設定値：128
手順 4	**link-aggregation admin-key <***0-65535***>**	（オプション）トランクグループに集約される資格を有するポートグループを設定します。 キー値の範囲：0 ～ 65535 の範囲で変更できます。
手順 5	**exit**	Privileged Exec モードに戻ります。
手順 6	**show link-aggregation ethernet**	入力を確認します。
手順 7	**write**	（オプション）設定ファイルに入力を保存します。

負荷分散基準の設定

はじめに Privileged Exec **モードに移行し、次の手順で負荷分散基準を設定します。**

	コマンド	内容
手順 1	**config terminal**	Global configuration **モードに移行します。**
手順 2	**lacp <** *1-6* **> [smac|dmac|sdmac|sip|dip|sdip]**	**負荷分散基準を設定します。**
手順 3	**exit**	Privileged Exec **モードに戻ります。**
手順 4	**show link-aggregation trunks**	**入力を確認します。**
手順 5	**write**	**（オプション）設定ファイルに入力を保存します。**

動的トランクグループのステータスの表示と決定

どのトランクグループが有効かに関し、動的トランク情報を表示するには、
Privileged Exec **モードで** show link-aggregation trunks **コマンドを実行します。**

どのトランクグループが有効か、すべてのポートに関し動的トランク情報を表示するには、
Privileged Exec **モードで** show link-aggregation ethernet [<portnum>|< **c r** >] **コマンドを実行します。**

どのトランクグループが有効かに関し、動的トランク隣接情報を表示するには、
Privileged Exec **モードで** show link-aggregation <1-6> neighbors **コマンドを実行します。**

動的トランクのシステム ID **を表示するには、**
Privileged Exec **モードで** show link-aggregation sys-id **コマンドを実行します。**

5.3 VLAN

5.3.1 VLAN の概要

VLAN（Virtual Local Area Network）は、LAN に接続している機器を、物理的にセグメント分けせず論理的にグループ化し、仮想的なワークグループを実現します。IEEE は 1999 年に、VLAN の実装手段の標準化を意図して IEEE 802.1Q を発行しました。VLAN のテクノロジを利用し、ネットワーク管理者は物理的な LAN を、異なるブロードキャストドメインに論理的に分割することができます。各 VLAN は同一のドメインに所属するワークステーションから構成されるグループを 1 つ有します。VLAN に所属するワークステーションは、必ずしも同一の物理的な LAN のセグメントに所属する必要はありません。

VLAN のテクノロジを使用すると、VLAN 内のブロードキャストトラフィックおよびユニキャストトラフィックは他の VLAN にフォワーディングされないため、ネットワークトラフィックの制御、機器への投資の削減、ネットワーク管理の合理化、またセキュリティの向上に役立ちます。

5.3.2 VLAN の設定

VLAN の設定には次の項目があります。

- VLAN の作成 / 削除
- VLAN ポートの PVID の設定
- VLAN ポートの設定 / 削除

VLAN を設定するには、まず、要件に従って VLAN を作成します。

VLAN の作成 / 削除

次のコマンドを使用し、VLAN の作成 / 削除をおこないます。

はじめに Privileged Exec モードに移行し、次の手順で VLAN を作成します。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**vlan static add vid** *vid port-list*	物理ポートの設定モードを入力します。
手順 3	**exit**	Privileged Exec モードに戻ります。
手順 4	**show vlan table**	入力を確認します。
手順 5	**write**	（オプション）設定ファイルに入力を保存します。

ポートの PVID 設定

次のコマンドを使用し、VLAN ポートの PVID を設定します。

はじめに Privileged Exec モードでログインし、次の手順で VLAN ポートの PVID を設定します。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**Vlan port pvid** *port-number pvid*	VLAN ポートの PVID を設定します。 pvid は 1 ～ 4096 の範囲で設定します。
手順 3	**exit**	Privileged Exec モードに戻ります。
手順 4	**show vlan port**	入力を確認します。
手順 5	**write**	（オプション）設定ファイルに入力を保存します。

VLAN ポートの設定 / 削除

次のコマンドを使用し、VLAN ポートの設定 / 削除をおこないます。

はじめに Privileged Exec モードでログインし、次の手順で VLAN ポートの PVID を設定します。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**vlan static set vid** *vid port-list*	VLAN ポートの設定 / 削除をおこないます。
手順 3	**exit**	Privileged Exec モードに戻ります。
手順 4	**show vlan table**	入力を確認します。
手順 5	**write**	（オプション）設定ファイルに入力を保存します。

5.3.3 VLAN 構築例

ネットワーク要件

ポート 1、2、3、4 **を** VLAN1 **から削除し、**VLAN2 **と** VLAN3 **を作成します。**VLAN2 **にポート** 1 **とポート** 2 **を追加し、**VLAN3 **にポート** 3 **とポート** 4 **を追加します。**

ネットワーク構成図

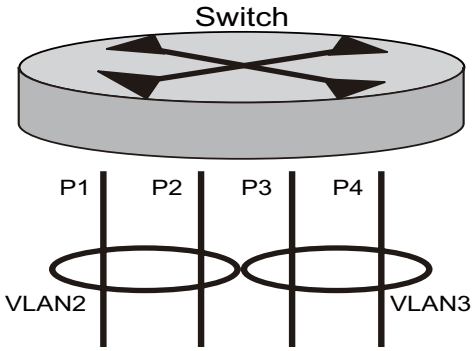


図 8　VLAN **構築例**

設定手順

（1**）デフォルト** VLAN（VLAN1）**からポート** 1、2、3、4 **を削除します。**
switch(config)#vlan static set vid 1 01-02-03-04-

（2**）**VLAN2 **を作成します。**
switch(config)#vlan static add vid 2 01u02u

（3**）ポート** 1 **とポート** 2 **の** VLAN **ポートの** PVID **を設定します。**
switch(config)#vlan port pvid 1 2
switch(config)#vlan port pvid 2 2

（4**）**VLAN3 **を作成します。**
switch(config)#vlan static add vid 3 03u04u

（5**）ポート** 3 **とポート** 4 **の** VLAN **ポートの** PVID **を設定します。**
switch(config)#vlan port pvid 3 3
switch(config)#vlan port pvid 4 3

5.4 GVRP の設定

5.4.1 GVRP の概要

GVRP（GARP VLAN Registration Protocol）は GARP アプリケーションのひとつです。GARP の動作メカニズムをベースにして、GVRP は本機の動的な VLAN 登録情報の維持管理機能を提供し、その情報を他のスイッチに伝播します。GVRP をサポートしているすべてのスイッチは VLAN 登録情報を他のスイッチから受け取り、アクティブなメンバ情報、どのポートを介してメンバが到達できるかなどのローカルの VLAN 登録情報を動的に更新します。GVRP をサポートするすべてのスイッチはそれぞれのローカルな VLAN 登録情報を他のスイッチに伝播し、ネットワーク内の GVRP をサポートしている機器が VLAN 情報の一貫性を維持できるようにします。GVRP によって伝播される VLAN 登録情報は、手入力により設定された静的なローカルの登録情報と、他のスイッチから得られた動的な登録情報との両方を含みます。

GVRP の詳細は、IEEE 802.1Q 標準で記述されています。本機は、IEEE 標準の GVRP を完全にサポートしています。

主な GVRP 設定には次の項目があります。

- グローバルな GVRP の有効 / 無効の設定
- ポートの GVRP の有効 / 無効の設定

5.4.2 GVRP の有効 / 無効（グローバル）

次のコマンドを使用し、グローバルな GVRP の有効 / 無効を設定します。

はじめに Privileged Exec モードに移行し、次の手順でグローバルな GVRP を有効にします。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**system gvrp enable**	グローバル GVRP を有効に設定します。 初期設定：グローバル GVRP 無効
手順 3	**exit**	Privileged Exec モードに戻ります。
手順 4	**show system configuration**	入力を確認します。
手順 5	**write**	（オプション）設定ファイルに入力を保存します。

グローバルな GVRP を無効に設定

モード	コマンド
Grobal Configuration	**system gvrp disable**

5.4.3 GVRP の有効 / 無効（ポート）

次のコマンドを使用し、GVRP の有効 / 無効をポートに設定します。

はじめに Privileged Exec モードに移行し、次の手順でポートの GVRP を有効にします。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**vlan port gvrp** *port-number* **enable**	ポートの GVRP を有効に設定します。 初期設定：ポート GVRP 無効
手順 3	**exit**	Privileged Exec モードに戻ります。
手順 4	**show vlan port**	入力を確認します。
手順 5	**write**	（オプション）設定ファイルに入力を保存します。

ポートの GVRP を無効に設定

モード	コマンド
Grobal Configuration	**vlan port gvrp port-number disable**

5.4.4 GVRP 構築例

ネットワーク要件

スイッチ間の VLAN 情報の登録と更新を動的におこなうには、GVRP を各スイッチで有効に設定する必要があります。

ネットワーク構成図

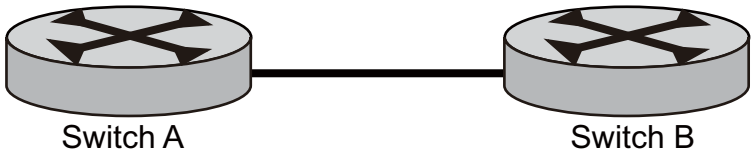


図 9 GVRP 構築例

設定手順

Switch A の設定

GVRP をグローバルに有効に設定します。

```
Switch(config)#system gvrp enable
```

Switch B の設定

GVRP をグローバルに有効に設定します。

```
Switch(config)#system gvrp enable
```

5.5 スパニングツリー

5.5.1 概要

本機は STP（Spanning Tree Protocol）および RSTP（Rapid Spanning Tree Protocol）をサポートしています。

STP はレイヤ 2 のリンクマネジメントプロトコルで、ネットワークでのループを防止するとともに、パスの冗長性を提供します。レイヤ 2 イーサネットネットワークが正しく機能するためには、2 局間で有効なパスがただ 1 つだけである必要があります。複数の有効なパスが終端局間にあると、ネットワークでループが発生します。ループがネットワークに存在すると、終端局は複製されたメッセージを受信することになります。スイッチはまた、複数のレイヤ 2 インターフェースにある終端局の MAC アドレスを学習する可能性があります。これらの状況によって、ネットワークが不安定になります。単一の LAN セグメントに接続しているのか、複数のセグメントをスイッチング交換しているのかを検出できない終端局はスパニングツリーの動作を透過的します。

STP はスパニングツリーアルゴリズムを使用し、冗長構成でネットワーク接続している 1 台のスイッチをスパニングツリーのルートとして選択します。各ポートにその有効なトポロジでのポートの役割に基づく各ポートの役割を割り当てることによって、このアルゴリズムは、スイッチ接続されたレイヤ 2 ネットワークでループのない最良のパスを算出します。

- ルート（Root）ポート：そのスパニングツリートポロジにおけるフォワーディングポート
- 指定（Designate）ポート：スイッチング接続されている LAN の各セグメントにおけるフォワーディングポート
- 代替（Alternate）ポート：スパニングツリー内でルートポートに対して代替パスを提供するブロッキングポート
- バックアップ（Backup）ポート：ループバック構成におけるブロッキングポート

割り当てられたこれらの役割を有するポートを含むスイッチは、ルートスイッチまたは指定スイッチと呼ばれます。

スパニングツリーによって、冗長構成のデータパスは強制的に待機（ブロッキング）状態になります。スパニングツリー内のネットワークセグメントに障害が発生し、代替パスが存在する場合、スパニングツリーアルゴリズムによるスパニングツリートポロジの再計算がおこなわれ、待機状態のパスを有効にします。スイッチは、BPDU（Bridge Protocol Data Unit）と呼ばれるスパニングツリーフレームを、一定の間隔で送受信します。本機はこれらのフレームをフォワーディングせず、これらを利用してループのないパスを構成します。BPDU には、スイッチの MAC アドレス、スイッチのプライオリティ、ポートのプライオリティ、またはパスコストなど、送信したスイッチとポートの情報が含まれています。スパニングツリーはこの情報を利用し、スイッチ接続されているネットワークのルートスイッチとルートポート、およびスイッチ接続されている各セグメントのルートポートと指定ポートを選出します。

スイッチで 2 つのポートがループの一部になった場合、スパニングツリーのポートプライオリティとパスコストの設定によって、各ポートがフォーワーディング状態に移行し、これがブロッキング状態に移行します。スパニングツリーのポートプライオリティ値はネットワークトポロジのポートの場所と、トラフィックを転送するためにどの場所に配置されているかを示します。パスコスト値はメディアの速度を示します。

5.5.2 スパニングツリーのトポロジと BPDU

スイッチ接続されたネットワークの、安定して有効なスパニングツリートポロジは、次の項目で制御されます。

- 各スイッチの各 VLAN に関連付けられたユニークなブリッジ ID（スイッチのプライオリティと MAC アドレス）。スタック構成のスイッチの場合、付与されている 1 つのスパニングツリーインスタンスに対しすべてのスイッチが同じブリッジ ID を使用します。
- ルートスイッチに対するスパニングツリーのパスコスト
- 各レイヤ 2 インターフェースに関連付けられているポートの識別子（ポートプライオリティと MAC アドレス）
  ネットワークでスイッチが起動すると、各スイッチがルートスイッチとして機能します。各スイッチは設定 BPDU をすべてのポートから送信します。この BPDU は通信され、スパニングツリーのトポロジを算出します。各設定 BPDU は次の情報を含むものです。
- スイッチのユニークなブリッジ ID
  （ルートスイッチとして識別される、送信スイッチの識別子）
- ルートに対するスパニングツリーのパスコスト
- 送信スイッチのブリッジ ID
- メッセージのエージング時間
- 送信インターフェースの識別子
- ハロータイム、フォワーディングディレイ、プロトコルの最大エージングの各タイマの値

スイッチがより優れた（より小さな値のブリッジ ID、より小さなパスコスト値などの）情報を含む設定 BPDU を受信すると、そのポートにこの情報を保持します。この BPDU がスイッチのルートポートで受信されると、指定ブリッジであることを示すために、すべての接続している LAN に更新情報を盛り込んだ BPDU もフォワーディングします。

スイッチがその時点でポートが保持している情報より悪い情報を含む設定 BPDU を受信すると、その BPDU は破棄されます。スイッチが LAN の指定スイッチで、この LAN から悪い情報の BPDU を受信すると、スイッチは LAN に向け更新情報を盛り込んで BPDU を送信します。このように、悪い情報は破棄され、より良い情報がネットワークに伝播されます。

BPDU の交換によって次の動作がもたらされます。

- ネットワークの 1 台のスイッチがルートスイッチ（スイッチ接続されているネットワークでのスパニングツリートポロジにおいて論理上の中心）に選定されます。スタック構成の場合、1 つのスタックメンバがスタックルートスイッチに選定されます。スタックルートスイッチは送信用のルートポート（Switch 1）を有します（図 10 参照）。

各 VLAN については、最も高いプライオリティ（一番小さなプライオリティ値）を有するスイッチがルートスイッチとして選定されます。すべてのスイッチが初期設定のプライオリティ（32768）に設定されている場合、その VLAN で一番小さな MAC アドレスを有するスイッチがルートスイッチになります。図 10 に示すように、スイッチのプライオリティ値はブリッジ ID の最上位ビットとなります。

- ルートポートが（ルートスイッチ以外の）各スイッチに 1 つ選択されます。スイッチがルートスイッチにパケットをフォワーディングする際、このポートは最良のパス（最も小さなコスト）を提供します。

スタック構成のスイッチでルートポートを選択する場合、スパニングツリーによって以下が実施されます。

－最小のルートブリッジ ID を選択

－ルートスイッチに対する最小のパスコストを選択

－最小の指定ブリッジ ID を選択

－最小の指定パスコストを選択

－最小のポート ID を選択

スタック構成のルートスイッチでは、1 つの送信用のポートのみルートポートとして選択されます。スタックのこれ以外のスイッチは、図 10 に示すように、指定スイッチ（Switch 2 と Switch 3）になります。

- ルートスイッチまでの最短距離がパスコストに基づき各スイッチで算出されます。
- 各 LAN のセグメントにおける指定スイッチが選定されます。指定スイッチが所属する LAN からルートスイッチへパケットをフォワーディングする場合、指定スイッチは、最小のパスコストを盛り込みます。LAN に接続している指定スイッチを経由するポートは、指定ポートと呼ばれます。

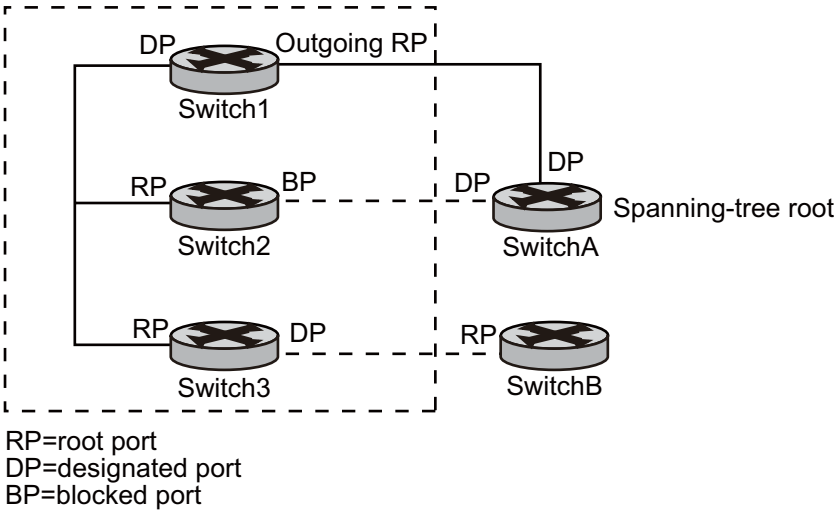


図 10　スタック構成のスイッチにおけるスパニングツリーのポートの状態

スイッチ接続されているネットワークのどこからもルートスイッチに到達する必要のないパスはすべてスパニングツリーブロッキングモードになります。

5.5.3 ブリッジ ID・スイッチプライオリティ・拡張システム ID

IEEE 802.1D 標準では、各スイッチにユニークなブリッジ識別子（ブリッジ ID）を 1 つ持つことを要件に定めており、このブリッジ ID はルートスイッチの選定を制御します。各 VLAN は、PVST+ とラピッド PVST+ を有する異なる論理的なブリッジだと考えられるため、同一のスイッチは、VLAN が設定しているのと同じ数の異なるブリッジ ID を持たなくてはなりません。スイッチの各 VLAN はユニークな 8byte のブリッジ ID を有します。最上位ビットから 2 つはスイッチのプライオリティを表し、残りの 6byte はスイッチの MAC アドレスから導かれます。

本機は IEEE 802.1t のスパニングツリー拡張機能をサポートしており、スイッチのプライオリティとしてすでに使用されたいくつかのビットは VLAN の識別子として使用します。その結果、ブリッジ ID の一意性を維持する間中ずっと、スイッチのために予約される MAC アドレスはほとんどなく、より大きな範囲の VLAN ID がサポートされます。以下の表に示すように、すでにスイッチプライオリティに使用された 2byte が 4bit のプライオリティ値に再割り当てされ、12bit の拡張システム ID 値が VLAN ID と一致しています。

Switch Priority Value				Extended System ID(Set Equal to the VLAN ID)											
Bit16	Bit15	Bit14	Bit13	Bit12	Bit11	Bit10	Bit 9	Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1
32768	16384	8192	4096	2048	1024	512	256	128	64	32	16	8	4	2	1

スパニングツリーは拡張システム ID、スイッチプライオリティ、および割り当てられたスパニングツリー MAC アドレスを使用して、各 VLAN に対して一意のブリッジ ID を作成します。スタック構成のスイッチは、ネットワークのそれ以外のリソースからは 1 台のスイッチとして解釈されるため、スタックに所属するすべてのスイッチはそのスパニングツリーと同じブリッジ ID を使用します。スタックのマスターに障害が発生すると、スタックメンバは、新たなスタックマスタの新しい MAC アドレスに基づき、すべての実行中のスパニングツリーのブリッジ ID を再算出します。

拡張システム ID のサポートによって、ルートスイッチ、セカンダリのルートスイッチ、および VLAN のスイッチプライオリティの設定手順に影響が生じます。たとえば、スイッチのプライオリティ値を変更する場合、スイッチがルートスイッチに選定されるようにプロバビリティを変更します。値が大きいとプロバビリティが減少し、値が小さいとプロバビリティが増加します。

5.5.4 スパニングツリーインターフェースのステータス

スイッチ接続されている LAN を介しプロトコル情報が転送される際、伝播遅延が発生します。その結果、スイッチ接続されているネットワークで非同時に、また各所でトポロジの変更が発生します。インターフェースがスパニングツリーの非所属状態からフォワーディング状態へ直接遷移する際、一時的にデータのループが発生します。インターフェースは、フレームのフォワーディングをおこなう前に、新しいトポロジ情報がスイッチ接続されている LAN に伝播することを待たなくてはなりません。古いトポロジで使用されフォワーディングされたフレームに対し、フレームの生存期限の満了を受用しなくてはなりません。スパニングツリーを使用しているスイッチの各レイヤ 2 インターフェースは、次のいずれかのステータスになります。

- ブロッキング（Blocking）：インターフェースはフレームのフォワーディングをおこないません。
- リスニング（Listening）：スパニングツリーによってこのインターフェースがフレームのフォワーディングをおこなうことを決定した際、ブロッキング状態後の最初の遷移状態です。
- ラーニング（Learning）：インターフェースがフレームのフォワーディングをおこなう準備をします。
- フォワーディング（Forwarding）：インターフェースがフレームのフォワーディングをおこないます。
- ディスエーブル（Disabled）：インターフェースがスパニングツリーに所属していない状態ですが、この理由はポートの閉塞、ポートのリンクが非アクティブ、またはポートでスパニングツリーインスタンスが実行されていないためです。

インターフェースは次のステータスの順に遷移します。

- 初期化からブロッキング
- ブロッキングからリスニングまたはディスエーブル
- リスニングからラーニングまたはディスエーブル
- ラーニングからフォワーディングまたはディスエーブル
- フォワーディングからディスエーブル

図 11 にインターフェースがこれらのステータスを遷移する様子を示します。

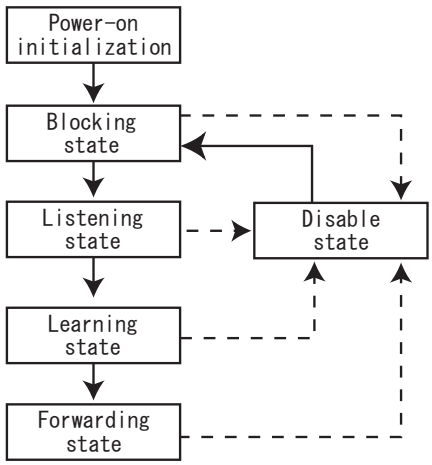


図 11 スパニングツリーインターフェースのステータス

本機を起動すると、初期状態ではスパニングツリーが有効になっており、スイッチの各インターフェース、VLAN、またはネットワークはブロッキング状態に移行し、リスニング、ラーニングと遷移します。スパニングツリーは各インターフェースをフォワーディングまたはブロッキングの状態で安定させます。

スパニングツリーアルゴリズムによって、レイヤ 2 インターフェースがフォワーディング状態に移行した際、次のプロセスが発生します。

(1) スパニングツリーが、インターフェースがブロッキング状態に遷移するためのプロトコル情報待ちの間は、インターフェースはリスニング状態になります。

(2) スパニングツリーが、フォワーディングディレイタイマの期限切れ待ちの間は、インターフェースはラーニング状態になり、フォワーディングディレイタイマはリセットされます。

(3) ラーニング状態では、スイッチが終端局の位置情報をデータベースへのフォワーディングのために学習した際、インターフェースはフレームのフォワーディングをおこないません。

(4) フォワーディングディレイタイマの期限が切れた際、スパニングツリーはインターフェースをフォワーディング状態に移行し、学習とフレームのフォワーディングが有効になります。

ブロッキング

ブロッキング状態のレイヤ 2 インターフェースはフレームのフォワーディングをおこないません。初期化後、BPDU が各スイッチのインターフェースに送信されます。スイッチは、当初、他のスイッチと BPDU の交換をおこなうまではルートとして機能します。BPDU の交換によって、ネットワークのどのスイッチがルートまたはルートスイッチであるかが決定されます。ネットワークにスイッチが 1 台しかない場合、BPDU の交換はおこなわれず、フォワーディングディレイタイマの期限が切れ、インターフェースはリスニング状態に移行します。インターフェースは、スイッチが初期化されると、常にブロッキング状態に移行します。

ブロッキング状態のインターフェースは次のように機能します。

- そのインターフェースで受信したフレームを破棄します。
- フォワーディングのため、他のインターフェースから転送されてきたフレームを破棄します。
- アドレスの学習をおこないません。
- BPDU を受信します。

リスニング

リスニング状態は、ブロッキング状態後、レイヤ 2 インターフェースが最初に移行する状態です。スパニングツリーがこのインターフェースはフレームのフォワーディングをおこなうべきだと判断すると、インターフェースはこの状態に移行します。

リスニング状態のインターフェースは次のように機能します。

- そのインターフェースで受信したフレームを破棄します。
- フォワーディングのため、他のインターフェースから転送されてきたフレームを破棄します。
- アドレスの学習をおこないません。
- BPDU を受信します。

ラーニング

ラーニング状態のレイヤ 2 インターフェースはフレームのフォワーディングの準備をおこないます。インターフェースはリスニング状態からラーニング状態に移行します。

ラーニング状態のインターフェースは次のように機能します。

- そのインターフェースで受信したフレームを破棄します。
- フォワーディングのため、他のインターフェースから転送されてきたフレームを破棄します。
- アドレスの学習をおこないます。
- BPDU を受信します。

フォワーディング

フォワーディング状態のレイヤ 2 インターフェースはフレームのフォワーディングをおこないます。インターフェースはラーニング状態からフォワーディング状態に移行します。

フォワーディング状態のインターフェースは次のように機能します。

- インターフェースで受信したフレームを受信およびフォワーディングします。
- 他のインターフェースから転送されてきたフレームをフォワーディングします。
- アドレスの学習をおこないます。
- BPDU を受信します。

無効（Disable）

ディスエーブル状態のレイヤ 2 インターフェースはフレームのフォワーディングをおこなわないか、またはスパニングツリーに所属していません。ディスエーブル状態のインターフェースは非動作状態です。

ディスエーブル状態のインターフェースは次のように機能します。

- そのインターフェースで受信したフレームを破棄します。
- フォワーディングのため、他のインターフェースから転送されてきたフレームを破棄します。
- アドレスの学習をおこないません。
- BPDU を受信しません。

5.5.5 スイッチ / ポートがルートになる流れ

ネットワークのすべてのスイッチが初期設定のスパニングツリー設定を有効にしている場合、最小の MAC アドレスを有するスイッチがルートスイッチになります。図 12 では、すべてのスイッチプライオリティが初期設定値（32768）に設定されており、Switch A が最小の MAC アドレスを有するため、Switch A がルートスイッチとして選定されます。しかし、トラフィック形態、フォワーディングインターフェースの数、リンクの種類から、Switch A は理想的なルートスイッチではありません。理想的なスイッチのプライオリティを高める（プライオリティ値を下げる）ことにより、理想的なスイッチがルートスイッチになり、スパニングツリーの再計算を強制的に実行し、この理想的なスイッチをルートとした新たなトポロジを形成することができます。

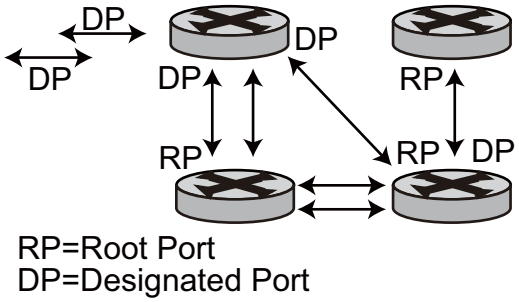


図 12　スパニングツリーのトポロジ

スパニングツリーのトポロジが初期パラメータに基づき算出されると、スイッチ接続されているネットワークの送信元終端局と宛先終端局間のパスが理想的ではなくなります。たとえば、ルートポートより高い番号のインターフェースに高速のリンクで接続している場合、ルートポートの変更が発生します。最終目的はルートポートへ最速のリンクを実現することです。

たとえば、Switch B のあるポートがギガビットイーサネットでリンクしており、Switch B の別のポート（10/100Mbps）がルートポートだと想定します。ネットワークトラフィックはギガビットイーサネットリンク経由の方がより効率的です。ギガビットイーサネットポートのスパニングツリーポートのプライオリティをルートポートより高める（プライオリティ値を下げる）ことにより、ギガビットイーサネットポートが新たなルートポートになります。

5.5.6 スパニングツリーと冗長接続性

図 13 に示すように、スイッチの 2 つのインターフェースを別の 1 台の機器または 2 台の機器に接続することによって、スパニングツリーで冗長的なバックボーンを構築できます。スパニングツリーにより、自動的に無効にしているインターフェースを、一方のインターフェースが切断した場合に有効にできます。一方のリンクが高速でもう一方が低速な場合、低速なリンクが常に無効に設定されます。速度が同じ場合、ポートプライオリティとポート ID が一緒に追加され、スパニングツリーによって、低いプライオリティのリンクが無効に設定されます。

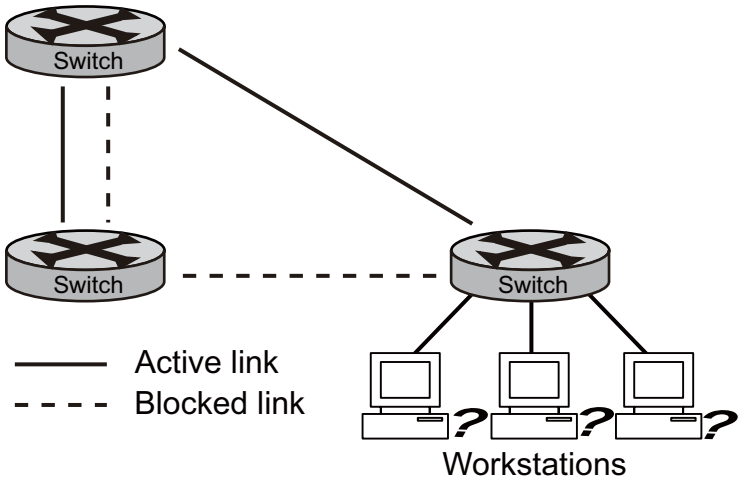


図 13　スパニングツリーと冗長接続性

5.5.7 スパニングツリーのアドレス管理

IEEE 802.1D では、異なるブリッジプロトコルで使用できる 17 つのマルチキャストアドレスを 0x00180C2000000 ～ 0x0180C2000010 の範囲で指定できます。このアドレスは、削除できない静的アドレスです。

スパニングツリーのステータスにかかわらず、スタック構成のスイッチは、0x0180C2000000 ～ 0x0180C200000F の範囲のアドレスにある場合には、パケットの受信はおこないますが、フォワーディングはおこないません。

スパニングツリーが有効の場合、スタック構成の各スイッチは 0x0180C2000000 ～ 0x0180C2000010 の範囲のパケットを受信します。スパニングツリーが無効の場合、スタック構成の各スイッチはこれらのパケットを未知のマルチキャストアドレスとしてフォワーディングします。

5.5.8 接続性維持のためのエージング加速

動的アドレスの初期設定のエージングは 5 分で、Global Configuration モードの mac address-table aging-time コマンドの初期設定です。しかし、スパニングツリーの再構築によって、多くの局の配置場所の変更が発生します。これらの局は再構築時に 5 分以上に渡って到達不能になる可能性があり、局のアドレスがアドレステーブルから削除されて再学習しようとし、アドレスのエージングタイムが加速されます。加速されたエージングタイムは、スパニングツリーの再構築時のフォワーディングディレイパラメータの値と同じです。

5.5.9 STP 機能の設定

本項では、次のスパニングツリー機能の設定方法について記載します。

- STP 実行モードの設定
- スイッチのブリッジプライオリティの設定
- スイッチのタイムパラメータの設定
- ポートのプライオリティの設定
- デバイスの STP 有効 / 無効設定
- ポートの STP 有効 / 無効設定

STP 実行モードの設定

次のコマンドを使用し、STP 実行モードを設定します。

はじめに Privileged Exec モードに移行し、次の手順で STP 実行モードを設定します。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**spanning-tree mode [stp | rstp]**	STP の実行モードを設定します。 (STP または RSTP)
手順 3	**exit**	Privileged Exec モードに戻ります。
手順 4	**show spanning-tree mode**	入力を確認します。
手順 5	**write**	（オプション）設定ファイルに入力を保存します。

ブリッジプライオリティの設定

スイッチがスパニングツリーのルートに選定されるか否かは、ブリッジプライオリティによって決まります。より小さなブリッジプライオリティ値を設定されているスイッチがルートになる可能性が高くなります。

はじめに Privileged Exec モードに移行し、次の手順でスイッチのブリッジプライオリティを有効にします。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**spanning-tree bridge priority** *priority*	指定ブリッジのブリッジプライオリティを設定します。
手順 3	**exit**	Privileged Exec モードに戻ります。
手順 4	**show spanning-tree bridge**	入力を確認します。
手順 5	**write**	（オプション）設定ファイルに入力を保存します。

[注意] プライオリティの範囲は、1 ～ 65535 で、初期設定値は 32768 です。この値を小さくすると、スイッチがルートスイッチに選定される可能性が高くなります。

- **スパニングツリーのルートの選定プロセスに関し、複数のスイッチが同じ一番小さなブリッジプライオリティ値を有する場合、最小の MAC アドレスを有するスイッチがルートとして選定されます。**

タイムパラメータの設定

本機は 3 つの時間に関連するパラメータ、フォワーディングディレイ、ハロータイム、およびエージング時間があります。フォワーディングディレイはスイッチの遷移メカニズムに関するものです。スパニングツリーは、リンクの切断により再計算され、その結果自身の構成が変化します。しかし、再計算された設定 BPDU はネットワーク全体に即時に伝播することができません。選定直後に新たなルートポートと指定ポートがデータのフォワーディングをおこなう場合、一時的なループが発生する可能性があります。したがって、プロトコルは状態遷移メカニズムを採用します。ルートポートと指定ポートがラーニング状態からフォワーディング状態へ遷移する場合、Forward Delay に指定しただけの間隔をとります。フォワーディングディレイにより、この間隔の間に新たな設定 BPD がネットワーク全体へ伝播するための一定時間が保証されます。

本機はハローパケットを、Hello Time に設定された間隔で定期的に送信し、切断されたリンクがないことを確認します。最大エージング時間は、設定 BPDU がいつ期限切れになるかを指定します。スイッチは期限切れの設定 BPDU を破棄します。

次のコマンドを使用し、スイッチの時間のパラメータを設定します。

はじめに Privileged Exec モードに移行し、次の手順で時間に関するパラメータの設定をおこないます。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**spanning-tree bridge forward** *centiseconds*	本機のフォワーディングディレイを設定します。 フォワーディングディレイは、400 ～ 3000 の範囲で設定し、初期設定値は 1500 です。
手順 3	**spanning-tree bridge hellotime** *centiseconds*	本機のハロータイムを設定します。ハロータイムは、100 ～ 1000 の範囲で設定し、初期設定値は 200 です。
手順 4	**spanning-tree bridge maxage** *centiseconds*	本機の最大エージング時間を設定します。 最大エージング時間は、10 ～ 1000000 の範囲で設定し、初期設定値は 2000 です。
手順 5	**exit**	Privileged Exec モードに戻ります。
手順 6	**show spanning-tree bridge**	入力を確認します。
手順 7	**write**	（オプション）設定ファイルに入力を保存します。

[注意] スイッチに設定するフォワーディングディレイはスイッチ接続されているネットワークの規模により異なります。通常、ネットワークの規模が大きければ、より長いフォワーディングディレイがサポートされます。フォワーディングディレイが短すぎるといくつかの冗長経路を一時的に再分配する可能性があり、長すぎるとネットワーク接続の再開に時間がかかる可能性があります。
初期設定値での使用を推奨します。

- 最適なハロータイムはスイッチでネットワークにおけるリンクの切断の検出を保証しますが、長く設定しすぎると、ネットワークリソースの占有を緩和します。
初期設定値での使用を推奨します。
- 最大エージング時間が短すぎると、ネットワーク機器が頻繁にスパニングツリーの計算をおこない、輻輳をリンクの切断と誤った判断をおこないます。しかし、最大エージング時間が長すぎると、ネットワーク機器はリンクの切断を検出できず、おこなうべきときにスパニングツリーの再計算をおこなえず、ネットワークの自動適応能力を弱めることになってしまいます。
初期設定値での使用を推奨します。

頻繁なネットワークの再計算を回避するため、ハロータイム、フォワーディングディレイ、および最大エージング時間は次の式を満たすように設定してください。

2 * (フォワーディングディレイ - 1 秒) >= 最大エージング時間

最大エージング時間 >= 2 * (ハロータイム + 1.0 秒)

stp root primary コマンドを使用し、ネットワークの規模、スイッチ接続されているネットワークのハロータイムの設定をおこなうことを推奨しますが、これによって MSTP がより最適な値を自動的に計算します。

ポートプライオリティの設定

ループが発生すると、スパニングツリーはインターフェースを選択してフォワーディング状態に移行する際にポートプライオリティを使用します。

最初に選択したいインターフェースに高いプライオリティ（小さい値）を割り当て、最後に選択したいインターフェースに低いプライオリティ（大きい値）を割り当てできます。すべてのインターフェースが同じプライオリティ値を有する場合、スパニングツリーによって最小のインターフェース番号を有するインターフェースがフォワーディング状態に移行し、他のインターフェースはブロックされます。

はじめに Privileged Exec モードに移行し、次の手順でポートのプライオリティを設定します。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**spanning-tree port** *port-number* **priority** *priority*	ポートのプライオリティを設定します。 ポートのプライオリティは、1 ～ 255 の範囲で設定し、初期設定値は 128 です。
手順 3	**exit**	Privileged Exec モードに戻ります。
手順 4	**show spanning-tree bridge**	入力を確認します。
手順 5	**write**	（オプション）設定ファイルに入力を保存します。

デバイスの STP 有効 / 無効設定

次のコマンドを使用し、本機の STP を有効に設定します。

はじめに Privileged Exec モードに移行し、次の手順で本機の STP を有効にします。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**system span enable**	本機の STP を有効に設定します。
手順 3	**exit**	Privileged Exec モードに戻ります。
手順 4	**show system config**	入力を確認します。
手順 5	**write**	（オプション）設定ファイルに入力を保存します。

機器の STP を無効に設定

モード	コマンド
Grobal Configuration	**system span disable**

STP が機器で有効に設定済みの場合にのみ、他の STP 設定が有効になります。

初期設定では、STP は無効に設定されています。

ポート上の STP 有効 / 無効設定

次のコマンドを使用し、ポートの STP の有効 / 無効を設定できます。本機のいくつかのイーサネットポートではスパニングツリーの計算をおこなわないように、このイーサネットポートを無効に設定できます。これは、STP の実行を柔軟に制御するための、また本機の CPU のリソースを節約するための手段のひとつです。

はじめに Privileged Exec モードに移行し、次の手順でポートの STP を有効にします。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**rstp port** *port-number* **enable**	ポートの STP を有効に設定します。
手順 3	**exit**	Privileged Exec モードに戻ります。
手順 4	**show spanning-tree ports**	入力を確認します。
手順 5	**write**	（オプション）設定ファイルに入力を保存します。

ポートの STP を無効に設定

モード	コマンド
Grobal Configuration	**rstp port** *port-number* **disable**

STP を無効に設定したあと、冗長経路が生成される可能性があることに注意してください。

初期設定では、機器に STP が有効に設定されている場合、すべてのポートの STP は有効に設定されています。

5.5.10 RSTP の設定

本項では、次の RSTP 機能の設定方法について記載します。

- STP 実行モードの設定
- スイッチのブリッジプライオリティの設定
- スイッチのタイムパラメータの設定
- ポートのプライオリティの設定
- ポートをエッジポートに設定
- ポートのパスコストの設定
- ポートの mCheck 変数の設定
- ポートをポイントツーポイントリンクで接続する（しない）ように設定
- デバイスの STP 有効 / 無効設定

STP 実行モードの設定

次のコマンドを使用し、RSTP 実行モードを設定します。

はじめに Privileged Exec モードに移行し、次の手順で RSTP 実行モードを設定します。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**spanning-tree mode [stp | rstp]**	RSTP の実行モードを設定します。 (STP または RSTP)
手順 3	**exit**	Privileged Exec モードに戻ります。
手順 4	**show spanning-tree mode**	入力を確認します。
手順 5	**write**	（オプション）設定ファイルに入力を保存します。

ブリッジプライオリティの設定

スイッチがスパニングツリーのルートに選定されるか否かは、ブリッジプライオリティによって決まります。より小さなブリッジプライオリティ値を設定されているスイッチがルートになる可能性が高くなります。

はじめに Privileged Exec モードに移行し、次の手順でスイッチのブリッジプライオリティを有効にします。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**rstp bridge priority** *priority*	指定ブリッジのブリッジプライオリティを設定します。
手順 3	**exit**	Privileged Exec モードに戻ります。
手順 4	**show spanning-tree bridge**	入力を確認します。
手順 5	**write**	（オプション）設定ファイルに入力を保存します。

[注意] プライオリティの範囲は、1 ～ 65535 で、初期設定値は 32768 です。この値を小さくすると、スイッチがルートスイッチに選定される可能性が高くなります。

- スパニングツリーのルートの選定プロセスに関し、複数のスイッチが同じ一番小さなブリッジプライオリティ値を有する場合、最小の MAC アドレスを有するスイッチがルートとして選定されます。

タイムパラメータの設定

本機は 3 つの時間に関連するパラメータ、フォワーディングディレイ、ハロータイム、およびエージング時間があります。フォワーディングディレイはスイッチの遷移メカニズムに関するものです。スパニングツリーは、リンクの切断により再計算され、その結果自身の構成が変化します。しかし、再計算された設定 BPDU はネットワーク全体に即時に伝播することができません。選定直後に新たなルートポートと指定ポートがデータのフォワーディングをおこなう場合、一時的なループが発生する可能性があります。したがって、プロトコルは状態遷移メカニズムを採用します。ルートポートと指定ポートがラーニング状態からフォワーディング状態へ遷移する場合、Forward Delay に指定しただけの間隔をとります。フォワーディングディレイにより、この間隔の間に新たな設定 BPD がネットワーク全体へ伝播するための一定時間が保証されます。

本機はハローパケットを、Hello Time に設定された間隔で定期的に送信し、切断されたリンクがないことを確認します。

最大エージング時間は、設定 BPDU がいつ期限切れになるかを指定します。スイッチは期限切れの設定 BPDU を破棄します。

次のコマンドを使用し、スイッチの時間のパラメータを設定します。

はじめに Privileged Exec モードに移行し、次の手順で時間に関するパラメータの設定をおこないます。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**rstp bridge forward** *centiseconds*	本機のフォワーディングディレイを設定します。 範囲：400 ～ 3000　初期設定値：1500
手順 3	**rstp bridge hellotime** *centiseconds*	本機のハロータイムを設定します。 範囲：100 ～ 1000　初期設定値：200
手順 4	**rstp bridge maxage** *centiseconds*	本機の最大エージング時間を設定します。 範囲：10 ～ 1000000　初期設定値：2000
手順 5	**exit**	Privileged Exec モードに戻ります。
手順 6	**show rstp bridge**	入力を確認します。
手順 7	**write**	（オプション）設定ファイルに入力を保存します。

[注意]　スイッチに設定するフォワーディングディレイはスイッチ接続されているネットワークの規模により異なります。通常、ネットワークの規模が大きければ、より長いフォワーディングディレイがサポートされます。フォワーディングディレイが短すぎるといくつかの冗長経路を一時的に再分配する可能性があり、長すぎるとネットワーク接続の再開に時間がかかる可能性があります。
初期設定値での使用を推奨します。

- **最適なハロータイムはスイッチでネットワークにおけるリンクの切断の検出を保証しますが、長く設定しすぎると、ネットワークリソースの占有を緩和します。**
初期設定値での使用を推奨します。
- **最大エージング時間が短すぎると、ネットワーク機器が頻繁にスパニングツリーの計算をおこない、輻輳をリンクの切断と誤った判断をおこないます。しかし、最大エージング時間が長すぎると、ネットワーク機器はリンクの切断を検出できず、おこなうべきときにスパニングツリーの再計算をおこなえず、ネットワークの自動適応能力を弱めることになってしまいます。**
初期設定値での使用を推奨します。

頻繁なネットワークの再計算を回避するため、ハロータイム、フォワーディングディレイ、および最大エージング時間は次の式を満たすように設定してください。

2 * (フォワーディングディレイ - 1 秒) >= 最大エージング時間

最大エージング時間 >= 2 * (ハロータイム + 1.0 秒)

stp root primary コマンドを使用し、ネットワークの規模、スイッチ接続されているネットワークのハロータイムの設定をおこなうことを推奨しますが、これによって MSTP がより最適な値を自動的に計算します。

ポートプライオリティの設定

ループが発生すると、スパニングツリーはインターフェースを選択してフォワーディング状態に移行する際にポートプライオリティを使用します。

最初に選択したいインターフェースに高いプライオリティ（小さい値）を割り当て、最後に選択したいインターフェースに低いプライオリティ（大きい値）を割り当てできます。すべてのインターフェースが同じプライオリティ値を有する場合、スパニングツリーによって最小のインターフェース番号を有するインターフェースがフォワーディング状態に移行し、他のインターフェースはブロックされます。

はじめに Privileged Exec モードに移行し、次の手順でポートのプライオリティを設定します。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**rstp port** *port-number* **priority** *priority*	ポートのプライオリティを設定します。 ポートのプライオリティは、1 ～ 255 の範囲で設定し、初期設定値は 128 です。
手順 3	**exit**	Privileged Exec モードに戻ります。
手順 4	**show rstp bridge**	入力を確認します。
手順 5	**write**	（オプション）設定ファイルに入力を保存します。

ポートをエッジポートに設定

エッジポートは、接続しているネットワークにおいて、直接スイッチに接続していないポートまたは非直接的にスイッチに接続しているポートを参照します。
エッジポートに設定すると、このポートは遅延なくブロッキング状態からフォワーディング状態へ高速に遷移できます。スイッチで BPDU 保護が有効に設定されていない場合、他のポートから BPDU を受信した際、設定されたエッジポートが再び非エッジポートに戻ります。BPDU 保護が有効に設定されている場合、ポートは無効です。

はじめに Privileged Exec モードに移行し、次の手順でポートをエッジポートに設定します。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**rstp port {** *port-number* | *all* **}** **edged-port enable**	ポートをエッジポートに設定します。 初期設定では、本機のすべてのイーサネットポートは非エッジポートに設定されています。
手順 3	**exit**	Privileged Exec モードに戻ります。
手順 4	**show rstp port** **{** *port-number* | *all* **}**	入力を確認します。
手順 5	**write**	（オプション）設定ファイルに入力を保存します。

エッジポートを無効に設定

モード	コマンド
Grobal Configuration	**rstp port {** *port-number* | *all* **} edged-port disable**

[注意]　直接ターミナルと接続してポートをエッジポートに設定し、ポートの BPDU 機能を有効に設定することを推奨します。これが、高速での状態遷移とスイッチへの攻撃の回避を可能にします。

ポートのパスコストの設定

パスコストはポートに接続しているリンクの速度に関連しているものです。
次の手順でポートのパスコストを設定できます。

はじめに Privileged Exec モードに移行し、次の手順でポートのパスコストを設定します。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**rstp port** **{** *port-number* | *all* **}** **pathcost value**	ポートのパスコストを設定します。value は 0 ～ 240 の範囲から設定し、初期設定値は auto です。
手順 3	**exit**	Privileged Exec モードに戻ります。
手順 4	**show rstp port** **{** *port-number* | *all* **}**	入力を確認します。
手順 5	**write**	（オプション）設定ファイルに入力を保存します。

ポートのパスコストを変更すると、MSTP がポートの役割を再算出し、状態の遷移をおこないます。

初期設定では、RSTP はポートのパスコストの計算をおこないます。

ポートの mCheck 変数の設定

本機のポートは STP または RSTP で動作します。

次の手順で、ポートの mCheck 動作を実行できます。

はじめに Privileged Exec モードに移行し、次の手順でポートの mCheck 変数の設定をおこないます。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**rstp port** {*port-number* | *all*} **mcheck**	ポートの mCheck 動作を実行します。
手順 3	**exit**	Privileged Exec モードに戻ります。
手順 4	**show rstp port** { *port-number* | *all* }	入力を確認します。
手順 5	**write**	（オプション）設定ファイルに入力を保存します。

このコマンドは本機が RSTP で稼動している場合にのみ使用できることに注意してください。本機が STP モードで稼動している場合、このコマンドは何の意味もありません。

ポートをポイントツーポイントリンクで接続する（しない）ように設定

ポイントツーポイントリンクは 2 台のスイッチを直接接続します。

次の手順で、ポートをポイントツーポイントリンクで接続する（しない）ように設定できます。

はじめに Privileged Exec モードに移行し、次の手順でポートをポイントツーポイントリンクで接続する（しない）よう設定をおこないます。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**rrstp port** {*port-number* | *all*} **point-to-point [force-true | force-false | auto]**	ポートをポイントツーポイントリンクで接続する（しない）ように設定します。force-true は、ポートがポイントツーポイントリンクで接続することを示します。force-false は、ポートがポイントツーポイントリンクで接続しないことを示します。
手順 3	**exit**	Privileged Exec モードに戻ります。
手順 4	**show rstp port** { *port-number* | *all* }	入力を確認します。
手順 5	**write**	（オプション）設定ファイルに入力を保存します。

ポートがポイントツーポイントリンクで接続している場合、ポートの役割の状況が一致すると、同期パケットの転送によって高速にフォワーディング状態に遷移でき、したがって不必要なフォワーディングディレイを削減できます。パラメータが auto モードに設定されている場合、その時点でのイーサネットポートがポイントツーポイントリンクで接続しているか否かは RSTP によって自動的に検出されます。

初期設定では、パラメータは auto に設定されています。

デバイスの STP 有効 / 無効設定

次のコマンドを使用し、本機の STP を有効に設定します。

はじめに Privileged Exec モードに移行し、次の手順で本機の STP を有効にします。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**system span enable**	本機の STP を有効に設定します。
手順 3	**exit**	Privileged Exec モードに戻ります。
手順 4	**show system config**	入力を確認します。
手順 5	**write**	（オプション）設定ファイルに入力を保存します。

機器の STP を無効に設定

モード	コマンド
Grobal Configuration	**system span disable**

STP が機器で有効に設定済みの場合にのみ、他の STP 設定が有効になります。初期設定では、STP は無効に設定されています。

5.6 IP アドレス

5.6.1 概要

アドレスクラスとアドレス表示

IP アドレスはインターネットへのアクセス機器に割り当てられる 32bit **のアドレスです。IP アドレスは** 2 **つのフィールドから構成されています。ネットワーク部とホスト部です。IP アドレスには** 5 **つの種類があります。次の図を参照してください。**

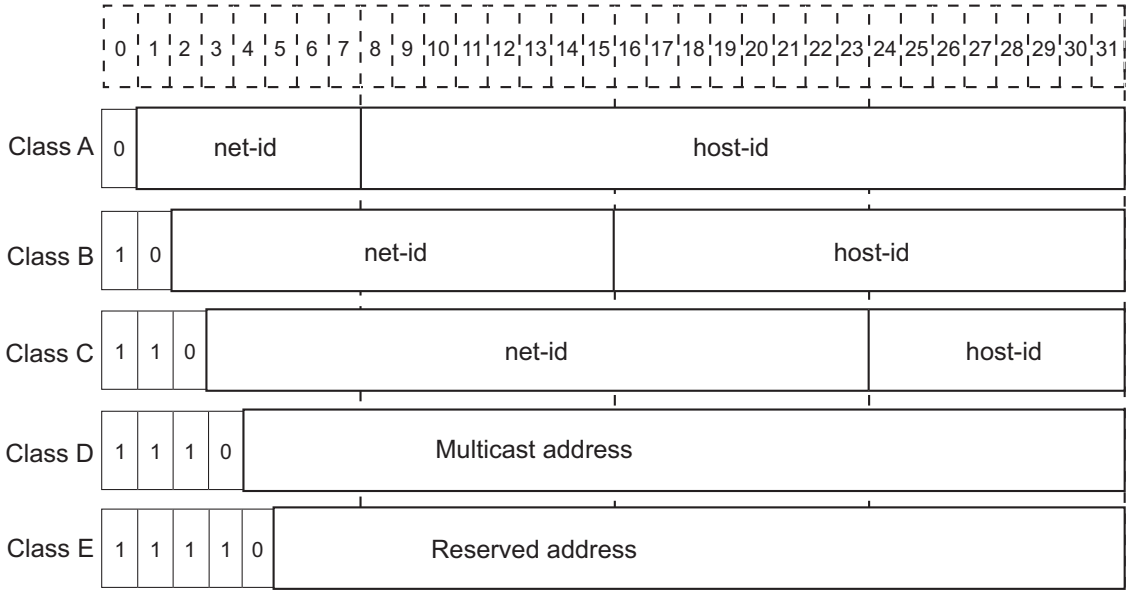


図 14　IP **アドレスの** 5 **つのクラス**

ここで、クラス A（Class A)、**クラス** B（Class B）**およびクラス** C（Class C）**はユニキャストアドレス、クラス** D（Class D）**はマルチキャストアドレス、またクラス** E（Class E）**は将来の特別なアプリケーションのために予約されています。最初の** 3 **つの種類はよく使用されます。**

IP **アドレスはドットを含む** 10 **進数のフォーマットです。各** IP **アドレスは** 4 **つの整数で、ドット付きの** 10 **進数で表記されています。各整数は** 1byte **になります。例：**10.110.50.101

IP **アドレスを使用する場合、いくつかは特別の使用のために予約されている、またはほとんど使用されないことにも注意が必要です。使用可能な** IP **アドレスを次の表に記載します。**

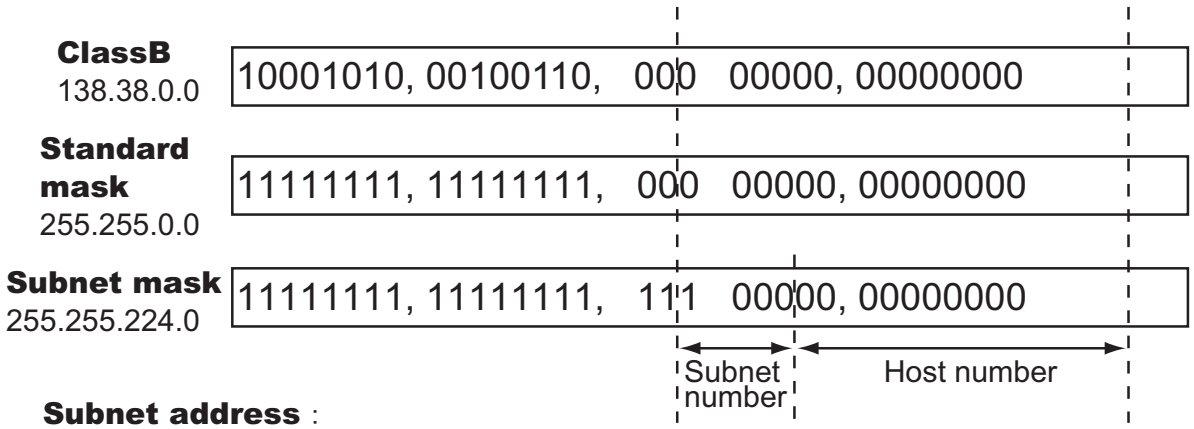
ネットワーククラス	アドレス領域	IP ネットワークの範囲	注記：
A	0.0.0.0 〜 127.255.255.255	1.0.0.0 〜 126.0.0.0	すべての桁が 0 のホスト ID は、この IP アドレスがネットワークアドレスでネットワークのルーティングで使用されることを示します。すべての桁が 1 のホスト ID はブロードキャストアドレスで、そのネットワークのすべてのホストに対しブロードキャストをおこなうことを示します。IP アドレス 0.0.0.0 は、起動後に使用しないホストに使用します。ネットワーク ID が 0 の IP アドレスは現在のネットワークであることを示し、ルータがネットワークアドレスを知らなくても処理できます。127.X.Y.Z のフォーマットのネットワーク ID は、自己ループバックテストのために予約されており、このアドレス宛てに送信されたパケットはネットワークへ送信されません。パケットは内部で処理され、受信されたパケットと判断されます。
B	128.0.0.0 〜 191.255.255.255	128.0.0.0 〜 191.254.0.0	すべての桁が 0 のホスト ID は、この IP アドレスがネットワークアドレスでネットワークのルーティングで使用されることを示します。すべての桁が 1 のホスト ID はブロードキャストアドレスで、そのネットワークのすべてのホストに対しブロードキャストをおこなうことを示します。
C	192.0.0.0 〜 223.255.255.255	192.0.0.0 〜 223.255.254.0	すべての桁が 0 のホスト ID は、この IP アドレスがネットワークアドレスでネットワークのルーティングで使用されることを示します。すべての桁が 1 のホスト ID はブロードキャストアドレスで、そのネットワークのすべてのホストに対しブロードキャストをおこなうことを示します。
D	224.0.0.0 〜 239.255.255.255	なし	クラス D のアドレスはマルチキャストアドレスです。
E	240.0.0.0 〜 239.255.255.254	なし	このアドレスは将来のために予約されています。
その他のアドレス	255.255.255.255	255.255.255.255	255.255.255.255 は LAN のブロードキャストアドレスです

サブネットとマスク

現在では、インターネットの急速な展開によって、IP アドレスは非常に早い速度で枯渇しつつあります。従来からの IP アドレス割り当て方法では IP アドレスを多大に浪費します。有効な IP アドレスを最大限に利用するため、マスクとサブネットの概念が提唱されました。

マスクは 32bit の、IP アドレスに対応した番号です。この番号は 1 と 0 から構成されています。基本的には、1 と 0 は無作為に組み合わされています。しかし、マスクを示す場合、最初の連続するビットは 1 に設定されます。マスクによって、IP アドレスは、次の 2 つの部分に分けられます。この 2 つの部分とは、サブネットアドレスとホストアドレスです。アドレスとマスクの連続する 1 はサブネットアドレスであることを示し、他のビットはホストアドレスであることを示します。サブネット部がない場合は、サブネットマスクが初期値になり、1 の長さ分がネットワーク部の長になります。したがって、クラス A、B、C の IP アドレスの場合、サブネットマスクの初期値はそれぞれ、255.0.0.0、255.255.0.0 または 255.255.255.0 となります。

マスクにより、16,000,000 以上のホストを有するクラス A のネットワークを、また 60,000 以上のホストを有するクラス B のネットワークを、複数の小さなネットワークに分割できます。それぞれの小さなネットワークをサブネットと呼びます。たとえば、クラス B ネットワークのアドレスが 138.38.0.0 の場合、マスク 255.255.224.0 は、ネットワークを次の 8 つのサブネットに分割するのに使用されます。これは 138.38.0.0、138.38.32.0、138.38.64.0、138.38.96.0、138.38.128.0、138.38.160.0、138.38.192.0 および 138.38.224.0 です（次の図を参照してください）。各サブネットには、8000 以上のホストを収容できます。



Subnet address :

- 000 Subnet address : 138.38. 0.0
- 000 Subnet address : 138.38. 32.0
- 000 Subnet address : 138.38. 64.0
- 000 Subnet address : 138.38. 96.0
- 000 Subnet address : 138.38.128.0
- 000 Subnet address : 138.38.160.0
- 000 Subnet address : 138.38.192.0
- 000 Subnet address : 138.38.224.0

図 15 IP アドレスの分割によるサブネット

5.6.2 IP アドレスの設定

IP アドレスの設定には次の項目があります。

- AUX ポートの IP アドレス設定
- VLAN インターフェースの IP アドレス設定

AUX ポートの IP アドレス設定

ローカルで Telnet や HTTP などのアプリケーションを使用する場合、IP アドレスを設定します。

はじめに Privileged Exec モードに移行し、次の手順で AUX ポートの IP アドレスを設定します。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**interface aux ipaddress set** *ip-address net-mask*	AUX ポートの IP アドレスを設定します。 初期設定値：192.168.1.168
手順 3	**exit**	Privileged Exec モードに戻ります。
手順 4	**show interface aux**	入力を確認します。
手順 5	**write**	（オプション）設定ファイルに入力を保存します。

AUX ポートの IP アドレスの削除

モード	コマンド
Grobal Configuration	**interface aux ipaddress delete** *ip-address*

VLAN インターフェースの IP アドレス設定

本機の各 VLAN インターフェースには IP アドレスを設定できます。通常、1 つのインターフェースに対して 1 つの IP アドレスを設定するので十分です。複数のサブネットから接続できるように、1 つのインターフェースに対して最大 32 の IP アドレスを設定することも可能です。

はじめに Privileged Exec モードに移行し、次の手順で VLAN インターフェースの IP アドレスをおこないます。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**ip address add vint** *interface-id ip-address nat-mask* **vid** *vlan-id* [**description** *string*]	VLAN インターフェースの IP アドレスを設定します。 interface-id は仮想的なインターフェース番号です。 範囲：0 ～ 32 初期設定：IP アドレスは設定されていません。
手順 3	**exit**	Privileged Exec モードに戻ります。
手順 4	**show ip address**	入力を確認します。
手順 5	**write**	（オプション）設定ファイルに入力を保存します。

VLAN インターフェースの IP アドレスの削除

モード	コマンド
Grobal Configuration	**ip address delete** *ip-address*

5.6.3 IP アドレスの設定例

ネットワーク要件

本機の VLAN 1 **に、**IP **アドレス** 129.2.2.1**、サブネットマスク** 255.255.255.0 **を設定します。**

ネットワーク構成図

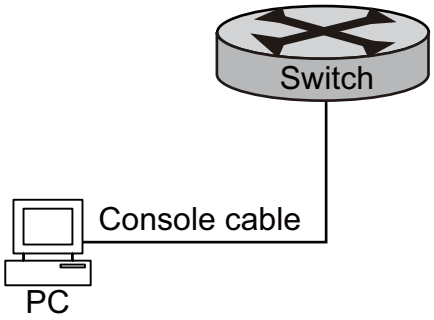


図 16　IP **アドレスを設定するネットワーク**

設定手順

Switch(config)#ip address add vint 1 129.2.2.1 255.255.255.0 vid 1

5.6.4 IP アドレス設定時のトラブルシューティング

障害 1: スイッチが LAN **上の特定のホストとの** ping **に失敗する。**

次の手順でトラブルシューティングを実行します。

- **スイッチの設定内容を確認します。**
  show arp **コマンドを使用し、スイッチが保持している** ARP **テーブルを確認します。**
- **トラブルシューティング：まず、どの** VLAN **に、ホストに接続するために使用されているスイッチのポートが所属しているかを確認します。**
- VLAN **は** VLAN **インターフェースの設定を完了しているかどうかを確認します。次に、**VLAN **インターフェースとホストの** IP **アドレスが同じネットワークセグメントのものであるかを確認します。**

5.7 ARP

5.7.1 概要

ARP の必要性

ネットワーク機器は MAC アドレスのみを識別できるため、IP アドレスはネットワーク機器間の通信で直接使用できません。IP アドレスはネットワークレイヤにおける、ホストの単なるアドレスです。ネットワークレイヤから転送されたデータパケットをデスティネーションホストへ送信するには、ホストの物理アドレスが必要です。そのため、IP アドレスが物理アドレスに解決されなくてはなりません。

ARP の実行手順

イーサネットで結ばれた 2 つのホストが通信する場合、両者は互いの MAC アドレスを知っていなくてはなりません。各ホストは ARP マッピングテーブルと呼ばれる IP-MAC アドレス変換テーブルを保持しています。最近ローカルホストとの通信で使用した、他のホストの IP アドレスと MAC アドレスの一連のマッピング情報が、ARP マッピングテーブルに保存されています。動的な ARP マッピング入力項目が一定期間使用されないと、メモリ空間を節約し、スイッチが ARP マッピングテーブルを検索する時間を短縮化するために、ホストが使用していない入力項目を ARP マッピングテーブルから削除します。

同一のネットワークセグメントに 2 つのホスト、ホスト A とホスト B があると想定します。ホスト A の IP アドレスは IP_A で、ホスト B の IP アドレスは IP_B とします。
ホスト A がメッセージをホスト B に転送しようとしています。ホスト A は自身の ARP マッピングテーブルをまずチェックし、IP_B に一致する ARP 入力がテーブルにあるか否かを確認します。対応する MAC アドレスが検出されたら、ホスト A は ARP マッピングテーブルのこの MAC アドレスを使用し、フレームで IP パケットをカプセル化してホスト B に送信します。対応する MAC アドレスが検出されない場合、ホスト A は転送用のキューに IP パケットを保持し、イーサネット全体に向けブロードキャストします。ARP リクエストパケットにはホスト B の IP アドレスと、ホスト A の IP アドレスおよび MAC アドレスを含みます。ARP リクエストパケットがブロードキャストされると、ネットワークセグメントに所属するすべてのホストがこのリクエストを受信できます。しかし、リクエストされたホスト（すなわちホスト B）だけがリクエストを処理する必要があります。ホスト B はまずリクエストの送信者（ホスト A）の IP アドレスと MAC アドレスを自身の ARP マッピングテーブルの ARP リクエストパケットに保持します。次にホスト B が、ホスト B の MAC アドレスを追加した ARP リプライパケットをホスト A に送信します。リプライパケットは、ブロードキャストされずに直接ホスト A に送信されます。ホスト A は、リプライパケットを受信すると、IP アドレスと対応するホスト B の MAC アドレスを抽出し、自身の ARP マッピングテーブルに追加します。そして、ホスト A はホスト B にキューで待ち状態であったすべてのパケットを送信します。

通常、動的な ARP の実行と、IP アドレスからイーサネット MAC アドレス解決のための自動検索が、ネットワーク管理者の介在なく実行されます。

5.7.2 ARP の設定

ARP マッピングテーブルは動的または手入力により維持できます。通常、手入力により設定される IP アドレスから MAC アドレスへのマッピング情報は、静的 ARP と呼ばれています。手入力用のメンテナンスコマンドを使用して ARP マッピングテーブルの表示、追加または削除ができます。

静的 ARP 設定には次の項目が含まれます。

- ARP マッピング項目の静的な追加と削除
- ARP マッピング項目の削除

ARP マッピング項目の静的な追加と削除

はじめに Privileged Exec モードに移行し、次の手順で静的な ARP マッピング入力を追加します。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**arp add** *ip-address mac-address*	静的な ARP マッピング入力を追加します。
手順 3	**exit**	Privileged Exec モードに戻ります。
手順 4	**show arp**	入力を確認します。
手順 5	**write**	（オプション）設定ファイルに入力を保存します。

静的な ARP マッピング入力の削除

モード	コマンド
Grobal Configuration	**use arp delete** *ip-address*

ARP マッピング項目の削除

はじめに Privileged Exec モードに移行し、次の手順で ARP マッピング入力項目を削除します。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**arp flush**	ARP マッピング入力項目を削除します。
手順 3	**exit**	Privileged Exec モードに戻ります。
手順 4	**show arp**	入力を確認します。
手順 5	**write**	（オプション）設定ファイルに入力を保存します。

5.8 IP ルーティング

本節では、本機で IP ルーティングを設定する方法について記載します。スイッチは、ネットワークの他のルータに対し、1 台のルータのように見られたり動作します。基本的なルーティング機能には、スタティックルーティング、RIP（Routing Information Protocol）、OSPF（Open Shortest Path First）プロトコルが含まれます。

5.8.1 概要

IP ルーティングとルーティングセグメント

ルータはインターネットの経路選択を実現します。ルータは次の方法で動作します。受信パケットのデスティネーションアドレスに従い、（ネットワークを経由する）適切なパスを選択し、このパケットを次のルータへフォワーディングします。次から次へとフォワーディングされ、パスの最後のルータはデスティネーションのホストまでパケットを送り、IP パケットのフォワーディングとネットワークセグメントをまたいだルーティングを完了する責務を負います。

ネットワークでは、ルータはパケットを送信するための 1 つのパスを論理的な経路の単位とみなし、これをホップと呼びます。たとえば、下図のように、ホスト A からホスト C に送信されるパケットは、2 台のルータを通過しなくてはならず、2 ホップとルータセグメントを介して転送されます。したがって、あるノードが他の 1 つのノードとネットワークを介して接続している場合、この 2 つのノード間には 1 つのホップがあり、この 2 つのノードはインターネット上で隣接しているとみなされます。同様に、隣接するルータは同じネットワークに接続する 2 台のルータを参照しています。同一ネットワーク上のルータとホスト間の経路セグメントの数は、0 と数えます。下図の、太線の矢印がホップを示します。ルータは、ネットワークを介してパケットのルーティングをおこなうため、経路セグメントの構成要素である物理的なリンクに接続します。

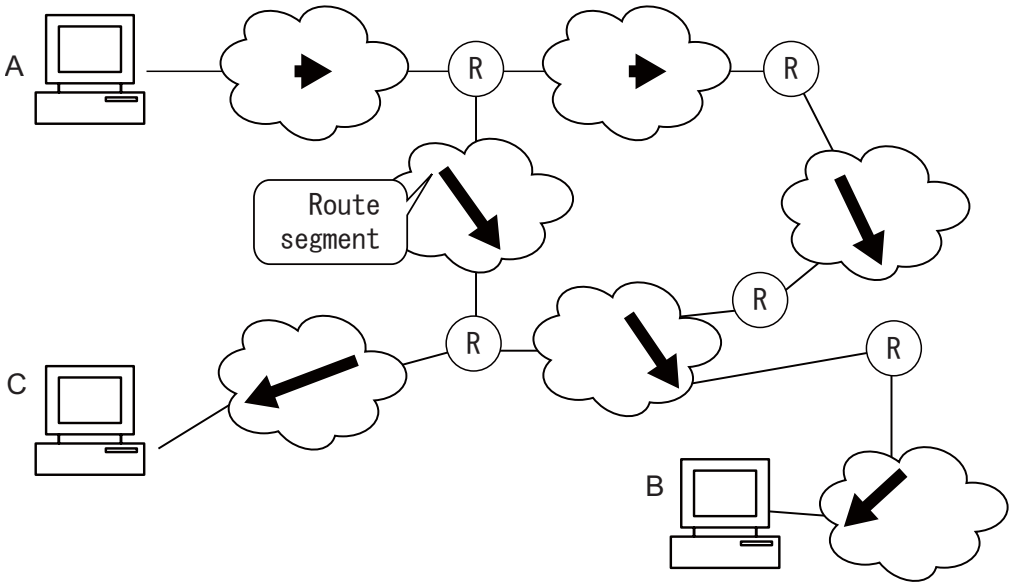


図 17　ホップ

ネットワークの規模は異なるため、ルータ間を結ぶセグメント長もそれぞれ異なります。経路セグメントに加重係数を乗算したものが、信号を伝送するパスの実効長のため補正された大きさとして機能できます。

ネットワークに配置されているルータがノードと見なされ、インターネットの経路セグメントがリンクと見なされる場合、インターネットで伝送されるメッセージの経路は、従来型のネットワークで伝送されるメッセージの経路と同様に機能します。最短の経路を介して伝送されるメッセージが必ずしも最適な経路にはなりません。たとえば、3 つの LAN の経路セグメントを介したルーティングは 2 つの WAN の経路セグメントを介した場合よりもより高速だと考えられます。

ルーティングテーブルからの経路選択

ルータがパケットをフォワーディングする場合のキーとなるものは、ルーティングテーブルです。各ルータはルーティングテーブルをメモリに保存しており、テーブルの各入力項目は、パケットが経路を介してサブネットやホストに送信されるルータの物理ポートを設定しています。したがって、特定のパスの次のルータに到達できるか、または直接接続されたネットワークを介してデスティネーションホストに到達できます。

ルーティングテーブルには次のような主な入力項目があります。

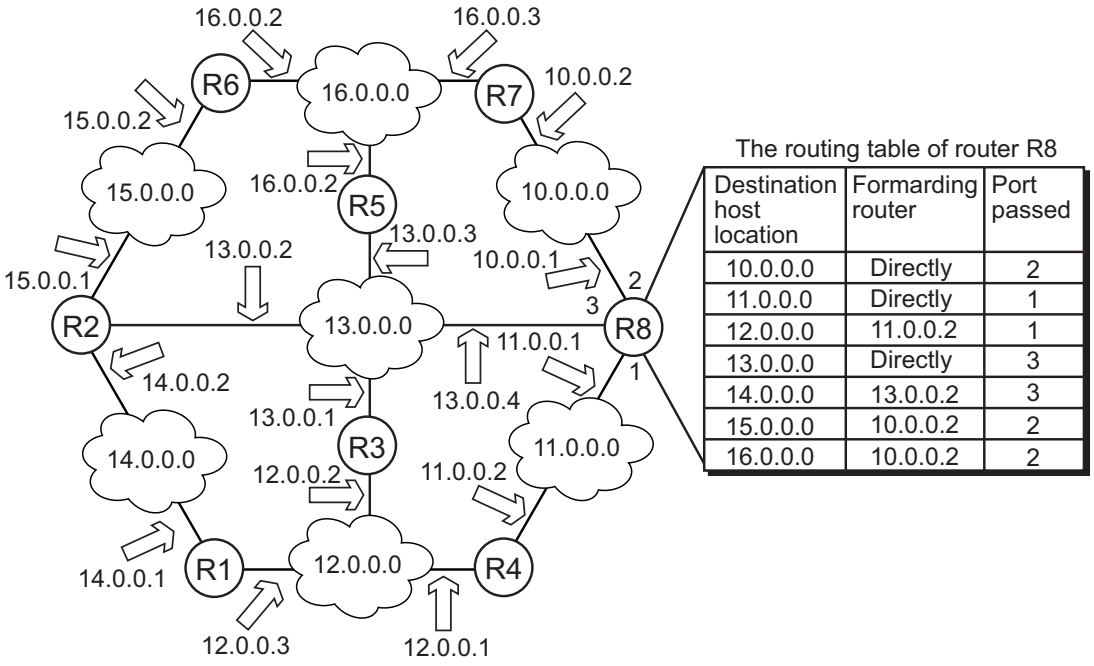
- デスティネーションアドレス：IP パケットの宛て先の IP アドレスまたは宛て先のネットワークを識別するために使用され、長さは 32bit です。
- ネットワークマスク：連続する 1 で構成されており、ドット区切りの 10 進フォーマットかまたはマスクの連続する 1 で表現されます。デスティネーションアドレスと組み合わされ、デスティネーションホストまたはルータのネットワークアドレスの識別に使用されます。デスティネーションアドレスとネットワークマスクで AND 演算すれば、宛て先のホストやルータが配置されているネットワークセグメントのアドレスが得られます。たとえば、デスティネーションアドレスが 129.102.8.10 でホストまたはルータのマスクが 255.255.0.0 のネットワークのアドレスは 129.102.0.0 になります。
- 送信用インターフェース：IP パケットがフォワーディングされるインターフェースを示します。
- ネクストホップアドレス：IP パケットが通過する次のルータを示します。
- IP ルーティングテーブルに追加される 1 つの経路用のプライオリティ：同じ宛て先に対して異なるネクストホップが存在する可能性があります。これらの経路は異なるルーティングプロトコルによって発見されるか、手入力によってスタティックルートとして設定できます。最も高いプライオリティ（一番小さな値）を持つものがその時点での最適な経路として選択されます。

宛て先別に、経路は次のように分けることができます。

- サブネットルート－宛て先はサブネットです。
- ホストルート－宛て先はホストで、さらに、宛て先のホストのネットワークが直接ルータに接続しているか否かで次の経路の種類に分かれます。
- ダイレクトルート－ 宛て先が置かれているネットワークに直接ルータが接続しています。
- インダイレクトルート－宛て先が置かれているネットワークに直接ルータが接続していません。

ルーティングテーブルのサイズに制限があるため、デフォルトルートを設定するオプションも可能です。適切な入力項目を検出できないパケットはすべて、このデフォルトルートを経由してフォワーディングされます。

次の図のように複雑なインターネットでは、各ネットワークの番号がネットワークアドレスです。ルータ R8 は 3 つのネットワークに接続し、そのためこのルータは 3 つの IP アドレスと 3 つの物理ポートを持っており、またルーティングテーブルは下の表に示します。



The routing table of router R8

Destination host location	Formarding router	Port passed
10.0.0.0	Directly	2
11.0.0.0	Directly	1
12.0.0.0	11.0.0.2	1
13.0.0.0	Directly	3
14.0.0.0	13.0.0.2	3
15.0.0.0	10.0.0.2	2
16.0.0.0	10.0.0.2	2

図 18　ルーティングテーブル

5.8.2 経路管理のポリシー

本機はスタティックルートに加え、RIP、OSPF などの一連のダイナミックルーティングプロトコルによる設定をサポートしています。スタティックルートはユーザによって設定され、ルーティングプロトコルによって検出されたダイナミックルートと一緒に管理されます。スタティックルートと異種ルーティングプロトコルにより学習・設定された経路とは、互いに共有できます。

ルーティングプロトコルと対応する経路のプリファレンス

（静的な設定と同様に）ルーティングプロトコルが異なると同じ宛て先でも異なる経路を生成する可能性がありますが、すべての経路が最適であるとは限りません。実際、瞬間的に、ただ 1 つのルーティングプロトコルがその時点での特定の宛て先への経路を決定できます。このように、これらの各ルーティングプロトコル（静的な設定を含む）はプリファレンスを設定され、複数の経路情報の送信元がある場合、最も高いプリファレンスを有するルーティングプロトコルにより発見された経路がその時点での経路になります。次の表に、ルーティングプロトコルと、これにより学習された経路の初期設定のプリファレンス（値が小さいほどプリファレンスが高くなる）を記載します。

ルーティングプロトコルまたは経路の種類	経路のプリファレンス
DIRECT	0
OSPF	10
STATIC	60
RIP	100
不明	255

上記の表で、0 はダイレクトルートを示します。255 は信頼できない情報の送信元からの経路であることを示します。ダイレクトルート以外は、様々な種類の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は、ユーザの要件に沿うよう手入力により設定できます。さらに、スタティックルートにはそれぞれ異なるプリファレンス値を設定できます。

負荷分散と冗長経路のサポート

負荷分散

マルチルートモードをサポートしているため、同じ宛て先に同じプリファレンスを使用して複数の到達経路を設定できます。同じ宛て先に複数の異なるパスを経由して到達でき、その優先順位は同じです。より高い優先順位の同じ宛て先への到達経路が存在しない場合、複数の経路が IP によって適応され、これによって負荷分散が実現されるようにこれらのパスを介してパケットが宛て先にフォワーディングされます。

同じ宛て先に対し、設定したルーティングプロトコルが複数の異なる経路を検出します。そのルーティングプロトコルがすべての有効なルーティングプロトコルのなかで最も優先順位が高い場合、これらの複数の経路はその時点で有効な経路と見なされます。このように、IP トラフィックの負荷分散がルーティングプロトコルの観点から保証されます。

冗長経路

経路のバックアップをサポートしています。主経路にエラーが発生した場合、システムは自動的に二次経路に切り替え、ネットワークの信頼性を高めます。経路の冗長化を図るため、実際の状況に基づき、ユーザが複数の経路を同じ宛て先に向けて設定できます。経路のうちの 1 つは最も高い優先順位を持ち、主経路と呼ばれます。その他の経路はそれより低い優先順位を持ち、バックアップ経路と呼ばれます。通常、ルータは主経路を介してデータを送信します。回線が切断した際、主経路が自身の姿を消し、ルータは残りの経路から優先順位が高いものをバックアップ経路として選択し、データを送信します。このように、主経路からバックアップ経路への切り替えが実現されます。主経路が復帰した場合、ルータは主経路を復元し、経路の再選択をおこないます。主経路が最も高い優先順位を有しているので、ルータは主経路を選択し、データを送信します。バックアップ経路から主経路へのこのプロセスは自動切り替えです。

ルーティングプロトコルによる経路の共有

様々なルーティングプロトコルのアルゴリズムは異なっているため、異なるプロトコルにより異なる経路が生成され、そのため異なるルーティングプロトコルにより異なる経路が作成された場合にこの差異を解決する方法に関し問題が生じます。本機は他のルーティングプロトコルの情報を取り込むことができます。各プロトコルは自身の経路の再分配メカニズムを有しています。

5.8.3 スタティックルートの設定

スタティックルートの概要

・スタティックルートの属性と機能

スタティックルートは特別な経路です。スタティックルートの設定により、相互接続するネットワークを構築できます。ネットワークで問題が発生した際のこの設定に関する問題は、スタティックルートはネットワーク管理者の介在なくノードの問題発生を回避するよう自動的に変更ができないことです。比較的にシンプルなネットワーク構成では、必要なことは、スタティックルートを設定してルータに通常の動作をさせるだけです。スタティックルートの正しい設定と使用により、ネットワークのパフォーマンスを向上し、重要なアプリケーションの帯域幅を保証します。

・デフォルトルート

デフォルトルートはスタティックルートでもあります。デフォルトルートは、ルーティングテーブルの入力項目に適切なものがない場合、また適切な経路が見つからない場合に使用されます。ルーティングテーブルでは、デフォルトルートネットワーク 0.0.0.0（マスクは 0.0.0.0）への経路になっています。display ip routing-table コマンドの出力結果によって、どのようにデフォルトルートが設定されているか確認できます。パケットのデスティネーションアドレスがルーティングテーブルのどの入力項目にも一致しない場合、ルータはデフォルトルートを選択し、このパケットをフォワーディングします。デフォルトルートが存在せず、パケットのデスティネーションアドレスがルーティングテーブルのどの入力項目とも一致しない場合、パケットは破棄され、ICMP（Internet Control Message Protocol）パケットが送信元のホストに送付されて、宛て先のホストまたはネットワークが到達不能であったことを知らせます。デフォルトルートはネットワークにおいて非常に役立ちます。典型的なネットワークがあり、これが数百台のルータから構成されていると仮定してみます。このネットワークでは、デフォルトルートを使用せずにすべての種類のダイナミックルーティングプロトコルを使用した場合、膨大な帯域幅が消費されることでしょう。デフォルトルートを使用することは、多くのユーザがやり取りする通信について、たとえ広い帯域幅を確立できない場合でも適正な帯域幅を提供できるでしょう。

スタティックルートの設定

スタティックルートの設定には次の項目があります。

● スタティックルートの設定
● デフォルトルートの設定

・スタティックルートの設定

Global Configuration モードで次の設定をおこないます。

はじめに Privileged Exec モードに移行し、次の手順でスタティックルートを設定します。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**ip route static add** *dst-ipaddress net-mask next-hop* **[description** *string* **| usehw** *{yes|no}* **| gateway** *{yes|no}* **| mac** *mac-address* **| port** *port-number* | **vid** *vlan-id***]**	スタティックルートを設定します。
手順 3	**exit**	Privileged Exec モードに戻ります。
手順 4	**show ip route static**	入力を確認します。
手順 5	**write**	（オプション）設定ファイルに入力を保存します。

スタティックルートの削除

モード	コマンド
Grobal Configuration	**ip route static delete** *dst-ipaddress*

パラメータの説明は次のとおりです。

- **dst-ipaddress および net-mask**
  dest-ipaddress および net-mask はドットで区切られた十進数のフォーマットです。32bit のマスクの 1 は連続していることが必要で、ドットで区切られた 10 進数のマスクがマスク長（マスクの連続する 1 の桁を参照する）によって置換されます。

- **lnext-hop アドレス**
  スタティックルートを設定する場合、実際の環境に従い、ゲートウェイアドレスを指定してネクストホップのアドレスを決定できます。
  実際、すべてのルーティング項目に対してネクストホップのアドレスを設定する必要があります。IP レイヤでパケットが転送される場合、パケットのデスティネーションアドレスに従ってルーティングテーブルで一致する経路が検索されます。経路のネクストホップアドレスが設定されている場合のみ、リンクレイヤが対応するリンクレイヤのアドレスを検出し、このアドレスに従ってパケットのフォワーディングをおこないます。

・デフォルトルートの設定

Global Configuration **モードで次の設定をおこないます。**

はじめに Privileged Exec **モードに移行し、次の手順でデフォルトルートを設定します。**

	コマンド	内容
手順 1	**config terminal**	Global configuration **モードに移行します。**
手順 2	**ip route static add 0.0.0.0 0.0.0.0** *next-hop* **[description** *string* **| usehw** *{yes|no}***| gateway** *{yes|no}***|mac** *mac-address* **| port** *port-number* **| vid** *vlan-id* **]**	**デフォルトルートの設定をおこないます。**
手順 3	**exit**	Privileged Exec **モードに戻ります。**
手順 4	**show route static**	**入力を確認します。**
手順 5	**write**	**（オプション）設定ファイルに入力を保存します。**

スタティックルートの削除

モード	コマンド
Grobal Configuration	**ip route static delete 0.0.0.0**

標準的なスタティックルートの設定例

・ネットワーク要件

下図に示すように、図中のすべての IP アドレスのマスクは 255.255.255.0 です。すべてのホストまたはルーティングをおこなうスイッチが、スタティックルートを設定することにより、ペアとなり相互接続できる必要があります。

・ネットワーク構成図

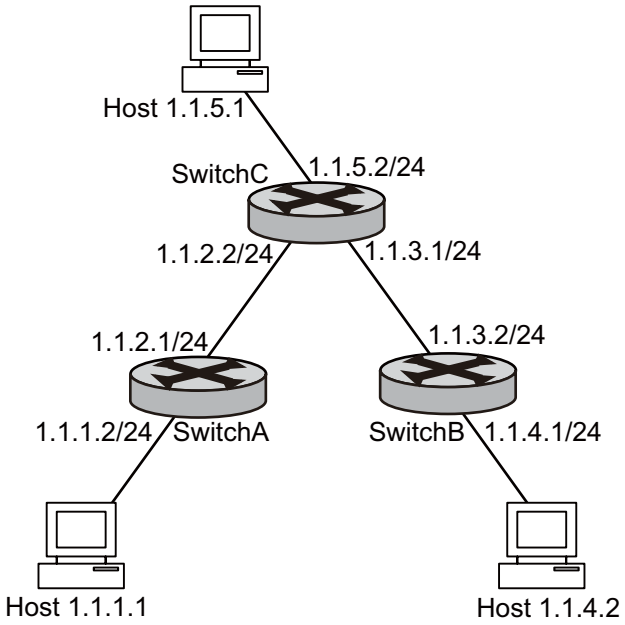


図 19　スタティックルート設定例のネットワーク構成図

スタティックルートの障害に関する診断とトラブルシューティング

障害：スイッチにダイナミックルーティングプロトコルが設定されていず、物理レイヤとリンクレイヤのインターフェースのプロトコル状態はアクティブだが、IP パケットは正常にフォワーディングできない。

トラブルシューティング：

show ip route static **コマンドを使用し、対応するスタティックルートが正しく設定されているか確認します。**

show ip route table **コマンドを使用し、対応する経路が有効か確認します。**

・設定手順

（1）Switch A の VLAN および VLAN の IP アドレスを設定します
```
switchA(config)#vlan static set vid 1 01-02-
switchA(config)#vlan static set vid 2 01u
switchA(config)#vlan static set vid 3 02u
switchA(config)#vlan port pvid 1 2
switchA(config)#vlan port pvid 2 3
switchA(config)#ip address add vint 1 1.1.1.2 255.255.255.0 vid 2
switchA(config)#ip address add vint 2 1.1.2.1 255.255.255.0 vid 3
```

（2）# Switch A のデフォルトルートを設定します。
```
switchA(config)#ip route static add 0.0.0.0 0.0.0.0 1.1.2.2
```

（3）Switch B の VLAN および VLAN の IP アドレスを設定します。
```
switchB(config)#vlan static set vid 1 01-02-
switchB(config)#vlan static set vid 2 01u
switchB(config)#vlan static set vid 3 02u
switchB(config)#vlan port pvid 1 2
switchB(config)#vlan port pvid 2 3
switchB(config)#ip address add vint 1 1.1.4.1 255.255.255.0 vid 2
switchB(config)#ip address add vint 2 1.1.3.2 255.255.255.0 vid 3
```

（4）Switch B のデフォルトルートを設定します。
```
switchB(config)#ip route static add 0.0.0.0 0.0.0.0 1.1.3.1
```

（5）Switch C の VLAN および VLAN の IP アドレスを設定します。
```
switchC(config)#vlan static set vid 1 01-02-03-
switchC(config)#vlan static set vid 2 01u
switchC(config)#vlan static set vid 3 02u
switchC(config)#vlan static set vid 4 03u
switchC(config)#vlan port pvid 1 2
switchC(config)#vlan port pvid 2 3
switchC(config)#vlan port pvid 3 4
switchC(config)#ip address add vint 1 1.1.2.2 255.255.255.0 vid 2
switchC(config)#ip address add vint 2 1.1.3.1 255.255.255.0 vid 3
switchC(config)#ip address add vint 3 1.1.5.2 255.255.255.0 vid 3
```

（6）Switch C のスタティックルートを設定します。
```
switchC(config)#ip route static add 1.1.1.0 255.255.255.0 1.1.2.1
switchC(config)#ip route static add 1.1.4.0 255.255.255.0 1.1.3.2
```

スタティックルート障害時の症状とトラブルシューティング

障害：

スイッチにダイナミックルーティングプロトコルが設定されていず、物理レイヤとリンクレイヤのインターフェースのプロトコル状態はアクティブだが、IP パケットは正常にフォワーディングできない。

トラブルシューティング：

- show ip route static **コマンドを使用し、対応するスタティックルートが正しく設定されているか確認します。**
- show ip route table **コマンドを使用し、対応する経路が有効か確認します。**

5.8.4 RIP

概要

RIP（Routing Information Protocol）は比較的シンプルなダイナミックルーティングプロトコルですが、大きなアプリケーションを含んでいます。RIP は D-V（Distance-Vector）アルゴリズムに基づくプロトコルでルーティング情報を UDP パケットを介して交換します。宛て先のホストまでの距離をホップ数（Hop Count）を使用して測定し、これをルーティングコスト（Routing Cost）と呼びます。RIP では、ルータから直接接続されているネットワークまでのホップ数は 0 で、別の 1 台のルータを介して到達可能なネットワークまでは 1 などとなります。収束時間を制限するため、RIP はこのコストの値を 0 ～ 15 の整数で規定します。16 以上のホップ数は無限大として定義され、宛て先のネットワークやホストは到達不能になります。

RIP はルーティングのリフレッシュメッセージを 30 秒ごとに送信します。ルーティングリフレッシュメッセージが 180 秒以内に近隣ネットワークから受信されない場合、RIP はこの近隣ネットワークのすべての経路を到達不能としてタグ付けします。ルーティングリフレッシュメッセージが 300 秒以内に近隣ネットワークから受信されない場合、RIP は最終的にこの近隣ネットワークの経路をルーティングテーブルから削除します。

パフォーマンスを向上させ、経路のループを回避するため、RIP はスプリットホライズンとポイズンリバースをサポートし、他のルーティングプロトコルによって発見された経路の取り込みを可能にしています。RIP を実行している各ルータはルーティングデータベースを管理し、このテーブルはネットワークの到達可能な全宛て先に対するルーティングの入力項目を保持しています。これらのルーティング入力項目は次の情報を含んでいます。

- デスティネーションアドレス：ホストまたはネットワークの IP アドレス
- ネクストホップアドレス：宛て先に到達するため、IP パケットが渡される次のルータのアドレス
- 送信用インターフェース：IP パケットをフォワーディングするインターフェース
- コスト：宛て先に到達するためのルータのコストで 0 ～ 16 の整数
- タイマ：ルーティングの入力項目が前回変更されてから現在までの時間 タイマはルーティングの入力項目が変更されたとき 0 にリセットされます。
- 経路タグ 内部、外部、どちらのルーティングプロトコルで生成された経路かを識別します。

RIP の起動から実行までの全体のプロセスは次のように説明できます。

（1）ルータで RIP が初めて有効になると、ルータはリクエストパケットを隣接ルータにブロードキャストまたはマルチキャストします。リクエストパケットを受信すると、隣接ルータ（このルータ上で RIP がすでに有効に設定されている）は、自身のローカルのルーティングテーブル情報を含むレスポンスパケットを返すことにより、このリクエストに応答します。

（2）レスポンスパケットを受信すると、リクエストを送信したルータは自身のルーティングテーブルを変更します。

（3）同時に、RIP は自身のルーティングテーブルを隣接ルータに 30 秒ごとにブロードキャストします。隣接ルータはパケットを受信したあと自身のルーティングテーブルを維持し、最適なルートを選択し、この変更情報をそれぞれの隣接ネットワークに広告して、更新された経路情報をグローバルに知らせます。さらに、RIP はタイムアウトメカニズムを使用して期限切れの経路を処理し、経路のリアルタイム性と有効性を確保します。これらのメカニズムを使用し、内部ルーティングプロトコルである RIP はルータがネットワーク全体のルーティング情報を学習することを可能にします。

RIP は、ルータおよびホストの経路情報を転送する方法として、圧倒的な実標準のひとつとなってきました。シンプルで広域の、ほとんどのキャンパスネットワークと地域ネットワークで使用できます。それより広く複雑なネットワークでは、RIP は推奨されません。

RIP の設定

RIP の設定には次の項目があります。

- RIP インターフェースを有効に設定
- インターフェースの RIP バージョンを設定
- RIP パケットの認証を設定
- 追加のルーティングメトリックを設定
- RIP プロトコルの有効 / 無効を設定

RIP インターフェースを有効に設定

RIP の動作を柔軟に制御するために、RIP ネットワークに配置するインターフェースとネットワークの設定ができ、インターフェースが RIP パケットの送受信ができます。

はじめに Privileged Exec モードに移行し、次の手順で RIP のインターフェースを有効にします。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**router rip network** *network-address*	指定したネットワークの RIP を有効に設定します。
手順 3	**exit**	Privileged Exec モードに戻ります。
手順 4	**show router rip config**	入力を確認します。
手順 5	**write**	（オプション）設定ファイルに入力を保存します。

特定のネットワークで RIP を無効に設定

モード	コマンド
Grobal Configuration	**router rip no network** *network-address*

インターフェースの RIP バージョンを設定

RIP には RIP-1 および RIP-2 の 2 つのバージョンがあります。インターフェースで処理される RIP パケットのバージョンを設定できます。

RIP-1 はパケットのブロードキャストをおこないます。RIP-2 はブロードキャストとマルチキャストの両方でパケットを転送できます。初期設定では、パケットの転送にマルチキャストが適用されています。RIP-2 では、マルチキャストアドレスは 224.0.0.9 です。マルチキャストモードでパケットの転送をおこなう上での利点は、同一ネットワーク上の RIP を使用していないホストが RIP のブロードキャストパケットの受信を拒否できることです。さらに、このモードは RIP-1 を実行しているホストに、RIP-2 のサブネットマスクで経路を不正に受信および処理させないことも可能です。インターフェースが RIP-2 のブロードキャストモードを実行している場合、RIP-1 パケットも受信できます。

はじめに Privileged Exec モードに移行し、次の手順でインターフェースの RIP のバージョンを設定します。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**router rip entry** *interface-id* **recvtype [rip1 | rip2 |rip1Orrip2 | doNotReceive]**	指定したインターフェースの受信時のメッセージの種類を設定します。
手順 3	**router rip entry** *interface-id* **sendtype [ripVersion1 | ripVersion2 | ripV1Demand | ripV2Demand | rip1Compatible | doNotSend]**	指定したインターフェースの送信時のメッセージの種類を設定します。
手順 4	**exit**	Privileged Exec モードに戻ります。
手順 5	**show router rip config**	入力を確認します。
手順 6	**write**	（オプション）設定ファイルに入力を保存します。

RIP-2 パケット認証を設定

RIP-1 はパケットの認証をサポートしていません。しかし、RIP-2 を実行するインターフェースの場合、パケットの認証を設定できます。

RIP-2 は次の 2 つの認証モードをサポートしています。単純な認証方法と MD5 認証です。MD5 認証では 2 つのパケットフォーマットを使用します。1 つは RFC2453 に準拠したもので、もう 1 つは RFC2082 に準拠したものです。

単純な認証方法ではセキュリティは保証されません。暗号化されない認証キーがパケットと一緒に送信されるため、単純な認証方法は高いセキュリティを必要とするケースでは適用できません。

はじめに Privileged Exec モードに移行し、次の手順で RIP-2 のパケット認証を設定します。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**router rip entry** *interface-id* **authtype [md5 | simplePass | noAuth]**	認証の種類を設定します。
手順 3	**router rip entry** *interface-id* **password** *string*	認証用パスワードを設定します。
手順 4	**exit**	Privileged Exec モードに戻ります。
手順 5	**show router rip config**	入力を確認します。
手順 6	**write**	（オプション）設定ファイルに入力を保存します。

標準のパケットフォーマットは RFC2453 に、非標準のフォーマットは RFC2082 に準拠しています。

追加のルーティングメトリックを設定

追加のルーティングメトリックは RIP の経路に追加される受信または送信のルーティングメトリックです。これは経路のメトリック値を変更するものではなく、インターフェースが経路を受信または送信する際、特定のメトリック値を追加するものです。

はじめに Privileged Exec モードに移行し、次の手順で追加のルーティングメトリックを設定します。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**router rip entry** *interface-id* **metric** *vlaue*	追加のルーティングメトリックを設定します。 初期設定：RIP がパケットを送信した際に経路に追加されるルーティングメトリックは 1。RIP がパケットを受信した際の追加のルーティングメトリックは 0
手順 3	**exit**	Privileged Exec モードに戻ります。
手順 4	**show router rip config**	入力を確認します。
手順 5	**write**	（オプション）設定ファイルに入力を保存します。

RIP プロトコルの有効 / 無効を設定

はじめに Privileged Exec モードに移行し、次の手順で RIP プロトコルを有効にします。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**router rip enable**	RIP プロトコルを有効に設定します。 初期設定では、RIP プロトコルは無効です。
手順 3	**exit**	Privileged Exec モードに戻ります。
手順 4	**show router rip config**	入力を確認します。
手順 5	**write**	（オプション）設定ファイルに入力を保存します。

RIP を無効に設定

モード	コマンド
Grobal Configuration	**router rip**

標準的な RIP の設定例

ネットワーク要件

次の図に示すように、ルーティング Switch C がイーサネットポートでサブネット 117.102.0.0 に接続しています。ルーティング Switch A および Switch B のイーサネットポートはそれぞれネットワーク 155.10.1.0 および 196.38.165.0 に接続しています。Switch C、Switch A および Switch B はイーサネット 110.11.2.0 を介して接続しています。正しく設定された RIP によって、Switch C、Switch A、および Switch B が相互接続できることを保証します。

ネットワーク構成図

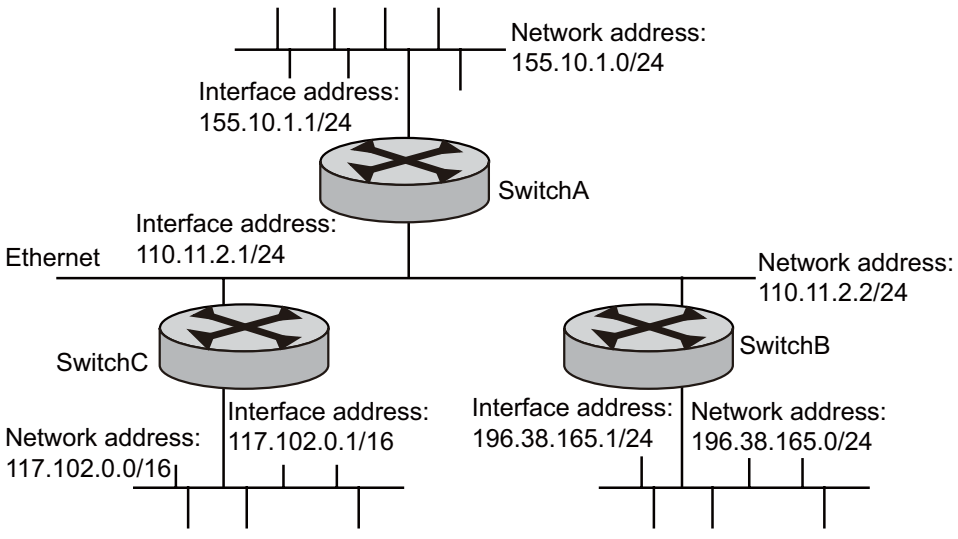


図 20　RIP を設定したネットワーク

設定手順

[注意] 次の設定では、RIP に関連する手順のみを示しています。次の設定をおこなう前に、イーサネットのリンクレイヤが正しく稼動していることを確認してください。

スイッチ A **の設定**

```
switchA(config)#router rip network 110.11.2.0
switchA(config)#router rip network 155.10.1.0
switchA(config)#router rip enable
```

スイッチ B **の設定**

```
switchB(config)#router rip network 110.11.2.0
switchB(config)#router rip network 196.38.165.0
switchB(config)#router rip enable
```

スイッチ C **の設定**

```
switchC(config)#router rip network 110.11.2.0
switchC(config)#router rip network 117.102.0.0
switchC(config)#router rip enable
```

5.8.5 OSPF

OSPF の概要

OSPF について

OSPF（Open Shortest Path First）は、IETF によって開発されたリンク状態に基づいた IGP（Interior Gateway Protocol）です。現時点では、OSPF バージョン 2（RFC2328）が使用され、これによって次のような機能が可能です。

- 適用範囲：様々な規模のネットワークをサポートしており、最大数百のルータに対応できます。
- 高速な収束：変更情報が AS 内で同期されるよう、ネットワークトポロジ変更後瞬時に更新パケットを転送できます。
- ループが発生しない：OSPF は収集したリンク状態に従い、最短パスツリーアルゴリズムによって経路を算出するため、アルゴリズム自体が経路のループを発生させません。
- エリアの分割：管理を簡単におこなうために AS のネットワークを異なるエリアに分割でき、これによりエリア間で転送される経路情報がさらに抜粋され、その結果ネットワーク帯域幅の消費を抑えます。
- 同じコストの複数経路：デスティネーションまで、同数コストの経路を複数サポートしています。
- 階層的な経路選択：OSPF は 4 レベルで経路を階層化します。OSPF では、経路は intra-area、inter-area、external type-1、external type-2 で優先順位付けされます。
- 認証：インターフェースベースのパケット認証をサポートしているため、経路を算出する場合のセキュリティが保証されます。
- マルチキャストによる転送：パケットの送受信において、マルチキャストアドレスをサポートしています。

OSPF による経路算出プロセス

OSPF プロトコルは、次のプロセスで経路の算出をおこないます。

- OSPF での処理が可能なルータは、AS 全体のトポロジを記述している LSDB（Link State Database）を維持します。自身のネットワークトポロジにしたがい、各ルータは LSA（Link State Advertisement）を生成します。ネットワーク上に配置されているルータは、互いにプロトコルパケットを転送しながら LSA を転送します。このように、各ルータは他のルータの LSA を受信し、これらすべての LSA によって LSDB が構成されます。
- LSA はルータのネットワークトポロジを記述し、LSDB はネットワーク全体のネットワークトポロジを記述します。ルータは簡単に LSDB を補正された有向グラフに変換し、これがネットワーク全体のトポロジアーキテクチャに実際に反映されます。もちろん、すべてのルータが寸分違わぬグラフを取得できます。
- ルータは SPF アルゴリズムで自身をルートとして最短パスのツリーを算出し、これによって自律システムのノードへの経路を示します。外部の経路情報は対象外のノードになります。ルータ情報を広告するルータは、情報にタグ付けし、自律システムの追加情報を記録します。もちろん、異なるルータによって取得されたルーティングテーブルは、異なります。

さらに、ブロードキャストネットワークでルーティングをおこなう機器の介在なしに、直接接続しているルータについて想定してみます。個々のルータが、AS 全体に対して、それぞれのローカルステータス情報をブロードキャストできるようにするには、その環境下の 2 台のルータが相互に隣接性を確立しなくてはなりません。しかし、この場合、ルータが被る変化によって、必ずしも必要ではなく、しかも貴重な帯域幅のリソースを無駄にする複数の転送が発生します。この問題を解決するために、「DR（Designated Router）」が OSPF で定義されます。そして、すべてのルータが DR にのみ、ネットワークにおけるネットワークリンクステータス情報のブロードキャストを送信します。このように、多重アクセスネットワークでのルータの近接関係は削減されます。OSPF はインターフェースベースのパケットの認証機能をサポートしており、経路の算出におけるセキュリティを保証します。また、IP マルチキャストによるパケットの送受信もおこないます。

OSPF パケット

OSPF は次の 5 種類のパケットを使用します。

- ハローパケット：
  ルータから近接ルータに定期的に送信される、最も一般的なパケットです。いくつかのタイマ、DR、BDR、および既知の近隣情報の値が含まれます。

- DD（Database Description）パケット：
  2 台のルータがデータベースを同期させる場合、DD パケットを使用して各 LSA のダイジェストを含む自身の LSDB を記述します。ダイジェストは、LSA を一意的に識別するのに使用される、LSA の HEAD を参照します。LSA トラフィック全体に対し、LSA の HEAD のみがこのほんの一部のみを占有するため、このような、ルータ間を転送されるトラフィックサイズの削減が可能です。HEAD によって、接続相手のルータがすでに LSA を有しているかどうかを判定できます。

- LSR（Link State Request）パケット：
  DD パケットを交換すると、この 2 台のルータは通信先のルータのどの LSA が自分の LSDB で欠如しているかを知ります。この場合、通信相手に対し、必要な LSA リクエストパケットを送信します。パケットは必要な LSA のダイジェストを含みます。

- LSU（Link State Update）パケット：
  パケットは通信相手に対し、必要な LSA の転送に使用されます。複数の LSA（コンテンツ一式）のコレクションを含みます。

- LSAck（Link State Acknowledgment）パケット：
  パケットは、受信した LSU パケットの確認応答に使用されます。ここには、LSA リクエストの確認応答の HEAD を含みます。

OSPF に関連する基本概念

- **ルータ** ID
  OSPF を実行するには、ルータはルータ ID を持つ必要があります。ルータ ID を設定しない場合、システムは自動的にその時点の IP アドレスをルータ ID として選択します。次の方法でルータ ID を選択します。ループバックインターフェースアドレスが存在する場合、システムはループバックアドレスと最も大きな IP アドレスの値をルータ ID として選択します。ループバックインターフェースが存在しない場合、物理インターフェースのアドレスと最も大きな IP アドレスの値がルータ ID になります。

- DR
  マルチアクセスのネットワークでは、2 台のルータが近接している場合、同じ LSA が繰り返し転送され、帯域のリソースが無駄になります。この問題を解決するために、OSPF プロトコルでは、マルチアクセスネットワークで DR が選定されなくてはならないことと、DR（および以下に記載する BDR）のみがそのネットワーク内で他のルータと近接関係を結べることを定めています。2 台の非 DR ルータ /BDR ルータは近接関係になれず、ルーティング情報を交換できません。どのルータがセグメント内で DR になれるのかは手入力では設定できません。その代わり、DR がセグメント内の他のすべてのルータによって選定されます。

- BDR
  DR が何らかの障害で不具合になると、新たな DR が選定され、同一セグメント内の他のルータと同期を取らなくてはなりません。このプロセスは比較的長時間かるため、この間に経路の算出結果に誤りが生じることになります。このプロセスを短縮化するため、OSPF に BDR が提案されました。実際、BDR は DR のバックアップをおこないます。DR と BDR が一時的に選定されます。BDR と同一セグメント上の他のすべてのルータとの間にも近接関係が確立され、経路情報が両者間でも交換されます。既存の DR が障害を発生すると、即時に BDR が DR になります。

- **エリア**
  ネットワークの規模がますます拡大しています。巨大なネットワークのすべてのルータが OSPF を実行している場合、非常に多くのルータが巨大な LSDB を構築することになり、この結果巨大な保存空間の消費、SPF アルゴリズムの複雑化から CPU の負荷が増大します。さらに、ネットワークがより拡大すると、トポロジの変更が発生することになりがちです。したがって、ネットワークは常に「混乱」状態になり、かなり多くの OSPF パケットが生成され、ネットワークへ転送されます。これはネットワークの帯域幅の有効性を下げてしまいます。さらに、それぞれの変更がこのネットワーク上のすべてのルータに発生し、経路の再算出が発生することになります。
  OSPF では 1 つの AS を異なるエリアに分割することによって、上記の問題を解決しています。エリアは論理的にルータをグループ化します。エリアの境界はルータによって形成されます。そのため、いくつかのルータは複数のエリアに所属することになります。ルータがバックボーンエリアに接続し、非バックボーンエリアは ABR（Area Border Router）と呼ばれます。ABR はバックボーンエリアに物理的または論理的に接続できます。

- バックボーンエリアと仮想リンク

  バックボーンエリア
  OSPF のエリアの分割が終わると、すべてのエリアが等しくはなくなります。この中で、あるエリアはすべての他のエリアと異なることになります。このエリア ID は 0 で、これがバックボーンエリアと呼ばれます。

  仮想リンク
  すべてのエリアがバックボーンエリアと接続するため、仮想リンクが採用され、物理的に分割されたエリアがバックボーンエリアへの論理的な接続を維持できるようにしています。

- ルート集約
  AS が、OSPF ABR で相互接続する異なるエリアに分割されています。エリア間の経路情報はルート集約を介して削減できます。したがって、ルーティングテーブルの数は削減でき、ルータの算出速度は向上されます。エリアのエリア間経路が算出されると、ABR は複数の OSPF 経路を 1 つの LSA に集約し、集約設定情報に従ってエリア外にこの LSA を送信します。

OSPF の設定

多種の設定のなかでも、最初に OSPF を有効にし、インターフェースとエリア ID を設定して、その後その他の機能を設定します。しかし、インターフェース関連機能は OSPF を有効にするしないにかかわらず限定されません。OSPF を無効に設定した場合、その後は OSPF に関連するインターフェースのパラメータもまた無効になることにも注意してください。

OSPF の設定には次の項目があります。

- OSPF Configuration モードへの移行
- OSPF プロセスの有効化
- インターフェースの設定
- インターフェースへパケットを送信するためのコストの設定
- DR 選定のためのインターフェースプライオリティの設定
- ハローパケット転送間隔の設定
- 近接ルータに対するデッドタイマの設定
- LSU パケットの送信間隔要件の設定
- 近接ルータ間の LSA 再転送間隔の設定
- OSPF の SPF（Shortest Path First）算出間隔の設定
- OSPF の STUB エリアの設定
- OSPF エリアのルート集約設定
- OSPF 仮想リンクの設定
- OSPF パケット認証の設定
- OSPF パケット送信のためのインターフェース無効化
- OSPF 経路再配布

OSPF Configuration モードへの移行

はじめに Privileged Exec **モードに移行し、次の手順で** OSPF Configuration **モードに移行します。**

	コマンド	内容
手順 1	**config terminal**	Global configuration **モードに移行します。**
手順 2	**router ospf**	OSPF configuration **モードに移行します。**

OSPF プロセスの有効化

はじめに OSPF Configuration **モードに移行し、次の手順で** OSPF **プロセスを有効にします。**

	コマンド	内容
手順 1	**service enable**	OSPF **プロセスを有効に設定します。初期設定では、** OSPF **は有効に設定されていません。**
手順 2	**exit**	Global configuration **モードに戻ります。**
手順 3	**exit**	Privileged Exec **モードに移行します。**
手順 4	**show ip ospf**	**入力を確認します。**
手順 5	**write**	**（オプション）設定ファイルに入力を保存します。**

OSPF プロセスを無効に設定

モード	コマンド
OSPF Configuration	**service disable**

インターフェースの設定

OSPF は先で AS を異なるエリアに分割します。エリアは論理的にルータをグループ化します。いくつかのルータは異なるエリアに所属します（このようなルータを ABR と言います）が、1 つのセグメントは 1 つのエリアのみに所属できます。言い換えると、各 OSPF インターフェースをエリア ID で識別される特定のエリアに所属させるように設定する必要があります。このエリアは経路情報を ABR を介してエリア間で転送します。

さらに、同一エリアに所属するすべてのルータのパラメータは同じでなくてはなりません。したがって、同一エリアのルータを設定する際は、ほとんどの設定は所属するエリアに基づくことに注意してください。設定を誤ると、近接ルータがルータ間で情報を転送することができなくなり、ルーティング情報の輻輳やセルフループを引き起こすことにまで至ります。

はじめに OSPF Configuration モードに移行し、次の手順でインターフェースを設定します。

	コマンド	内容
手順 1	**network** *ip-address ip-mask* **area** *area-id*	OSPF を実行するためにインターフェース設定をします。
手順 2	**exit**	Global configuration モードに戻ります。
手順 3	**exit**	Privileged Exec モードに移行します。
手順 4	**show ip ospf**	入力を確認します。
手順 5	**write**	（オプション）設定ファイルに入力を保存します。

設定したネットワークを無効に設定

モード	コマンド
OSPF Configuration	**no network** *ip-address ip-mask* **area** *area-id*

[注意] OSPF を有効に設定したあと、OSPF を適用するセグメントの設定が必要です。

インターフェースへパケットを送信するためのコスト設定

異なるメッセージ送信コストを異なるインターフェースに設定することによって、ユーザ側でのネットワークトラフィックの制御が可能です。この設定をおこなわない場合、現時点のインターフェースの通信速度に基づき、OSPF は自動的にコストを算出します。

はじめに Privileged Exec モードに移行し、次の手順でインターフェースへのパケット送信のための設定をおこないます。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**Interface vint** *interface-id*	Interface configuration モードに移行します。
手順 3	**ip ospf cost** *value*	インターフェースパケットを送信するための コストを設定します。 初期設定：インターフェースは自動的に通信速度に基づきコストを算出します。計算式は次のとおりです。 100 Mbps/ インターフェースの現時点での通信速度
手順 4	**exit**	Global configuration モードに戻ります。
手順 5	**exit**	Privileged Exec モードに戻ります。
手順 6	**show ip ospf interface [vint** *interface-id* **]**	入力を確認します。
手順 7	**write**	（オプション）設定ファイルに入力を保存します。

インターフェースへパケットを送信するためのコストを初期設定の内容に復帰

モード	コマンド
OSPF Configuration	**no ip ospf cost**

DR 選定のためのインターフェースプライオリティの設定

ルータインターフェースのプライオリティは DR 選定時のインターフェースの品質を決定し、選定時に輻輳が発生した場合、高いプライオリティのルータは最初に考慮されます。

DR は手入力による定義はできず、セグメントのすべてのルータによって選定されます。
ネットワークのプライオリティ > 0 のルータは、有資格「候補者」になります。
DR になることを自己宣言したすべてのルータの中から、最も高いプライオリティを有するルータが選定されます。
2 台のルータが同じプライオリティを有する場合、ルータ ID がより高いほうが DR に選定されます。投票はハローパケットでおこないます。
各ルータがパケットに期待する DR を記述し、セグメントの他のすべてのルータに送信します。同一セグメントに接続する 2 台のルータが同時に DR になりたいと宣言した場合、より高いプライオリティを有するほうが選定されます。
プライオリティが同じ場合、ルータ ID の大きいほうが選定されます。ルータのプライオリティが 0 の場合、DR または BDR には選定されません。
DR が何らかの理由で障害に陥ると、そのネットワークのルータは新たな DR を選定し、この新たな DR と同期しなくてはなりません。このプロセスは比較的長時間に渡り、この間、経路の算出は正しくはありません。このプロセスを高速化するため、OSPF は BDR の概念を提唱しました。実際、BDR は DR のバックアップをおこないます。DR と BDR が一時的に選定されます。BDR と同一セグメント上の他のすべてのルータとの間にも近接関係が確立され、経路情報が両者間でも交換されます。DR が障害に陥ると、BDR が即時に DR になります。再選定は必要でなく、近接関係がすでに確立されているので、プロセスにかかる時間は非常に短くなります。しかしこの場合、あらたな BDR が選定されなくてはなりません。これにも非常に長い時間がかかりますが、経路の算出に影響を与えることはありません。しかし、次の各点に注意してください。

- ネットワークの DR は必ずしも最高のプライオリティを有するルータではありません。同様に、BDR は必ずしも第 2 のプライオリティを有するルータではありません。DR または BDR の選定後、新たなルータが追加された場合、最高のプライオリティを有していた場合でもこのルータが DR になることは不可能です。

- DR は特定のセグメントにあるルータインターフェースに基づくものです。あるルータは特定のインターフェースの DR の可能性がありますが、別のインターフェースの BDR または DR になりうる可能性があります。

はじめに Privileged Exec モードに移行し、次の手順で DR 選定のためのインターフェースプライオリティの設定をおこないます。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**Interface vint** *interface-id*	Interface configuration モードに移行します。
手順 3	**ip ospf priority** *priority_num*	DR 選定のため、インターフェースにプライオリティを設定します。（範囲：0 ～ 255） 初期設定：1
手順 4	**exit**	Global configuration モードに戻ります。
手順 5	**exit**	Privileged Exec モードに戻ります。
手順 6	**show ip ospf interface [vint** *interface-id* **]**	入力を確認します。
手順 7	**write**	（オプション）設定ファイルに入力を保存します。

初期設定のインターフェースプライオリティへ復帰

モード	コマンド
Interface Configuration	**no ip ospf priority**

ハローパケット転送間隔の設定

ハローパケットは最も頻繁に使用されるパケットの種類で、近接関係の探索と維持のため、また、DR および BDR の選定のために、近接ルータに定期的に送信されます。ハロータイマの設定はユーザがおこなうことができます。

RFC2328 によると、ネットワークの近接同士がハローパケットの送信間隔が一定であることが維持されなくてはなりません。ハローパケットの間隔の値は、経路の輻輳率とネットワーク負荷に対し反比例になります。

はじめに Privileged Exec モードに移行し、次の手順でハローパケットとの転送間隔を設定します。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**Interface vint** *interface-id*	Interface configuration モードに移行します。
手順 3	**ip ospf hello-interval** *seconds*	そのインターフェースのハローパケットの送信間隔を設定します。 初期設定：ハローパケットを 10 秒間隔で送信します。
手順 4	**exit**	Global configuration モードに戻ります。
手順 5	**exit**	Privileged Exec モードに戻ります。
手順 6	**show ip ospf interface [vint** *interface-id* **]**	入力を確認します。
手順 7	**write**	（オプション）設定ファイルに入力を保存します。

初期設定のハローパケット送信間隔に復帰

モード	コマンド
Interface Configuration	**no ip ospf hello-interval**

近接ルータ間の LSA 再転送間隔の設定

近接ルータのデッドタイマは、近接ルータからハローパケットを受信しない場合にルータがその近接ルータがダウンしたとみなす間隔です。近接ルータのデッドタイマは、ユーザが設定をおこなえます。

はじめに Privileged Exec モードに移行し、次の手順で近接ルータのためのデッドタイマの設定をおこないます。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**Interface vint** *interface-id*	Interface configuration モードに移行します。
手順 3	**ip ospf dead-interval** *seconds*	近接ルータに対するデッドタイマの設定をおこないます。　初期設定：40 秒
手順 4	**exit**	Global configuration モードに戻ります。
手順 5	**exit**	Privileged Exec モードに戻ります。
手順 6	**show ip ospf interface [vint** *interface-id* **]**	入力を確認します。
手順 7	**write**	（オプション）設定ファイルに入力を保存します。

初期設定の近接ルータのデッドタイマへ復帰

モード	コマンド
Interface Configuration	**no ip ospf dead-interval**

LSU パケット送信間隔要件の設定

LSU パケットの LSA のエージングタイムに、転送遅延の秒数を設定する必要があります。このようにこのパラメータを設定することにより、パケットを転送するためにインターフェースが必要とする持続時間が主に考慮されます。

LSU メッセージの送信間隔は、ユーザが設定をおこなうことができます。あきらかに、低速のネットワークでは、この項目により注意を払うことが必要です。

はじめに Privileged Exec モードに移行し、次の手順で LSU パケット送信間隔要件の設定をおこないます。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**Interface vint** *interface-id*	Interface configuration モードに移行します。
手順 3	**ip ospf transmit-delay** *seconds*	LSU パケット送信間隔を設定します。 初期設定：1 秒
手順 4	**exit**	Global configuration モードに戻ります。
手順 5	**exit**	Privileged Exec モードに戻ります。
手順 6	**show ip ospf interface [vint** *interface-id* **]**	入力を確認します。
手順 7	**write**	（オプション）設定ファイルに入力を保存します。

初期設定の LSU パケット送信間隔へ復帰

モード	コマンド
Interface Configuration	no ip ospf transmit-delay

近接ルータ間の LSA 転送間隔の設定

ルータが LSA（Link State Advertisements）を通信相手に転送した場合、相手からの確認応答パケットを必要とします。再転送では確認応答パケットは受信せず、LSA を近接に再転送します。再転送の値はユーザ側で設定できます。

はじめに Privileged Exec モードに移行し、次の手順で近接ルータ間での LSA 再送信間隔の設定をおこないます。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**Interface vint** *interface-id*	Interface configuration モードに移行します。
手順 3	**ip ospf retransmit-interval** *seconds*	近接ルータに対する LSA 再送信間隔の設定をおこないます。　初期設定：5 秒
手順 4	**exit**	Global configuration モードに戻ります。
手順 5	**exit**	Privileged Exec モードに戻ります。
手順 6	**show ip ospf interface [vint** *interface-id* **]**	入力を確認します。
手順 7	**write**	（オプション）設定ファイルに入力を保存します。

近接ルータに対する LSA 再送信間隔を初期設定に復帰

モード	コマンド
Interface Configuration	**no ip ospf retransmit-interval**

[注意]　間隔の値は、2 台のルータ間でパケットが転送され、戻ってくる時間よりも大きくなくてはなりません。LSA 再転送間隔を短くしすぎないよう設定することに注意してください。短くしすぎると、不要な再転送が発生します。

OSPF の SPF（Shortest Path First）算出間隔の設定

OSPF の LSDB が変更すると、そのたびに最短パスの再算出が必要になります。変更にともなう最短パスの算出は多大なリソースを消費するとともに、ルータの効率的な動作に悪影響を与えます。しかし、SPF 算出間隔を調整すると、頻繁なネットワーク変更に伴うリソースの消費を抑えることができます。

はじめに OSPF Configuration モードに移行し、次の手順で OSPF の SPF（Shortest Path First）算出間隔の設定をおこないます。

	コマンド	内容
手順 1	**timers spf** *delay-seconds hold-seconds*	SPF の再算出間隔を設定します。 初期設定：5 秒
手順 2	**exit**	Global configuration モードに戻ります。
手順 3	**exit**	Privileged Exec モードに戻ります。
手順 4	**show ip ospf**	入力を確認します。
手順 5	**write**	（オプション）設定ファイルに入力を保存します。

SPF 算出間隔を復帰

モード	コマンド
Interface Configuration	**no timers spf**

OSPF の STUB エリアの設定

STUB エリアはある特別の LSA エリアで、このエリア内では ABR は学習した AS の外部ルータ情報を伝播しません。このエリアでは、ルータのルーティングテーブルサイズとルーティングトラフィックは大幅に削減されます。

STUB エリアはオプションで設定する属性ですが、すべてのエリアがこの設定状況に一致するわけではありません。通常、AS 境界に配置される STUB エリアは、1 つの ABR だけを有する非バックボーンエリアです。たとえこのエリアが ABR を複数有している場合でも、ABR 間で仮想リンクは確立されません。

ルータが AS 外のデスティネーションに対して到達可能な状態を確実なものにするには、このエリアの ABR がデフォルトルート（0.0.0.0）を生成し、このエリアの非 ABR ルータにこれを広告します。

STUB エリアを設定する際は、次の項目に注意してください。

- バックボーンエリアは STUB エリアに設定できず、仮想リンクは STUB エリアを介して転送できません。
- エリアを STUB エリアに設定する場合、このエリアのすべてのルータにこの属性を設定しなくてはなりません。
- ASBR は STUB エリアには存在できません。言い換えると、AS の外部ルータは STUB エリアで伝播されません。

はじめに OSPF Configuration モードに移行し、次の手順で OSPF の STUB エリアの設定をおこないます。

	コマンド	内容
手順 1	**area** *area-id* **stub [CR|no-summary]**	エリアを STUB エリアに設定します。
手順 2	**area** *area-id* **default-cost** *value*	OSPF で STUB エリアに転送されるデフォルトルートのコストを設定します。 初期設定：STUB エリアは設定されていず、STUB エリアへのデフォルトルートのコストは 1 です。
手順 3	**exit**	Global configuration モードに戻ります。
手順 4	**exit**	Privileged Exec モードに戻ります。
手順 5	**show ip ospf**	入力を確認します。
手順 6	**write**	（オプション）設定ファイルに入力を保存します。

設定済みの STUB エリアを削除

モード	コマンド
OSPF Configuration	**no area** *area-id* **stub [CR|no-summary]**

STUB エリアへのデフォルトルートのコストを削除

モード	コマンド
OSPF Configuration	**no area** *area-id* **default-cost value**

OSPF エリアのルート集約設定

ルート集約では ABR が同じ接頭辞の経路情報を集約でき、他のエリアの唯一の経路に広告できます。エリアは複数の集約セグメントを設定できるため、OSPF はこれらを集約できます。ABR が他のエリアへ経路情報を転送する際、ネットワークごとに Sum_net_Lsa （type-3 LSA）を生成します。このエリアでいくつかの継続的なネットワークが存在する場合、abr-summary コマンドを使用し、これらのセグメントを 1 つのセグメントに集約できます。したがって、ABR のみが集約した LSA を送信する必要があり、このコマンドによって設定される集約セグメントの範囲にあるすべての LSA は別々に転送されません。

特定のネットワークの集約セグメントがエリアに追加されると、集約セグメントの範囲にあるこの IP アドレスのすべての内部経路は、もはや他のエリアへ別々に広告をおこないません。集約ネットワーク全体のルート集約のみが広告されます。しかし、セグメントの範囲がキーワード「広告しない」によって制限されると、このセグメントのルート集約は広告されません。このセグメントは IP アドレスとマスクで表現されます。ルート集約は ABR にこれが設定されている場合にのみ有効になります。

はじめに OSPF Configuration モードに移行し、次の手順で OSPF エリアのルート集約の設定をおこないます。

	コマンド	内容
手順 1	**summary-address** *ip-address mask* **[CR|not-advertise|tag** *value***]**	OSPF エリアのルート集約の設定をおこないます。 初期設定：エリア内の経路は集約されません。
手順 2	**exit**	Global configuration モードに戻ります。
手順 3	**exit**	Privileged Exec モードに戻ります。
手順 4	**show ip ospf**	入力を確認します。
手順 5	**write**	（オプション）設定ファイルに入力を保存します。

OSPF エリアのルート集約を解除

モード	コマンド
OSPF Configuration	**no summary-address** *ip-address mask*

OSPF 仮想リンクの設定

RFC2328 によると、OSPF のエリアの分割が終わると、すべてのエリアが等しくはなくなります。この中で、あるエリアはすべての他のエリアと異なることになります。このエリア ID は 0.0.0.0 で、これがバックボーンエリアと呼ばれます。非バックボーンエリア間の OSPF ルータはバックボーンエリアの助けを得て更新されます。OSPF では、すべての非バックボーンエリアはバックボーンエリアとの接続性を維持しなくてはならないと規定しています。つまり、ABR のインターフェースの少なくとも 1 つはエリア 0.0.0.0 に含まれなくてはなりません。エリアがバックボーンエリア 0.0.0.0 と直接の物理的なリンクを取れない場合、仮想リンクが作成されます。

ネットワークトポロジの制限により、物理的な接続が確保されない場合、仮想リンクがこの要件を満たすことになります。仮想リンクは、2 つの ABR 間の非バックボーン内部経路のエリアを介してセットアップされる論理チャネルを参照します。論理チャネルの両端は ABR でなくてはならず、この両端が設定されている場合にのみ接続が有効になります。仮想リン

クはリモートルータの ID によって識別されます。仮想リンクの両端に非バックボーンエリアの内部経路を提供するエリアをトランジットエリアと呼びます。トランジットエリアの ID は設定をおこなう際に指定しなくてはなりません。

トランジットエリアを介して渡された経路が算出されたあと、仮想リンクが有効になり、これは 2 つの終端を結ぶポイントツーポイント接続と等価です。したがって、物理インターフェース同様、このリンクにハロータイマのような、様々なインターフェースパラメータを設定することもできます。

「論理チャネル」は、2 つの ABR 間で OSPF を実行している複数のルータがパケットフォワーディングの役割を担うことを意味します（このプロトコルパケットのデスティネーションアドレスはこれらのルータではなく、これらのルータにはこのパケットは透過的であるため、ルータが通常の IP パケットとしてこれらをフォワーディングします）。経路情報は直接この 2 つの ABR 間で転送されます。したがって経路情報は ABR によって生成される type-3 LSA を参照し、このためこのエリアに所属するルータの同期モードが変更されます。

はじめに OSPF Configuration モードに移行し、次の手順で OSPF 仮想リンクの設定をおこないます。

	コマンド	内容
手順 1	**area** *area-id* **virtual-link** *router-id* **[CR | hello-interval** *seconds* **| retransmit-interval** *seconds* **| transmit-delay** *seconds* **| dead-interval** *seconds* **| authentication-simple** *password* **| authentication-md5** *keyid key*]	仮想リンクの作成と設定をおこないます。 初期設定：ハロータイマ 10 秒、再転送 5 秒、 転送遅延は 1 秒、デッドタイマ 40 秒 （area-id および router-id には初期値はありません。）
手順 2	**exit**	Global configuration モードに戻ります。
手順 3	**exit**	Privileged Exec モードに戻ります。
手順 4	**show ip ospf**	入力を確認します。
手順 5	**write**	（オプション）設定ファイルに入力を保存します。

既存の仮想リンクを削除

モード	コマンド
OSPF Configuration	**no area** *area-id* **virtual-link** *router-id* **[CR | hello-interval** *seconds* **| retransmit-interval** *seconds* **| transmit-delay** *seconds* **| dead-interval** *seconds* **| authentication-simple** *password* **| authentication-md5** *keyid key* **]**

OSPF パケット認証の設定

OSPF は近接ルータ間での単純な認証または MD5 認証をサポートしています。

このエリアのすべてのルータは同じ認証モード（認証しない、単純なテキスト認証、または MD5 暗号によるテキスト認証）を使用しなくてはなりません。サポートする認証モードが設定されると、同一セグメントのすべてのルータが同じ認証キーを使用する必要があります。単純なテキスト認証キーを設定するには、ospf authentication-mode simple コマンドを使用します。また、エリアが MD5 暗号によるテキスト認証モードに設定されている場合、ospf authentication-mode md5 コマンドを使用して MD5 暗号テキスト認証キーを設定します。

はじめに Privileged Exec モードに移行し、次の手順で OSPF パケット認証を設定します。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**Interface vint** *interface-id*	Interface configuration モードに移行します。
手順 3	**ip ospf authentication-simple** *password*	OSPF の単純なテキスト認証用パスワードを設定します。 初期設定：インターフェースは単純な認証また MD5 認証のどちらにも設定されていません。
手順 4	**ip ospf authentication-md5** *key_id key*	キー ID と OSPF MD5 認証キーを設定します。
手順 5	**exit**	Global configuration モードに戻ります。
手順 6	**exit**	Privileged Exec モードに戻ります。
手順 7	**show ip ospf interface [vint** *interface-id* **]**	入力を確認します。
手順 8	**write**	（オプション）設定ファイルに入力を保存します。

インターフェースの単純な認証を解除

モード	コマンド
Interface Configuration	**no ip ospf authentication-simple**

インターフェースの MD5 認証を解除

モード	コマンド
Interface Configuration	**no ip ospf authentication-md5**

OSPF パケット送信のためのインターフェース無効化

特定のネットワークのルータから OSPF 経路情報が取得されないように設定するには、passive コマンドを使用し、インターフェースが OSPF パケットを転送しないようにすることが必要です。

はじめに Privileged Exec モードに移行し、次の手順でインターフェースが OSPF パケットの送信をおこなわないように設定します。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**Interface vint** *interface-id*	Interface configuration モードに移行します。
手順 3	**ip ospf passive**	インターフェースを OSPF パケット送信をおこなわないよう設定します。 初期設定：すべてのインターフェースは OSPF パケットの送受信ができます。
手順 4	**ip ospf authentication-md5** *key_id key*	キー ID と OSPF MD5 認証キーを設定します。
手順 5	**exit**	Global configuration モードに戻ります。
手順 6	**exit**	Privileged Exec モードに戻ります。
手順 7	**show ip ospf interface [vint** *interface-id* **]**	入力を確認します。
手順 8	**write**	（オプション）設定ファイルに入力を保存します。

インターフェースが OSPF パケットを送信可能に設定

モード	コマンド
Interface Configuration	**no ip ospf passive**

OSPF インターフェースがサイレント状態に設定されても、このインターフェースは依然としてダイレクトルートの告知をおこなえます。しかし、このインターフェースの OSPF ハローパケットはブロックされ、近接との関係はこのインターフェースでは確立されません。したがって、OSPF がネットワークに適用できるように機能拡張でき、システムリソースの消費を抑制します。本機は、このコマンドによって、指定した VLAN インターフェースで OSPF パケットの送信を有効 / 無効に設定できます。

経路再配布

下記コマンドで、OSPF において、他のルーティングプロトコルの経路再配布の設定が可能です。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**router ospf**	OSPF configuration モードに移行します。
手順 3	**redistribute [bgp | connected | rip | static]**	ルーティングプロトコルを選択し、経路再配布の設定を行います。

OSPF の表示とデバッグ

上記の設定を終了したら、いずれかのコマンドモードで show コマンドを実行し、実行中の OSPF の設定内容を表示して設定の結果を確認します。

OSPF の表示とデバッグ

操作	コマンド
OSPF ルーティングプロセスについての短い情報を表示	show ip ospf
OSPF 近接情報の表示	show ip ospf neighbor
OSPF ルーティングテーブルの表示	show ip ospf routing
OSPF 仮想リンクの表示	show ip ospf virtual-links
OSPF 統計情報の表示	show ip ospf database
OSPF の LSDB 情報の表示	show ip ospf lsa
OSPF インターフェース情報の表示	show ip ospf interface

標準的な OSPF の設定例

ネットワーク要件

次の図で、Area 2 と Area 0 は直接接続していません。Area 1 は Area 2 と Area 0 を接続するトランジットエリアとして必要です。OSPF サービスをスイッチで有効に設定し、Area 1 の Switch B と Switch C の仮想リンクを正しく設定します。

ネットワーク構成図

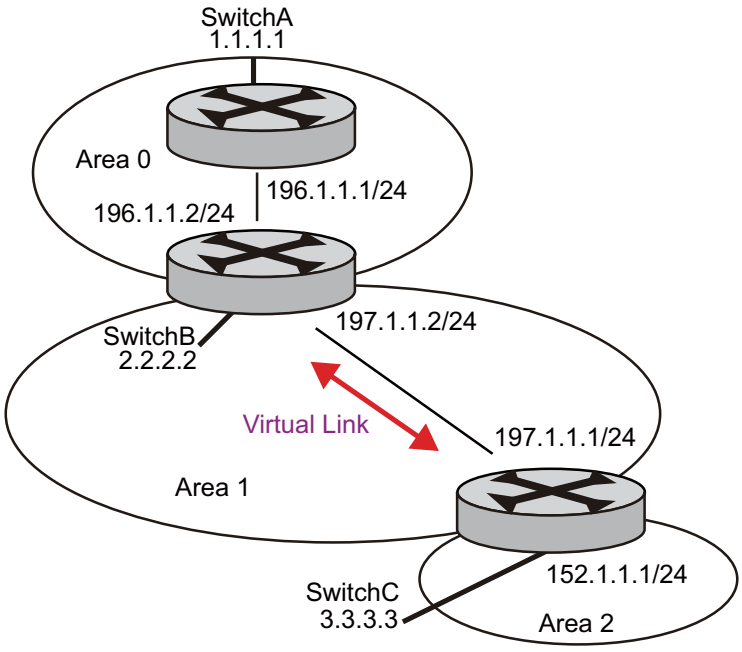


図 21　OSPF 仮想リンクを設定しているネットワーク

OSPF 障害時の症状とトラブルシューティング

障害 1: OSPF を上記で述べた手順に従い設定したが、ルータの OSPF は正しく動作できない。

トラブルシューティング：次の手順に従って確認してください。

ローカルのトラブルシューティング：

直接接続している 2 台のルータのプロトコルが正常な動作をしているか確認します。正常なサインは、2 台のルータの通信相手の状態マシンが FULL の状態に達しています。（注記：ブロードキャストまたは NBMA ネットワークでは、2 台のルータのインターフェースが DROther ステータスの場合、2 台のルータの通信相手の状態マシンは FULL 状態ではなく 2 方向の状態です。DR/BDR と他のすべてのルータについては、通信相手の状態マシンは FULL 状態です。

- show ip ospf neighbour コマンドを実行し、近接の情報を表示します。
- show ip ospf interface コマンドを実行し、インターフェースの OSPF 情報を表示します。
- 物理的な接続と下位レイヤプロトコルが正常に動作しているか確認します。ping コマンドを実行してテストできます。ローカルルータが通信相手のルータに ping を実行できない場合、物理リンクまたは下位プロトコルに障害が発生していることを示します。
- 物理リンクと下位レイヤプロトコルが正常な場合、インターフェースの OSPF パラメータの設定を確認します。パラメータは、近接ルータのインターフェースのパラメータの設定と同じでなくてはなりません。同じエリア ID を使用し、IP アドレスとマスクも一貫性がなくてはなりません。（ポイントツーポイントまたは仮想リンクのセグメントは異なるセグメントとマスクを有することができます。）同一インターフェースのデッドタイマが少なくともハロータイマの 4 倍の値であることを確認します。
- ネットワークの種類がブロードキャストまたは NBMA の場合、少なくとも 1 つのインターフェースが 0 より大きいプライオリティでなくてはなりません。
- エリアを STUB エリアに設定している場合、このエリアにルータが接続していることになります。これらルータ側のエリアも STUB エリアに設定されていなくてはなりません。
- 近接ルータでは同じインターフェース種別が採用されていなくてはなりません。
- 2 エリア以上が設定されている場合、少なくとも 1 つのエリアがバックボーンエリア（つまり、エリア ID が 0）として設定されていなくてはなりません。
- バックボーンエリアがすべてのエリアと接続していることを確認します。
- 仮想リンクが STUB エリアを経由して転送することはできません。

グローバルなトラブルシューティング：

上記の手順は正しく実施したが、OSPF がリモートルータを探索できない場合、次の設定を確認してください。

- **ールータに 2 つ以上のエリアが設定されている場合、少なくとも 1 つはバックボーンエリアとして設定されている必要があります。**

次の図を参照してください。RTA と RTD は 1 つのエリアにのみ所属するように設定されており、RTB（area0 および area1）と RTC（area1 と area2）は 2 つのエリアに所属するように設定されています。ここで、RTB は area0 にも所属していますが、これは要件に準拠しているためです。しかし、RTC が所属していないエリアは area0 です。従って仮想リンクが RTC と RTB の間に確立されます。area2 と area0（バックボーンエリア）が正しいことを確認してください。

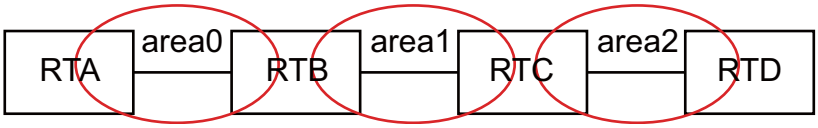


図 22　OSPF のエリア

- **バックボーンエリア（area0）は STUB エリアに設定できず、仮想リンクは STUB エリアを介して転送できません。つまり、仮想リンクが RTB と RTC の間に確立された場合、area1 または area0 は STUB エリアとして設定されえません。上記の図では、area2 のみが STUB エリアとして設定できます。**
- **STUB エリアのルータは外部ルータに再配分できません。**
- **バックボーンエリアはすべてのノードの接続性を保証しなくてはなりません。**

5.9 IP マルチキャストプロトコル

5.9.1 概要

ユニキャスト / ブロードキャストの問題

インターネットの絶え間ない展開とネットワーク上の多用途なデータ、音声、または映像の情報は、e コマース、ネットワーク会議、オンラインオークション、VoD（Video on Demand）、e ラーニングなどの新たなサービスの出現を推進してきました。これらのサービスはより高い情報セキュリティと大きな見返りを必要とします。

ユニキャスト

ユニキャストモードでは、情報を受信したい各ユーザは、それぞれに向け個別に確立されたシステムのチャネルを介して複製を受信します。図 23 を参照してください。

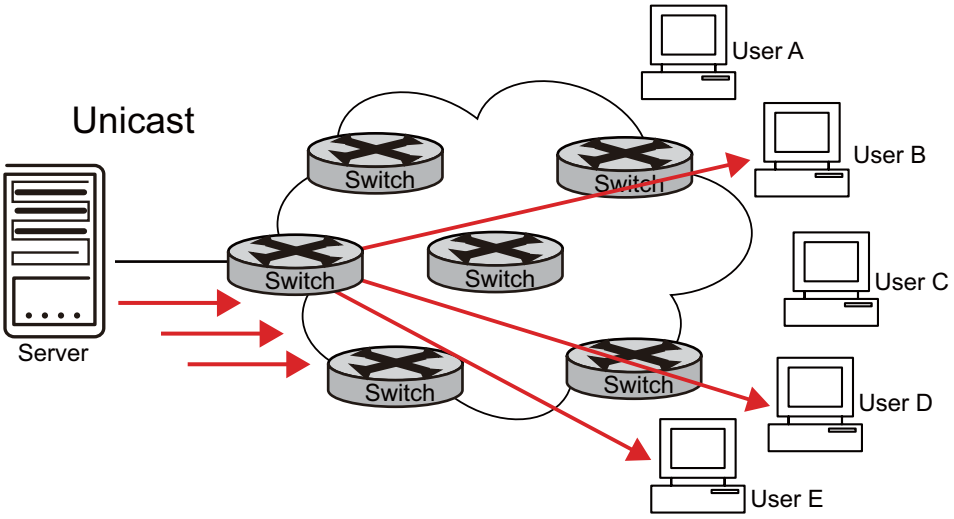


図 23　ユニキャストモードでのデータ転送

User B、D、および E が情報を必要としており、その情報の送信元の Server はそれぞれに向けて伝送チャネルを確立しています。ユーザ数に従い伝送におけるトラフィックは増大するため、膨大な数のユーザがこの情報を必要とした場合は多大な数の情報の複製がネットワークに流れます。帯域幅が足りなくなるため、ユニキャストモードは膨大な伝送をおこなうことはできません。

ブロードキャスト

ブロードキャストモードでは、ネットワークの各ユーザが必要であるなしにかかわらず、情報を受信します。図 24 のブロードキャストモードでのデータ転送について参照してください。

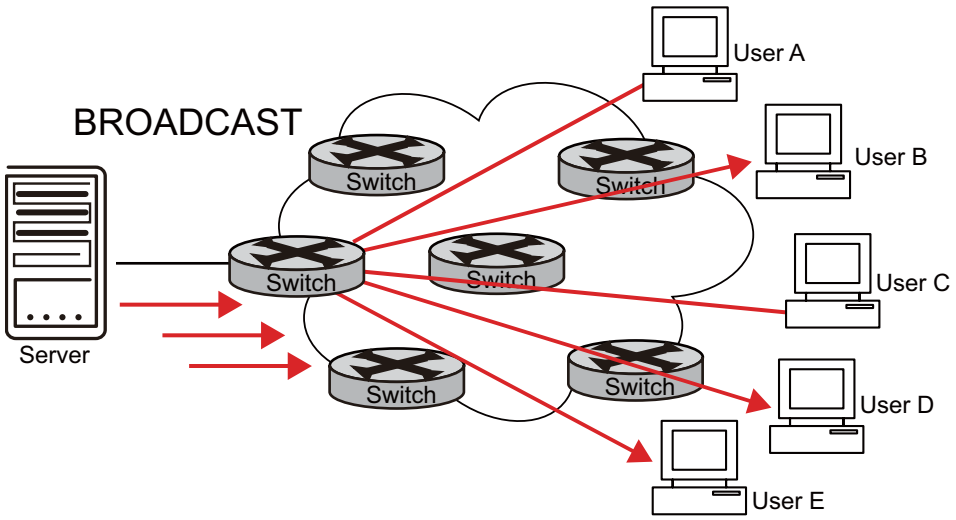


図 24　ブロードキャストモードでのデータ転送

User B、D、E が情報を必要としており、この情報の送信元の Server は、情報をルータ経由でブロードキャストし、User A と User C もまたこの情報を受信します。この場合、情報セキュリティとサービスの達成は保証されません。さらに、2、3 のユーザのみがこの情報を必要としているのに帯域幅は恐ろしいほど無駄遣いされます。

端的には、ユーザがネットワークに分散して配置されている場合はユニキャストモードが、ネットワークに過密にユーザが存在している場合はマルチキャストモードが適しています。ユーザ数が明確でない場合、ユニキャストまたはマルチキャストモードの採用は効率を下げてしまいます。

マルチキャストの利点

マルチキャスト

IP マルチキャストの技術はこれらの問題を解決します。IP マルチキャストはマルチキャストの送信元が情報の送信を 1 度のみ実行すればよく、マルチキャストルーティングプロトコルで確立されたツリー形式の経路に接続する送信先に到達する場合にのみ情報の複製や配布を実行することを可能にします。図 14-3 のマルチキャストモードでのデータ転送について参照してください。

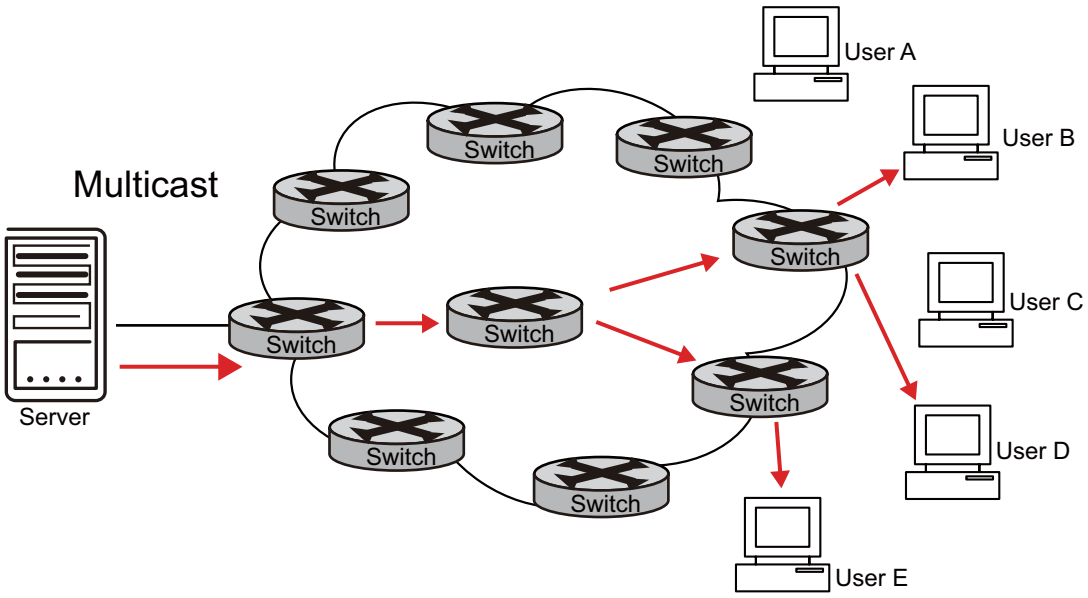


図 25　マルチキャストモードでのデータ転送

User B、D、E が情報を必要としていることを想定し、情報がスムーズに到達することを確実にするために、これらを 1 つの受信グループに組み込みます。このネットワークのルータは、このグループのユーザの配布に基づき、情報を複製し、フォワーディングします。

マルチキャストモードでは、情報の送信元は「マルチキャストソース」、受信側は「マルチキャストグループ」、マルチキャスト情報を転送するルータは「マルチキャストルータ」と呼ばれます。マルチキャストグループのメンバはネットワークに分散することができるので、マルチキャストグループには地理的な制限がありません。マルチキャストソースは必ずしもマルチキャストグループに所属している必要がないことに注意してください。マルチキャストソースはマルチキャストグループにデータを送信しますが、必ずしも受信者である必要はありません。マルチキャストソースは複数のパケットをマルチキャストグループに同時に送信できます。

利点

主なマルチキャストの利点は次のとおりです。

- 効率の強化：ネットワークトラフィックを削減し、サーバや CPU の負荷を軽減します。
- パフォーマンスの最適化：トラフィックの冗長性を排除します。
- 分配されたアプリケーション：マルチポイントアプリケーションを有効にします。

マルチキャストのアプリケーション

IP マルチキャストの技術は効果的に 1 対多の高速なフォワーディングを実現することにより、ネットワークの帯域幅を多大に節約し、ネットワークの負荷を解放できます。IP マルチキャストはまた、オンラインライブショー、Web テレビ、e ラーニング、遠隔治療、ネットワークラジオ局、リアルタイム音声 / テレビ会議などの、オンラインインターネット情報サービス分野で付加価値の高い新しいサービスの開発を促進します。IP マルチキャストは、以下に関して積極的な役割を担っています。

IP マルチキャストの技術は効果的に 1 対多の高速なフォワーディングを実現することにより、ネットワークの帯域幅を多大に節約し、ネットワークの負荷を解放できます。IP マルチキャストはまた、オンラインライブショー、Web テレビ、e ラーニング、遠隔治療、ネットワークラジオ局、リアルタイム音声 / テレビ会議などの、オンラインインターネット情報サービス分野で付加価値の高い新しいサービスの開発を促進します。IP マルチキャストは、以下に関して積極的な役割を担っています。

- マルチメディアおよびストリーミングメディアアプリケーション
- トレーニングおよび連携に関し、随時のコミュニケーション手段
- データストレージおよび金融（株）の運用
- 1 対多のデータ配布

IP ネットワークを介したマルチメディアサービスの広がりが甚大になってきたため、マルチキャストは自身の市場を確立しつつあります。

5.9.2 マルチキャストの実現

マルチキャストアドレス

マルチキャストモードでは、情報をどこに送信するか、デスティネーションをどのように配置するか、またはどのように受信者を知るかという疑問が生じます。これらすべての疑問はマルチキャストアドレスを理解すれば削減されます。マルチキャストソースとマルチキャストグループの間の通信を保証するには、相互に関連するリンクレイヤの MAC マルチキャストアドレスと、ネットワークレイヤのマルチキャストアドレス（つまり IP マルチキャストアドレス）が必要です。以下に、これら 2 つの種類のアドレスについて紹介します。

IP マルチキャストアドレス

IANA（Internet Assigned Number Authority）の定義によると、IP アドレスは次の 4 種類に分類されます。クラス A、クラス B、クラス C およびクラス D です。パケットの規模に応じ、ユニキャストパケットはクラス A、クラス B またはクラス C の IP アドレスを使用します。マルチキャストパケットは、デスティネーションアドレスのクラス D の IP アドレスを使用しますが、クラス D の IP アドレスは送信元の IP パケットの IP フィールドには含めることができません。

ユニキャストデータの送信中、パケットは送信元アドレスからデスティネーションアドレスへ、「ホップごと」に転送されます。しかし、IP マルチキャストの環境では、パケットは 1 つ以上のデスティネーションアドレスまたはアドレスグループを含みます。情報の受信者はすべて 1 つのグループに追加されます。受信者がグループに加入すると、このアドレスグループ宛てのデータは受信者へ送信され始めます。このグループのすべてのメンバはこのパケットを受信できます。

メンバへの加入は動的で、ホストはいつでもグループに加入・脱退できます。マルチキャストグループは永久的な場合と一時的な場合があります。いくつかのマルチキャストグループアドレスは IANA によって割り当てられ、このマルチキャストグループはパーマネントマルチキャストグループと呼ばれます。パーマネントマルチキャストグループの IP アドレスは変更できませんが、メンバ構成は変更可能で、このメンバ数は不定です。パーマネントグループにとって、1 つのメンバを含んでないことはかなりありうることです。パーマネントマルチキャストグループとして予約されていない IP アドレスはテンポラリマルチキャストグループによって使用されます。クラス D マルチキャストアドレスの範囲は 224.0.0.0 から 239.255.255.255 です。詳細情報は以下の表のクラス D アドレスの範囲と意味に掲載します。

クラス D アドレスの意味と範囲

クラス D のアドレス範囲	内容
224.0.0.0-224.0.0.255	予約済みのマルチキャストアドレス（パーマネントグループのアドレス）。224.0.0.0 以外はルーティングプロトコルに割り当てることができます。
224.0.1.0-238.255.255.255	ユーザが利用可能なマルチキャストアドレス（テンポラリアドレスグループ）。ネットワーク全体で有効です。
239.0.0.0-239.255.255.255	ローカル管理用マルチキャストアドレス。設定されたローカルの範囲にのみ有効です。

よく使用される予約済みのマルチキャストアドレスを次の表に記載します。

予約済みのマルチキャストアドレス一覧

クラス D のアドレス範囲	内容
224.0.0.0	基本のアドレス（予約）
224.0.0.1	すべてのホストアドレス
224.0.0.2	すべてのマルチキャストルータのアドレス
224.0.0.3	割り当て不可
224.0.0.4	DVMRP ルータ
224.0.0.5	OSPF ルータ
224.0.0.6	OSPF の DR
224.0.0.7	ST ルータ
224.0.0.8	ST ホスト
224.0.0.9	RIP-2 ルータ
224.0.0.10	IGMP ルータ
224.0.0.11	稼動中のエージェント
224.0.0.12	DHCP サーバ / リレーエージェント
224.0.0.13	すべての PIM ルータ
224.0.0.14	RSVP カプセル化
224.0.0.15	すべての CBT ルータ
224.0.0.16	設定された SBM
224.0.0.17	すべての SBMS
224.0.0.18	VRRP

イーサネットマルチキャスト MAC アドレス

ユニキャスト IP パケットがイーサネットで転送された場合、デスティネーション MAC アドレスは受信者の MAC アドレスになります。しかし、マルチキャストパケットの場合、デスティネーションはもはや特定の受信者ではなく、不特定のメンバにより構成されているグループです。したがって、マルチキャスト MAC アドレスが使用される必要があります。

IANA（Internet Assigned Number Authority）の定義では、マルチキャスト MAC アドレスの上位 24bit は 0x01005e で、MAC アドレスの下位 23bit は、マルチキャスト IP アドレスの下位 23bit です。

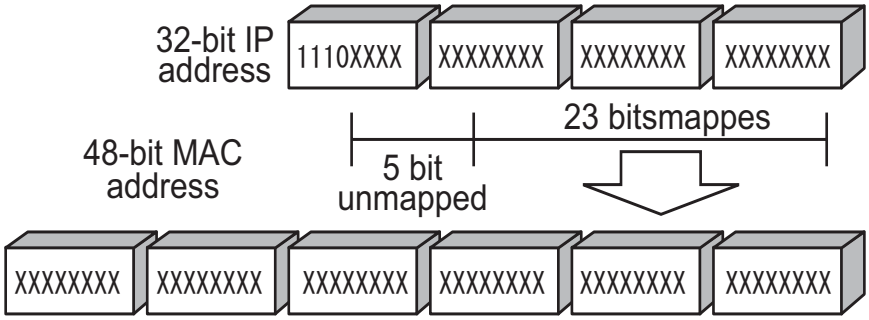


図 26　マルチキャスト IP アドレスとイーサネット MAC アドレスのマッピング

マルチキャストアドレスの最初の 4bit は 1110 で、マルチキャストの識別子を意味します。残る 28bit の 23bit のみが MAC アドレスにマッピングされ、その他の 5bit は破棄されます。この結果、32 の IP アドレスが同じ MAC アドレスにマッピングされます。

IP マルチキャストプロトコル

マルチキャストには、マルチキャストグループマネージメントプロトコルとマルチキャストルーティングプロトコルが含まれます。これらのアプリケーションのポジショニングを、図 14-5 マルチキャスト関連プロトコルのアプリケーションポジショニングに示します。

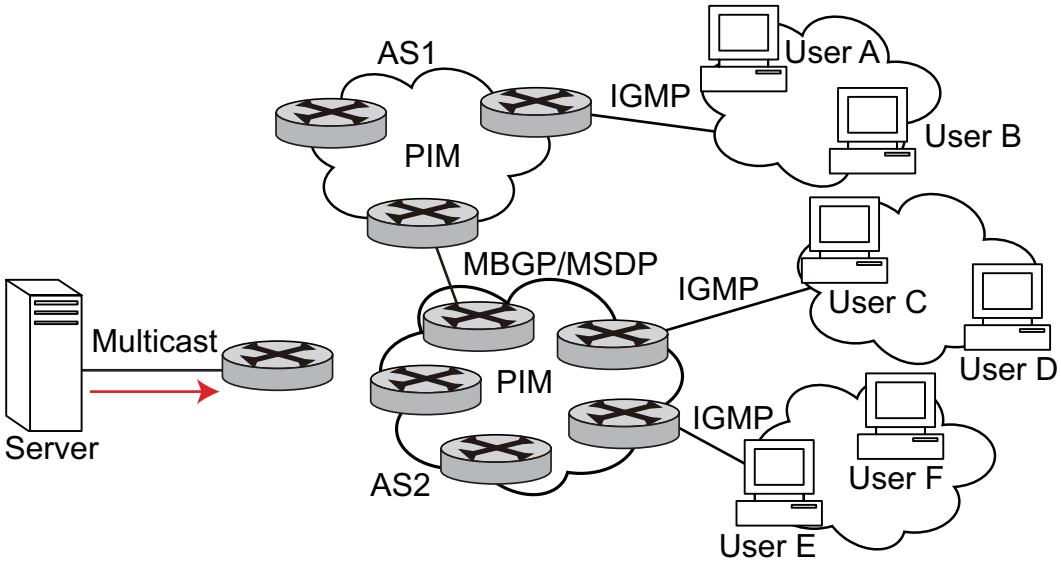


図 27　マルチキャスト関連プロトコルのアプリケーションポジショニング

マルチキャストグループマネージメントプロトコル

マルチキャストグループは IGMP（Internet group management protocol）をマネージメントプロトコルとして使用します。IGMP は、スイッチとマルチキャストルータとの間で起動し、相互のメンバ構成の確立と維持メカニズムを定義します。

マルチキャストルーティングプロトコル

マルチキャストルーティングプロトコルはマルチキャストルータ間で実行され、マルチキャストルータがマルチキャストパケットの正しく効果的なフォワーディングを開始、維持できるようにします。マルチキャストルーティングによって、1 つの送信元から複数の受信者へ、ループのないデータ転送パスが作成されます。マルチキャストルーティングプロトコルの役割は、配送の木構造を構築することです。マルチキャストルータは複数の手法でデータ転送用のパス、デストリビューションツリーを構築できます。

ユニキャストルーティングでは、マルチキャストルーティングもまたドメイン内、ドメイン間が可能です。ドメイン内マルチキャストルーティングは、より成熟しており、ユニキャストルーティングプロトコルと一緒になって動作するドメイン内プロトコルとして、PIM（protocol independent multicast）が最も一般的に使用されています。ドメイン内ルーティングでは、AS 間でどのように経路情報を転送するかを最初に解決する必要があります。AS は異なるキャリアに所属している可能性があるため、ドメイン内経路情報は距離情報に加え、キャリアのポリシーを含んだものでなくてはなりません。現時点では、ドメイン内ルーティングプロトコルは、MSDP（Multicast Source Discovery Protocol）および MBGP マルチキャスト拡張を含んでいます。

5.9.3 IP マルチキャストパケットのフォワーディング

マルチキャストパケットがルータに最短のパスを経由して到達することを確実なものにするには、ユニキャストルーティングテーブルか、マルチキャスト用に独立して提供されるユニキャストルーティングテーブルに従い、マルチキャストルータはマルチキャストパケットの受信インターフェースをチェックしなくてはなりません。このチェックメカニズムは、ほとんどのマルチキャストルーティングプロトコルがマルチキャストフォワーディングを実行する上での基本であり、RPF（Reverse Path Forwarding）チェックとして知られています。マルチキャストルータは受信したマルチキャストパケットの送信元アドレスを使用してユニキャストルーティングテーブルまたは独立型マルチキャストルーティングテーブルに問い合わせをおこない、受信インターフェースが受信局から送信元までの最短のパスであることを決定します。送信元のツリーが使用される場合、マルチキャストパケットを送信している送信元ホストのアドレスが送信元アドレスになります。共用のツリーが使用されると、送信元アドレスは共用ツリーの RP アドレスです。ルータで受信されたマルチキャストパケットは、RPF チェックに合格した場合はマルチキャストフォワーディングテーブルの入力項目に従ってフォワーディングされますが、合格しなかった場合は破棄されます。

5.9.4 IGMP スヌーピングの設定

IGMP スヌーピングの概要

IGMP スヌーピングの基本原則

IGMP（Internet Group Management Protocol）スヌーピングは、レイヤ 2 イーサネットスイッチで稼動するマルチキャストを制御するメカニズムの 1 つで、マルチキャストグループのマネジメントと制御に使用されます。

IGMP スヌーピングはリンクレイヤで稼動します。ホストとルータ間で転送された IGMP メッセージを受信した場合、レイヤ 2 イーサネットスイッチは IGMP スヌーピングを使用し、IGMP メッセージで運ばれた情報を解析します。IGMP のホストからの IGMP ホストレポートメッセージをスイッチが受信すると、スイッチはこのホストを対応するマルチキャストテーブルに追加します。IGMP のホストからの IGMP ホストリーブメッセージをスイッチが受信すると、スイッチはこのホストを対応するマルチキャストテーブルから削除します。スイッチは、継続的に IGMP メッセージのリスニングをおこない、レイヤ 2MAC マルチキャストアドレステーブルを作成、管理します。そして、その後この MAC マルチキャストアドレステーブルに従い、スイッチは上流のルータから転送されてきたマルチキャストパケットをフォワーディングできるようになります。

IGMP スヌーピングが無効になると、パケットはレイヤ 2 でマルチキャストされます。次の図を参照してください。

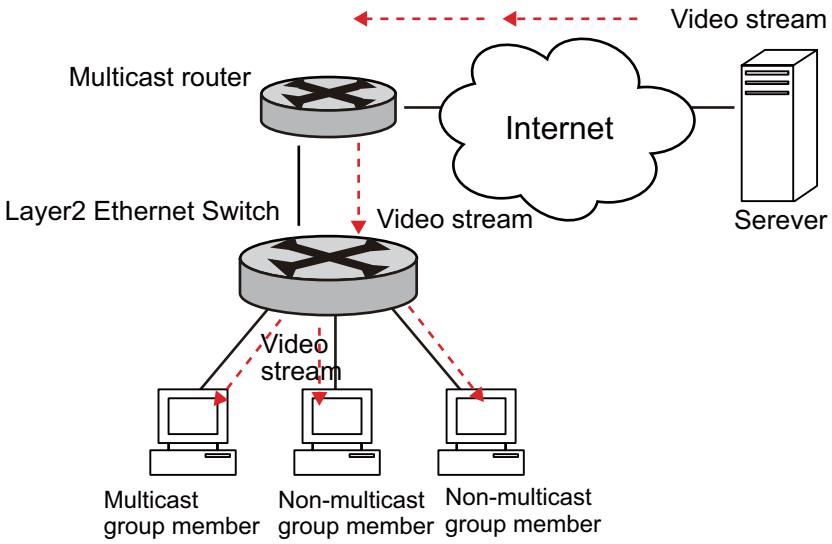


図 28　IGMP スヌーピングが無効の場合のマルチキャストパケットフォワーディング

IGMP スヌーピングが稼動している場合、パケットはレイヤ 2 でブロードキャストされません。次の図を参照してください。

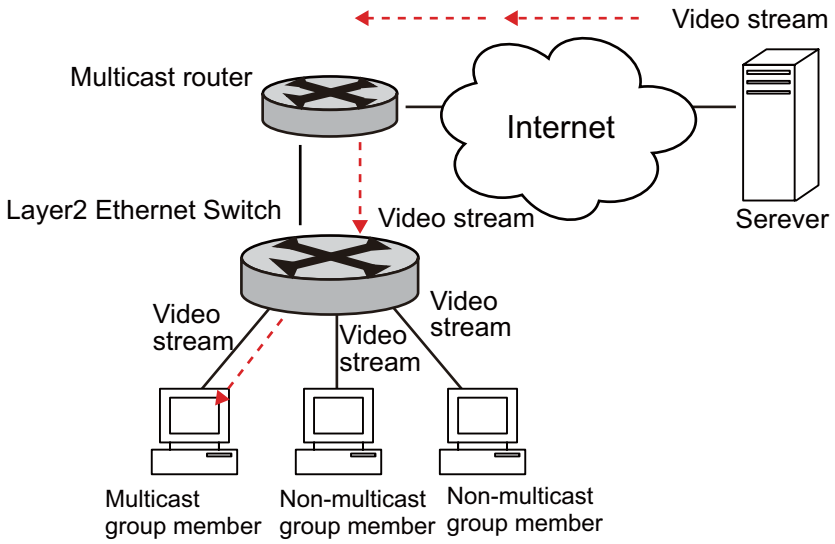


図 29　IGMP スヌーピングが稼働時のマルチキャストパケットフォワーディング

IGMP スヌーピングの実装

- IGMP スヌーピングに関連する概念
  説明をよりご理解いただくために、本項ではまずスイッチに関連する IGMP スヌーピングの概念についていくつか紹介します。

  －ルータポート：マルチキャストルータに直接接続しているスイッチのポートです。

  －マルチキャストメンバポート：マルチキャストメンバに接続しているポートです。マルチキャストメンバはマルチキャストグループに加入しているホストを参照します。

  － MAC マルチキャストグループ：MAC マルチキャストアドレスで識別され、イーサネットスイッチで管理される、マルチキャストグループです。

  －ルータポートエージングタイム：ルータポートのエージングタイマとして設定されている時間です。このタイマのタイムアウトまでにスイッチが IGMP ジェネラルクエリメッセージを受信しない場合、スイッチはこのポートがもやはルータポートではないと見なします。

  －マルチキャストグループメンバポートエージングタイム：ポートが IP マルチキャストグループに加入すると、ポートのエージングタイマがカウントを始めます。マルチキャストグループメンバポートエージングタイマはこのエージングタイマとして設定されます。このタイマのタイムアウト前にスイッチが IGMP レポートメッセージを受信しない場合、スイッチは IGMP クエリメッセージをこのポート宛に転送します。

  －最大応答時間：スイッチが IGMP クエリメッセージをマルチキャストメンバポートに送信した場合、イーサネットスイッチが応答用のタイマを開始しますが、クエリに応答するまでの時間をカウントします。このタイマがタイムアウトするまでにスイッチが IGMP レポートメッセージを受信しない場合、スイッチはこのポートをマルチキャストメンバポートから削除します。

- レイヤ 2 マルチキャストへの IGMP スヌーピングの実装
  このイーサネットアドレスは IGMP スヌーピングを稼動し、対応するマルチキャストグループアドレスに対し、IGMP メッセージのリスニングと、ホストとスイッチポートとのマッピングをおこないます。IGMP スヌーピングの実装では、下図に示す方法で、レイヤ 2 イーサネットスイッチが異なる IGMP メッセージの処理をおこないます。

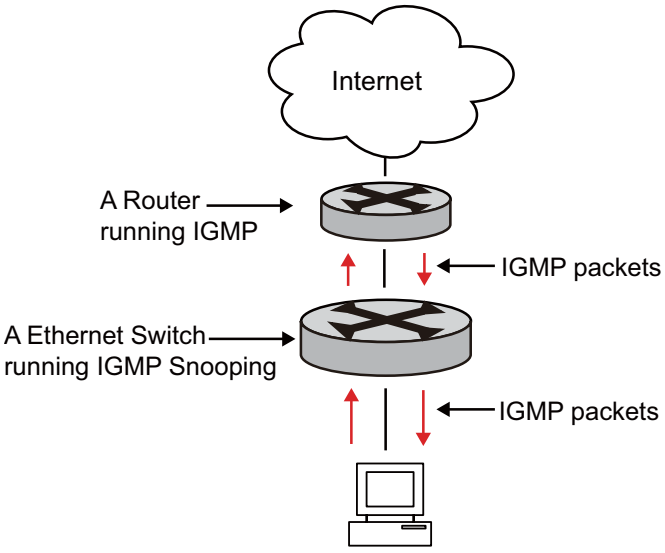


図 30　IGMP スヌーピングの実装

(1) IGMP ジェネラルクエリメッセージ：マルチキャストルータからマルチキャストグループメンバに転送され、どのマルチキャストグループがメンバを含んでいるかを問い合わせます。IGMP ジェネラルクエリメッセージがルータポートに届くと、イーサネットスイッチはポートのエージングタイマをリセットします。ルータポートではないポートが IGMP ジェネラルクエリメッセージを受信すると、イーサネットスイッチがマルチキャストルータに、ポートがマルチキャストグループに加入する準備が終わっていることを知らせ、ポートのエージングタイマを開始します。

(2) IGMP スペシフィッククエリメッセージ：マルチキャストルータからマルチキャストメンバへ転送され、特定のグループがメンバを含んでいるかどうかの問い合わせに使用されます。IGMP スペシフィッククエリメッセージを受信すると、スイッチはスペシフィッククエリメッセージを、問い合わせされた IP マルチキャストグループのみに転送します。

(3) IGMP レポートメッセージ ホストからマルチキャストルータへ転送され、マルチキャストグループへの適用または IGMP クエリメッセージへの応答に使用されます。IGMP レポートメッセージを受信すると、パケットが加入準備を終えている IP マルチキャストグループに対応する MAC マルチキャストグループが存在するかどうか、スイッチがチェックします。対応する MAC マルチキャストグループが存在しない場合、スイッチはルータにメンバはマルチキャストグループに加入する準備を終えていると通知のみをおこない、新たな MAC マルチキャストグループを作成し、メッセージを受信したポートをこのグループに追加し、ポートのエージングタイマを開始し、ポートの VLAN に所属するすべてのルータポートを MAC マルチキャストフォワーディングテーブルに追加し、その後 IP マルチキャストグループを作成し、レポートメッセージを受信するポートを追加します。対応する MAC マルチキャストグループが存在するが、レポートメッセージを受信したポートを含んでいない場合、スイッチがこのポートをマルチキャストグループに追加し、このポートのエージングタイマを開始します。それから、スイッチが対応する IP マルチキャストグループが存在するかどうかをチェックします。存在しない場合、スイッチは新たな IP マルチキャストグループを作成し、レポートメッセージを受信したポートをこのグループに追加します。存在する場合、スイッチはそのポートをこの IP マルチキャストグループに追加します。メッセージに対応する MAC マルチキャストグループが存在し、このメッセージを受信したポートを含む場合、スイッチはこのポートのエージングタイマのリセットのみをおこないます。

(4) IGMP リーブメッセージ マルチキャストグループメンバからマルチキャストルータに転送され、ホストがマルチキャストグループを抜けたことをルータに通知します。IP マルチキャストグループのリーブメッセージを受信すると、ホストが依然このグループの他のメンバを有しているかを確認するため、イーサネットスイッチはグループからメッセージを受信したポートに関するスペシフィッククエリメッセージを転送し、その後最大応答タイマを開始します。スイッチがマルチキャストグループからレポートメッセージを受信しなかった場合、ポートは対応する MAC マルチキャストグループから削除されます。MAC マルチキャストグループにメンバが所属していない場合、スイッチはマルチキャストルータにマルチキャストツリーからこのグループを削除するよう通知します。

IGMP スヌーピングの設定

主な IGMP スヌーピング設定には以下が含まれます。

● IGMP スヌーピングの有効化 / 無効化

● マルチキャストグループメンバポートのエージングタイム設定

上記の設定項目のなかで、IGMP スヌーピングの有効化は必須ですが、その他は必要な場合のオプションです。

IGMP スヌーピングの有効化 / 無効化

次のコマンドを使用し、IGMP スヌーピングの有効 / 無効を設定して MAC マルチキャストフォワーディングテーブルが作成され、レイヤ 2 で管理されているかどうかを制御します。

はじめに Privileged Exec モードに移行し、次の手順でポートの IGMP スヌーピングを有効にします。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**sys igmp-snooping enable**	IGMP スヌーピングを有効に設定します。 初期設定：無効
手順 3	**exit**	Privileged Exec モードに戻ります。
手順 4	**show system config**	入力を確認します。
手順 5	**write**	（オプション）設定ファイルに入力を保存します。

IGMP スヌーピングの無効

モード	コマンド
Grobal Configuration	**sys igmp-snooping disable**

マルチキャストグループメンバのエージングタイム設定

この作業では、マルチキャストグループメンバポートのエージングタイムを手入力により設定します。スイッチが、メンバポートのエージングタイム中にマルチキャストグループレポートメッセージを受信しない場合、スイッチはスペシフィッククエリメッセージをこのポートに転送し、最大応答タイマを開始します。

はじめに Privileged Exec モードに移行し、次の手順でマルチキャストグループメンバのエージングタイムを設定します。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**igmp-snooping timeout** *seconds*	エージングタイムを設定します。 初期設定：300 秒
手順 3	**exit**	Privileged Exec モードに戻ります。
手順 4	**show igmp-snooping time-out**	入力を確認します。
手順 5	**write**	（オプション）設定ファイルに入力を保存します。

IGMP スヌーピングの設定例

ネットワーク要件

本機に IGMP スヌーピングを実装するには、まず IGMP スヌーピングを有効にします。スイッチはルータポートを介してルータと接続しており、非ルータポートを介してユーザの PC と接続しています。

ネットワーク構成図

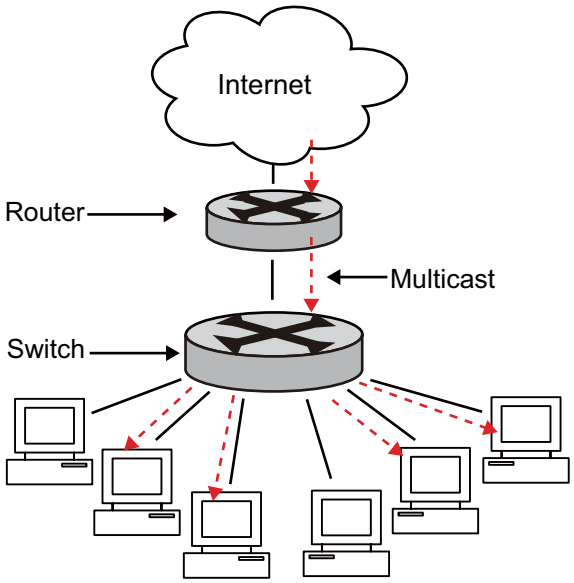


図 31　IGMP スヌーピングを設定しているネットワーク

設定手順

スイッチで IGMP スヌーピングを有効にします。

```
switch(config)#system igmp-snooping enable
```

IGMP スヌーピングのトラブルシューティング

障害：マルチキャスト機能をスイッチに実装できない。

トラブルシューティング：

（1）IGMP **スヌーピングが無効**

- display current-configuration **コマンドを入力し、**IGMP **スヌーピングの状態を表示します。**
- **スイッチで** IGMP **スヌーピングが無効の場合、**IGMP **スヌーピングがグローバルで無効なのか、**VLAN **で無効なのかを確認します。グローバルで有効でない場合、まず** System View **モード、次に** VLAN View **モードで** igmp-snooping enable **コマンドを入力します。**VLAN **で有効でない場合、同じコマンドを** VLAN View **モードで入力します。**

（2）IGMP **スヌーピングのマルチキャストフォワーディングテーブルの設定に誤りがある。**

- display igmp-snooping group **コマンドを入力し、マルチキャストの経路が所望のものかを確認します。**
- IGMP **スヌーピングにより作成されたマルチキャストグループが正しくない場合、専門の保守担当者に相談してください。**
- **第** 2 **の手順を完了したら、診断** 3) **を続けてください。**

（3）**下位レイヤのマルチキャストフォワーディングテーブルの設定に誤りがある。**

- User View **モードで** IGMP **スヌーピンググループを有効にし、**command display gmp-snooping group **コマンドを入力して、下位レイヤの** MAC **マルチキャストフォワーディングテーブルと** IGMP **スヌーピングにより作成されたものが一貫しているかを確認します。いずれかのモードで** input the isplay mac vlan **コマンドを入力し、下位レイヤの** VLAN ID **の** MAC **マルチキャストテーブルと** IGMP **スヌーピングにより作成されたものが一貫しているかを確認します。**
- **一貫していない場合、保守担当者に連絡し相談してください。**

5.9.5 スタティックマルチキャストグループの設定

スタティックマルチキャストグループの概要

スタティックマルチキャストグループの設定はマルチキャストグループマネージメントモードの 1 つで、マルチキャストフォワーディングテーブルの設定等をおこないます。

スタティックマルチキャストグループの設定

スタティックマルチキャストグループの設定には次の項目があります。

● スタティックマルチキャストグループの追加 / 削除

はじめに Privileged Exec モードに移行し、次の手順でスタティックマルチキャストグループを追加します。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**multicast-group static add vid** *vlan-id mac-address port-list*	スタティックマルチキャストグループの追加をおこないます。mac-address はマルチキャストグループアドレスです。port-list はポートメンバリストで、フォーマットは 01m のようにポート番号に m を付けたものです。
手順 3	**exit**	Privileged Exec モードに戻ります。
手順 4	**show multicast-group**	入力を確認します。
手順 5	**write**	（オプション）設定ファイルに入力を保存します。

IGMP スヌーピングの無効

モード	コマンド
Grobal Configuration	**multicast-group static add vid** *vlan-id mac-address*

5.9.6 IGMP

IGMP の概要

IGMP の紹介

IGMP（Internet Group Management Protocol）は TCP/IP スイートのプロトコルの 1 つで、IP マルチキャストメンバの管理に関与します。IGMP は、IP ホストと直接接続している近接ルータとの、マルチキャストメンバ構成の確立、維持に使用されます。IGMP には、マルチキャストルーティングプロトコルによって完備されるマルチキャストルータ間のメンバ構成情報の転送と維持は含まれません。マルチキャストに参加するすべてのホストは IGMP を実装している必要があります。

IP マルチキャストに参加しているソフトはマルチキャストグループにいつでも加入・脱退ができます。マルチキャストグループのメンバ数は整数単位でいくつでも可能で、配置場所はどこでもかまいません。マルチキャストルータはすべてのホストのメンバ構成情報を必要とせず、維持できません。マルチキャストルータは IGMP を使用し、マルチキャストグループの受信者（グループメンバ）が各インターフェースのサブネットに存在しているかどうかのみを学習します。ホストは加入しているのがどのマルチキャストグループかのみを保持する必要がありません。

IGMP はホストとルータに対称的ではありません。ホストは、マルチキャストルータからの IGMP クエリメッセージに対して、ルータへのグループメンバ構成情報のレポーティングなど、応答する必要があります。ルータはメンバ構成の問い合わせメッセージを定期的に送信し、受信した応答メッセージに従い、サブネットの特定のグループにホストが加入しているかどうかを探索します。ルータがホストがグループを脱退したというレポートを受信した場合、ルータはグループを特定する問い合わせのパケット（IGMP Version 2）を送信し、いかなるメンバもそのグループに存在していないかどうかを探索します。

現在までに、IGMP には 3 つのバージョン、IGMP バージョン 1（RFC1112 により定義）、IGMP バージョン 2（RFC2236 により定義）、および IGMP バージョン 3 があります。現時点では、IGMP バージョン 2 が最も広く使用されているバージョンです。

IGMP バージョン 2 は IGMP バージョン 1 に対して次のような改良された項目があります。

- **共有ネットワークセグメントのマルチキャストルータ選定メカニズム**
  共用ネットワークセグメントは、ネットワークセグメントに複数のマルチキャストルータが存在するということを意味します。この場合、ネットワークセグメント上の IGMP を稼動しているすべてのルータは、ホストからメンバ構成レポートを受信できます。したがって、メンバ構成問い合わせメッセージを送信するために、1 台のルータのみが必要です。この場合、問い合わせ者のルータを特定するために、ルータの選定メカニズムが必要です。IGMP バージョン 1 では、問い合わせ者の選定は、マルチキャストルーティングプロトコルによって決定されます。一方、IGMP バージョン 2 では、同一ネットワークセグメントに複数のマルチキャストルータが存在する場合、最も小さい IP アドレスを有するマルチキャストルータが問い合わせ者として選定されます。
- **グループからのリーブメカニズム**
  IGMP バージョン 1 では、ホストは、マルチキャストルータに通知せずに、マルチキャストグループから静かに脱退します。この場合、マルチキャストルータはマルチキャストグループの応答時間のタイムアウトのみに依存して、ホストがグループから抜けたことを確認します。IGMP バージョン 2 では、ホストは抜ける意図を示し、このホストが最新のメンバ構成問い合わせメッセージについて責任を有している場合、リーブグループメッセージを送信します。

- **グループクエリ**
  IGMP バージョン 1 では、マルチキャストルータの問い合わせはネットワークセグメントの全マルチキャストグループを対象にしており、これをジェネラルクエリといいます。IGMP バージョン 2 の場合、グループスペシフィッククエリがジェネラルクエリのほかに追加されます。問い合わせパケットのデスティネーション IP アドレスはマルチキャストグループの IP アドレスです。パケットのグループアドレスドメインもまた、マルチキャストグループの IP アドレスです。これにより、他のマルチキャストグループのホストのメンバが、応答メッセージの送信をおこなわないようにします。

- **最大応答時間**
  最大応答時間は IGMP バージョン 2 で追加されました。これは、ホストの許可された最大時間を動的に調整し、メンバ構成の問い合わせメッセージを応答するために使用されます。

IGMP の設定

（1）IGMP の基本設定には次の項目があります。

- マルチキャストルーティングの有効化
- インターフェースの IGMP の有効化

（2）IGMP の高度な設定には次の項目があります。

- IGMP バージョンの設定
- IGMP 問い合わせメッセージ送信間隔の設定
- IGMP パケット問い合わせ間隔の設定
- IGMPv2 での IGMP 問い合わせタイムアウト変更
- IGMPv2 の最大問い合わせ応答時間の変更
- ルータのマルチキャストグループへの参加を設定
- 静的メンバとしてスイッチを設定

マルチキャストルーティングの有効化

IGMP とマルチキャストルーティングプロトコルを有効にする前に、まずマルチキャストを有効化します。

はじめに Privileged Exec モードに移行し、次の手順で IP マルチキャストルーティングを有効にします。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**ip multicast-routing enable**	IP マルチキャストルーティングを有効にします。 初期設定 : 無効
手順 3	**exit**	Privileged Exec モードに戻ります。
手順 4	**show ip mroute**	入力を確認します。
手順 5	**write**	（オプション）設定ファイルに入力を保存します。

マルチキャストルーティングを無効に設定

モード	コマンド
Grobal Configuration	ip multicast-routing disable

インターフェース IGMP の有効化

マルチキャスト機能は ip multicast-routing enable コマンドの実行によってのみ有効に設定できます。このあと、IGMP 機能の設定を実行できます。

はじめに Privileged Exec モードに移行し、次の手順でインターフェースの IGMP を有効にします。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**ip pim interface** *interface-id* **sparse-mode enable**	インターフェースの IGMP を有効にします。 初期設定：無効
手順 3	**exit**	Privileged Exec モードに戻ります。
手順 4	**show ip igmp interface** *interface-id*	入力を確認します。
手順 5	**write**	（オプション）設定ファイルに入力を保存します。

マルチキャストルーティングを無効に設定

モード	コマンド
Grobal Configuration	**ip pim interface** *interface-id* **sparse-mode disable**

IGMP バージョンの設定

はじめに Privileged Exec モードに移行し、次の手順で IGMP バージョンの設定をおこないます。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**ip igmp interface** *interface-id* **version { 1 | 2 }**	スイッチが使用する IGMP バージョンを設定します。**注記：**バージョン 1 に変更する場合、Interface Configuration モードの **ip igmp query-interval** または **ip igmp query-max-response-time** コマンドは設定できません。 初期設定：IGMP バージョン 2
手順 3	**exit**	Privileged Exec モードに戻ります。
手順 4	**show ip igmp interface** *interface-id*	入力を確認します。
手順 5	**write**	（オプション）設定ファイルに入力を保存します。

初期設定：IGMP バージョン 2 が使用されます。

[注意] サブネットのすべてのルータが同じ IGMP バージョンをサポートしていなくてはなりません。IGMP バージョン 1 のシステムの存在を検出後は、ルータは自動的にバージョン 1 に切り替えることはできません。

IGMP 問い合わせメッセージ送信間隔の設定

マルチキャストルータは IGMP 問い合わせメッセージを送信し、接続しているネットワークにどのマルチキャストグループが存在するかを探索します。マルチキャストルータは定期的に問い合わせメッセージを送信し、ネットワークに存在しているメンバ情報を更新します。

はじめに Privileged Exec モードに移行し、次の手順で IGMP 問い合わせメッセージの送信間隔を設定します。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**ip igmp query-interval** *seconds*	IGMP クエリメッセージの送信間隔の設定をおこないます。（範囲：1 ～ 65535） 初期設定：60 秒
手順 3	**exit**	Privileged Exec モードに戻ります。
手順 4	**write**	（オプション）設定ファイルに入力を保存します。

ネットワークセグメントに複数のマルチキャストルータが存在する場合、問い合わせ者は IGMP 問い合わせメッセージを LAN 上のすべてのホストに対して送信する責任を負っています。

IGMP パケット問い合わせ間隔の設定

共用ネットワークでは、クエリルータ（問い合わせ者）がインターフェースの IGMP メンバ情報の維持をおこないます。IGMP 問い合わせ者が IGMP リーブグループメッセージをホストから受信した場合、最後のメンバ問い合わせ間隔はグループスペシフィッククエリで設定できます。

- ホストは IGMP リーブメッセージを送信します。
- このメッセージを受信すると、IGMP 問い合わせ者は指定したグループの IGMP 問い合わせメッセージを指定した時間に（igmp robust-count コマンドの robust-value で設定した値で、初期設定では 1 秒）、特定の送信間隔（igmp lastmember-queryinterval コマンドの秒（seconds）で設定した値で、初期設定では 2）で送信します。
- 他のホストが IGMP の問い合わせ者からのメッセージを受信し、このグループに関心を持った場合、IGMP メンバ構成情報レポートメッセージを設定済みの最大応答時間内に返します。
- IGMP 問い合わせ者が他のホストから robust-value と同じ範囲内でレポートメッセージを受信すると、IGMP 問い合わせ者はこのグループに対するメンバ構成情報の維持を継続します。
- 他のホストからこの範囲内にレポートメッセージを受信しなかった場合、タイムアウトと見なし、このグループのメンバ構成情報の維持を終了します。

このコマンドは、IGMP バージョン 1 ではグループを脱退した際 IGMP リーブグループメッセージを送信しないため、問い合わせ者が IGMP バージョン 2 を稼動している場合のみ使用できます。

はじめに Privileged Exec モードに移行し、次の手順で IGMP パケット問い合わせの間隔を設定します。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**ip igmp last-query-interval** *seconds*	IGMP パケットの問い合わせ間隔を設定します。 （範囲：1 ～ 65） 初期設定：1 秒
手順 3	**exit**	Privileged Exec モードに戻ります。
手順 4	**write**	（オプション）設定ファイルに入力を保存します。

IGMP v2 での IGMP 問い合わせタイムアウト変更

IGMP v2 を使用している場合、スイッチがインターフェースの問い合わせ者を引き継ぐ前の一定時間を設定できます。初期設定では、スイッチは、Interface Configuration モードの ip igmp query-interval コマンドにより制御される問い合わせ間隔を 2 度待ちます。この時間のあと、スイッチが問い合わせを受信しない場合、スイッチが問い合わせ者になります。

Privileged Exec モードで show ip igmp interface interface-id コマンドを入力することにより、問い合わせの間隔を設定できます。

はじめに Privileged Exec モードに移行し、次の手順で IGMP 問い合わせタイムアウトの変更をおこないます。この手順は必須ではありません。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**ip igmp querier-timeout** *seconds*	IGMP 問い合わせのタイムアウトを設定します。 （範囲：60 ～ 300） 初期設定：60 秒（問い合わせ間隔の 2 倍）
手順 3	**exit**	Privileged Exec モードに戻ります。
手順 4	**write**	（オプション）設定ファイルに入力を保存します。

IGMP v2 の最大問い合わせ応答時間の変更

IGMP v2 を使用している場合、IGMP 問い合わせ者から広告される最大問い合わせ応答時間を変更できます。この最大問い合わせ応答時間は、LAN でグループメンバが直接接続しているディレクトリが存在しないことをスイッチがすばやく探索できるようにします。この値を削減すると、スイッチがグループをより高速に除去できます。

はじめに Privileged Exec モードに移行し、次の手順で最大問い合わせ応答時間の変更をおこないます。

この手順は必須ではありません。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**ip igmp query-max response** *seconds*	IGMP の問い合わせで広告される、最大問い合わせ応答時間を変更します。（範囲：1 ～ 25） 初期設定値：10 秒
手順 3	**exit**	Privileged Exec モードに戻ります。
手順 4	**write**	（オプション）設定ファイルに入力を保存します。

ルータのマルチキャストグループへの参加を設定

通常、IGMP を稼動しているホストはマルチキャストルータの IGMP 問い合わせパケットに応答します。応答に失敗すると、マルチキャストルータはこのネットワークセグメントにマルチキャストメンバが存在しないと見なし、対応しているパスを無効にします。ルータのあるインターフェースをマルチキャストメンバとして設定すると、この問題を回避できます。このインターフェースが IGMP 問い合わせパケットを受信すると、ルータは応答し、このインターフェースが接続するネットワークセグメントが通常マルチキャストパケットを受信できることを確実にします。

イーサネットスイッチの場合、VLAN インターフェースのポートをマルチキャストグループに加入できるよう設定します。

はじめに Privileged Exec モードに移行し、次の手順でルータが特定のマルチキャストグループに加入できるよう設定します。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**ip igmp interface** *interface-id* **join-group** *group-address*	ルータが指定したマルチキャストグループに加入できるよう設定します。 初期設定：ルータはグループに加入しません。
手順 3	**exit**	Privileged Exec モードに戻ります。
手順 4	**write**	（オプション）設定ファイルに入力を保存します。

グループから抜ける場合

モード	コマンド
Grobal Configuration	ip igmp interface interface-id leave-group group-address

静的メンバとしてスイッチを設定

時として、ネットワークセグメントのグループメンバまたはホストのどちらも IGMP を使用してグループメンバ構成情報をレポートできません。しかし、マルチキャストトラフィックをそのネットワークセグメントに通したい場合があります。マルチキャストトラフィックをネットワークセグメントへ通すには、次の方法があります。

- Global Configuration モードで ip igmp interface interface-id join-group コマンドを使用します。この方法では、スイッチはマルチキャストパケットのフォワーディングに加え、受信をおこないます。マルチキャストパケットを受信すると、スイッチが高速な切り替えをおこなえないようにします。
- Global Configuration モードで ip igmp interface interface-id static-group コマンドを使用します。この方法では、スイッチはパケットを受信せず、フォワーディングのみをおこないます。この方法は高速な切り替えを可能にします。IGMP のキャッシュに送信インターフェースが表示されますが、スイッチ自身はメンバではなく、マルチキャストルーティングの入力で L（Local）フラグがないことによって証明されます。

はじめに Privileged Exec モードに移行し、次の手順でスイッチがグループの静的に接続されたメンバになるよう（および高速なスイッチングを有効にするよう）に設定します。

この手順は必須ではありません。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**ip igmp interface** *interface-id* **static-group add** *group-address*	本機をグループの静的に接続されたメンバに設定します。初期設定では、この機能は無効に設定されています。
手順 3	**exit**	Privileged Exec モードに戻ります。
手順 4	**write**	（オプション）設定ファイルに入力を保存します。

グループのメンバからスイッチを削除

モード	コマンド
Grobal Configuration	**ip igmp interface** *interface-id* **static-group delete** *group-address*

5.9.7 PIM-SM

PIM-SM の概要

PIM-SM の紹介

PIM-SM（Protocol Independent Multicast, Sparse Mode）はスパースモードのマルチキャストルーティングプロトコルです。PIM-SM は主に広い範囲の大規模ネットワークで、この中のグループメンバは比較的分散しているような場合に適用されます。

密集型のフラッドアンドプルーン主義とことなり、明示的なパケットのリクエストがある場合を除き、PIM-SM はすべてのホストがマルチキャストパケットを受信する必要はないことを前提にしています。

PIM-SM は RP（Rendezvous Point）および BSR（Bootstrap Router）を使用してマルチキャスト情報をすべての PIM-SM ルータに広告し、ルータの加入、脱退情報を使用して RPT（RP-rooted shared tree）を構築し、その結果データパケットに占有される帯域幅の削減、パケットの制御、およびルータのオーバヘッドの処理の軽減をおこないます。マルチキャストデータは、マルチキャストグループメンバが所属しているネットワークセグメントの共有ツリーに沿って流れます。データトラフィックが十分な場合、マルチキャストデータフローは送信元の SPT（Shortest Path Tree）を介して流れることができ、ネットワーク遅延を削減します。PIM-SM は特定のユニキャストルーティングプロトコルに依存していませんが、その時点でのユニキャストルーティングテーブルを使用して RPF チェックを実行します。

PIM-SM の稼動には、RP および BSR 候補の設定が必要です。BSR は RP 候補から情報を収集し、その情報を広告することを担います。

PIM-SM 動作原則

PIM-SM 動作のプロセスは以下のとおりです。近隣探索、RPT（RP-rooted shared tree）の構築、マルチキャスト送信元登録、SPT 切り替えなど。近隣探索メカニズムは PIM-DM と同じですが、ここでは深く言及しません。

- RPT（RP Shared tree）の構築
  ホストがマルチキャストグループ G に加入する場合、ホストに直接接続しているリーフルータは IGMP メッセージを送信してマルチキャストグループ G の受信者を学習します。この方法で、リーフルータはマルチキャストグループ G の対応する RP（ランデブーポイント）を算出し、RP に対し、より高い階層のノードにジョインメッセージを送信します。リーフルータと RP 間のパスに配置されている各ルータは、マルチキャストグループ G に送信されるすべてのパケットはどの送信元から送信された入力でも適用されるということを意味する、(*, G) 入力をフォワーディングテーブルに生成します。RP がマルチキャストグループ G に送信されたパケットを受信すると、このパケットは構築されたパス沿いのリーフルータに送信され、ホストに到達します。この方法で、下図のように RPT（RP-rooted tree）が構築されます。

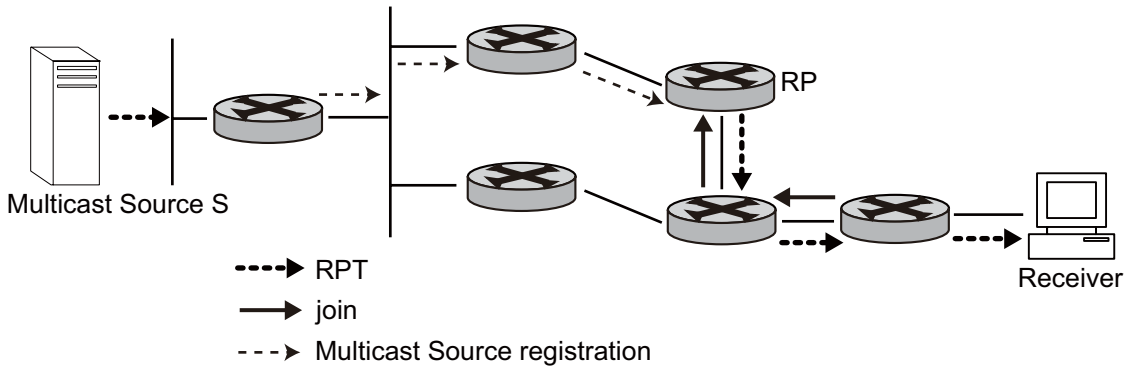


図 32　RPT 概略図

- **マルチキャスト送信元の登録**
  マルチキャストの送信元 S **がマルチキャストパケットをマルチキャストグループ** G **に送信する場合、**S **に直接接続している** PIM-SM **マルチキャストルータが受信したパケットをレジストレーションパケットにカプセル化し、対応する** RP **宛にユニキャスト方式で送信します。複数の** PIM-SM **マルチキャストルータがネットワークセグメントに存在する場合、**DR（Designated Router）**がこのマルチキャストパケットの送信に応答します。**

PIM-SM 設定前の準備

- RP **候補者の設定**
  PIM-SM **ネットワークでは、複数の** RP（RP **候補者**）**を設定できます。各** C-RP（Candidate-RP、RP **候補者**）**が、特定領域のデスティネーションアドレスを有するマルチキャストパケットのフォワーディングに責任を負います。複数の** C-RP **を設定することにより、**RP **の負荷分散を実現できます。これらの** C-RP **は等しいものです。**BSR **が広告する** C-RP **メッセージの受信後、すべてのマルチキャストルータは同じアルゴリズムを用いてマルチキャストグループに対応する** RP **を算出します。**1 **つの** RP **が複数のマルチキャストグループあるいはすべてのマルチキャストグループに対して動作することに注意が必要です。一方、各マルチキャストグループは複数のマルチキャスト** RP **ではなく、**1 **度に** 1 **つの** RP **にのみ一意的に対応が可能です。**

- BSR **の設定**
  BSR **は** PIM-SM **ネットワークでの管理機能のコアになります。**C-RP（Candidate-RP）**は** BSR **に通知を送信し、これがすべての** C-RP **に関する情報の収集と広告を担います。ネットワークで** BSR **になれるのは** 1 **つだけですが、複数の** C-BSR **を設定できることに注意が必要です。この場合、ある** BSR **がダウンすると、別の** BSR **に切り替えできます。**BSR **は、**C-BSR **の中から自動的に選定されます。最も高いプライオリティを有する** C-BSR **が** BSR **として選定されます。プライオリティが同じ場合には、最も大きな** IP **アドレスを有する** C-BSR **が** BSR **に選定されます。**

- **静的** RP **の設定**
  RP **の役割を担うルータは、マルチキャストルータのコアルータです。**BSR **メカニズムにより選定された動的** RP **が何らかの理由により無効である場合、静的** RP **を** RP **として設定できます。動的** RP **のバックアップとして、静的** RP **はネットワークの堅牢性を向上し、マルチキャストネットワークの操作性と管理性能を強化します。**

PIM-SM の設定

（1）PIM-SM の基本設定には次の項目があります。

- マルチキャストの有効化
- PIM-SM の有効化
- C-BSR（candidate-BSR）の設定
- C-RP（candidate-RP）の設定
- 静的 RP の設定

（2）PIM-SM の高度な設定には次の項目があります。

- インターフェースのハローパケット送信間隔の設定
- マルチキャスト送信元 / グループのフィルタリング設定
- PIM 近接のフィルタリング設定
- インターフェースでの最大の PIM 近接数の設定
- DR が送信した登録メッセージのフィルタリングのための RP の設定
- PIM ルーティングテーブルからのマルチキャストルート項目の消去
- PIM 近接の消去

[注意]　PIM-SM ドメイン全体で少なくとも 1 つのルータを C-RP および C-BSR として設定すべきことに注意が必要です。

マルチキャストの有効化

P124 「マルチキャストルーティングの有効化」を参照してください。

PIM-SM の有効化

この設定は、マルチキャストが有効な状態である場合にのみ有効です。
はじめに Privileged Exec モードに移行し、次の手順で PIM-SM を有効にします。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**ip pim interface** *interface-id* **sparse-mode enable**	IP マルチキャストルーティングを有効にします。
手順 3	**exit**	Privileged Exec モードに戻ります。
手順 4	**show ip igmp interface** *interface-id*	入力を確認します。
手順 5	**write**	（オプション）設定ファイルに入力を保存します。

この設定を繰り返し、他のインターフェースの PIM-SM を有効にします。インターフェースで一度に有効にできるのは、1 つのマルチキャストルーティングプロトコルのみです。

C-BSR（candidate-BSR の設定）

PIM ドメインでは、1 つまたは複数の C-BSR の設定が必要です。BSR（Bootstrap Router）が C-BSR から選定されます。BSR は RP 情報の収集と広告を担います。

C-BSR からのこの自動選定は次のようにおこなわれます。

ルータを C-BSR に設定する場合、PIM-SM を起動した 1 つのインターフェースを設定しなくてはなりません。
まず、各 C-BSR は自身を所属している PIM-SM ドメインの BSR であると見なし、インターフェースの IP アドレスを BSR アドレスに採用して Bootstrap メッセージを送信します。

他のルータから Bootstrap メッセージを受信すると、C-BSR はこの新たに受信した Bootstrap メッセージを自身のものと比較します。比較方法にはプライオリティと IP アドレスが含まれます。プライオリティが同一の場合には、より大きな IP アドレスがより良いと判断されます。新たな BSR アドレスのほうがよりよい場合、C-BSR は BSR アドレスに置き換え、自身を BSR に見なすことをやめます。
そうでない場合、C-BSR は自身の BSR アドレスを保持し、自身を BSR に見なします。

はじめに Privileged Exec モードに移行し、次の手順で C-BSR を設定します。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**ip pim bsr-candidate** *interface-id* **[priority** *priority* **]**	C-BSR を設定します。初期設定では、BSR は設定されていません。priority の初期設定値は 0 です。priority は 0 ～ 255 の範囲で設定します。
手順 3	**exit**	Privileged Exec モードに戻ります。
手順 4	**show ip pim bsr-router**	入力を確認します。
手順 5	**write**	（オプション）設定ファイルに入力を保存します。

[注意]　C-BSR はネットワークバックボーンのルータに設定する必要があります。

- **1 台のルータに対し、1 つの C-BSR のみを設定できます。C-BSR が他のインターフェースに設定された場合、この設定が前の設定に置き換わります。**

C-RP（candidate-RP の設定）

PIM-SM では、マルチキャストルーティング情報により構築された共用ツリーは RP がルートになっています。マルチキャストグループから RP へのマッピングがあります。マルチキャストグループは RP にマッピングされることが可能です。異なるグループを 1 つの RP にマッピング可能です。

はじめに Privileged Exec モードに移行し、次の手順で C-RP を設定します。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**ip pim rp-candidate** *interface-id* **[priority** *priority***]**	C-RP を設定します。初期設定の priority は 0 です。priority は 0 ～ 255 の範囲で設定します。
手順 3	**exit**	Privileged Exec モードに戻ります。
手順 4	**show ip pim rp**	入力を確認します。
手順 5	**write**	（オプション）設定ファイルに入力を保存します。

RP を設定する場合、対象となるマルチキャストグループが設定されていない際は RP はすべてのマルチキャストグループに対して機能します。設定されている際は、対象となるマルチキャストグループは設定されている領域のマルチキャストグループです。バックボーンルータの C-RP を設定することを推奨します。

静的 RP の設定

静的 RP は動的 RP のバックアップとして機能し、ネットワークの堅牢性を向上します。

はじめに Privileged Exec モードに移行し、次の手順で静的 RP を設定します。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**ip pim rp-address set** *ip-address*	静的 RP を設定します。
手順 3	**exit**	Privileged Exec モードに戻ります。
手順 4	**show ip pim rp**	入力を確認します。
手順 5	**write**	（オプション）設定ファイルに入力を保存します。

静的 RP が使用されている場合、PIM ドメインのすべてのルータが同一の設定を採用しなくてはなりません。設定された静的 RP アドレスが稼動状態のローカルルータのインターフェースアドレスである場合、このルータは静的 RP として機能します。静的 RP として機能するインターフェースの PIM を有効に設定する必要はありません。

BSR メカニズムにより BSR から選定された RP が有効な場合、静的 RP は動作しません。

PIM ルータ問い合わせメッセージ間隔の変更

PIM ルータとマルチレイヤスイッチは PIM ルータクエリメッセージを送信し、どの機器が各 LAN セグメント（サブネット）の DR かを検出します。DR は直接接続している LAN に所属しているすべてのホストに IGMP ホストクエリメッセージを送信する責務を負っています。

PIM-SM の動作では、DR はマルチキャストの送信元に直接接続している機器です。DR は PIM 登録メッセージを送信し、送信元からのマルチキャストトラフィックを共有ツリーにフォワーディングされなくてはならないことを RP に通知します。この場合、DR は最も大きい IP アドレスを有する機器です。

はじめに Privileged Exec モードに移行し、次の手順でルータクエリメッセージ間隔の変更をおこないます。

この手順は必須ではありません。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**ip pim query-interval** *seconds*	スイッチが PIM ルータクエリメッセージを送信する頻度を設定します。（範囲：1 ～ 65535） 初期設定値：30 秒
手順 3	**exit**	Privileged Exec モードに戻ります。
手順 4	**show ip igmp interface** *interface-id*	入力を確認します。
手順 5	**write**	（オプション）設定ファイルに入力を保存します。

5.10 ACL

5.10.1 概要

パケットがフィルタリングされる前に一連の適合ルールを設定してパケットを認識する必要があります。パケットが指定したものとして識別された場合のみネットワークは対応する動作をおこない、事前に設定したポリシーに従ってフォワーディングの許可または拒否をおこないます。ACL（Access control list）はこれらの機能を達成することを目的にしています。

ACL は一連の適合ルール（送信元アドレス、デスティネーションアドレス、およびポート ID）を使用してパケットの識別をおこないます。ACL はスイッチでグローバルに、またスイッチがパケットのフォワーディングあるいは破棄をおこなう 1 つのポートのみで使用できます。

ACL で定義された適合ルールは、たとえば QoS ルールでのトラフィックのクラス分けの定義など、他の状況での異なるトラフィックへも取り込みができます。

ACL ルールには多くのサブルールを含むことができ、これにはパケットの異なるサイズを定義できます。適合順は、ACL の照合に含まれます。

5.10.2 ACL の設定

ACL の設定には次の項目があります。

- ACL の定義
- ACL の起動

設定手順は順番に実行することを推奨しますので、まず ACL を定義し、
最後に ACL を起動します。

ACL の定義

本機はいくつかの種類の ACL をサポートしており、本項でこれらについて説明します。次の手順に従って ACL を定義します。

（1）対応する ACL 設定モードを入力します。

（2）ACL サブルールを定義します。

[注意] ACL は起動後いつでも有効になります

- **ule コマンドを複数回使用し、ACL に対して複数のルールを定義できます。**
- **本機は、エグレス IP ACL またはエグレス MAC ACL の明示的な「deny any any」ルールをサポートしていません。**

はじめに Privileged Exec モードに移行し、次の手順で ACL を定義します。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**access-list ruleid** *rule-id* **[deny | permit] priority** *priority* [*port-list* **| default]**	対応する ACL 設定モードを入力します。rule-id の範囲は 1 ～ 999 です。priority の範囲は 0 ～ 8 で、8 が最高レベルです。port-list には、ルールを関連付けるポートメンバを、01m のようにポート番号に m を付けて指定します。 初期設定：すべてのポートを対象。
手順 3	**subset ip {any |** *source-add source-mask* } [*dst-add dst-mask*]	IP ACL ルールに基づく設定をおこないます。
手順 4	**subset mac {any |** *dst-mac***} {any |** *source-mac***}**	MAC ACL ルールに基づく設定をおこないます。
手順 5	**subset protocol {***type-number* **| igmp | ipinip | ospf | pim | icmp | tcp [src-port** *src-port* **| dst-port** *dst-port* **| established [src-port** *src-port* **| dst-port** *dst-port* **]] | udp [src-port** *src-port* **| dst-port** *dst-port* **]}**	プロトコル ACL ルールに基づく設定をおこないます。
手順 6	**subset vlan-id** *vlan-id*	VLAN ID ACL ルールに基づく設定をおこないます。
手順 7	**exit**	Privileged Exec モードに戻ります。
手順 8	**show access-list ruleid** *rule-id*	入力を確認します。
手順 9	**write**	（オプション）設定ファイルに入力を保存します。

ACL を削除

モード	コマンド
Grobal Configuration	**no access-list ruleid** *rule-id*

コマンドの属性

- source-add /dst-add：**送信元 / 宛先の** IP **アドレス** Any **を使用すると、どのアドレスにも一致します。**
- source-mask/dst-mask：**ルールの送信元 / 宛先アドレスがこのサブネットマスクに一致しなくてはならない。送信元 / 宛先** IP **アドレスがホストの場合、このマスクは** 255.255.255.255 **でなくてはならず、ネットワークアドレスの場合、マスクは対応するサブネットマスクでなくてはなりません。**
- source-mac/dst-mac：**送信元 / 宛先** MAC **アドレスで、**Any **を使用するとすべてのアドレスを含みます。**
- type-number：**特定のプロトコル番号（**0 ～ 255**）**
- source-port/dst-port：**指定したプロトコル種別の送信元 / 宛先のポート番号 （範囲：**0-65535)

ACL の起動

ACL **の設定をおこなったら、**ACL **を起動します。この設定によりこれらの** ACL **が起動し、ハードウェアによりフォワーディングされるパケットのフィルタリングと分類をおこないます。**

はじめに Privileged Exec **モードに移行し、次の手順で** ACL **を起動します。**

	コマンド	内容
手順 1	**config terminal**	Global configuration **モードに移行します。**
手順 2	**packet-filter enable ruleid** *rule-id*	ACL **を起動します。**
手順 3	**exit**	Privileged Exec **モードに戻ります。**
手順 4	**show access-list ruleid** *rule-id*	**入力を確認します。**
手順 5	**write**	**（オプション）設定ファイルに入力を保存します。**

ACL **の停止**

モード	コマンド
Grobal Configuration	**packet-filter disable ruleid** *rule-id*

5.10.3 デフォルト ACL の設定

ポートに ACL **を設定すると、システムは自動的にデフォルト** ACL **をポートに作成し、このデフォルト** ACL **ルールがあらゆるパケットを許可します。そのため、スイッチがポートへのすべてのパケットを拒否する必要がある場合、デフォルト** ACL **を手作業で設定する必要があります。**

はじめに Privileged Exec **モードに移行し、次の手順でデフォルト** ACL **を設定します。**

	コマンド	内容
手順 1	**config terminal**	Global configuration **モードに移行します。**
手順 2	**access-list default set** *port-list* **{deny | permit}**	**デフォルト** ACL **の設定をおこないます。**
手順 3	**exit**	Privileged Exec **モードに戻ります。**
手順 4	**show access-list default**	**入力を確認します。**
手順 5	**write**	**（オプション）設定ファイルに入力を保存します。**

5.10.4 ACL の設定例

ネットワーク要件

イントラネットは部門間で 100Mbps **ポートで接続しています。経理部のサーバはポート** 1 **（サブネットアドレス** 129.110.1.2**）を介して接続しています。正しい** ACL **設定により、** CEO **のオフィスからはこのサーバにアクセスできますが、他の部署はアクセスできません。**

ネットワーク構成図

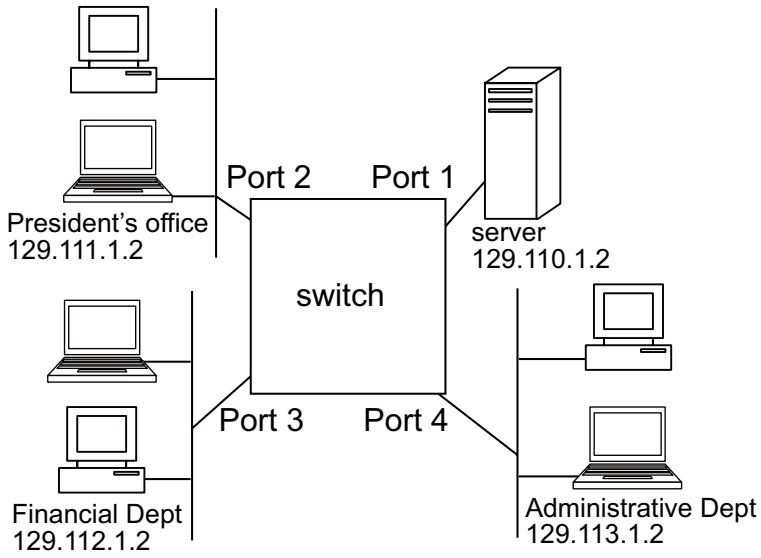


図 33　**高度な** ACL **を設定したネットワーク**

5.11 QoS

5.11.1 概要

CoS（Class of Service）を使用すると、輻輳時、トラフィックがスイッチにバッファリングされた場合、どのデータパケットがより高い優先順位を有するかを指定できます。本機は各ポートごとに 4 つのプライオリティキューを用いる CoS をサポートしています。ポートの高いプリオリティキューに置かれたデータパケットは、低いプライオリティキューのものより先に転送されます。各インターフェースに対するプライオリティの設定と、本機のプライオリティキューに対するフレームのプライオリティタグのマッピングの設定をおこなえます。

エグレスキューに対する CoS 値のマッピング

本機は、CoS（Class of Service）プライオリティタグトラフィックの処理を、各ポートで 8 つのプライオリティを使用し、サービスの実行はストリクトまたは WRR（Weighted Round Robin）に基づいて実行します。IEEE 802.1p では、最大 8 つの異なるトラフィックプライオリティを定義しています。次の表に示すように、初期設定のプライオリティレベルは、IEEE 802.1p 標準の勧告に準拠して割り当てられています。

エグレスキューのプライオリティマッピング

キュー	0	1	2	3	4	5	6	7
プライオリティ	0	1	2	3	4	5	6	7

IEEE 802.1p 標準で勧告された、異種ネットワークアプリケーションに対するプライオリティレベルを次の表に示します。

CoS プライオリティレベル

0	ベストエフォート型
1	バックグラウンド
2	（予備）
3	エクセレントフォート型
4	制御された負荷
5	動画（100 ミリ秒未満の遅延およびジッタ）
6	動画（10 ミリ秒未満の遅延およびジッタ）
7	ネットワーク制御

5.11.2 キューモードの設定

キューィングの実行に際し、高いプライオリティキューのすべてのトラフィックを低いプライオリティキューより先に処理するストリクトルールに基づいておこなうか、または各キューに対して相対的な重み付けを設定する WRR（Weighted Round-Robin）に基づいておこなうかを本機に対して設定できます。WRR はあらかじめ各キューに定義した相対的な重み付けを使用しますが、この相対的な重み付けはスイッチが次のキューに移る前に各キューに処理をおこなうサービスタイムの割合（%）を定義するものです。これにより、ストリクトプライオリティキューイングで発生しがちなヘッドオブラインブロッキング現象を回避します。

はじめに Privileged Exec モードに移行し、次の手順でキューモードを設定します。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**traffic-policy running-mode {strict-queue | weighted-queue }**	キューの実行モードを設定します。
手順 3	**exit**	Privileged Exec モードに戻ります。
手順 4	**show traffic-policy all**	入力を確認します。
手順 5	**write**	（オプション）設定ファイルに入力を保存します。

5.11.3 ポートプライオリティの設定

本機の各ポートに対し、ポートプライオリティを設定できます。本機に到達するタグなしパケットは指定したポートプライオリティでタグ付けされ、それから送信ポートの適切なプライオリティキューに並べ変えられます。
本機は各ポートごとに 4 つのプライオリティキューを提供します。WRR を使用してヘッドオブラインブロッキングの問題を回避します。
ポートで受信されたタグなしフレームにプライオリティが適用され、すべての種類のフレーム（タグなしおよびタグ付きの両方のフレームなど）が受信されるよう設定されます。このプライオリティは IEEE 802.1Q VLAN のタグ付きフレームには適用されません。IEEE 802.1Q VLAN のタグ付きフレームを受信した場合、IEEE 802.1p は User Priority ビットを使用します。
送信ポートが関連付けている VLAN のタグなしメンバの場合、転送前にこれらのフレームからすべての VLAN タグを除去します。
はじめに Privileged Exec モードでログインし、次の手順でポートプライオリティを設定します。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**traffic-policy link-group set** *group-id port -list* **local-precedence** *priority*	関連付けるグループを作成し、ポートプライオリティを設定します。（group-id の範囲：1 ～ 26）port-list には、ポートメンバを、01m のようにポート番号に m を付けて指定します。（priority の範囲：0 ～ 7）で、7 が最高の優先順位です。
手順 3	**traffic-policy link-group enable** *group-id*	トラフィックポリシーを有効にし、ポートプライオリティを設定します。
手順 4	**exit**	Privileged Exec モードに戻ります。
手順 5	**show traffic-policy all**	入力を確認します。
手順 6	**write**	（オプション）設定ファイルに入力を保存します。

関連付けるグループを削除

モード	コマンド
Grobal Configuration	**no traffic-policy link-group** *group-id*

トラフィックポリシーを無効に設定し、ポートプライオリティを設定

モード	コマンド
Grobal Configuration	**traffic-policy link-group disable** *group-id*

5.11.4 IP Precedence の設定

IPv4 ヘッダの ToS（Type of Service）オクテットには、ネットワーク制御パケット用の最高のプライオリティから通常のトラフィック用の最低のプライオリティを範囲とする、異なる 8 つのプライオリティレベルを定義する優先順位ビットを 3 ビット含みます。デフォルトの IP 優先順位値は、1 対 1 で CoS 値にマッピングされています（例：優先順位値 0 は CoS 値 0 にマッピングされている、など）。ビット 6 および 7 はネットワーク制御に使用され、他のビットは様々なアプリケーションの種類に使用されます。ToS ビットは次の表のように定義されています。

IP 優先順位のマッピング

プライオリティレベル	トラフィック種別
0	通常
1	プライオリティ
2	即時
3	瞬時
4	瞬時の上書き
5	重大
6	ネットワーク内制御
7	ネットワーク制御

はじめに Privileged Exec モードに移行し、次の手順で IP 優先順位を有効にしてローカルの優先順位とマッピングをおこないます。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**traffic-policy tos set default [** *port-list* **]**	IP 優先順位を、1 対 1 でポートのローカルの優先順位ポリシーとマッピングをおこないます。port-list には、ポートメンバを、01m のようにポート番号に m を付けて指定します。
手順 3	**traffic-policy tos enable**	IP 優先順位マッピングのトラフィックポリシーを有効にします。
手順 4	**exit**	Privileged Exec モードに戻ります。
手順 5	**show traffic-policy all**	入力を確認します。
手順 6	**write**	（オプション）設定ファイルに入力を保存します。

IP 優先順位マッピングのトラフィックポリシーの無効

モード	コマンド
Grobal Configuration	**traffic-policy tos disable**

5.11.5 ACL ルールに基づくプライオリティの変更

定義した ACL ルールと一致するフレームのトラフィックプライオリティの変更をおこなうことができます。

[注意] これら QoS 設定作業の実行前に、まず対応する ACL を定義しなくてはなりません。それから正しい ACL を軌道することにより、パケットフィルタリングを実行できます。

はじめに Privileged Exec モードに移行し、次の手順で ACL ルールに基づくプライオリティの変更をおこないます。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**traffic-policy acl-group set** *group-id* **access-list ruleid** *rule-id* **local-precedence** *precedence*	ACL ルールに基づくトラフィックポリシーを作成します。group-id：ACL ルールに基づくトラフィックポリシーのグループ ID。（範囲：0 ～ 999）precedence：範囲 0 ～ 7 で、7 が最高の優先順位です。
手順 3	**traffic-policy acl-group enable** *group-id*	ACL ルールに基づくトラフィックポリシーを有効にします。
手順 4	**exit**	Privileged Exec モードに戻ります。
手順 5	**show traffic-policy all**	入力を確認します。
手順 6	**write**	（オプション）設定ファイルに入力を保存します。

ACL ルールに基づくトラフィックポリシーの無効

モード	コマンド
Grobal Configuration	**traffic-policy acl-group disable** *group-id*

5.12 IEEE802.1x

5.12.1 概要

802.1x の概要

IEEE 802.1X はポートベースのネットワークアクセス制御プロトコルです。2001 年に IEEE がこれを発行し、関連のベンダーがこのプロトコルを LAN へのユーザアクセス認証時の標準プロトコルとして採用するよう提言しました。IEEE 802.1x は IEEE 802.11 標準、無線 LAN のユーザアクセスに関する標準に由来します。IEEE 802.1x の最初の目的は、無線 LAN におけるユーザアクセス認証を実現するというものでした。この方法は IEEE 802 標準に準拠しているすべての LAN に広く適用されるため、このプロトコルは無線 LAN の多くのアプリケーションを検出します。IEEE 802 標準に準拠している LAN では、ユーザは、LAN スイッチに類する LAN アクセス制御機器への接続によって、その LAN の機器へのアクセスとリソース共有が可能です。しかし、商業 LAN（典型的な例では商用ビルの LAN）や移動オフィスなどでは、LAN の提供者は一般にユーザアクセスの制御を望みます。これらの場合、上記に記載した「ポートベースのネットワークアクセス制御」送信者の要件になります。

名前が示すように、ポートベースのネットワークアクセス制御は LAN アクセス制御機器のポートにおける認証とすべてのアクセス機器の制御をおこなうことを意味します。ポートに接続しているユーザの機器は認証を通過できた場合、ユーザは LAN のリソースにアクセスできます。そうでない場合、ユーザは LAN のリソースにアクセスできません。これは、ユーザが物理的に切断していることと同じです。

IEEE 802.1x はポートベースのネットワークアクセス制御プロトコルを定義しており、アクセス機器とアクセスポートのポイントツーポイント接続のみを定義しています。ポートは物理的または論理的のいずれでも可能です。典型的なアプリケーション環境は次のとおりです。LAN スイッチの各物理ポートは 1 台のユーザワークステーション（物理ポートベース）および IEEE 802.11 標準（論理ポートベース）で定義された無線 LAN アクセス環境にのみ接続します。

802.1x システムの構造

IEEE 802.1x を使用するシステムは、典型的なクライアントサーバ型のシステムアーキテクチャです。次の図に示すように、このシステムは 3 つのエンティティを含みます。サプリカントシステム（Supplicant System）、オーセンティケータシステム（Authenticator System）、および認証サーバシステム（Authentication Sever System）です。

LAN アクセス制御機器は、IEEE 802.1x のオーセンティケータシステムを提供する必要があります。コンピュータなどのユーザ側機器には、IEEE 802.1x クライアントサポートソフトウェア（Microsoft Windows XP の IEEE 802.1x クライアントなど）をインストールする必要があります。IEEE 802.1x 認証サーバシステムは通常通信事業者の AAA センターに配置されます。

オーセンティケータおよび認証サーバは EAP（Extensible Authentication Protocol）フレームで情報を交換します。サプリカントとオーセンティケータは、IEEE 802.1x で定義している EAPoL（Extensible Authentication Protocol over LAN）フレームで情報を交換します。認証データは、複雑なネットワークを通って認証サーバに到達するよう、EAP フレームでカプセル化され、これがさらに他の AAA 上位レイヤプロトコルパケット（RADIUS など）でカプセル化されます。この手順を EAP リレーと呼びます。

オーセンティケータには 2 種類のポートがあります。1 つは無制限ポート、もう 1 つは制限ポートです。無制限ポートは常に双方向の接続状態にあります。ユーザはいつでもこのポートを経由してネットワークリソースへのアクセスと共用をおこなうことができます。制限ポートはユーザが認証を通過した場合のみ接続状態になります。その後、ユーザはネットワークリソースへのアクセスが許可されます。

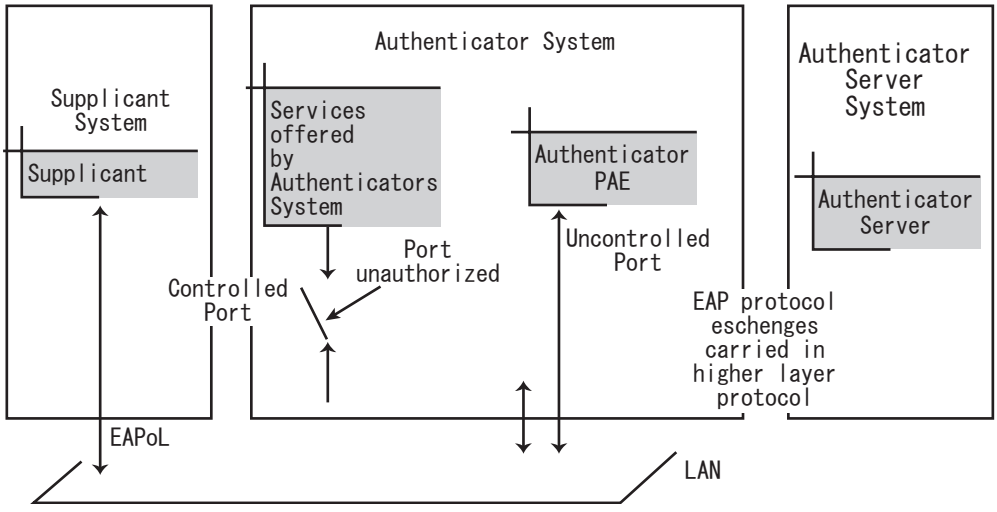


図 34　IEEE 802.1x システムアーキテクチャ

802.1x 認証プロセス

IEEE 802.1x は EAP フレームを設定して認証情報を伝達します。この規格では次の種類の EAP フレームを定義しています。

- EAP パケット：認証情報を伝達するために使用される、認証情報フレーム
- EAPoL-Start：サプリカントによって自発的に発信される、認証発信フレーム
- EAPoL-Logoff：認証状態を自発的に終了する、ログオフ要求フレーム
- EAPoL-Key：EAP パケットの暗号化をサポートする、キー情報フレーム
- EAPoL-Encapsulated-ASF-Alert：ASF（Alert Standard Forum）の警告メッセージをサポート

EAPoL-Start、EAPoL-Logoff および EAPoL-Key は、サプリカントとオーセンティケータとの間でのみ存在します。EAP パケット情報はオーセンティケータのシステムで再カプセル化され、認証サーバシステムへ転送されます。EAPoL-Encapsulated-ASF-Alert はネットワーク管理情報に関連し、オーセンティケータによって終了されます。

IEEE 802.1x はユーザ ID による認証ソリューションを実装しています。しかし、IEEE 802.1x 自身のみではこの理論の実装に十分ではありません。IEEE 802.1x でユーザ ID 認証を実装するようにするには、アクセス機器の管理者は RADIUS やローカルの認証に関する設定をおこなう必要があります。

イーサネットスイッチの 802.1x 実装

本機は、IEEE 802.1x で規定しているポートアクセス認証方法のみならず、次のように IEEE 802.1x を拡張、最適化しています。

- 物理ポートを経由したダウンストリームにおいて、複数の終端局への接続をサポート
- MAC アドレスに基づくアクセス制御（ユーザ認証方式）

このように、システムのセキュリティが高まり、管理が簡単になります。

5.12.2 802.1x の設定

IEEE 802.1x の設定には次の項目があります。

- IEEE 802.1x の有効 / 無効
- ポート認証状態の設定
- 各ポートを経由するユーザの最大数

802.1x の有効 / 無効

次のコマンドで、IEEE 802.1x のグローバルな有効 / 無効を設定します。

はじめに Privileged Exec モードに移行し、次の手順で IEEE 802.1x の有効 / 無効を設定します。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**dot1x system-auth-control enable**	IEEE 802.1x を有効に設定します。
手順 3	**exit**	Privileged Exec モードに戻ります。
手順 4	**show dot1x system-auth-control**	入力を確認します。
手順 5	**write**	（オプション）設定ファイルに入力を保存します。

IEEE 802.1x を無効に設定

モード	コマンド
Grobal Configuration	**dot1x system-auth-control disable**

ポート認証状態の設定

次のコマンドで、ポート認証状態を設定します。

はじめに Privileged Exec モードでログインし、次の手順でポート認証状態を設定します。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**dot1x ports** *port-list*	ポート認証状態を設定します。 port-list：ポート番号に m（ポートメンバ） または -（ポートメンバ外）を付けて指定します。
手順 3	**exit**	Privileged Exec モードに戻ります。
手順 4	**show dot1x ports**	入力を確認します。
手順 5	**write**	（オプション）設定ファイルに入力を保存します。

各ポートを経由するユーザの最大数

次のコマンドを使用し、IEEE 802.1x によって許可される、指定したポートに対するユーザ数を設定します。ポートが設定されていない場合、すべてのポートが同じ数のサプリカントを許可します。

はじめに Privileged Exec モードに移行し、次の手順で各ポートの最大ユーザ数を設定します。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**dot1x multiple-host-num** *number*	各ポートを経由する最大ユーザ数を設定します。（範囲：1 ～ 256）
手順 3	**exit**	Privileged Exec モードに戻ります。
手順 4	**show dot1x ports**	入力を確認します。
手順 5	**write**	（オプション）設定ファイルに入力を保存します。

5.12.3 802.1x の設定例

ネットワーク要件

下図に示すように、ユーザのワークステーションがスイッチのポート 1 に接続しています。

スイッチの管理者は IEEE 802.1x をすべてのポートに有効に設定し、サプリカントの認証をおこなってインターネットへのアクセスを制御します。アクセス制御モードは MAC アドレスに基づくように設定します。

サーバグループは 2 台の RADIUS サーバ、それぞれ 10.11.1.1 および 10.11.1.2 により構成され、スイッチに接続しています。前者のサーバは認証 / アカウンティングのプライマリサーバとして機能します。後者のサーバは認証 / アカウンティングのセカンダリサーバとして機能します。システムが RADIUS サーバとパケットを交換する場合の暗号鍵は「test」で設定します。

システムには、RADIUS サーバへのリアルタイムのアカウンティングパケットを 15 分間隔で転送するよう設定します。

ローカルの IEEE 802.1x アクセスユーザのユーザ名は local user でパスワードは local pass（プレーンテキストでの入力）です。

ネットワーク構成図

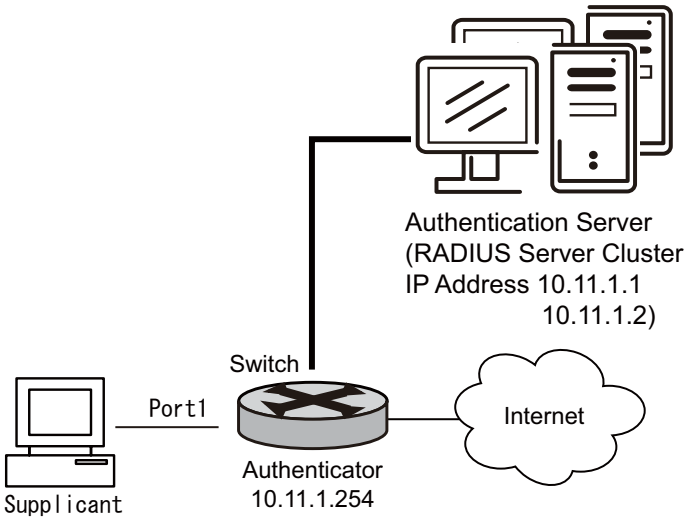


図 35　サプリカントで AAA を実行するよう IEEE 802.1x と RADIUS を有効化

設定手順

[注意]　次の例は、ほとんどの RADIUS 設定コマンドに関係しています。詳細については、RADIUS プロトコルの設定の章を参照してください。

IEEE 802.1x **を設定します。**

```
switch(config)#dot1x system-auth-control enable
switch(config)#dot1x ports 01m
```

RADIUS **クライアントサービスを設定します。**

```
switch(config)#radiusclient ipaddress 10.1.1.254
switch(config)#radiusclient service enable
switch(config)#radiusclient accounting interval 1
```

RADIUS **サーバを設定します。**

```
switch(config)#radiusserver master_ipaddress 10.1.1.1
switch(config)#radiusserver slave_ipaddress 10.1.1.2
switch(config)#radiusserver master_port 1812 1813
switch(config)#radiusserver slave_port 1812 1813
switch(config)#radiusserver master_key test
switch(config)#radiusserver slave_key test
```

5.13 RADIUS プロトコル

5.13.1 概要

RADIUS とは？

RADIUS（Remote Authentication Dial-In User Service）は、クライアントサーバアーキテクチャにおける一種の分散情報転送プロトコルです。RADIUS によりネットワークが非認証アクセスによる割り込みを回避でき、RADIUS は高いセキュリティとリモートアクセス管理の両方を必要とするネットワーク環境でしばしば使用されます。たとえば、シリアルポートとモデムを使用している、多くの、また分散したダイヤルアップユーザの管理にしばしば使用されます。RADIUS システムは NAS（Network Access Server）の補足的な部分で重要です。

RADIUS システムを起動すると、ユーザが NAS（公衆交換電話網環境の場合のダイヤルアップアクセスサーバ、イーサネット環境の場合のイーサネットスイッチ）経由での接続で他のネットワークへのアクセス権やネットワークリソースの使用権を得たい場合、NAS（つまり RADIUS クライアントの終端）はユーザの AAA リクエストを RADIUS サーバに送信します。RADIUS サーバには、すべてのユーザ認証情報とネットワークサービスアクセス情報が登録されているユーザデータベースがあります。NAS からユーザリクエストを受信すると、RADIUS サーバはユーザデータベースへの問い合わせと更新を通じて AAA を実行し、NAS へ設定情報とアカウンティングデータを返します。ここで、NAS はサプリカントおよび対応する接続を制御し、一方 RADIUS プロトコルはどのように設定アカウンティング情報を NAS と RADIUS 間で転送するか調整をおこないます。

NAS と RADIUS はこの情報を UDP パケットで交換します。この相互交換時、ユーザ設定情報（パスワードなど）を送信する前に、両側でキーによりパケットを暗号化して傍受や盗み見を回避します。

RADIUS の動作

RADIUS サーバは、通常、アクセスサーバに類する機器のプロキシ機能を使用してユーザ認証を実行します。動作のプロセスは次のようになっています。まず、ユーザが RADIUS サーバにリクエストメッセージ（ユーザ名と暗号化されたパスワードを含みます）を送信します。次に、ユーザは RADIUS サーバから様々な種類の応答メッセージを受信しますが、ACCEPT メッセージはユーザが認証を通過したことを示し、REJECT メッセージはユーザが認証を通過できなかったためユーザ名とパスワードを再度入力する必要があり、そうしない場合はアクセスを拒否することを示します。

5.13.2 イーサネットスイッチへの RADIUS 実装

ここまでで上記に示した RADIUS の枠組みと、ユーザアクセス機器あるいは NAS として機能する本機は、RADIUS クライアントの終端であることを理解しました。つまり、RADIUS クライアント機能を本機に実装することになります。

5.13.3 RADIUS プロトコルの設定

RADIUS プロトコルの設定には次の項目があります。

- RADIUS クライアントサービスの有効 / 無効の設定
- RADUS クライアントの IP アドレス設定
- リアルタイムアカウンティングの設定
- RADIUS サーバの IP アドレス設定
- RADIUS サーバのポート設定
- RADIUS パケット暗号鍵の設定

RADIUS クライアントサービスの有効 / 無効

はじめに Privileged Exec モードに移行し、次の手順で RADIUS クライアントサービスを有効に設定します。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**radiusclient service enable**	RADIUS クライアントサービスを有効に設定します。
手順 3	**exit**	Privileged Exec モードに戻ります。
手順 4	**show radiusclient service**	入力を確認します。
手順 5	**write**	（オプション）設定ファイルに入力を保存します。

RADIUS クライアントサービスを無効に設定

モード	コマンド
Grobal Configuration	**radiusclient service disable**

RADIUS クライアントの IP アドレス設定

はじめに Privileged Exec モードに移行し、次の手順で RADIUS クライアントの IP アドレスを設定します。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**radiusclient ipaddress** *ip-address*	RADUS クライアントの IP アドレスを設定します。ip-address は VLAN インターフェースの IP アドレスです。
手順 3	**exit**	Privileged Exec モードに戻ります。
手順 4	**show radiusclient ipaddress**	入力を確認します。
手順 5	**write**	（オプション）設定ファイルに入力を保存します。

リアルタイムアカウンティングの設定

アルタイムアカウンティング機能を実装するには、リアルタイムアカウンティング間隔の設定が必要です。この属性を設定したあと、NAS は接続中ユーザのアカウンティング情報を RADIUS サーバに定期的に送信します。

次のコマンドを使用し、リアルタイムアカウンティング間隔を設定します。

はじめに Privileged Exec モードに移行し、次の手順でリアルタイムアカウンティング間隔を設定します。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**radiusclient accounting interval** *minutes*	リアルタイムアカウンティング間隔を設定します。minutes は RADIUS サーバと同じ値を設定します。minutes に 0 を設定した場合、RADIUS クライアントは更新メッセージを RADIUS サーバへ送信しません。
手順 3	**exit**	Privileged Exec モードに戻ります。
手順 4	**show radiusclient accounting interval**	入力を確認します。
手順 5	**write**	（オプション）設定ファイルに入力を保存します。

RADIUS サーバの IP アドレス設定

プライマリ / セカンダリ、認証 / 承認サーバとアカウンティングサーバなど、RADIUS サーバの IP アドレスを設定します。

次のコマンドを使用し、RADIUS サーバの IP アドレスを設定します。

はじめに Privileged Exec モードに移行し、次の手順で RADIUS サーバの IP アドレスを設定します。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**radiusserver master_ipaddress** *ip-address*	RADIUS サーバ（プライマリ）の IP アドレスを設定します。 初期設定：プライマリ / セカンダリ、認証 / 承認・アカウンティングサーバすべての IP アドレスは 0.0.0.0
手順 3	**radiusserver slave_ipaddress** *ip-address*	（オプション）RADIUS サーバ（セカンダリ）の IP アドレスを設定します。
手順 4	**show radiusserver master_ipaddress**	入力を確認します。
手順 5	**show radiusclient accounting interval**	入力を確認します。
手順 6	**write**	（オプション）設定ファイルに入力を保存します。

RADIUS サーバのポート設定

プライマリ / セカンダリ、認証 / 承認サーバとアカウンティングサーバなど、RADIUS サーバのポートを設定します。

次のコマンドを使用し、RADIUS サーバのポート番号を設定します。

はじめに Privileged Exec モードに移行し、次の手順で RADIUS サーバのポートを設定します。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**radiusserver master_port** *authentication-port account-port*	RADIUS サーバ（プライマリ）のポートを設定します。ポートは更新メッセージを RADIUS サーバへ送信しません。
手順 3	**radiusserver slave_port** *authentication-port account-port*	（オプション）RADIUS サーバ（セカンダリ）のポートを設定します。
手順 4	**show radiusserver master_port**	入力を確認します。
手順 5	**show radiusserver slave_port**	入力を確認します。
手順 6	**write**	（オプション）設定ファイルに入力を保存します。

RADIUS パケット暗号鍵の設定

RADIUS クライアント（本機）と RADIUS サーバは MD5 アルゴリズムを使用し、交換するパケットの暗号化をおこないます。暗号鍵を設定し、両端がパケットを検証します。この鍵の同一性を確認できた場合のみ、両端はパケットを互いに受信し、応答します。

次のコマンドを使用し、RADIUS パケットの暗号鍵を設定します。

はじめに Privileged Exec モードに移行し、次の手順で RADIUS パケットの暗号鍵を設定します。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**radiusserver master_key** *string*	RADIUS サーバ（プライマリ）の暗号鍵を設定します。初期設定：RADIUS 認証 / 承認、アカウンティングパケットすべての鍵は「test」
手順 3	**radiusserver slave_key** *string*	（オプション）RADIUS サーバ（セカンダリ）の暗号鍵を設定します。
手順 4	**show radiusserver master_key**	入力を確認します。
手順 5	**show radiusserver slave_key**	入力を確認します。
手順 6	**write**	（オプション）設定ファイルに入力を保存します。

5.13.4 RADIUS プロトコルの設定例

RADIUS プロトコルと IEEE 802.1x プロトコルとを両方含む設定例について、P150 「 サプリカントで AAA を実行するよう IEEE 802.1x と RADIUS を有効化」を参照してください。

5.14 DHCP プロトコル

本章では、本機に対する DHCP サーバおよび DHCP リレー機能の設定方法について解説します。

5.14.1 DHCP リレーの設定

DHCP リレーの概要

ネットワークが拡大してネットワークの複雑さがひどくなると、ネットワークの設定がさらに複雑になります。DHCP（Dynamic Host Configuration Protocol）は、コンピュータが頻繁に移動されるような場所、あるいはホスト数が割り当てられている IP アドレスを超過するような場所でのユーザのネットワークへの高速なアクセスとログアウト、および IP アドレス使用の向上を目的として発行されました。DHCP はクライアントサーバ型で動作します。このプロトコルを使用すると、DHCP クライアントは動的に設定情報をリクエストし、DHCP サーバはこの情報をクライアントの便利性のために設定することができます。

初期においては、DHCP はこのような場合にのみ使用されていたので、DHCP クライアントと DHCP サーバが同一のサブネットに配置され、ネットワークセグメントをまたいだ動作はできませんでした。この初期の DHCP を使用してホストの設定を動的におこなう場合、各サブネットごとに DHCP サーバを配置しなくてはならず、これでは非常に不経済です。DHCP リレーの導入によりこの問題が解決されます。DHCP リレーは異なるサブネットに配置されている DHCP クライアントと DHCP サーバの間を中継します。DHCP パケットは、ネットワークを越えて、デスティネーション DHCP サーバ（クライアント）に中継することができます。その結果、異なるネットワークの DHCP クライアントが同じ DHCP サーバを使用できます。これは集中化された管理において経済的で便利な方法です。

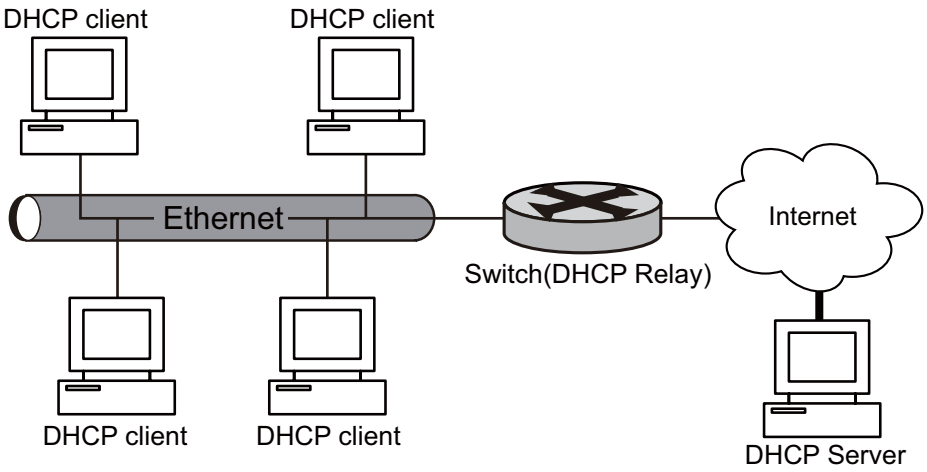


図 36　DHCP リレーの典型的なアプリケーション

DHCP リレーは次の法則に基づき動作します。

- 起動時と DHCP の初期化時には、DHCP クライアントはローカルネットワークに対して設定リクエストメッセージを広告します。
- ローカルネットワークに DHCP サーバが存在する場合、DHCP リレーが不要であることを知らせる DHCP 設定ディレクトリを送信できます。
- そうでない場合、ローカルネットワークに接続しており DHCP リレーを有効に設定している機器がこのメッセージを受信すると、必要な処理をおこない、指定した他のネットワーク上の DHCP サーバにこのメッセージをフォワーディングします。
- DHCP サーバは、DHCP クライアントからの情報に従って設定をおこない、DHCP リレー経由で設定結果を DHCP クライアントに送信します。

実際には、DHCP クライアントを動的に設定するには、数回の相互動作が必要な場合があります。

DHCP リレーの設定

DHCP リレーの設定には次の項目があります。

● DHCP パケットフォワーディングのための VLAN インターフェース設定
● DHCP サーバの IP アドレス設定
● DHCP リレーサービスの有効 / 無効を設定

DHCP パケットフォワーディングのための VLAN インターフェース設定

はじめに Privileged Exec モードに移行し、次の手順で DHCP パケットをフォワーディングする VLAN インターフェースを設定します。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**dhcpr listen add** *index vlan-interface*	DHCP パケットのフォワーディングのための、VLAN インターフェースを設定します。vlan-interface は vint にインターフェース番号を付けて設定します。
手順 3	**exit**	Privileged Exec モードに戻ります。
手順 4	**show dhcpr listen**	入力を確認します。
手順 5	**write**	（オプション）設定ファイルに入力を保存します。

DHCP パケットフォワーディングのための VLAN インターフェースの削除

モード	コマンド
Grobal Configuration	**dhcpr listen delete** *index*

DHCP サーバの IP アドレスの設定

はじめに Privileged Exec **モードに移行し、次の手順で** DHCP **サーバの** IP **アドレスを設定します。**

	コマンド	内容
手順 1	**config terminal**	Global configuration **モードに移行します。**
手順 2	**dhcpr targetip add** *index server-ipaddress*	DHCP **サーバの** IP **アドレスを設定します。**
手順 3	**exit**	Privileged Exec **モードに戻ります。**
手順 4	**show dhcpr targetip**	**入力を確認します。**
手順 5	**write**	**（オプション）設定ファイルに入力を保存します。**

DHCP サーバの IP アドレスの削除

モード	コマンド
Grobal Configuration	**dhcpr targetip del** *index*

DHCP リレーサービスの有効 / 無効を設定

はじめに Privileged Exec **モードに移行し、次の手順で** DHCP **リレーサービスを有効に設定します。**

	コマンド	内容
手順 1	**config terminal**	Global configuration **モードに移行します。**
手順 2	**dhcpr service enable**	DHCP **リレーサービスの有効 / 無効を設定します。**
手順 3	**exit**	Privileged Exec **モードに戻ります。**
手順 4	**show dhcpr service**	**入力を確認します。**
手順 5	**write**	**（オプション）設定ファイルに入力を保存します。**

DHCP リレーサービスを無効に設定

モード	コマンド
Grobal Configuration	**dhcpr service disable**

DHCP サーバの設定

DHCP サーバの設定には次の項目があります。

- DHCP パケットフォワーディングのための VLAN インターフェース設定
- DHCP サーバサービスの有効 / 無効を設定
- IP アドレスプールの追加
- DHCP サーバの DNS 設定（オプション）
- DHCP サーバのリースタイム設定（オプション）

DHCP パケットフォワーディングのための VLAN インターフェース設定

はじめに Privileged Exec **モードに移行し、次の手順で** DHCP **パケットをフォワーディングする** VLAN **インターフェースを設定します。**

	コマンド	内容
手順 1	**config terminal**	Global configuration **モードに移行します。**
手順 2	**dhcps listen add** *index vlan-interface*	DHCP **パケットのフォワーディングのための、**VLAN **インターフェースの設定** vlan-interface **は** vint **にインターフェース番号を付けて設定します。**
手順 3	**exit**	Privileged Exec **モードに戻ります。**
手順 4	**show dhcpr listen**	**入力を確認します。**
手順 5	**write**	**（オプション）設定ファイルに入力を保存します。**

DHCP **パケットフォワーディングのための** VLAN **インターフェースの削除**

モード	コマンド
Grobal Configuration	**dhcps listen delete** *index*

DHCP サーバサービスの有効 / 無効を設定

はじめに Privileged Exec **モードに移行し、次の手順で** DHCP **サーバサービスを有効に設定します。**

	コマンド	内容
手順 1	**config terminal**	Global configuration **モードに移行します。**
手順 2	**dhcps service enable**	DHCP **サーバサービスを有効に設定します。**
手順 3	**exit**	Privileged Exec **モードに戻ります。**
手順 4	**show dhcpr service**	**入力を確認します。**
手順 5	**write**	**（オプション）設定ファイルに入力を保存します。**

DHCP **サーバサービスの無効**

モード	コマンド
Grobal Configuration	**dhcps service disable**

IP アドレスプールの追加

はじめに Privileged Exec **モードに移行し、次の手順で** IP **アドレスプールを追加します。**

	コマンド	内容
手順 1	**config terminal**	Global configuration **モードに移行します。**
手順 2	**dhcps addresspool add** *name start-ip end-ip gate-way net-mask* **[dns1** *dns1-ip* **| dns2** *dns2-ip* **|leasetime** *seconds* **| parameters** *string***]**	IP **アドレスプールを設定します。**
手順 3	**exit**	Privileged Exec **モードに戻ります。**
手順 4	**show dhcps addresspool**	**入力を確認します。**
手順 5	**write**	**（オプション）設定ファイルに入力を保存します。**

IP アドレスプールの削除

モード	コマンド
Grobal Configuration	**dhcps addresspool del name**

DHCP サーバの DNS 設定（オプション）

はじめに Privileged Exec **モードに移行し、次の手順で** DHCP **サーバの** DNS **を設定します。**

	コマンド	内容
手順 1	**config terminal**	Global configuration **モードに移行します。**
手順 2	**dhcps dns** *dns-ip*	DHCP **サーバの** DNS **を設定します。**
手順 3	**exit**	Privileged Exec **モードに戻ります。**
手順 4	**show dhcps dns**	**入力を確認します。**
手順 5	**write**	**（オプション）設定ファイルに入力を保存します。**

DHCP サーバのリースタイム設定（オプション）

はじめに Privileged Exec **モードに移行し、次の手順で** DHCP **サーバのリースタイムを設定します。**

	コマンド	内容
手順 1	**config terminal**	Global configuration **モードに移行します。**
手順 2	**dhcps leasetime** *seconds*	DHCP **サーバのリースタイムを設定します。** **初期設定：**691200**（秒）**
手順 3	**exit**	Privileged Exec **モードに戻ります。**
手順 4	**show dhcps dns**	**入力を確認します。**
手順 5	**write**	**（オプション）設定ファイルに入力を保存します。**

5.14.2 DHCP スヌーピングの設定

DHCP スヌーピングの概要

DHCP スヌーピングは、DHCP snooping biding テーブルという binding データベースを作成し、信頼できない DHCP メッセージをフィルタする、DHCP セキュリティ機能です。

DHCP スヌーピングは、DHCP Server と信頼できないクライアント間で、ファイアーウォールのような動作をします。

DHCP スヌーピングを使用して信頼できない（untrusted）インタフェースに接続されているエンドユーザと、信頼できる（trusted）インタフェースに接続されている DHCP サーバや他のスイッチからの DHCP パケットを区別することが可能です。

[注意] DHCP スヌーピングが適切に機能するために、すべての DHCP サーバは信頼できる（trusted）インタフェースを通してスイッチに接続してください。

untrusted なメッセージとは、ネットワークまたはファイアーウォールの外から受信したメッセージをいいます。例えば DHCP スヌーピングをサービスプロバイダ環境で使用した場合、untrusted なメッセージはカスタマースイッチなど、サービスプロバイダネットワークの外部にあるデバイスから送信されたことを意味します。不明なデバイスから送信されたメッセージは攻撃の原因になる可能性があるため信頼されません。

DHCP スヌーピングの binding データベースには、MAC アドレス、IP アドレスリース期間、binding タイプ、VLAN 番号、untrusted なインタフェースの情報が含まれています。trusted なインタフェースと接続されているホストに関する情報は含まれません。サービスプロバイダネットワーク内の trusted なインタフェースとは、同じネットワーク内にあるデバイスと接続されているポートを指します。

スイッチが untrusted なインタフェースでパケットを受信し、そのインタフェースで DHCP スヌーピングが有効になっている VLAN に属している場合、スイッチは送信元の MAC アドレスと DHCP クライアントの MAC アドレスを比較します。アドレスがマッチした場合、スイッチはパケットを転送します。もしアドレスが不一致の場合、スイッチはパケットをドロップします。

スイッチが DHCP パケットをドロップするのは、以下の条件の中の内どれか 1 つでも当てはまる場合です。

- DHCP サーバから出されるパケット（DHCPOFFER、DHCPACK、DHCPNAC、DHCPLEASEQUERY）を外部のネットワークから受信した場合
- untrusted なインタフェースでパケットが受信され、送信元 MAC アドレスと DHCP クライアントの MAC アドレスが一致しない場合
- スイッチが DHCPRELESE、DHCPDECLINE ブロードキャストメッセージを受信し 、それらのメッセージの MAC アドレスが DHCP スヌーピング binding テーブルに 存在するが、受信したインタフェースの情報がマッチしない場合
- DHCP Relay Agent が relay-agent IP アドレスが 0.0.0.0 でないものを含む DHCP パケットを転送する場合

DHCP スヌーピング設定ガイドライン

スイッチが L 2 VLAN で構成されている場合、DHCP スヌーピング機能のみ有効にすることができます（L2 DHCP Snooping）この場合、DHCP リレーまたは DHCP サーバ機能を設定する必要はありません。
もしスイッチが L3 インターフェースで構成されている場合、DHCP スヌーピング（L3 DHCP スヌーピング）を有効にする前に、DHCP リレー または DHCP サーバ機能を設定してください。

[注意] L2 DHCP スヌーピングと L3 DHCP スヌーピングは同時に機能させることができないことにもご注意ください。

L2 DHCP スヌーピング設定ガイドライン

L2 DHCP スヌーピングの設定ガイドラインは以下になります。

- スイッチでは、DHCP スヌーピングをグローバルに有効にする必要があります。
- ユーザーポートの指定と同じように、ポートで DHCP スヌーピングを有効にします。(untrusted ポート)
- サーバーポートを指定します。(trusted ポート)

L3 DHCP スヌーピング設定ガイドライン

L3 DHCP スヌーピングの設定ガイドラインは以下になります。

- スイッチでは、DHCP スヌーピングをグローバルに有効にする必要があります。
- ユーザーポートの指定と同じように、ポートで DHCP スヌーピングを有効にします。(untrusted ポート)
- L3 DHCP を可能にする前に、DHCP リレーまたは DHCP サーバ機能を設定する必要があります。

L2 DHCP スヌーピングの設定

L2 DHCP スヌーピングの設定には次の項目があります。

- スイッチの L2 DHCP スヌーピング有効 / 無効設定
- ユーザーポートの指定
- サーバーポートの指定

スイッチの L2 DHCP スヌーピング有効 / 無効設定

はじめに Privileged Exec モードに移行し、次の手順で L2 DHCP スヌーピングを設定します。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**dhcp-snooping layer2 service enable**	L2 DHCP スヌーピングを有効にします。
手順 3	**exit**	Privileged Exec モードに戻ります。
手順 4	**show dhcp-snooping layer2 service**	入力を確認します。
手順 5	**write**	（オプション）設定ファイルに入力を保存します。

L2 DHCP スヌーピングを無効にする。

モード	コマンド
Grobal Configuration	**dhcp-snooping layer2 service disable**

ユーザーポートの指定

はじめに Privileged Exec モードに移行し、次の手順で L2 DHCP スヌーピングのユーザーポートを設定します。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**dhcp-snooping layer2 user-ports** *port-list*	ユーザーポートを指定します。（untrusted ポート） *port-list* はポート番号 +"**m**/- " で指定します。 （"m" はメンバーポート、"-" は非メンバーポート）
手順 3	**exit**	Privileged Exec モードに戻ります。
手順 4	**show dhc-snooping layer2 user-ports**	入力を確認します。
手順 5	**write**	（オプション）設定ファイルに入力を保存します。

サーバーポートの指定

はじめに Privileged Exec **モードに移行し、次の手順で** L2 DHCP **スヌーピングのサーバーポートを設定します。**

	コマンド	内容
手順 1	**config terminal**	Global configuration **モードに移行します。**
手順 2	**dhcp-snooping layer2 server-ports** *port-list*	**サーバーポートを指定します。**（trusted **ポート**） *port-list* **はポート番号** +"**m**/- **" で指定します。** （"m" **はメンバーポート、**"-" **は非メンバーポート**）
手順 3	**exit**	Privileged Exec **モードに戻ります。**
手順 4	**show dhc-snooping layer2 server-ports**	**入力を確認します。**
手順 5	**write**	**（オプション）設定ファイルに入力を保存します。**

L3 DHCP スヌーピングの設定

L2 DHCP スヌーピングの設定には次の項目があります。

- スイッチの L3 DHCP スヌーピング有効 / 無効設定
- ユーザーポートの指定

スイッチの L3 DHCP スヌーピング有効 / 無効設定

はじめに Privileged Exec モードに移行し、次の手順で L3DHCP スヌーピングを設定します。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**dhcp-snooping layer3 service enable**	L3 DHCP スヌーピングを有効にします。
手順 3	**exit**	Privileged Exec モードに戻ります。
手順 4	**show dhcp-snooping layer3 service**	入力を確認します。
手順 5	**write**	（オプション）設定ファイルに入力を保存します。

L3 DHCP スヌーピングを無効にする。

モード	コマンド
Grobal Configuration	**dhcp-snooping layer3 service disable**

ユーザーポートの指定

はじめに Privileged Exec モードに移行し、次の手順で L3 DHCP スヌーピングのユーザーポートを設定します。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**dhcp-snooping layer3 user-ports** *port-list*	ユーザーポートを指定します。（untrusted ポート） *port-list* はポート番号 +"**m**/- " で指定します。 （"m" はメンバーポート、"-" は非メンバーポート）
手順 3	**exit**	Privileged Exec モードに戻ります。
手順 4	**show dhc-snooping layer3 user-ports**	入力を確認します。
手順 5	**write**	（オプション）設定ファイルに入力を保存します。

DHCP スヌーピングの表示

前項の設定を行った後、いずれかのコマンドモードで show **コマンドを実行し、実行中の** L2 DHCP **スヌーピングまたは** L3 DHCP **スヌーピング設定内容を確認してください。**

DHCP **スヌーピングの表示とデバッグ**

コマンド	オペレーション
Display L2 DHCP Snooping global state	L2 DHCP **スヌーピングの設定情報を表示。**
Display untrusted port for L2 DHCP Snooping	L2 DHCP **スヌーピングの** untrusted **ポートを表示。**
Display trusted port fof L2 DHCP Snooping	L2 DHCP **スヌーピングの** trusted **ポートを表示。**
Display L2 DHCP Snooping binding database	L2 DHCP **スヌーピングの** binding **データベースを表示。**
Display L3 DHCP Snooping global state	L3 DHCP **スヌーピングの設定情報を表示。**
Display untrusted port for L3 DHCP Snooping	L3 DHCP **スヌーピングの** untrusted **ポートを表示。**
Display L3 DHCP Snooping binding database	L3 DHCP **スヌーピングの** binding **データベースを表示。**

5.14.3 DHCP の設定例

DHCP リレーの設定例

ネットワーク要件

DHCP クライアントのセグメントのアドレスは、10.110.0.0 で、スイッチの VLAN2 に所属しているポートに接続されています。DHCP サーバの IP アドレスは、202.38.1.2 です。DHCP パケットは DHCP リレーを有効に設定しているスイッチ経由でフォワーディングされます。DHCP クライアントは、IP アドレスや他の設定情報を DHCP サーバから取得できます。

ネットワーク構成図

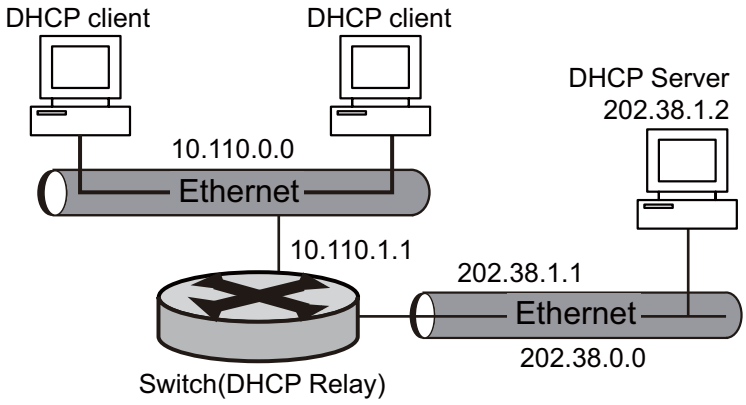


図 37　DHCP リレーを設定しているネットワーク構成図

設定手順

VLAN を設定し、VLAN の IP アドレスを設定します。

```
switch(config)#vlan static set vid 1 01-
switch(config)#vlan static add vid 2 01u
switch(config)#vlan port pvid 1 2
switch(config)#ip address add vint 1 202.38.1.1 255.255.255.0 vid 1
switch(config)#ip address add vint 2 10.110.1.1 255.255.255.0 vid 2
```

DHCP リレーを設定します。

```
switch(config)#dhcpr listen add 1 vint1
switch(config)#dhcpr listen add 2 vint2
switch(config)#dhcpr targetip add 1 202.38.1.2
switch(config)#dhcpr service enable
```

DHCP サーバの設定例

ネットワーク要件

DHCP クライアントのセグメントのアドレスは、10.110.0.0 で、スイッチの VLAN2 に所属しているポートに接続されています。DHCP サーバサービスが有効に設定されると DHCP クライアントは、IP アドレスや他の設定情報を DHCP サーバから取得できます。

ネットワーク構成図

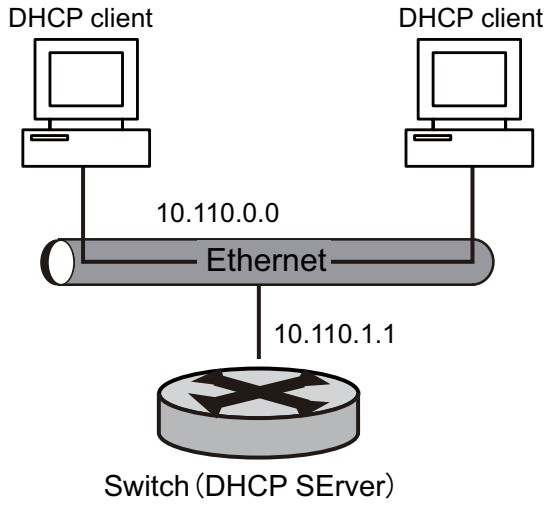


図 38　DHCP サーバーを設定しているネットワーク構成図

設定手順

VLAN を設定し、VLAN の IP アドレスを設定します。

```
switch(config)#vlan static set vid 1 01-
switch(config)#vlan static add vid 2 01u
switch(config)#vlan port pvid 1 2
switch(config)#ip address add vint 2 10.110.1.1 255.255.255.0 vid 2
```

DHCP サーバを設定します。

```
switch(config)#dhcps listen add 1 vint2
switch(config)#dhcps service enable
switch(config)#dhcps addresspool add pool1 10.110.1.2 10.110.1.254 10.110.1.1
255.255.255.0 dns1 202.96.128.68 dns2 211.95.193.97
```

5.15 SNMP

5.15.1 概要

コンピュータネットワーク分野において、SNMP（Simple Network Management Protocol）が群を抜いて最も豊富なアプリケーションをサポートしてきています。実際に、SNMP が業界標準として継続的に使用され、広く受け入れられてきています。これは、2 つのノード間で、マネージメント情報の転送を確実なものにするため使用されます。この方法を使用すれば、ネットワーク管理者はネットワーク上のノード情報を簡単に検索し、修正できます。その間に、ネットワーク管理者は障害箇所を即座に特定し、障害対策を実装し、容量の計画をおこない、レポートを発行できます。SNMP は、ポーリングメカニズムを採用し、非常に基本的な機能セットを提供します。これは、小規模、高速かつローコストな環境で最適です。必要とするものは、確認をおこなわないトランスポートレイヤのプロトコルである UDP のみで、したがって、多くの製品で広く SNMP がサポートされてきました。

仕組みの点からみると、SNMP は 2 つの部分、ネットワークマネージメントステーションとエージェントに分けることができます。ネットワークマネージメントステーションはクライアントプログラムを動作しているワークステーションです。現時点では、ネットワークマネージメントプラットフォームとして、Sun の NetManager や、IBM の NetView などが広く使用されています。エージェントはネットワーク機器で動作するサーバソフトウェアです。ネットワークマネージメントステーションはエージェントに対して GetRequest、GetNextRequest および SetRequest メッセージを送信できます。ネットワークマネージメントステーションからのリクエストを受信すると、エージェントはメッセージの種類に応じて Read（読み取り）または Write（書き込み）の操作をおこない、応答メッセージを生成してネットワークマネージメントステーションに返します。一方、エージェントはトラップメッセージを自発的にネットワークマネージメントステーションに送信し、新たな機器の検出や再起動など何らかの異常に遭遇した際に常にイベントをレポートします。

5.15.2 SNMP バージョンおよびサポートしている MIB

SNMP メッセージに含まれるマネージメント変数を一意的に識別するために、SNMP は階層型の命名スキームを適用して管理対象オブジェクトを特定します。これはツリー形式になっています。下図に示すように、ツリーのノードが管理対象オブジェクトになります。したがって、オブジェクトはルートを基点とした一意のパスで識別できます。

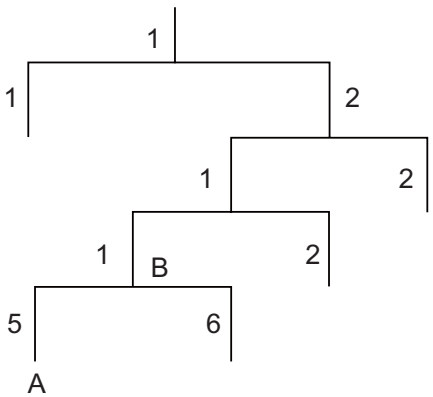


図 39　MIB ツリーの構造

MIB（Management Information Base）はツリーの階層構造を記述するのに使用され、監視対象のネットワーク機器の標準変数によって定義されたセットです。上記の図では、管理対象のオブジェクト B は数の文字列｛1.2.1.1｝によって一意的に特定できます。この数の文字列は管理対照オブジェクトのオブジェクト識別子です。

本機が現時点でサポートする SNMP エージェントは、SNMP V1 および V2C です。次の表にサポートされている MIB を記載します。

本機がサポートしている MIB

MIB の属性	MIB の内容	参照
Public MIB	TCP/IP ネットワーク機器の MIB II	RFC1213
	BRIDGE MIB	RFC1493 RFC2675
	RIP MIB	RFC1724
	RMON MIB	RFC2819
	Ethernet MIB	RFC2665
	OSPF MIB	RFC1253
	IF MIB	RFC1573
Private MIB	VLAN MIB	
	機器のマネージメント	

5.15.3 SNMP 設定

SNMP の主な設定には次の項目があります。

- コミュニティ名の設定
- トラップの送信先アドレスの設定
- トラップパラメータの設定

コミュニティ名の設定

SNMP V1 および SNMP V2C は、コミュニティ名認証スキームを採用しています。機器で設定したものと異なるコミュニティ名を持つ SNMP メッセージは破棄されます。SNMP コミュニティは文字列で命名され、コミュニティ名と呼ばれます。様々なコミュニティがリードオンリー（読み取りのみ）またはリード / ライト（読み取りと書き込み）のアクセスモードを有することができます。リードオンリー権限を持つコミュニティは機器情報の問い合わせのみが可能ですが、リードライト権限を持つコミュニティは機器の設定も可能です。

はじめに Privileged Exec モードでログインし、次の手順でコミュニティ名を設定します。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**snmp community set** *index string* **{read-only|read-write}**	コミュニティストリングを設定します。 index：1 ～ 8 の範囲で設定します。
手順 3	**exit**	Privileged Exec モードに戻ります。
手順 4	**show snmp community**	入力を確認します。
手順 5	**write**	（オプション）設定ファイルに入力を保存します。

コミュニティストリングの削除

モード	コマンド
Grobal Configuration	**snmp community delete** *index*

トラップ送信先アドレスの設定

次のコマンドを使用し、トラップのデスティネーションアドレスの設定または削除をおこないます。

はじめに Privileged Exec モードに移行し、次の手順でトラップのデスティネーションアドレスを設定します。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**snmp traps host** *host-number* **hostaddr** *ip-address* **[port** *udp-port***]**	トラップのデスティネーションアドレスを設定します。 host-number：1 ～ 3 の範囲で設定します。
手順 3	**exit**	Privileged Exec モードに戻ります。
手順 4	**show snmp traps**	入力を確認します。
手順 5	**write**	（オプション）設定ファイルに入力を保存します。

トラップパラメータの設定

次のコマンドを使用して、トラップパラメータの設定をおこないます。

はじめに Privileged Exec モードに移行し、次の手順でトラップパラメータを設定します。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**snmp traps parameters** *index* **mpmodel {v1 |v2c | v3} securemodel {v1 | v2c | usm} securename** *string* **securelevel {AuthNoPriv |AuthPriv |noAuthNoPriv }**	トラップパラメータを設定します。
手順 3	**exit**	Privileged Exec モードに戻ります。
手順 4	**show snmp traps**	入力を確認します。
手順 5	**write**	（オプション）設定ファイルに入力を保存します。

5.15.4 SNMP の設定例

ネットワーク要件

イーサネット経由でネットワークマネージメントステーションとイーサネットスイッチが接続しています。ネットワークマネージメントステーションの IP アドレスは 129.102.149.23、スイッチの VLAN インターフェースの IP アドレスは 129.102.0.1 です。次の設定をスイッチにおこないます。コミュニティ名の設定とトラップホストのアドレスの設定をおこないます。

ネットワーク構成図

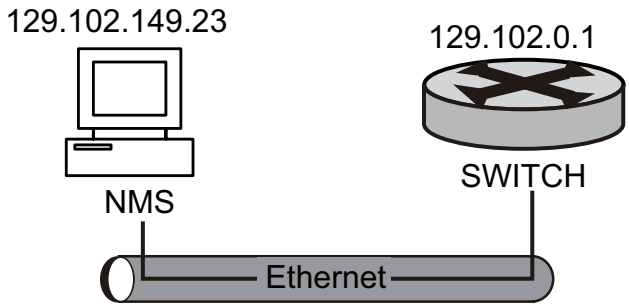


図 40　SNMP 構築例

設定手順

コミュニティストリングを設定します。

```
switch(config)#snmp community set 1 public read-write
```

トラップホストを設定します。

```
switch(config)#snmp traps host 1 hostaddr 129.102.149.23
```

5.16 syslog の設定

本章では、本機のシステムのメッセージログを設定する方法を解説します。

5.16.1 syslog の概要

syslog メッセージ機能は、使用中のスイッチで発生した障害をネットワークマネージャに通知します。syslog メッセージは、プライオリティに応じて emergency、alert、critical、error、warning、notece、info の 7 つのレベルに分類されています。Emergency（緊急）が最も高いプライオリティで、Info（情報）が最低のプライオリティです。syslog メッセージのレベルはユーザにより割り当てが可能で、割り当てたレベルより低いメッセージをユーザに転送することは不可能です。たとえば、すべてのレベルのメッセージを受信したい場合、Info レベルを選択しなくてはなりません。Error レベルを選択した場合、Error より高い、Error、Critical、Alert および Emergency レベルのメッセージは受信できます。

5.16.2 ログの有効化

syslog は初期設定では無効に設定されています。この機能を有効に設定し、任意の宛先にメッセージを送信します。有効に設定すると、ログメッセージはログ機能のプロセスに送信されますが、これはメッセージを指定したロケーションに非同期的にログを取り、メッセージを生成する一連のプロセスです。

はじめに Privileged Exec モードに移行し、次の手順でメッセージログ機能を有効にします。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**syslog enable**	メッセージログ機能を有効に設定します。
手順 3	**exit**	Privileged Exec モードに戻ります。
手順 4	**show syslog configurationig**	入力を確認します。
手順 5	**write**	（オプション）設定ファイルに入力を保存します。

メッセージログ機能を無効に設定

モード	コマンド
Grobal Configuration	**syslog disable**

5.16.3 メッセージを表示するデスティネーション機器の設定

メッセージログ機能が有効に設定されると、メモリに加え、メッセージを特定の機器に送信できます。

はじめに Privileged Exec **モードに移行し、次の手順でメッセージを表示するデスティネーション機器を設定します。**

	コマンド	内容
手順 1	**config terminal**	Global configuration **モードに移行します。**
手順 2	**syslog monitor-terminal enable**	**（オプション）現在のセッション中ログメッセージのコンソールターミナルへの送信を有効に設定します。**
手順 3	**syslog server enable**	**（オプション）ログメッセージの** UNIX **の** syslog **サーバホストへの送信を有効に設定します。**
手順 4	**syslog server add** *A.B.C.D* **{ port <** *1-65535* **> }** **{ facility <** *0-7* **> }**	**（オプション）** syslog **サーバホストの** IP **アドレスを設定します。ログメッセージを受信する複数の** syslog **サーバを構築する場合、このコマンドを複数回実行します。**port **は** syslog **サーバが使用している** UDP **ポートです。**facility **はログメッセージのレベルです。**
手順 5	**exit**	Privileged Exec **モードに戻ります。**
手順 6	**show syslog configurationig**	**入力を確認します。**
手順 7	**write**	**（オプション）設定ファイルに入力を保存します。**

コンソールターミナルへのログメッセージを無効に設定

モード	コマンド
Grobal Configuration	**syslog monitor-terminal disable**

syslog **サーバホストへのログメッセージを無効に設定**

モード	コマンド
Grobal Configuration	**syslog server disable**

syslog **サーバホストを削除**

モード	コマンド
Grobal Configuration	**syslog server delete** *A.B.C.D*

5.16.4 コンソールターミナルへのログメッセージの最低レベルの設定

コンソールターミナルへのログメッセージの最低レベルを設定すると、この最低レベルと同じかこのレベルより高いレベルのログメッセージのみをコンソールターミナルに表示できます。

はじめに Privileged Exec **モードに移行し、次の手順でコンソールターミナルへのログメッセージの最低レベルを設定します。**

	コマンド	内容
手順 1	**config terminal**	Global configuration **モードに移行します。**
手順 2	**syslog lowest-level <** *0 - 7* **>**	**コンソールターミナルへのログメッセージの最低レベルを設定します。初期設定では最低レベルは** 4 **です。** **内容** EMERG:0 ALERT:1 CRIT:2 ERR:3 WARNING:4 NOTICE:5 INFO:6 DEBUG:7
手順 3	**exit**	Privileged Exec **モードに戻ります。**
手順 4	**show syslog configurationig**	**入力を確認します。**
手順 5	**write**	**（オプション）設定ファイルに入力を保存します。**

5.16.5 syslog サーバへのログ送信の設定例

ネットワーク要件

ネットワーク要件は次のとおりです。

- **スイッチのログ情報を** syslog **サーバへ送信します。**
- syslog **サーバの** IP **アドレスは** 202.10.1.10 **です。**

ネットワーク構成図

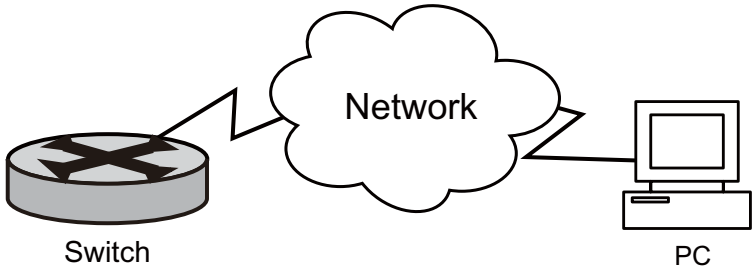


図 41　SNMP **構築例**

設定手順

メッセージログの有効化

```
switch(config)#syslog enable
```

syslog **サーバへのログメッセージの有効化と** syslog **サーバの設定**

```
switch(config)#syslog server enable
switch(config)#syslog server add 202.10.1.10
```

5.17 SNTP の設定

5.17.1 SNTP の概要

ネットワークトポロジがより複雑になるにつれ、ネットワーク全体の装置の時計を同期することが重要になってきました。SNTP（Simple Network Time Protocol）は TCP/IP のプロトコルでネットワーク全体に正確な時間を広告します。

本機が SNTP クライアントとして機能する場合、次の 2 つのモードを動作できます。

- ユニキャスト：本機は指定した SNTP サーバへリクエストパケットを送信し、SNTP クライアントが SNTP サーバから応答パケットを受信すると、SNTP サーバの時間に同期します。
- エニキャスト：SNTP クライアントが SNTP サーバの IP アドレスを知らない場合、SNTP クライアントはブロードキャストタイムリクエストパケットを送信し、SNTP サーバがこのリクエストパケットを受信すると、SNTP サーバはユニキャストパケットを応答します。この手順後、SNTP クライアントと SNTP サーバはユニキャストパケットでのコミュニケーションをおこないます。

本機が SNTP サーバとして機能する場合、次の 2 つのモードを動作できます。

- アクティブ：本機はブロードキャストタイムパケットをネットワーク宛に送信し、SNTP クライアントリクエストに応答します。
- l パッシブ：本機はブロードキャストタイムパケットをネットワーク宛に送信しませんが、SNTP クライアントリクエストに応答します。

5.17.2 SNTP の設定

SNTP の設定には次の項目があります。

- SNTP クライアントの動作モードの設定
- SNTP クライアントサービスの有効 / 無効の設定
- SNTP クライアントパラメータの設定
- SNTP サーバの動作モードの設定
- SNTP サーバサービスの有効 / 無効の設定
- SNTP サーバパラメータの設定

5.17.3 SNTP クライアントの動作モードの設定

はじめに Privileged Exec **モードに移行し、次の手順で** SNTP **クライアントの動作モードを設定します。**

	コマンド	内容
手順 1	**config terminal**	Global configuration **モードに移行します。**
手順 2	**sntp-client mode** < *unicast / anycast*>	SNTP **クライアントの動作モードを設定します。**
手順 3	**exit**	Privileged Exec **モードに戻ります。**
手順 4	**show sntp-client**	**入力を確認します。**
手順 5	**write**	**（オプション）設定ファイルに入力を保存します。**

5.17.4 SNTP クライアントサービスの有効 / 無効の設定

[注意] SNTP クライアント動作モードがユニキャストの場合、SNTP クライアントサービスを有効に設定する前に SNTP サーバの IP アドレスを設定しなくてはなりません。

はじめに Privileged Exec **モードに移行し、次の手順で** SNTP **クライアントサービスの有効 / 無効を設定します。**

	コマンド	内容
手順 1	**config terminal**	Global configuration **モードに移行します。**
手順 2	**ssntp-client** < *enable*| *disable* >	SNTP **クライアントサービスの有効 / 無効を設定します。**
手順 3	**exit**	Privileged Exec **モードに戻ります。**
手順 4	**show sntp-client**	**入力を確認します。**
手順 5	**write**	**（オプション）設定ファイルに入力を保存します。**

5.17.5 SNTP クライアントパラメータの設定

はじめに Privileged Exec **モードに移行し、次の手順で** SNTP **クライアントパラメータを設定します。**

	コマンド	内容
手順 1	**config terminal**	Global configuration **モードに移行します。**
手順 2	**sntp-client server ipaddr** < *A.B.C.D* >	**（オプション）**SNTP **クライアントの動作モードがユニキャストの場合、**SNTP **サーバの** IP **アドレスを設定します。**
手順 3	**sntp-client update-interval** < *64 - 1024* >	SNTP **クライアントのタイムパケット更新間隔を設定します。** **範囲：**64 ～ 1024 **秒　初期設定値：**64 **秒**
手順 4	**exit**	Privileged Exec **モードに戻ります。**
手順 5	**show sntp-client**	**入力を確認します。**
手順 6	**write**	**（オプション）設定ファイルに入力を保存します。**

5.17.6 SNTP サーバの動作モードの設定

はじめに Privileged Exec **モードに移行し、次の手順で** SNTP **サーバの動作モードを設定します。**

	コマンド	内容
手順 1	**config terminal**	Global configuration **モードに移行します。**
手順 2	**sntp-server mode** **<** *active / passive* **>**	SNTP **サーバの動作モードを設定します。**
手順 3	**sntp-client update-interval** **<** *64 - 1024* **>**	SNTP **クライアントのタイムパケット更新間隔を設定します。 範囲：**64 ～ 1024 **秒初期設定値：**64 **秒**
手順 4	**exit**	Privileged Exec **モードに戻ります。**
手順 5	**show sntp-server**	**入力を確認します。**
手順 6	**write**	**（オプション）設定ファイルに入力を保存します。**

5.17.7 SNTP サーバサービスの有効 / 無効の設定

はじめに Privileged Exec **モードに移行し、次の手順で** SNTP **サーバサービスの有効 / 無効を設定します。**

	コマンド	内容
手順 1	**config terminal**	Global configuration **モードに移行します。**
手順 2	**sntp-server** **<** *enable* | *disable* **>**	SNTP **サーバサービスの有効 / 無効を設定します。**
手順 3	**exit**	Privileged Exec **モードに戻ります。**
手順 4	**show sntp-server**	**入力を確認します。**
手順 5	**write**	**（オプション）設定ファイルに入力を保存します。**

5.17.8 SNTP サーバパラメータの設定

はじめに Privileged Exec **モードに移行し、次の手順で** SNTP **サーバパラメータを設定します。**

	コマンド	内容
手順 1	**config terminal**	Global configuration **モードに移行します。**
手順 2	**sntp-server broadcast-interval** **<***64-1024***>**	SNTP **サーバのタイムパケット更新間隔を設定します。**64 ～ 1024 **秒の範囲で設定します。初期設定値は** 64 **秒です。**
手順 3	**exit**	Privileged Exec **モードに戻ります。**
手順 4	**show sntp-client**	**入力を確認します。**
手順 5	**write**	**（オプション）設定ファイルに入力を保存します。**

5.17.9 SNTP の表示

上記の設定を終了したら、いずれかのコマンドモードで show **コマンドを実行し、実行中の** SNTP **の設定内容を表示してこの設定の結果を確認します。**

VRRP **の表示とデバッグ**

コマンド	オペレーション
show sntp	SNTP **設定情報の表示**
show system configration	**システムクロックの表示**

5.18 VRRP

5.18.1 概要

Virtual Router Redundancy Protocol (VRRP) は、フォルトトレラントプロトコルです。

通常、デフォルトルート（図 42 のネットワーク構成図では 10.100.10.1）はネットワーク上ですべてのホストにたいして配置されます。ホストから他のネットワークへ向かうパケットは、ホストと外部ネットワーク間のコミュニケーションを行う L3 スイッチ１へのデフォルトルートを通過します。

もしスイッチ１がダウンした場合、デフォルトルートの次のホップとしてスイッチ１を通過する全てのパケットは外部ネットワークへ出ていくことができなくなります。

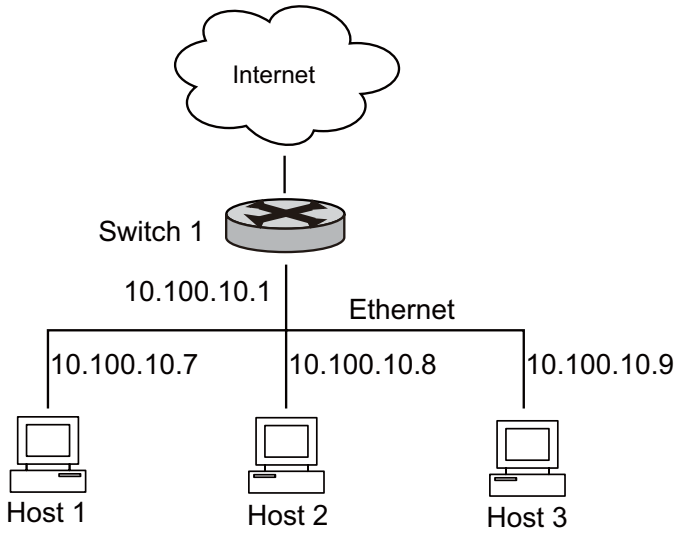


図 42　VRRP

VRRP は、上のような問題を解決します。

図 43 は VRRP 実装の基本概念を説明しています。

VRRP はバーチャルルーター（バックアップグループ）の中に LAN スイッチのグループ（マスターといくつかのバックアップ）を結合します。

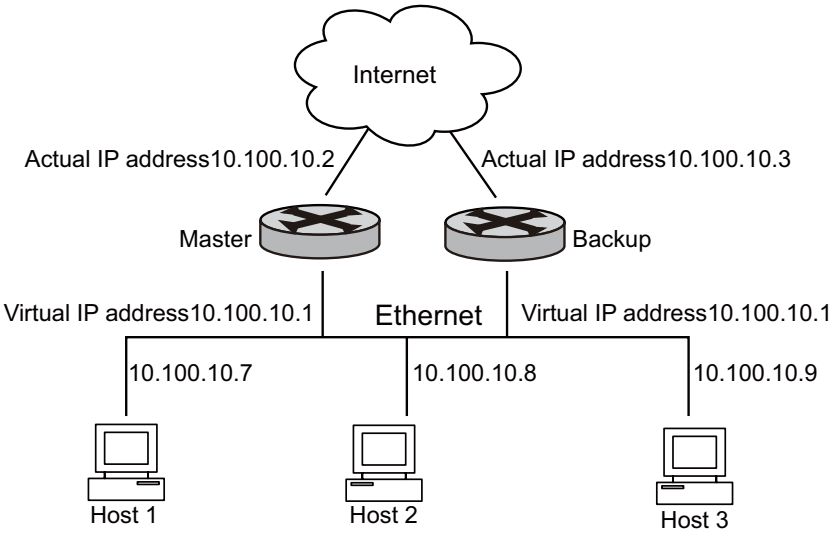


図 43　VRRP **実装の基本概念**

バーチャルルータはそれ自身の IP **アドレスを持ちます。（例：**10.100.10.1**）**

バーチャルルータ内のスイッチもそれぞれに IP **アドレスを持ちます**

（例えば 10.100.10.2 **をマスタースイッチに設定し、**10.100.10.3 **をバックアップスイッチに設定）**LAN **内のホストはバーチャルルータのアドレス（この場合** 10.100.10.1**）だけでなくマスタースイッチの** IP **アドレス** 10.100.10.2 **とバックアップスイッチのアドレス** 10.100.10.3 **も知っています。**

それらは自身のデフォルトルートをこのバーチャルルーターの IP **アドレス（**10.100.10.1**）として設定します。その結果、ネットワークの中のホストはこのバーチャルルーターを経由している外部ネットワークとコミュニケーションします。**

バーチャルグループ内のマスタースイッチがダウンした時は他のバックアップスイッチが新しいマスタースイッチとして機能し、外部ネットワークとホストの間でコミュニケーションが中断することのないよう、ホストへルーティングを供給し続けます。

5.18.2 VRRP の設定

- バーチャル IP アドレスの追加と削除
- バーチャルルータ内スイッチの優先度を設定
- バーチャルルータ内スイッチのプリエンプションを設定
- VRRP タイマーの設定
- VRRP インターフェーストラックの設定

[注意] VRRP の設定を行う前に、ARP Proxy サービスが有効になっていることを確認してください。ARP Proxy サービスを有効にするには Global configuration モードで "arp proxy service enable" コマンドを実行してください。

バーチャル IP アドレスの追加と削除

次のコマンドはローカルセグメントの IP アドレスをバーチャルルータへ追加または、割り当てられたバーチャルルータのバーチャル IP アドレスを削アドレスリストから削除します。

はじめに Privileged Exec モードに移行し、次の手順でバーチャル IP アドレスの追加を行います。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**vrrp add vrid** *virtual-router-ID* **virtual-ip** *virtual-ipaddress interface-id*	バーチャル IP アドレスを追加します。 virtual-router-ID：1 ～ 255 の範囲で設定します。 Interface-id：vint+ 番号（例：vint1）
手順 3	**exit**	Privileged Exec モードに戻ります。
手順 4	**show vrrp configuration** *interface-id*	入力を確認します。
手順 5	**write**	（オプション）設定ファイルに入力を保存します。

バーチャル IP アドレスの削除

モード	コマンド
Grobal Configuration	**vrrp delete vrid** *virtual-router-ID* **virtual-ip** *virtual-ipaddress interface-id*

virtual-router-ID は 1 から 255 までの範囲をカバーします。

virtual-router-ID はバーチャルルータが存在するネットワーク内で使用されていないアドレスまたはバーチャルルータのインターフェース IP アドレスが使用可能です。もし、IP アドレスがスイッチのものである場合、それも同じように設定されます。この場合、スイッチは IP アドレスオーナーと呼ばれます。

バーチャルルータに最初の IP アドレスを設定する時、システムはそれに応じて新しいバーチャルアドレスを作成します。その後このバックアップグループに新しいアドレスを加える際、システムはバーチャル IP アドレスリストの中に直接追加を行います。

バーチャルルータ内スイッチの優先度を設定

仮想のルーターのそれぞれのスイッチの状況はそれ自身の VRRP プライオリティによって決定されます。一番高いプライオリティを持つスイッチがマスターになります。

プライオリティの範囲は 0 から 255（大きい数が高いプライオリティ）ですが、実際に設定可能な値は 0 から 254 です。プライオリティ 0 は特別使用のため確保され、255 はシステムにより、IP アドレスオーナーのために確保されています。

はじめに Privileged Exec モードに移行し、次の手順でバーチャルルータ内スイッチの優先度を設定します。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**vrrp set vrid** *virtual-router-ID* **priority** *priority*	バーチャルルータ内のスイッチプライオリティを設定します。1 ～ 254 の範囲で設定します。 初期設定：100
手順 3	**exit**	Privileged Exec モードに戻ります。
手順 4	**show vrrp configuration vrid** *virtual-router-ID*	入力を確認します。
手順 5	**write**	（オプション）設定ファイルに入力を保存します。

バーチャルルータ内スイッチのプリエンプションの設定

バーチャルルータの内スイッチの内、一つがマスタースイッチになります。それが適切に機能している限り、他のスイッチがより高いプライオリティに設定しなおされたとしても、プリエンプションモードで動作していない限りはマスタースイッチにはなれません。

プリエンプションモードの場合、スイッチが、自身のプライオリティが現在のマスタースイッチよりも高いと判断した時マスタースイッチになります。その際、それまでのマスタースイッチはバックアップになります。

はじめに Privileged Exec モードに移行し、次の手順でプリエンプションの設定を行います。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**vrrp set vrid** *virtual-router-ID* **preempt enable**	スイッチのプリエンプションを設定します。
手順 3	**exit**	Privileged Exec モードに戻ります。
手順 4	**show vrrp configuration vrid** *virtual-router-ID*	入力を確認します。
手順 5	**write**	（オプション）設定ファイルに入力を保存します。

プリエンプションを無効に設定

モード	コマンド
Grobal Configuration	**vrrp set vrid** *virtual-router-ID* **preempt disable**

VRRP タイマーの設定

スイッチマスターはその通常オペレーション状態を、常に (adver-interval で)VRRP パケットを送ることによって、VRRP バーチャルルータ内のスイッチへ通知します。

もし、バックアップが一定の時間 (specified by master-down-interval にて設定) が経過してもマスタースイッチからの VRRP パケットを受け取れない場合、バックアップはマスターがダウンしたと判断し、マスタに代わって新しいマスタとなります。

はじめに Privileged Exec モードに移行し、次の手順で VRRP タイマーの設定を行います。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**vrrp set vrid** *virtual-router-ID* **adv-interval** *adv-interval*	VRRP タイマーの設定を行います。 adv-interval：1 ～ 255（秒）の範囲で設定します。 初期設定：1（秒）
手順 3	**exit**	Privileged Exec モードに戻ります。
手順 4	**show vrrp configuration vrid** *virtual-router-ID*	入力を確認します。
手順 5	**write**	（オプション）設定ファイルに入力を保存します。

VRRP インターフェーストラックの設定

VRRP インタフェーストラック機能はバックアップ機能が拡張されたものです。

バックアップがバーチャルルーターに存在するインタフェースにだけではなく、他の誤作動している スイッチインターフェースに提供されます。

次のコマンドを実行することで、いずれかのインターフェースの追跡を行えます。

もし、トラックされているインターフェースがダウンしたら、そのインターフェースを含むスイッチのプライオリティは自動的に低い値になります。比較の結果に従ってバーチャルルーターの中で比較的高いプライオリティのスイッチの内一つがこのインタフェースの跡を追うようにマスタースイッチに代わります。

はじめに Privileged Exec モードに移行し、次の手順で VRRP インターフェーストラックの設定を行います。

	コマンド	内容
手順 1	**config terminal**	Global configuration モードに移行します。
手順 2	**vrrp set vrid** *virtual-router-ID* **track** *interface-id* **reduce** *reduce-value*	指定したインターフェースのトラック設定を行います。初期設定：reduce-value は 10 です。
手順 3	**exit**	Privileged Exec モードに戻ります。
手順 4	**show vrrp configuration** *interface-id*	入力を確認します。
手順 5	**write**	（オプション）設定ファイルに入力を保存します。

[注意] スイッチが IP アドレスのオーナーである場合、そのインターフェースはトラックされることができません。

- **もしトラックされているインターフェースが復旧した場合、スイッチのプライオリティ、含まれるインターフェースは自動的に更新されます。**
- **１つのバックアップグループ内で最大 8 インターフェースのトラックが可能です。**

5.18.3 VRRP の表示とデバッグ

前項の設定を行った後、いずれかのコマンドモードで show **コマンドを実行し、実行中の** VRRP **設定内容を確認してください。**

VRRP **の表示とデバッグ**

コマンド	オペレーション
show vrrp configuration *interface-id*	インターフェースの設定情報を表示。
show vrrp statistics *interface-id*	インターフェースの統計情報を表示。
show vrrp configuration vrid *virtual-router-ID*	バーチャルルータの設定情報を表示。
show vrrp statistics vrid *virtual-router-ID*	バーチャルルータの統計情報を表示。
debug vrrp trace	VRRP デバッグのトレース情報を表示。

5.18.4 VRRP の設定例

ネットワーク要件

ホスト A はスイッチ A と B を内包する VRRP バーチャルルータを使用します。

スイッチ A とスイッチ B は、インターネット上のホスト B を訪問する際のデフォルトゲートウェイです。VRRP バーチャルルータ情報は、バーチャルルータ ID1、バーチャル IP アドレス 202.38.160.111、マスタースイッチ A、バックアップスイッチ B を含みます。

ネットワーク構成図

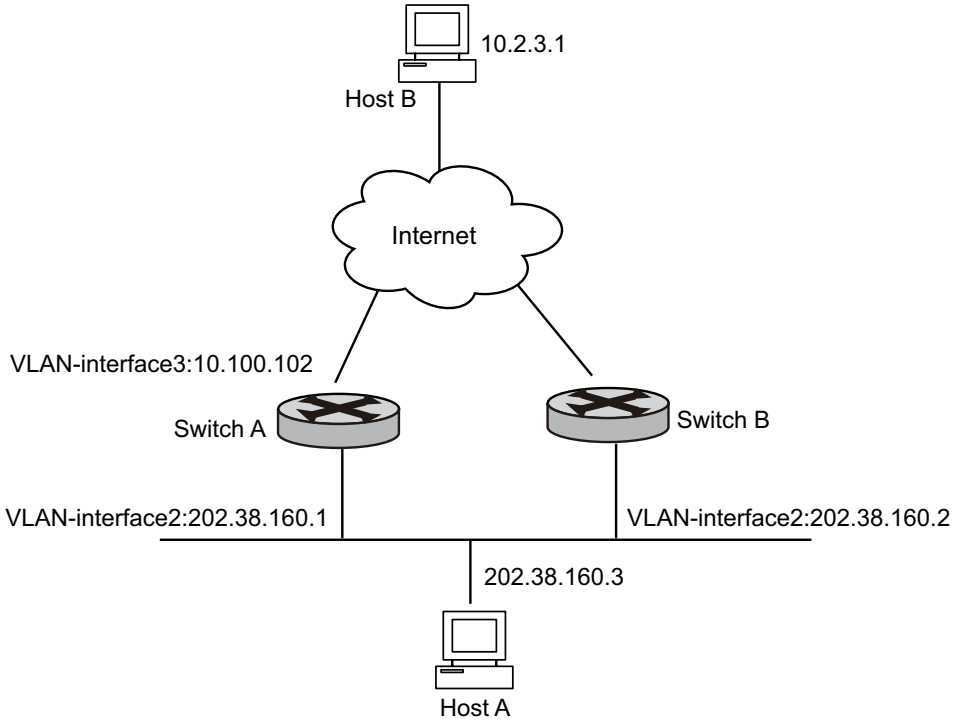


図 44 VRRP 構築例

5.18.5 VRRP 障害時のトラブルシューティング

VRRP の設定はそれほど複雑ではありません。誤動作のほとんどが、設定とデバッキングインフォメーションを見ることによって解決ができます。ここでは発生する可能性のある不具合とそれに対応するトラブルシューティングを掲載しています。

障害 1: コンソール上で頻繁に設定エラープロンプトが出る。

これは、不正な VRRP パケットが受信されたことを示します。

バーチャルルータ内の他のスイッチに一貫しない設定が存在する可能性があります。
または、外部の装置が非合法なパケットを送出しているかもしれません。

前者の場合設定を修正することで解決ができます。後者の場合は悪意ある第三者の試みによって行われている可能性があります。

障害 2: 一つ以上のマスターが同一バーチャルルータ内に存在する。

2 つの原因が考えられます。

- 多数のマスタースイッチ短時間共有－これは正常であり手作業での修正は必要ありません。
- 多数のマスタースイッチ長時間共有－いくつかのマスターが他から VRRP パケットを受け取れないかあるいは不正なパケットを受け取っている可能性があります。

この問題を解決するために、マススタースイッチ間で Ping の送信を行ってみてください。
もし Ping が失敗するならば、それは他の問題が存在していることを示します。
Ping に成功する場合、問題は一貫しない設定によって起きています。

バーチャルルータの設定を一貫させるため、バーチャル IP アドレスの数、それぞれのバーチャル IP アドレス、タイマー持続時間、認証タイプに完全な一貫性を持たせてください。

障害 3: 頻繁にスイッチオーバーが発生する。

このような問題は、バーチャルルータのタイマー持続時間が短すぎる時に発生します。
持続時間を延長するか、プリエンプションの遅延を設定することで解決ができます。

FXC3524 Management Guide (FXC07-DC-200003-R1.0)

初版 2007 年 5 月

Management Guide FXC3524

Management Guide FXC3524
Management Guide FXC3524
Management Guide FXC3524
Management Guide FXC3524
Management Guide FXC3524
Management Guide FXC3524
Management Guide FXC3524
Management Guide FXC3524
Management Guide FXC3524
Management Guide FXC3524
Management Guide FXC3524
Management Guide FXC3524
Management Guide FXC3524
Management Guide FXC3524
Management Guide FXC3524
Management Guide FXC3524
Management Guide FXC3524
Management Guide

FXC株式会社