Future X Communications

FXC7024
ユーザーマニュアル

Version 1.0
Jan. 2005

目次

図版目次

表目次

1. はじめに

1.1 このマニュアルについて

このマニュアルは、FXC7024（以下、本製品）のインストール、設定、および管理を担当するネットワーク管理者を対象に書かれています。そのため、次の項目に関する基本的な作業知識があることを前提としています。

- ローカルエリアネットワーク（LAN）
- イーサネットの概念
- イーサネットのスイッチングとブリッジングの概念
- ルーティングの概念
- インターネットプロトコル（IP）の概念
- IP マルチキャストの概念

1.2 機能の概要

本製品には、ベーシックソフトウェアイメージがインストールされています。このベーシックソフトウェアイメージに含まれる機能は、次のとおりです。

- 10BASE-T/100BASE-TXFull/Half Duplex
- 1000BASE-T、1000BASE-SX、1000BASE-LX Full Duplex
- IEEE802.1D MAC ブリッジ
- バーチャル LAN（VLAN）IEEE802.1Q
- GVRP
- スパニングツリープロトコル（STP）
- ファースト STP
- IEEE802.1p プライオリティキューイング
- IEEE802.3x フローコントロール
- IEEE802.3adLACP
- ポートミラーリング
- ブロードキャストストリームリカバリ（BSR）
- VLAN ルーティング
- スタティックおよびデフォルトの IP ルーティング
- クラスレスドメイン間ルーティング（CIDR）
- ルーティングインフォメーションプロトコル（RIP1、RIP1c、RIP2）

- オープンショーテストパスファースト（OSPFv2）
- セカンダリ IP アドレス
- 仮想ルータ冗長プロトコル（VRRP）
- ルータ検出
- ネットワークアドレス変換（NAT）
- ハイレベルアクセスコントロールリスト（H-ACL）
- ローレベルアクセスコントロールリスト（L-ACL）
- ソフトウェアアクセスコントロールリスト（SACL）
- DiffServ
- DoS 攻撃防止（DAP）
- 帯域幅割り当て（ポート単位/VLAN 単位）
- 管理インタフェース用のブートストラッププロトコル（BOOTP）クライアントとダイナミックホスト構成／制御プロトコル（DHCP）クライアント
- 回線トラフィックインタフェース用の DHCP/BOOTP リレー
- DHCP サーバ機能
- 管理インタフェース用の簡易ファイル転送プロトコル（TFTP）クライアント
- シリアル管理ポート上の XMODEM
- ユーザインタフェース
- コマンドラインインタフェース（CLI）
- Web ベースのインタフェース（WBI）
- 簡易ネットワーク管理プロトコル（SNMP）
    - SNMP- v1、v2c、v3、Trap
    - RMON セクション I（1、2、3、9）

本製品でフルレイヤ 3 ライセンス（別売）を使用すると、BGP4、PIM-DM、PIM-SM、DVMRP もサポートされます。フルレイヤ 3 ライセンス（別売）では、次の機能をサポートしています。

- Border Gateway Protocol Version 4（BGP4）
- マルチキャストプロトコル
    - Distance Vector Multicast Routing Protocol（DVMRP）
    - Protocol Independent Multicast – Dnse Mode（PIM-DM）
    - Protocol Independent Multicast – Sparse Mode（PIM-SM）

フルレイヤ 3 ライセンス（別売）イメージによってサポートされる機能がアクティブになるのは、システムに有効なライセンスキーがインストールされている場合だけです。ライセンスキーがインストールに関する詳細は、「3.2.8　高度な機能セットのアクティブ化」（P.13）を参照してください。

1.3　工場出荷時のデフォルト設定

本製品の工場出荷時のデフォルト設定は、次のとおりです。

- User Account – admin
- Password – L3SW
- Telnet – 有効
- System IP Address – 0.0.0.0
- Subnet Mask – 0.0.0.0
- Default Gateway IP Address – 0.0.0.0
- Network Configuration Protocol – なし
- Web Mode – 有効
- Web Java Mode – 無効
- Broadcast Storm Recovery Mode – 無効
- IEEE802.3x Flow Control Mode – 有効
- Link Trap – 有効
- LACP Mode – 有効
- Port Mirroring Mode – 無効
- STP Port State – 無効
- Port Mirroring – 無効
- VLAN traffic – タグ無し
- Ingress Filtering – 無効
- GVRP – 無効
- OSPF – 無効
- ASBR Mode – 無効
- RIP Admin Mode – 無効
- Router Discovery Advertise Mode – 無効
- VRRP Default Admin Mode – 無効
- BGP Admin mode – 無効
- Multicast protocols admin mode – 無効
- CIDR – 有効
- BOOTP/DHCP Relay Admin Mode – 無効
- Access Control List – 無効
- NAT – 無効

このマニュアルで使用されている略語の正式名称については、「付録 A: 略語一覧」（P.259）を参照してください。

2. ハードウェアに関する説明

この章では、本製品のハードウェア機能について説明します。

2.1 前面パネル

本製品は、効率的に使用できるよう設計されており、前面パネルからファーストイーサネットポートやギガビットポートにアクセスできます。また、シリアルポートやコンソール管理ポートにアクセスすることもできます。図 2-1 に、前面パネルを示します。前面パネルから次のネットワークポートにアクセスできます。

- 10BASE-T/100BASE-TX ポート(24 ポート)
- mini-GBIC スロット(2 スロット)
- 拡張モジュールスロット(2 スロット)

拡張モジュールスロットには、1000BASE-T モジュール、100BASE-FX モジュール、mini-GBIC スロットモジュールなどが搭載できます。

使用できる機能カードには、1000BASE-T カード、100BASE-FX カード、SFP カードがあります。

図 2-1:前面パネル

2.2 LED の意味

前面パネルには、ポートやスイッチの状態を示す次の LED があります。

- 24 個の 10BSE-T/100BASE-TX ポート用の LED(24 組)
- 拡張スロット/モジュール用 1000Mbps ポート用の LED(4 組)
- 電源状態を示す 3 個の LED(製品本体右側)

各 LED の詳細については、「2.4 LED の意味」(P.6)を参照してください。

2.3 背面パネル

背面パネルには、電源ソケットと通信用のコネクタがあります。また、背面パネルの薄い金属板の隣には、2 つのファンの通風孔が配置されています。図 2-2 に、背面パネルを示します。

- AC 電源コネクタ(AC 電源コードは標準で装置に付属しています):110VAC か

ら 240VAC まで（周波数の範囲は 50 から 60Hz まで）の AC 電源で動作します。

- スイッチ管理用の RS-232C シリアルポート
- 管理用の RJ45 10/100Mbps ファーストイーサネットコンソールポート。このポートは、サービスポートとも呼ばれます。本製品の管理は、このサービスポート経由するか、前面パネル上のいずれかのネットワークポートを使用したインバンド管理によって実行できます。

図 2-2：背面パネル

2.4 LED の意味

LED は、デバイスの稼動状況のモニタリングや診断に使用できます。ポートの LED で確認できる内容は、次のとおりです。

- ポートの状態
- データの送受信状況
- リンク速度（10/100/1000Mbps）

表 2-1 に、LED の状態と意味を示します。

LED（ポート番号）	色	状態
LINK/ACT（1－24）	緑	リンク時に点灯、データ送受信時に点滅
100M（1－24）	橙	100M でリンク時に点灯、10M 時は消灯
LINK/ACT（M1－M4）	緑	リンク時に点灯、データ送受信時に点滅
1000M（M1－M4）	橙	1000M でリンク時に点灯、10/100M 時は消灯
PWR	緑	電源投入時に点灯
OK	緑	装置に問題が無い場合に点灯
FLT	緑	障害発生時に点灯

表 2-1：LED の意味

3. 管理用アクセス

本製品は、スイッチの動作状況の制御やモニタリングを行うネットワーク管理者を支援する包括的な管理機能のセットを備えています。ネットワーク管理者は、次の 3 つの管理インタフェースのいずれかを選択して使用できます。

- CLI
- WBI
- SNMP

CLI ベースの管理: CLI コマンドを使用して、専用のシリアルインタフェースや telnet セッション経由で管理できます。アクセスレベルに応じて、ユーザはスイッチを管理する際に次のコマンドセットを使用できます。

- 特権レベル（読み書きユーザ）

  `clear` スイッチをリセットしたり、設定を工場出荷時のデフォルト設定にリセットしたりする

  `config` スイッチのオプションや設定を指定する

  `debug` トラブルシューティングユーティリティ

  `help` CLIコマンドのヘルプを表示する

  `logout` このセッションを終了する。保存していない変更は失われます。

  `ping` 指定したIPアドレスにICMPエコーパケットを送信する

  `reset` スイッチをリセットする

  `save` スイッチ設定を保存する

  `show` スイッチのオプションや設定を表示する

  `transfer` スイッチのソフトウェアのアップグレード、設定のアップロードおよびダウンロードを実行する

  `shell` Shellモードに移行し、tracerouteなどのコマンドを実行する

- ユーザレベル（読み取り専用ユーザ）

  `help` CLI コマンドのヘルプを表示する

  `logout` このセッションを終了する

  `show` スイッチのオプションや設定を表示する

CLI: CLI コマンドにより、ユーザはさまざまなスイッチ機能（ARP、スパニングツリープロトコル、VLAN、RIP、OSPF、VRRP など）を設定したり、メンテナンスに関連する機能のセット（ユーザログイン管理、ログトラップ、サービスポートの設定、telnet セッションなど）を実行したりすることができます。

WBI: Web ブラウザによるグラフィカルインタフェースを使用して本製品を管理できます。柔軟性と一貫性がある画面セットで、ユーザはインターネット経由で本製品上で利用できるリソースの

設定と管理を実行できます。さらに、アラームや統計などのリアルタイムイベントは、WBI を使用してモニタリングできます。

SNMP:本製品は、外部の SNMP マネージャを使用して管理することもできます。本製品は、標準的な MIB と一部の独自仕様の MIB(スイッチがサポートしている追加の機能を管理する企業独自の拡張機能)に準拠した SNMP エージェントを実装しています。外部の SNMP ベースのマネージャ(HP-Openview など)を使用して、スイッチの設定や管理を実行できます。本製品の SNMP エージェントには、トラップ機能も実装されているため、SNMP マネージャでスイッチからのトラップを確認できます。

管理アクセス方法では、ネットワーク管理者は次のアクセスインタフェースを使用してローカル／リモートで管理および制御を実行できます。

- シリアルポート(製品背面)
- イーサネットサービスポート(製品背面にある 10BASE-T/100BASE-TX ポート)
- イーサネットポート

シリアルポートやイーサネットサービスポートは、アウトオブバンドインタフェースと呼ばれ、イーサネットポートは、「インバンドインタフェース」と呼ばれます。アウトオブバンドインタフェースは、管理専用のインタフェースです。一方、インバンドインタフェースは、ユーザのネットワーク用と本製品の管理用の両方で使用されます。

3.1 さまざまなインタフェースによってサポートされる管理方法

管理には、次の 3 種類のインタフェースのいずれかを使用できます。

3.1.1 シリアルポートインタフェース

- CLI

3.1.2 サービスポートインタフェース

- CLI
- WBI
- SNMP

3.1.3 インバンドネットワーク管理インタフェース

- CLI
- WBI
- SNMP

3.2 管理ステーションのセットアップ

次節で、本製品を管理する管理ステーションのセットアップについて説明します。

3.2.1 端末アクセスのセットアップ

前面パネルには、RS-232C シリアルインタフェースがあります。標準的な RS-232C シリアルケーブルを使用すれば、VT100 端末エミュレーション機能を備えた任意の端末に接続できます。シリアル通信インタフェースを正常に動作させるには、次の端末設定を指定する必要があります。

- **ボーレート = 9600**
- **データビット = 8**
- **パリティ = なし**
- **ストップビット = 1**
- **フローコントロール = なし**

3.2.2 CLI の構文規則

コマンド	内容
コマンドおよびパラメータ	入力するコマンドとパラメータは、表示されている通りに正確に入力する必要があります。コマンド構文の後に、使用例を示します。出力されるコマンドは、イタリック体または画面例で示します。
<パラメータ>	< >（かぎ括弧）は、そのパラメータがコマンドの実行に必須であることを示します。
[パラメータ]	[ ]（角括弧）は、そのパラメータがオプションであることを示します。
選択肢 1 / 選択肢 2	/（スラッシュ）は、いずれか一方のパラメータだけを入力する必要があることを示します。
ipaddr	このパラメータは、ドット（.）で区切られた 4 つの 10 進数のバイトで構成される有効な IP アドレスです。各バイトの範囲は、0 から 255 までです。通常、デフォルトの IP は 0.0.0.0 です。
macaddr	MAC アドレスの形式は、コロンで区切られた 6 つの 16 進数です（たとえば、0:20:10:32:0e:40）。
areaid	エリア ID には、ドット de 区切りの 10 進数の表記法（たとえば、0.0.0.1）で入力できます。0.0.0.0 のエリア ID は、バックボーン用に予約されています。
slot.port	このパラメータは、有効なスロット番号と有効なポート番号を示します。たとえば、0.1 は、スロット 0 のポート 1 を示します

CLI コマンドの例は、「3.2.4 サービスポートアクセスのセットアップ」(P.10)を参照してください。

このマニュアルでは、次の規則を使用して、CLI コマンドの構文を説明し、そのコマンドの使用例を示します。

コマンドの構文

L3SW> config serviceport protocol <none/bootp/dhcp>

使用例

```
L3SW> config serviceport protocol none
```

3.2.3 ポートの番号付け規則

次のポート番号付け規則を使用して、前面パネルのイーサネットポートを識別します。ファーストイーサネットポートには、0.1 から 0.24 までの番号が付けられています。上の列には、ポート 0.1 から 0.12 までが含まれ、下の列には、ポート 0.13 から 0.24 までが含まれています。拡張スロットには、1.1 から 1.4 までの番号が割り振られています。ポート 1.1 とポート 1.2 は拡張スロットモジュールに関連付けられたポートで、ポート 1.3 とポート 1.4 は mini-GBIC/SFP スロットに関連付けられたポートです。

3.2.4 サービスポートアクセスのセットアップ

管理用に利用できる 1 個の 10/100 Mbps ファーストイーサネットのアウトオブバンドポート(サービスポート)を備えています。サービスポートを使用して本製品を設定する場合は、最初に、管理ステーションがスイッチの背面パネルにあるサービスポートに接続されていることを確認します。次のコマンドを実行し、サービスポートに関連するパラメータを設定します。

1. DHCP を使用している場合、設定は不要です。デフォルトで、DHCP は有効です。
2. スタティック IP アドレスを使用している場合は、次のコマンドを実行して、ポートの IP アドレスを設定します。

   L3SW> config serviceport protocol <none/bootp/dhcp>

   ```
   L3SW> config serviceport protocol none
   Changing protocol mode will reset ip configuration.
   Are you sure you want to continue? (y/n) y
   ```

   L3SW> config serviceport parms <ipaddr> <netmask> [gateway]

   ```
   L3SW> config serviceport parms 172.30.40.221 255.255.255.0 172.30.40.2
   ```

ここで、172.30.10.221 と 172.30.40.2 は、それぞれサービスポートとデフォルトゲートウェイの IP アドレスです。

現時点で、サービスポートがサポートしているのは、10MbpsHalf Duplex モードだけです。

3.2.5 ネットワークポートアクセスのセットアップ

いずれかのネットワークポートがインバンド管理用に使用されていて、本製品がレイヤ 2 スイッチとして設定されている(つまり、IP インタフェースが設定されていない)場合は、次のコマンドを実行して設定する必要があります。

1. DHCP を使用している場合は、次のコマンドを実行して、DHCP プロトコルを設定します

   L3SW> config network protocol <none/bootp/dhcp>

```
L3SW> config network protocol dhcp
Changing protocol mode will reset ip configuration.
Are you sure you want to continue? (y/n) y
```

2. スタティック IP アドレスを使用している場合は、次のコマンドを実行して、IP アドレスを設定します。

```
L3SW> config network protocol <none/bootp/dhcp>

L3SW> config network protocol none
Changing protocol mode will reset ip configuration.
Are you sure you want to continue? (y/n) y

L3SW> config network parms <ipaddr> <netmask> [gateway]

L3SW> config network parms 172.30.10.101 255.255.255.0 172.30.10.2
```

ここで、172.30.10.101 と 172.30.10.2 は、それぞれネットワークポートとデフォルトゲートウェイの IP アドレスです。

本製品がレイヤ 3 スイッチとして設定されている場合は、6 節を参照して、スイッチ内の IP ポートを設定します。本製品は、ネットワークポートのいずれかに割り当てられた IP アドレスを使用してインバンドで管理できます。

サービスポート経由の管理がサポートされるのは、直接接続された IP サブネットからだけです。

WBI、SNMP、または CLI セッションの確立を試みる前に、管理ステーションから ping コマンドを実行して、本製品への接続性を確認しておいてください。

3.2.6 ログインユーザのセットアップ

本製品にアクセスして管理しようとするすべてのユーザに、ユーザ ID とパスワードが必要です。パスワードは、MD5 暗号化形式で保存されます。本製品は、次の複数のレベルのアクセス権限をサポートします。

- 読み取り専用レベルのアクセス:「show」コマンドを実行して設定やスイッチ統計を表示する際に使用します。
- 読み書き(admin)レベルのアクセス:config、reset、save、clear、debug の各コマンドを実行して、本製品の設定、管理、トラブルシューティングを実行する際に使用します。admin アカウントは、設定済みで削除できませんが、パスワードは変更できます。ネットワーク管理者は、ユーザレベル(読み取り専用または読み書き)アクセス権限を持つログインアカウントを作成できます。

ユーザアカウントを作成したり、管理したりするには、次の CLI コマンドのセットを使用できます。

- ユーザアカウントを作成するには、次のコマンドを実行します。

```
L3SW> config users add <name>

L3SW> config users add netadmin
```

- ユーザアカウントを削除するには、次のコマンドを実行します。

L3SW> config users delete <name>

```
L3SW> config users delete netadmin
```

- 既存のユーザのパスワードを変更するには、次のコマンドを実行します。

L3SW> config users password <user>

```
L3SW> config users password netadmin
Enter old password:*****
Enter new password:*****
Confirm new password:*****
Password Changed!
```

- 現在のユーザのリストを表示するには、次のコマンドを実行します。

L3SW> show users

```
L3SW> show users
```

```
L3SW>show users

User Name Access Node
---------------------
admin    Read/Write
debug    Read Only
guest    Read Only

L3SW>
```

図 3-1：ユーザリストの表示

3.2.7 telnet アクセスのセットアップ

本製品への telnet セッションは、管理ステーション上で telnet クライアントソフトウェアを起動すれば開始できます。たとえば、Windows が動作している PC から、「telnet a.b.c.d」と入力します（a.b.c.d はスイッチポートの IP アドレス）。

有効なユーザ ID とパスワードを入力したら、CLI プロンプトが表示されます。

admin 権限を持つユーザは、telnet サービスに関連する次のパラメータを設定できます。

- Configure maximum number of sessions：CLI を通じて、5 つまでの同時 telnet セッションを設定できます。

  L3SW> config telnet maxsessions <0-5>

  ```
  L3SW> config telnet maxsessions 3
  ```

- Enable/Disable telnet Mode：telnet 経由の管理を有効または無効にするには、次のコマンドを実行します。

  L3SW> config telnet mode <enable/disable>

  ```
  L3SW> config telnet mode enable
  ```

- Inactivity Timeout：telnet セッションは、アイドル状態で数分（0～160 分）経過した後、自動的にタイムアウトするよう設定できます。

  L3SW> config telnet timeout <0-160>

```
L3SW> config telnet timeout 10
```

telnet のタイムアウト時間を 0 分に設定した場合、telnet セッションでタイムアウトは発生しなくなります。

同時に複数の telnet 管理セッションがアクティブな場合は、複数の telnet セッションから config コマンドが実行されると、競合が発生して互いにクラッシュしてしまいます。このようなシナリオでは、最後に実行された config コマンドが有効になります。WBI や SNMP からコマンドが同時に実行された場合も同様です。一般的に、セッションを 1 つだけアクティブする場合は、admin 権限を使用し、複数のセッションをアクティブする場合は、読み取り専用の権限を使用するよう推奨します。

3.2.8 高度な機能セットのアクティブ化

BGP、DVMRP、PIM-DM、PIM-SM などアドバンス機能を有効にするには、フルレイヤ 3 ライセンス（別売）のライセンスキーをインストールする必要があります。ライセンスキーでアドバンス機能を有効にするまで、CLI と WBI の各インタフェース上にあるこれらの機能に関連するすべてのコマンドは使用不可の状態になっています。

フルレイヤ 3 ライセンスを購入した後、ライセンスキーを入手するためには、challenge メッセージ（スイッチ固有の詳細情報をエンコードしたもの）を取得する必要があります。challenge メッセージを取得するためには、次のコマンドを実行します。

取得した challenge メッセージは弊社または弊社販売代理店からの求めに応じて提供してください。

```
L3SW> show license info <smmary/detailed>
```

```
L3SW> show license info summary
```

```
L3SW>show license info summary

Challenge... ED34590F248A54F2821467FAACD3281B

Feature Name  State
------------  ----------
Basic         Enabled
Advanced      Disabled
```

表 3-1：ライセンスの要約情報の表示

表 3-1 は、ライセンス要約情報の例です。ライセンスキーを取得する場合、show license info コマンドによって表示されたライセンス要約情報の中から、challenge メッセージの部分を弊社または弊社販売代理店に提供する必要があります。その後、弊社または弊社販売代理店から発行されるフルレイヤ 3 ライセンスのライセンスキーを使ってアドバンス機能を有効化します。

次のコマンドを実行して、ライセンスキーを入力します。

```
L3SW> config license <feature name> <license key>
```

feature name パラメータには「advanced」を指定します。ライセンスキーは、32 桁の 16 進数の

文字列で構成されています。

```
L3SW> config license advanced 256789F214FBDE406743820B521A71BA
```

スイッチの不揮発性領域にライセンスキーが適切に保存されていることを確認するには、show license info detailed コマンドを実行します。表 3-2 に、スイッチに表示されるライセンスの詳細情報を示します。

```
L3SW>show license info detailed

Permanent License Challenge ..... ED34590F248A54F2821467FAACD3281B

Evaluation License Challenge ..... EE8237652456A32B18E65FAC93FB18CD

                                                                  Time      Time
Feature Name   State      License Key                             Granted   Left

------------   ----------  --------------------------------   -------  -----

Basic          Enabled
Advanced       Permanent   256789F214FBDE406743820B521A71BA
```

表 3-2:ライセンスの詳細情報の表示

ライセンスキーをインストールした後、高度な機能セットをアクティブにするには、スイッチを再起動する必要があります。次のコマンドを実行して、高度な機能セットをアクティブにします。

```
L3SW> reset system
```

After inputting the license key, the system must be rebooted using "reset system" command.

ライセンスキーを入力した後、「reset system 」コマンドを使用してシステムを再起動する必要があります。

3.2.9 WBI アクセスのセットアップ

WBI 経由で本製品を管理するには、互換性のある Web ブラウザを使用する必要があります。推奨する Web ブラウザは、Microsoft Internet Explorer(バージョン 5.5 以上)です。

スイッチに接続するには、http://a.b.c.d(a.b.c.dはサービスポートまたはネットワークポートに割り当てられているIPアドレス)形式のURLを使用します。サービスポートまたはインバンドポートを管理用に設定するには、「3.2.4 サービスポートアクセスのセットアップ」(P.10)と「3.2.5 ネットワークポートアクセスのセットアップ」(P.10)を参照してください。

接続が確立すると、ブラウザには図 3-2 に示すようなログイン画面が表示されます。

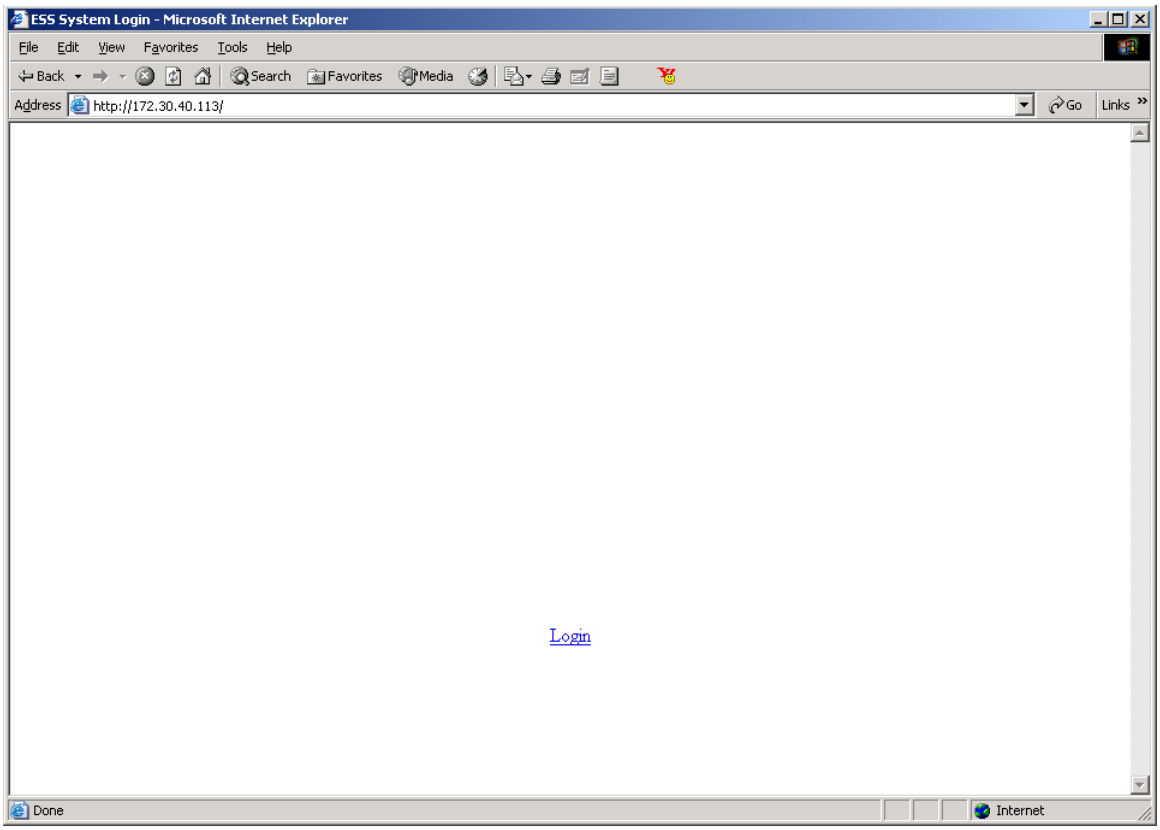

図 3-2：WBI ログイン画面

[Login]リンクをクリックすると、図 3-3 に示すようなユーザ認証ウィンドウが表示されます。

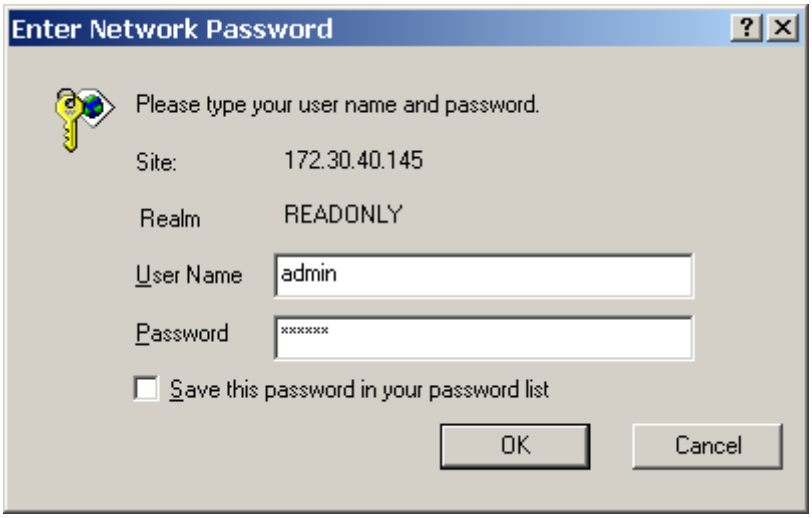

図 3-3：ユーザ認証ウィンドウ

有効なパスワードとユーザ名を入力すると、図 3-4 に示すような WBI 管理インタフェースが表示されます。

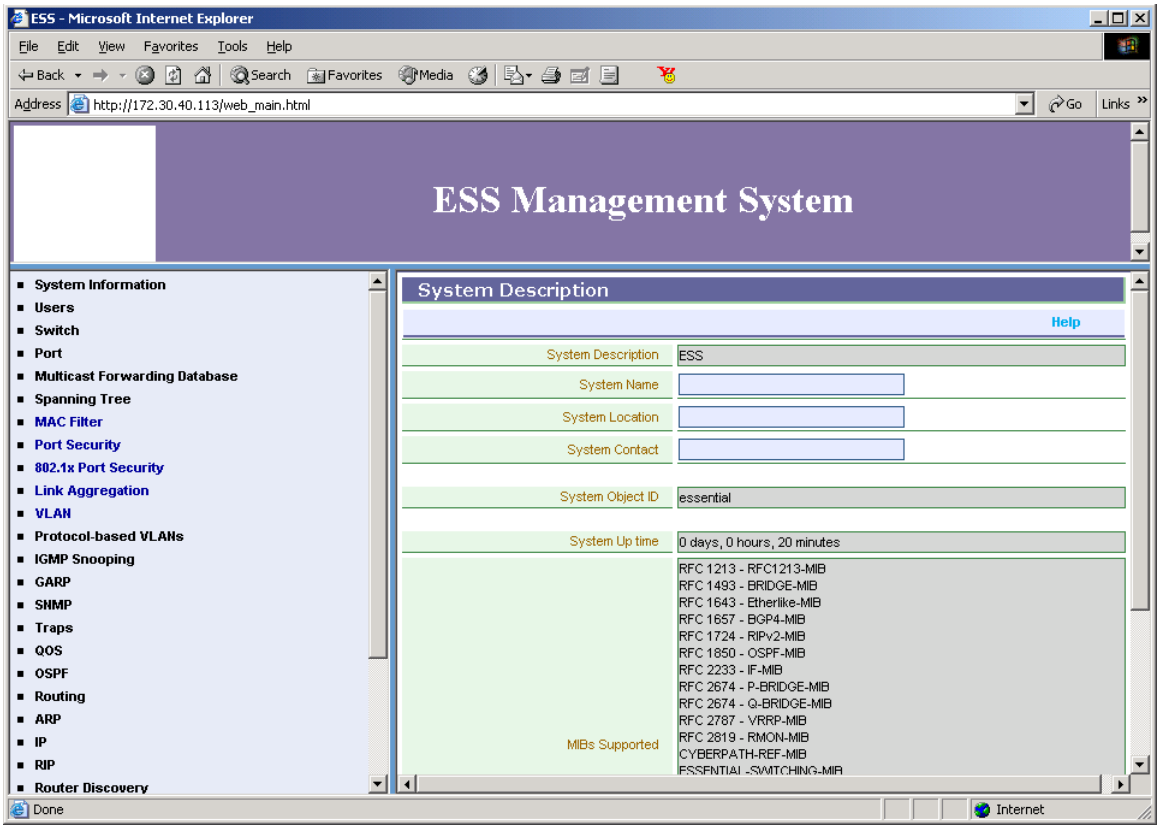

図 3-4:WBI 管理インタフェース

適切な設定画面を選択するには、ブラウザウィンドウの左側に表示されるナビゲーションツリーを使用する必要があります。ナビゲーションツリーでは、本製品がサポートしているさまざまな機能の設定がフォルダ構造でまとめられています。ブラウザウィンドウの右側には、対応する設定画面が表示されます。

3.2.9.1 Java アプレットの有効化

WBI で Java アプレットを有効にすれば、本製品のフォトリアルなビューが表示できるようになります。このビューは、さまざまなポートの状態を視覚的に示すもので、さまざまなポートの設定に使用することもできます。

CLI から WBI Java アプレットモードをアクティブにするには、次のコマンドを実行します。

L3SW> config network javamode <enable/disable>

```
L3SW> config network javamode enable
```

WBI から WBI Java アプレットをアクティブにするには、下図に示すように、Switch¥WBI Interface Configuration ナビゲーションツリーをクリックし、右側の画面の[Java Mode]のドロップダウンコントロールから[Enable]を選択して[Submit]ボタンをクリックします。

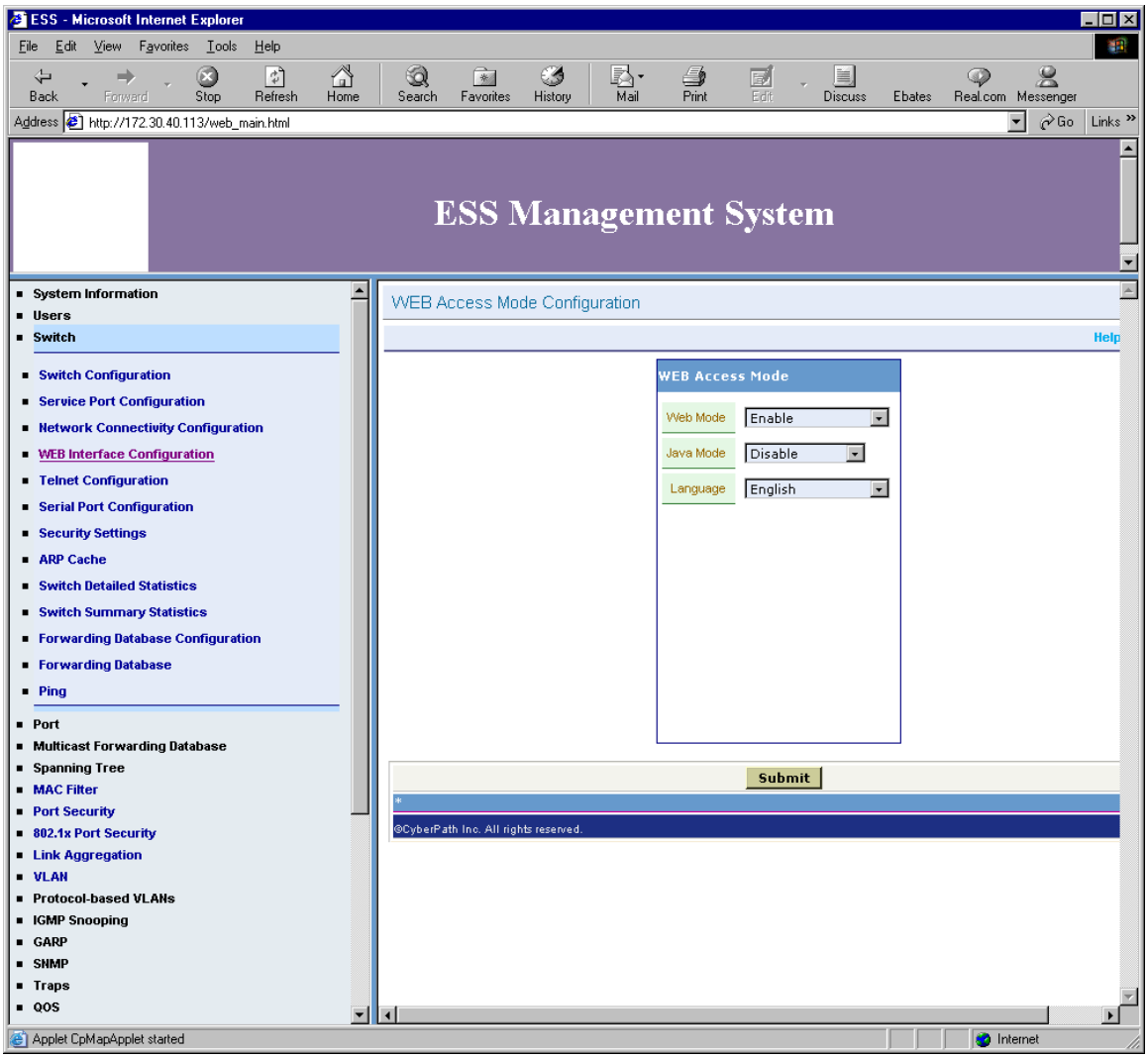

図 3-5：WBI から Java アプレットを有効にする

下図に示すように、ブラウザウィンドウの上部に、本製品のフォトリアルなビューが表示されます。

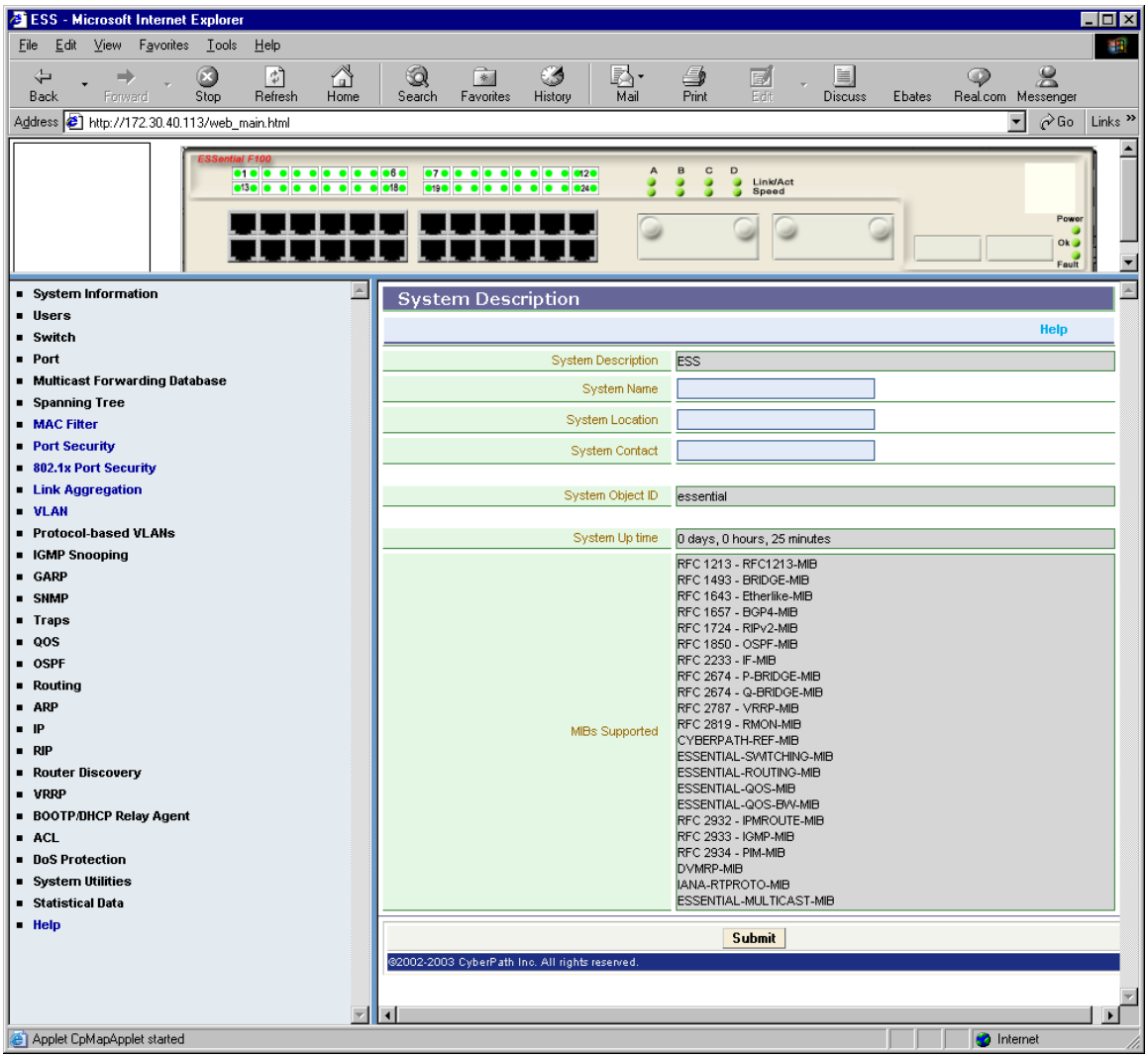

図 3-6：Java アプレットを使用した画面

フォトリアルなビュー内の任意のポートを右クリックすると、そのポートを設定することができます。

Java モードで正常に動作させるには、管理ステーションに JDK（バージョン 3.1 以上）がインストールされているか、インターネットに接続している必要があります。インターネットに接続していれば、管理ステーションに JDK がインストールされていない場合でも、自動的にインターネットから正しい JDK コンポーネントをダウンロードしようとします。

3.2.9.2 言語の設定

WBI がサポートしている言語は、英語と中国語です。

CLI から WBI の言語を変更するには、次のコマンドを実行します。

L3SW> config language <english/chinese>

```
L3SW> config language chinese
```

WBI から WBI の言語を変更するには、Switch¥Web Interface Configuration ナビゲーションツリーをクリックし、右側の画面の［Language Mode］のドロップダウンコントロールから［Enable］を選

択して[Submit]ボタンをクリックします。この表示のスクリーンキャプチャは、図 3-5 を参照してください。

3.2.9.3 言語の表示

CLI から現在の WBI の言語設定を表示するには、次のコマンドを実行します。

```
L3SW> show language
```

```
L3SW> show language
```

WBI から現在の WBI の言語設定を表示するには、Switch¥Web Interface Configuration ナビゲーションツリーをクリックします。

3.2.10 SNMP アクセスのセットアップ

SNMP アクセス用にセットアップするには、コミュニティ名、IP アドレス、およびアクセスモードを設定する必要があります。

- CLI から SNMP コミュニティ名を設定します

```
L3SW> config snmpcommunity create <name>
```

name は SNMP コミュニティ名（16 文字まで）です。

```
L3SW> config snmpcommunity create marketing
```

- CLI から SNMP アクセス用の IP アドレスとマスクを設定します（デフォルトの IP アドレスは 0.0.0.0）

```
L3SW> config snmpcommunity ipaddr <ipaddr> <name>
```

```
L3SW> config snmpcommunity ipaddr 172.30.10.101 marketing
```

```
L3SW> config snmpcommunity ipmask <ipmask> name
```

```
L3SW> config snmpcommunity ipmask 172.30.40.201 marketing
```

- CLI から SNMP アクセスモードを設定するには、次のコマンドを実行します

```
L3SW> config snmpcommunity accessmode <ro/rw> <name>
```

```
L3SW> config snmpcommunity accessmode ro marketing
```

上記のコマンドは、「marketing」という SNMP コミュニティ名に「読み取り専用」アクセス権限を設定する際に使用します。

「show traplog」コマンドを実行すると、トラップイベントの発生が絶対時間で表示されます。トラップイベントの発生時間を特定する場合に、SNMP マネージャに送信されるトラップメッセージで使用される相対時間（sysUpTime）より絶対時間の方が便利であるため、トラップログ情報の表示に絶対時間が使用されます。

3.3 リモートモニタリング（RMON）

3.3.1 概要

RMON は、現在および履歴の MAC 層の統計やコントロールオブジェクトを定義する標準の MIB です。この MIB を使用して、ネットワークマネージャは、ネットワーク全体のリアルタイム情報をキャプチャできます。RMON 規格は、イーサネットに関する RFC 1757（以前の RFC 1271）で定義されています。

通常の RMON 構成は、中央のネットワーク管理ステーションと、RMON エージェントと呼ばれるリモートモニタリングデバイスから成ります（たとえば、本製品は RMON エージェントです）。管理ステーションから、RMON からの情報を要求する SNMP コマンドを発行できます。RMON エージェントは、要求された情報を管理ステーションに送信します。管理ステーションとの通信ができなかったり、効率的でなかったりした場合でも、MIB によって、診断を実行したり、統計を継続的に収集したりするようネットワークエージェントを設定できます。また、例外的な状況が発生した場合に、ネットワークエージェントは管理ステーションに通知しようとします。

MIB 内のオブジェクトは、Ethernet statistics、history control、Ethernet history、alarm、host、hostTopN、matrix、filter、packet capture、および event group という各グループに分けられます。RFC によると、これらのグループの一部はオプションです。

本製品には、Ethernet statistics、history control、Ethernet history、alarm、および event group の MIB が実装されています。

3.3.2 RMON の設定

MIB グループに関連する RMON を設定できるのは、SNMP インタフェースを経由した場合だけです。Set 操作を実行するには、SNMP 管理ステーションで適切なコミュニティストリングが使用される必要があります。次に、本製品がサポートしている RMON グループについて説明します。

3.3.2.1 event group

event group は、本製品からのイベントの生成と通知を制御し、eventTable と logTable で構成されます。

3.3.2.1.1 eventTable

eventTable 内の各エントリは、トリガできるイベントのパラメータを示します。イベントは、実行されるアクションのタイプです。たとえば、リンクは、イベントに基づいてアップまたはダウンします。

オプションで、各イベントエントリは、イベント発生時に作成されるログエントリを指定できます。また、イベント発生時に SNMP トラップを生成するよう指定することもできます。トラップメッセージのコミュニティは、関連付けられた eventCommunity オブジェクト内で指定されます。risingAlarm トラップと fallingAlarm トラップは、イベントを生成する標準のトラップとして RMON MIB 内に定義されます。これらのトラップを使用するのは、イベントを生成する場合だけです。

デフォルトで、eventTable 内に 13 個のエントリを作成します。各エントリの eventDescription 属性は、各イベントエントリの目的を示しています。

これらのエントリが作成されるため、外部のマネージャは新しいエントリを作成する代わりに、こ

れらの定義済みのエントリを使用できます。ただし、外部のマネージャが新しいイベントエントリを作成したい場合は、最初に SNMP Set 要求を送信し、eventStatus に createRequest(2)を設定します。ネットワークエレメントが Set 要求を受信したら、eventStatus に underCreation (3)が表示されます。これで、マネージャはこのイベントエントリの各フィールドに適切な値を設定できます。たとえば、eventType を none (1) 、log (2) 、snmptrap (3) 、または logandtrap (4)のいずれかの値に設定できます。

eventStatus 属性が valid (1)に設定されると、変更が有効になります。eventStatus が valid (1)に設定されると、このイベントエントリの他の属性は変更できなくなることに注意してください。その後、このエントリに対して実行できる操作は削除だけです。削除するには、Set 要求を発行して、eventStatus を invalid (4)に変更します。

eventTable に対して 138 個までのエントリをサポートします。デフォルトで作成されているエントリでは、eventOwner ストリングが「monitorEvent」に設定されており、所有者が本製品であることを示します。

作成したエントリは、eventTable に Get 要求を発行すれば、SNMP マネージャ経由で表示できます。CLI から、作成したエントリを表示するには、次のコマンドを実行します。

L3SW > show rmon event <all/eventId>

L3SW > show rmon event <all/eventId>

このコマンドでは、指定した eventIndex に対してログ記録されたイベントに関する情報も表示されます。ログ記録された情報は、次の属性で構成されます。

- logIndex
- logTime
- logDescription

```
L3SW>show rmon event all
eventlndex _ _           :1
eventDescription         :No Action
eventE ventType          :none(1)
eventCommunity           :public
eventLastTimeSent        :0days 00h:00m:00s
eventOwner               :monitorEvent
eventStatus              :valid(1)
loglndex     logTime          logDescription
Are you sure to display one more entry? (y/n) y
eventlndex _             :2
eventDescription         :Send Trap
eventEventType           :log-and-trap(4)
eventCooomunity          :public
eventLastTimeSent        :0days 00h:00oa:00s
eventOwner               :monitorEvent
eventStatus              :valid(1)
loglndex     logTime          logDescription
Are you sure to display one more entry? (y/n)
```

図 3-7:RMON のイベントの表示

3.3.2.1.2 logTable

logTable は、eventIndex と logIndex でインデックス化され、ログ記録されたイベントのリストを保持します。各種の eventIndex に対して 10 個までのログエントリをサポートします。ログエントリを SNMP ブラウザに表示するには、logTable に Get 要求を発行するか、イベント情報を付けた次の CLI コマンドを実行します。

L3SW > show rmon event <all/eventId>

L3SW > show rmon event all

3.3.2.2 alarm グループ

alarmGroup モジュールは、本製品から統計サンプルを定期的に収集し、それらの値を設定済みのしきい値と比較します。モニタリングしている変数が、しきい値を横切ると、イベントが生成されます。ユーザは、このようなしきい値を横切るかどうかをモニタリングしている変数のエントリを alarmTable 内に作成する必要があります。

3.3.2.2.1 alarmTable

alarmTable には、変数、そのポーリング期間、およびしきい値のパラメータを定義する設定エントリが保存されます。サンプルがしきい値を横切ったことが判明すると、イベントが生成されます。この方法でモニタリングできるのは、ASN.1 のプリミティブな型である INTEGER(整数)の変数だけです。ユーザは、定義済みのイベントエントリの一つから eventIndex を指定し、ログやトラップなどの適切なアクションを実行する必要があります。

本製品は、アクティブな各物理ポートに 1 つのデフォルトのエントリを作成します。これらのデフォルトのエントリは、alarmInterval 時間(つまり、各サンプルの時間)を 30 秒に定義します。この

ようなデフォルトの各エントリは、そのインタフェース上で受信したブロードキャストパケットをモニタリングします。また、上昇アラームに定義済みの eventIndex 8、下降アラームに eventIndex 9 をそれぞれ使用します。さらに、インタフェースのタイプに応じて、定義済みの上昇や下降のしきい値も使用します。

外部のマネージャが新しいアラームエントリを作成したい場合は、最初に SNMP Set 要求を送信し、alarmStatus に createRequest (2)を設定する必要があります。要求が完了したら、alarmStatus の状態が underCreation (3)に変わります。これで、SNMP マネージャはこの alarmEntry の各フィールドに適切な値を設定できます。たとえば、alarmVariable にモニタリングしている OID を設定したり、alarmInterval に新しいサンプリング間隔を秒単位で設定したり、alarmRisingEventIndex に、しきい値が alarmRisingThreshold を上回ると生成される eventTable 内の eventIndex を設定したりすることができます。下降アラームイベントを定義するには、alarmFallingEventIndex に、しきい値が alarmFallingThreshold を下回ると生成される eventTable 内の eventIndex を設定します。最後に、alarmSampleType は、次のいずれかの値に設定されます。

- `AbsoluteValue` (1)
- `DeltaValue` (2)

これらのフィールドが設定されたら、alarmStatus を valid (1)に設定できます。alarmStatus が valid (1)に設定されると このアラームエントリの他の属性は変更できなくなることに注意してください。その後、このエントリに対して実行できる操作は削除だけです。削除するには、Set 要求を発行して、alarmStatus を invalid (4)に変更します。

本製品は、alarmTable に対して 138 個までのエントリをサポートします。デフォルトで作成されるエントリでは、alarmOwner ストリングが「monitorAlarm」に設定されており、所有者が本製品であることを示します。

作成したエントリは、alarmTable に Get 要求を発行すれば、SNMP マネージャ経由で表示できます。CLI から、作成したエントリを表示するには、次のコマンドを実行します。

```
L3SW > show rmon alarm <all/alarmId>

L3SW > show rmon alarm all
```

```
L3SW >show rmon alarm all
alarmlndex                :8
alarmlnterval             :30
alarmlnterval             :etherStatsBroadcastPkts,8
alarmSampleType           :deltaValue(2)
alarmValue                :0
alarmStartup Alarm        :risingAlarm(l)
alarmRisingThreshold      :892800
alarmRisingThreshold      :446400
alarmRisingEventlndex     :8
alarmFallingEventlndex    :9
alarmFallingEventlndex   :monitorAlarm
alarmStatus              :valid(1)
Are you sure to display one more entry? (y/n) y
alarmlndex                :9
alarmlnterval             :3
alarmlnterval             :etherStatsBroadcastPkts, 9
alarmSampleType           :deltaValue(2)
alarmValue                :0
alarmStartupAlarm          :risingAlarm(l)
alarmRisingThreshold       :892800
alarmRingThreshold         :446400
alarmRisingEventlndex      :8
alarmFallingEventlndex     :9
alarmFallingEventlndex     :monitorAlarm
alarmStatus                :valid(1)
L3SW >
```

図 3-8：RMON のアラームの表示

3.3.2.3 history control グループ

historyControlGroup は、さまざまなタイプのインタフェースからのデータの定期的な統計サンプリングを制御します。このグループは、historyControlTable で構成されます。本製品には、historyControlTable が実装されています。ただし、RFC によると、historyControlTable はオプションです。

historyControlTable には、インタフェース（ポーリング期間や他のパラメータ）を定義する設定エントリが保存されます。historyControlDataSource は、サンプリングが必要なオブジェクト ID（OID）を定義します。OID は、関連するすべてのカウンタを効果的に収集するインタフェース自身のことです。historyControlInterval は、その OID に対して実行するサンプリングの間隔を秒単位で定義します。historyControlBucketsRequested は、保存するよう要求されたバケットまたはインスタンスの数を定義します。historyControlBucketsGranted は、保存するよう要求されたバケットに対して、許可されたバケット数を定義します。この制限は、本製品内のリソースに限りがあるためです。historyControl エントリごとに 10 を超えるバケットを指定することはできません。

各物理ポートに 2 つのデフォルトエントリを作成します。1 つは 30 秒のサンプリングで、もう 1 つは 1800 秒（つまり、30 分）のサンプリングです。また、各エントリに 30 個のバケットを割り当てると、最後の 10 個のインスタンスデータは 30 秒の間隔と 30 分の間隔で利用できます。履歴データは、後述する historyTable に保存されます。

外部のマネージャが新しい historyControlEntry を作成したい場合は、最初に SNMP Set 要求

を送信し、historyControlStatus に createRequest (2)を設定する必要があります。ネットワークエレメントが Set 要求を受信したら、historyControlStatus の状態が underCreation (3)に変わります。これで、マネージャは、この historyControlEntry の各フィールドに適切な値を設定できます。たとえば、historyControlDataSource にモニタリングする必要があるインタフェースの ifIndex を設定したり、historyControlInterval にサンプリング間隔を秒単位で設定したり、historyControlBucketsRequested に保存したいバケット／インスタンスの数を設定したりすることができます。

これらのフィールドが設定されたら、historyControlStatus 属性を valid (1)に設定する必要があります。historyControlStatus が valid (1)に設定されると この historyControlEntry の他の属性は変更できなくなることに注意してください。その後、このエントリに対して実行できる操作は削除だけです。削除するには、Set 要求を発行して、historyControlStatus を invalid (4)に変更します。

L3SW > show rmon history <all/slot.port>

```
L3SW > show rmon history all
```

3.3.2.4 Ethernet history グループ

ethernetHistoryGroup は、イーサネットインタフェースからの定期的な統計サンプルを記録して保存し、後で検索できるようにします。このグループは、etherHistoryTable で構成されます。本製品には、etherHistoryTable が実装されています。ただし、RFC によると、etherHistoryTable はオプションです。

etherHistoryTable は、Ethernet history エントリのリストで構成されます。各エントリには、イーサネットインタフェースの Ethernet statistics の履歴サンプルが保存されます。履歴サンプルは、これらのサンプルを定期的に収集するためのパラメータをセットアップする historyControlEntry に関連付けられます。統計サンプルには、次の情報が含まれています。

- **etherHistoryIntervalStart**
- **etherHistoryDropEvents**
- **etherHistoryOctets**
- **etherHistoryPkts**
- **etherHistoryBroadcastPkts**
- **etherHistoryMulticastPkts**
- **etherHistoryCRCAlignErrors**
- **etherHistoryUndersizePkts**
- **etherHistoryOversizePkts**
- **etherHistoryFragments**
- **etherHistoryJabbers**
- **etherHistoryCollisions**
- **etherHistoryUtilization**

10 個のインスタンスが予約されています。それぞれは、デフォルトで作成された対応する historyControlEntry に関連付けされている各インタフェースに対する 30 秒のサンプリングと 30 分のサンプリング用です。ただし、これらのインスタンス内の値が意味を持つのは、これらのインスタンス内にデータが入力されるのに十分な時間が経過した場合だけです。

履歴データを SNMP 経由で表示するには、etherHistoryTable に GET 要求を発行します。CLI から履歴データを表示するには、次のコマンドを実行します。

L3SW > show rmon history <all/slot.port>

```
L3SW > show rmon history all
```

出力は、サンプリングされた各データの対応する historyControlEntry を示します。

3.3.2.5 Ethernet statistics グループ

ethernetStatisticsGroup には、モニタリングされた各イーサネットインタフェースに対して本製品が測定した統計が含まれています。このグループは、etherStatsTable で構成されます。本製品には、etherStatsTable が実装されています。ただし、RFC によると、etherStatsTable はオプションです。

etherStatsTable は、Ethernet statistics エントリで構成されます。各エントリには、1 つのイーサネットインタフェースに対して測定した統計が保存されます。これらの統計は、エントリが作成されると、ゼロから始まるカウンタが実行される形式をとります。エントリは、システムが起動するとデフォルトで作成されます。エントリは、SNMP ブラウザから SET 操作を使用して作成することはできません。

etherStatsTable 内の各エントリには、次の情報が含まれています。

- etherStatsDataSource
- etherStatsDropEvents
- etherStatsOctets
- etherStatsPkts
- etherStatsBroadcastPkts
- etherStatsMulticastPkts
- etherStatsCRCAlignErrors
- etherStatsUndersizePkts
- etherStatsOversizePkts
- etherStatsFragments
- etherStatsJabbers
- etherStatsCollisions
- etherStatsPkts64Octets
- etherStatsPkts65to127Octets
- etherStatsPkts128to255Octets
- etherStatsPkts256to511Octets
- etherStatsPkts512ti1023Octets
- etherStatsPkts1024to1518Octets
- etherStatsOwner
- etherStatsStatus

デフォルトで作成された各エントリの etherStatsStatus は valid (1)に設定されます。

Ethernet statistics データを SNMP 経由で表示するには、etherStatsTable に GET 要求を発行します。CLI から Ethernet statistics データを表示するには、次のコマンドを実行します。

L3SW > show stats port detailed <slot.port>

L3SW > show stats port detailed 0.9

```
L3SW>show stats port detailed 0.9

Total Packets Received (Octets) ..........  3351718
Packets Received 64 Octets  ..............  3
Packets Received 65-1 27 Octets  .........  1 1 03
Packets Received 1 23-255 Octets  ........  23
Packets Received 256-511 Octets  .........  4
Packets Received 51 2-1 023 Octets  ......  3
Packets Received 1024-1513 Octets  .......  2133
Packets Received 1519-1530 Octets  .......  0
Packets Received } 1530 Octets  ..........  0
Total Packets Received Without Errors  ...  3279
Unicast Packets Received  ................  3229
Multicast Packets Received ...............  0
Broadcast Packets Received  ..............  50

Total Packets Received with MAC Errors ....  0
Jabbers Received  ........................  0
Fragments/Undersize Received  ............  0
Alignment Errors  ........................  0
FCS Errors  ..............................  0
Overruns  ................................  0
--More—or (q)uit
```

図 3-9：RMON の詳細なポート統計の表示

3.3.2.6 CLI の特殊キー

CLI では、さまざまなキーの組み合わせを使用して、コマンド履歴やコマンドヘルプなどを検索できます。表 2-1 に、CLI でサポートされている特殊キーのリストを示します。

Backspace	文字を消去します
Ctrl-U	行を削除します
Ctrl-W	最後の単語を消去します
Ctrl-C	現在の入力を中断し、次の行に移動します
Ctrl-F	右に 1 文字移動します
Ctrl-B	左に 1 文字移動します
Ctrl-A	行頭に移動します
Ctrl-E	行末に移動します
Ctrl-H	ポインタより左の文字を削除します
Ctrl-D	ポインタより右の文字を削除します
Ctrl-K	行末で強制終了します
Ctrl-P	履歴バッファ内の前の行に移動します
Down-arrow	元の行に戻ります
Exit	現在のモードから前のモードに移行します

End	現在のコマンドレベルを中断し、最初のレベルのプロンプトに戻ります
Tab	コマンドライン補完を使用するには、<Tab>キーを押します
Up-arrow	以前に入力したコマンドをスクロールして表示します
?	コマンドヘルプを表示します

表 3-3：CLI 操作用の特殊キー

3.3.2.7 CLI のエラーメッセージ

正しくない設定、正しくない構文、または不完全なコマンドの応答として、さまざまなメッセージが表示されます。これらのメッセージの一部を以下に紹介します。

ユーザが入力したコマンドが認識されなかったり、読み取り専用のユーザが config コマンドにアクセスしようとしたりした場合は、次のメッセージが表示されます。

Command not found! Use ? to list commands.

- コマンドのパラメータが正しくないか、範囲外である場合は、次のようなメッセージが表示されます。

Incorrect input! Use 'name <"name"> <1-4094>'

3.3.2.8 CLI のヘルプ

特定の CLI ツリー内にあるすべての CLI コマンドのリストや個々のコマンド／パラメータの詳細な構文を表示するには、CLI プロンプトで「?」文字を入力します。

4. システム設定とユーティリティコマンド

4.1 電源投入時セルフテスト(POST)結果の表示

show post コマンドを実行すると、POST の結果に関連する情報が表示されます。POST でテストされるコンポーネントは、ASIC、CAM、コンパクトフラッシュ、ハードウェアモニタ、管理ポート、すべての物理ポート、RDRAM、および SDRAM などです。

L3SW> show post

```
L3SW> show post
```

「show post」コマンドの応答には、ポート 1.1 から 1.4 までを含むすべてのポートに対する内部 MAC レベルのテスト結果だけが表示されます。その結果、ポート 1.1 と 1.2 にモジュールが装着されていない場合でも、これらのポートに対する「show post」コマンドの応答として「PASS」が表示されることがあります。

4.2 CPU 負荷のモニタリング

CPU 負荷のしきい値と、最新の 1 分間、5 分間、15 分間の平均 CPU 負荷を表示するには、次のコマンドを実行します。

L3SW> config cpuloadthreshold <hi-threshold (1-100)> <lo-threshold (1-100)>

```
L3SW> config cpuloadthreshold 70 40
```

CPU 負荷のしきい値と、最新の 1 分間、5 分間、15 分間の平均 CPU 負荷を表示するには、次のコマンドを実行します。

L3SW> show cpuload

```
L3SW> show cpuload
```

```
L3SW>show cpuload

          CPU Hi Threshold(%)           70
          CPU Low Threshold             40
        CPU Load (1min, 5min, 15min)  2 2 2

                      L3SW>
```

表 4-1:CPU 負荷の表示

4.3 Shell モード

UNIX ライクな Shell モードで、ping や traceroute などの一般的に使用されるユーティリティコマンドを実行することができます。Shell モードでは、pwd や ls などの Shell コマンドもサポートされています。これらのコマンドは、通常のコマンドの場合と同様に、すべてのコマンドレベルのオプションをサポートしています。Shell モードでは、コマンドリコールや状況依存型ヘルプなどの ESS CLI モードの操作はサポートされていません。また、Shell モードでは、すべての ESS CLI コマンドがブロックされます。ESS CLI コマンドにアクセスする場合は、Shell モードを終了する必要があります。現時点でサポートされているのは、これらの 2 つのコマンドだけです。将来的には、他の機能もサポートされる予定です。Shell モードに移行するには、次のコマンドを実行します。Shell モードでは、コマンドプロンプトが「$」になります。

L3SW> shell

```
L3SW> shell
$
```

Shell モードに移行すると、ping や traceroute などのコマンドを実行できます（次図）。

表 4-2に、tracerouteコマンドに?オプションを付けて実行した結果を示します。

```
$ traceroute 172.30.40.2
$ traceroute -?
```

```
$traceroute -?

Traceroute: invalid option --?
BusyBox v0.60.2 (2004.05.18-14:04:0000) multi-call binary

Usage: traceroute [-dnrv] [-m max_ttl] [-p port#] [-q
nqueries]
        [-s src_addr] [-t tos] [-w wait] hos [data size]
L3SW>
```

表 4-3：Shell モードでの traceroute の表示

4.4 スイッチ設定

4.4.1 インベントリ

show inventory コマンドを実行すると、すべての製品情報が表示されます。この情報には、MAC アドレス、ソフトウェアバージョン、ハードウェアチップバージョン、マシンタイプ、モデルとシリアル番号、パート番号が含まれます。

```
L3SW>show inventory
System Description  ..................... Layer3 Switch
Machine Type  ..........................  L3-200
Machine Model  .........................  1000TX
Serial Number  .........................  GA04040010
Part Number  ...........................  070-00024-20
Maintenance Level,  ....................  24333
Manufacturer  ..........................  0x0002
Burned In MAC Address  .................  00:50:A8:00:03:00
Software Version,  .....................  2.5.0.7
Operating System,  .....................  Linux version 2.4.17_mv121-ess
Network Processing Device  .............  CXE1000 REV k
Additional Packages  ...................  BGP-4
                                          Bandwidth Provisioning
                                          Multicast
L3SW>
```

L3SW> show inventory

表 4-4:スイッチのインベントリの表示

インベントリ情報は、製造時に作成され、ユーザが変更することはできません。

4.4.2 システム情報

show sysinfo コマンドを実行すると、RFC 1213 MIB-II 情報を表示することができます。この情報には、システムの説明、システム名、システムの設置場所、システムの問い合わせ先、システムのオブジェクト ID、システムの稼動時間が含まれます。表 4-5 に本製品のシステム情報詳細の表示を示します。

L3SW> show sysinfo

```
L3SW>show sysinfo
System Description  ..................  Layer3 Switch
System Name  ........................
System Contact  .....................
System Object ID  ...................  l3switch
IP Address  .........................  0.0.0.0
System Up Time  .....................  0 days 0 hrs 18 mins 2 secs
System Time  ........................  2002-08-02 01:32:34 UTC+00:00
MIBs Supported:
RFC 1213 - RFC1213-MIB     Management Information Base for Network
                           Management of TCP/IP-based internets: MIB-II
RFC 1493 - BRIDGE-MIB      Definitions of Managed Objects for Bridges
                           (dotld)
RFC 1643 - Ether like-MIB  Definitions of Managed Objects for the
                           Ethernet-like Interface Types (dot3)
— More— or (q)uit

RFC 1657 - BGP4-MIB        Definitions of Managed Objects for the
Fourth
                           Version of the Border Gateway Protocol (BGP-
4)
                           using SMIv2
RFC 1724 - RIPv2-MIB       RIP Version 2 MIB Extension
RFC 1850 - OSPF-MIB        OSPF Version 2 Management Information Base
RFC 2233 - IF-MIB          The Interfaces Group MIB using SMIv2
RFC 2674 - P-BRIDGE-MIB   Definitions of Managed Objects for Bridges
with
Q-BRIDGE-MIB               Traffic Classes, Multicast Filtering and
                           Virtual LAM Extensions
RFC 2787 - VRRP-MIB        Definitions of Managed Objects for the
Virtual
                           Router Redundancy Protocol
RFC 2819 - RMON-MIB        Remote Network Monitoring Management
                           Information Base
ESSENTIAL-SWITCHING-MIB    ESSENTIAL Switching - Layer 2
— More— or (q)uit
ESSENTIAL-ROUTING-MIB      ESSENTIAL Routing - Layer 3
ESSENTIAL-QOS-MIB          ESSENTIAL Flex QOS support
ESSENTIAL-QOS-BW-MIB       ESSENTIAL Flex QOS Bandwidth Allocation
RFC 2932 - IPMROUTE-MIB    IPv4 Multicast Routing
MIB RFC 2933 - IGMP-MIB    Internet Group Management Protocol
MIB RFC 2934 - PIM-MIB     Protocol Independent Multicast MIB for IPv4
DVMRP-MIB                  Distance-Vector Multicast Routing Protocol
MIB
IANA-RTPROIO-MIB           IANA IP Route Protocol and IP MRoute
Protocol
                           Textual Conventions
L3SW>
```

表 4-5:システム情報の表示

次のコマンドは、ユーザが変更できる sysinfo のパラメータを定義します。

L3SW> config syscontact <"contact">

L3SW> config syscontact network-administrator

L3SW> config sysname <"name">

```
L3SW> config sysname layer3switch
```

L3SW> config syslocation <"location">

```
L3SW> config syslocation third-floor
```

L3SW> config systime <date> <time> <timezone>

```
L3SW> config systime 2002-08-01 12:22:30 -5:00
```

本製品の時計をネットワークタイムサーバ（NTS サーバ）と同期するように設定するには、次のコマンドを実行します。

L3SW> config timeserver <IP> <interval>

```
L3SW> config timeserver 201.10.0.213 5
```

NTS サーバとの同期を解除にするには、次のコマンドを実行します。

```
L3SW> config timeserver 0.0.0.0 0
```

4.4.3 システムプロンプト

デフォルトでは、システムプロンプトは「ESS rx.x>」（x.x はリリース番号）に設定されています。システムプロンプトを変更するには、次のコマンドを実行します。

ESS r2.5> config prompt <"system prompt">

```
ESS r2.5> config prompt L3SW
```

4.4.4 イッチ設定

スイッチ設定を要約形式で表示するには、次のコマンドを実行します。

```
L3SW> show switchconfig summary
```

```
L3SW>show switchconfig summary

Broadcast Storm Recovery Mode  ..........  Disable
802.3x Flow Control Mode  ..............  Disable
802.1p Priority Mode  ..................  Disable
TOS Priority Mode  .....................  Disable

L3SW>
```

表 4-6：スイッチ設定要約の表示

4.4.5 CAM とテーブルのサイズ

本製品では、連想記憶メモリ(CAM)を使用して、高速なテーブル検索を実現しています。 CAM には、MAC アドレステーブル、IP 転送テーブル、ARP キャッシュ、テーブル、マルチキャストアドレステーブルなどのいくつものテーブルが保存されます。次の表には、0、1、3 番の CAM メモリ設定でサポートされているエントリ数が表示されています。 表 4-7 に、0 CAM、1 CAM 、3 CAM の各設定のルックアップテーブルのサイズが示されています。

項目	テーブルサイズ
IP ルーティング	13824
IP ARP	6992
ダイナミック MAC	14080
L2 マルチキャスト	1024
VLAN	2560
L2 マルチキャスト	1024
CAM のサイズ	40960

表 4-7:テーブルのサイズ

show cam コマンドを実行すると、検出された CAM のサイズとアドレスルックアップテーブルの割り当て情報が表示されます。このテーブルには、IP ルーティングテーブル、IP ARP テーブル、ダイナミック MAC テーブル、L2 マルチキャストテーブル、L3 マルチキャストテーブルが含まれます。 表 4-7 で示す L2 マルチキャストエントリは、GMRP-IGMP スヌーピングから収集されます。一方、L3 マルチキャストエントリは、PIM-DVMRP から収集された RTF(Reverse Tree Forwarding)パスエントリです。

VLAN の数値は、使用できるテーブルのサイズと使用中のサイズです。表 4-7 に、スイッチがサポートしているテーブルのサイズ例を示します。

L3SW> show cam

```
L3SW>show cam

Type       Available  In use
IP Route   13312      6
IP ARP     6784       1
Dyna MAC   13824      1
L2 Mcast   1024       3
VLAM       2560       3
L3 Mcast   1024       64
CAM Size   40960

L3SW>
```

表 4-8:CAM 情報の表示

4.4.6 スイッチ統計

スイッチ管理ポート関連の統計を要約形式で表示するには、次のコマンドを実行します。

L3SW> show stats switch summary

```
L3SW>show stats switch summary

Packets Received Without Error ........  0
Broadcast Packets Received ............  0
Packets Received With Error ...........  0
Packets Transmitted Without Error      0
            Broadcast Packets Transmitted            0
             Transmit Packet Errors                 0
            Address Entries Currently in Use         29
             VLAN Entries Currently in Use          0
 Time Since Counters Last Cleared         0 day 3 hr 11 tnin 7 sec
                                L3SW>
```

表 4-9:スイッチ統計の要約の表示

スイッチ統計の詳細を表示するには、次のコマンドを実行します。

L3SW> show stats switch detail

```
L3SW>show stats switch detail

Packets Received Without Error ........ 0
Multicast Packets Received ............ 0
Broadcast Packets Received ............ 0
Packets Transmitted Without Errors .... 0
Unicast Packets Transmitted ........... 0
Broadcast Packets Transmitted ......... 0
Most Address Entries Ever Used ........ 29
Address Entries Currently in Use....... 29
Maximum VLAW Entries .................. 256
Most VLAM Entries Ever Used ........... 1
Static VLAM Entries ................... 1
VLAM Deletes .......................... 0
— More — or (q)uit
Time Since Counters Last Cleared ...... 0 day 3 hr 13 min 35 sec

L3SW>
```

表 4-10:スイッチ統計の詳細の表示

4.4.7 シリアルポート

show serial シリアルコマンドを実行すると、シリアルポート設定とスイッチのシリアルポートのタイムアウトに関する情報を表示することができます。

L3SW> show serial

```
L3SW>show serial
Serial Port Login Timeout (minutes)  .. 5
Baud Rate  ............................ 9600
Character Size  ....................... 8
Flow Control:  ........................ Disable
Stop Bits  ............................ 1
Parity Type  .......................... None

L3SW>
```

表 4-11:シリアルポート設定の表示

シリアルポートによるログインのタイムアウト時間を変更するには、次のコマンドを実行します。

L3SW> config serial timeout <0-160>

L3SW> config serial timeout 160

タイムアウトなしでシリアルポートをセットアップするには、次のコマンドを実行します。

L3SW> config serial timeout 0

シリアルポートのボーレートを変更するには、次のコマンドを実行します。

L3SW> config serial baudrate <1200/2400/4800/9600/19200/38400/57600/115200>

L3SW> config serial baudrate 115200

通常は、ボーレートとして 9600 が使用されます。115200 のボーレートは、XMODEM モードでファイルをダウンロード／アップロードする際に使用します。外部端末のボーレートとスイッチ上のシリアルポートのボーレートが同じでないと、正常に通信できません。

4.4.8 ネットワーク管理

本製品の管理は、イーサネットサービスポート経由またはネットワークポート経由で実行します。前者をアウトオブバンド管理、後者をインバンド管理とそれぞれ呼びます。ネットワークポート経由のインバンドで管理されている場合、インバンド管理設定の詳細を表示するには、次のコマンドを実行します。

L3SW> show network

```
L3SW>show network

IP Address. ... 172.30.40.103
Subnet Mask, .. 255.255.255.0
Default Gateway. ......................... 172.30.40.2
Burned In MAC Address ..................... 00:50:A8:00:30:00
Locally Administered MAC Address ......... 00:00:00:00:00:00
Network Configuration Protocol Current ...None
Web Mode ................................. Enable
Java Mode ................................ Enable

L3SW>
```

表 4-12:ネットワーク設定の表示

ネットワーク設定を変更するには、「3.2.5 ネットワークポートアクセスのセットアップ」(P.10)を参照してください。

4.4.9 管理サービスポート

アウトオブバンド管理サービスポートの設定を確認するには、次のコマンドを実行します。

L3SW> show serviceport

```
L3SW>show servlceport
IP Address ....  ............................  172.30.40.67
Subnet Mask ...  ............................ 255.255.255.0
Default Gateway. ............................  172.30.40.2
ServPort Configuration Protocol Current .......  DHCP
Burned In MAC Address .......................  00:50:A8:00:30:01

L3SW>
```

表 4-13:管理サービスポート設定の表示

管理サービスポート設定を変更するには、「3.2.4 サービスポートアクセスのセットアップ」(P.10)を参照してください。

4.4.10 Telnet

本製品では、複数の telnet ログインセッションを開始できます。ユーザが現在ログインしているセッションの telnet 情報を表示するには、次のコマンドを実行します。

L3SW> show telnet

```
L3SW>show telnet

Telnet Login Timeout (minutes) ..... 5
Maximum Number of Telnet Sessions ..... 5
Allow Mew Telnet Sessions ..... Yes

L3SW>
```

表 4-14:telnet セッションの詳細

telnet セッションのログイン時のタイムアウト時間を変更するには、次のコマンドを実行します。

L3SW> config telnet timeout <0-160>

L3SW> config telnet timeout 160

telnet ログインタイムアウトを無効にするには、次のコマンドを実行します。

L3SW> config telnet timeout 0

4.4.11 ログ記録

ログメッセージには、7 つのレベルがあります。ネットワーク管理者は、メッセージの重要度を確認することで、適切な管理アクションを実行できます。ログメッセージは次の 7 つのレベルです。

- **0 = 緊急**
- **1 = アラート**
- **2 = 重要**
- **3 = エラー**
- **4 = 警告**
- **5 = 通知**
- **6 = 報告**

すべてのログメッセージは、RAM バッファに保存されます。セキュリティレベルが「緊急」から「エラー」までのメッセージは、メッセージのコピーがフラッシュメモリにも保存されます。不揮発性のフラッシュメモリに保存されたメッセージは再起動後も表示できますが、RAM に保存されたメッセージは再起動後は消去されます。

RAM バッファには 128 個までのメッセージを保存でき、FLASH バッファには 32 個までのメッセージを保存できます。メッセージバッファは、循環キューで構成されているので、すべてのバッファが使用されると最も古いメッセージが破棄され、その領域に新しいメッセージが保存されます。

4.4.11.1 ログ記録設定の表示

ログ設定やシステムメッセージを表示するには、次のコマンドを実行します。表 4-15 にログ生成モードを示します。

L3SW> show lat info

```
L3SW>show lat info
Log Generation Mode ............................. Enable
Log Console Output Mode ......................... Disable
Log syslog Output Mode .......................... Disable
syslog .......................................... Disable
Log Filtering Level ............................. I

L3SW>
```

表 4-15:ログ生成モードの表示

4.4.11.2　ログ記録の有効化／無効化

デフォルトではログ生成モードは有効になっています。ログ生成モードを有効または無効にするには、次のコマンドを実行します。

L3SW> config lat mode <enable/disable>

```
L3SW> config lat mode disable
```

4.4.11.3　ログコンソール表示の設定

ログメッセージをコンソールに表示するか、syslog サーバにリダイレクトするかを定義します。次のコマンドを実行して、シリアルポートに接続したコンソールにログメッセージをリアルタイムで出力するかどうかを設定します。

L3SW> config lat console <enable/disable>

```
L3SW> config lat console enable
```

4.4.11.4　syslog サーバの設定

syslog 機能を使用してリモートログ記録を有効にするには、次の手順を実行します。

- メッセージを受信してログを記録するために、リモートホスト上に syslog サーバをセッティングします。
- syslog サーバの IP アドレスを設定してリモートログ記録を有効にするには、次のコマンドを実行します。

L3SW> config lat remote add <ipaddr>

```
L3SW> config lat remote add 192.168.10.231
```

4.4.11.5　ログフィルタの設定

セキュリティレベルが低いログメッセージを記録しないようにするには、次のコマンドを実行します。

L3SW> config lat severity <0-6>

```
L3SW> config lat severity 5
```

例の config lat コマンドでは、ログレベルが「通知（notification）」レベル以上に変更されます。この設定では、「報告（informational）」またはデバッグログメッセージは記録されません。ログメッセージフィルタリング設定の変更は、syslog サーバに送信されるメッセージにも適用されます。

4.4.11.6　RAM バッファ内のログメッセージの表示

RAM バッファ内のログメッセージを表示するには、次のコマンドを実行します。

L3SW> show lat msg <0-6>

L3SW> show lat msg 0

バッファ内にログメッセージが保存されていない場合、次のメッセージが表示されます。

Message Log Empty

4.4.11.7　フラッシュメモリ内のログメッセージの表示

フラッシュメモリに保存されているログメッセージは、すぐに表示することもできますし、システムの再起動後に表示することもできます。原因不明でシステムがクラッシュしたような場合、システムを再起動した後にフラッシュメモリ内のログメッセージを確認すると、問題の分析に役立つ情報が得られます。

フラッシュバッファ内のログメッセージを表示するには、次のコマンドを実行します。

L3SW> show lat error

```
L3SW >show lat error
2002-08-02 05:59:14:IPSEC-M:PHY: Pll, ISR0x401b, SR0xc51f,  LU1,  FD1,  S100,  F0C0.
2002-08-02 05:59:14:IPSEC-M:PHY: Pll, ISR0x4015, SR0x753a,  Strange link down interrupt
2002-08-02 05:59:14:IPSEC-M:PHY: Pll, ISR0x401f, SR0x0002,  LU0,  FD0,  S10,  F0C0.
2002-08-02 05:59:14:IPSEC-M:PHY: P27, ISR0x0000, SR0xl002,  LU0,  FD0,  S10,  F0C0.
2002-08-02 05:59:14:IPSEC-M:PHY: P26, ISR0x0000; SR0xl002,  LU0,  FD0,  S10,  F0C0.
2002-08-02 05:59:14:IPSEC-M:PHY: P25, ISR0x0000, SR0xl002,  LU0,  FD0,  S10,  F0C0.
2002-08-02 05:59:14:IPSEC-M:PHY: P24, ISR0x0000, SR0xl002,  LU0,  FD0,  S10,  F0C0.
2002-08-02 05:59:14:IPSEC-M:PHY: P23, ISR0x0000, SR0xl002,  LU0,  FD0,  S10,  F0C0.
2002-08-02 05:59:14:IPSEC-M:PHY: P22, ISR0x0000, SR0xl002,  LU0,  FD0,  S10,  F0C0.
2002-08-02 05:59:14:IPSEC-M:PHY: P21, ISR0x0000, SS0xl002,  LU0,  FD0,  S10,  F0C0.
2002-08-02 05:59:14:IPSEC-M:PHY: P20, ISR0x0000, SR0xl002,  LU0,  FD0,  S10,  F0C0.
2002-08-02 05:59:14:IPSEC-M:PHY: P19, ISR0x0000, SR0xl002,  LU0,  FD0,  S10,  F0C0.
2002-08-02 05:59:14:IPSEC-M:PHY: P18, ISR0x0000, SR0xl002,  LU0,  FD0,  S10,  F0C0.
2002-08-02 05:59:14:IPSEC-M:PHY: P17, ISR0x0000, SR0xl002,  LU0,  FD0,  S10,  F0C0.
2002-08-02 05:59:14:IPSEC-M:PHY: P16, ISR0x0000, SR0xl002,  LU0,  FD0,  S10,  F0C0.

Would  you  like to display the next 15  entries? (y/n)

L3SW >
```

表 4-16:ログメッセージの表示

4.4.11.8　ログメッセージの消去

すべてのログメッセージを消去するには、次のコマンドを実行します。

L3SW> clear lat

```
L3SW>clear lat
Are you sure you want to clear the log? (y/n) y
Log cleared.
L3SW>
```

表 4-17:ログメッセージの消去

4.4.12 設定の消去

システム設定を工場出荷時のデフォルト設定にリセットするには、次のコマンドを実行します。

L3SW> clear config

```
L3SW>clear config
Clearing configuration will force system reset. Are you sure
you want to clear the configuration? (y/n) y

Configuration Cleared! Trying to reset system.

PPCBoot 1.0.4 (Jun 11, 2004 - 13:44:43)
```

表 4-18:工場出荷時設定にリセット

このコマンドが正常に実行されると、工場出荷時の設定が復元され、システムが再起動されます。

4.5 ポート設定

4.5.1 ポート設定の表示

show port コマンドを実行すると、インタフェース情報(速度、二重モード、コネクタタイプ、クロックモード)が表示されます。各ポートの設定を表示するには、show port コマンドの後にポート番号(たとえば、0.12)を指定します。また、すべてのポートの設定を表示するには、show port コマンドの後に「all」を指定します。

L3SW> show port <slot.port/all/clockmode>

L3SW> show port all

```
L3SW> show port all
Slot        STP   Admin  Physical  Physical  Link   Link    LACP
Conn
Port Type  State  Mode   Mode      Status    Status Trap    Mode
Type
0.1        F     Enable  Auto      100 Full  up     Enable  Enable RJ45
0.2        D     Enable  Auto      100 Full  Down   Enable  Enable RJ45
0.3        F     Enable  Auto      100 Full  up     Enable  Enable RJ45
0.4        F     Enable  Auto      100 Full  up     Enable  Enable RJ45
0.5        D     Enable  Auto      100 Full  Down   Enable  Enable RJ45
0.6        D     Enable  Auto      100 Full  Down   Enable  Enable RJ45
0.7        D     Enable  Auto      100 Full  Down   Enable  Enable RJ45
0.8        D     Enable  Auto      100 Full  Down   Enable  Enable RJ45
0.9        D     Enable  Auto      100 Full  Down   Enable  Enable RJ45
0.10       D     Enable  Auto      100 Full  Down   Enable  Enable RJ45
0.11       D     Enable  Auto      100 Full  Down   Enable  Enable RJ45
0.12       D     Enable  Auto      100 Full  Down   Enable  Enable RJ45
0.13       D     Enable  Auto      100 Full  Down   Enable  Enable RJ45
0.14       D     Enable  Auto      100 Full  Down   Enable  Enable RJ45
0.15       D     Enable  Auto      100 Full  Down   Enable  Enable RJ45
0.16       D     Enable  Auto      100 Full  Down   Enable  Enable RJ45
0.17       D     Enable  Auto      100 Full  Down   Enable  Enable RJ45
0.18       D     Enable  Auto      100 Full  Down   Enable  Enable RJ45
0.19       D     Enable  Auto      100 Full  Down   Enable  Enable RJ45
 —More— or  (q)uit
0.20       D     Enable  Auto      100 Full  Down   Enable  Enable RJ45
0.21       D     Enable  Auto      100 Full  Down   Enable  Enable RJ45
0.22       D     Enable  Auto      100 Full  Down   Enable  Enable RJ45
0.23       D     Enable  Auto      100 Full  Down   Enable  Enable RJ45
0.24       D     Enable  Auto      100 Full  Down   Enable  Enable RJ45
1.1        D     Enable  Auto      1000 Full Down   Enable  Enable LC
1.2        D     Enable  Auto      1000 Full Down   Enable  Enable LC
1.3        D     Enable  Auto      1000 Full Down   Enable  Enable LC
1.4        D     Enable  Auto      1000 Full Down   Enable  Enable LC
4.1        F     Enable  100       100       up     Disable Disable
4.2        F     Enable  100       100       up     Disable Disable
4.3        F     Enable  100       100       up     Disable Disable

L3SW>
```

表 4-19:ポートの詳細の表示

1 列目には、物理／論理ポートのタイプとそのポートに関連付けられているポート番号を示す Slot.Port が表示されます。次に、設定できる Slot オプションの値を示します。

- 0:フロントパネルの物理ポート(10BASE-T/100BASE-TX ポート)
- 1:フロントパネルの物理ポート(拡張モジュール/mini-GBIC スロット)
- 2:LAG ポートとして設定されている論理ポート
- 3:予約済み
- 4:ルーティング用に設定されている論理ポート

2 列目には、ポートの Type が表示されます。通常のポートの場合、このフィールドは空白になります。特殊なポートの場合、次のいずれかの値が表示されます。

- Probe（ポートミラーリング設定のポートの場合）
- Mirror（ポートミラーリング設定のポートの場合）
- LAG（LAG 設定のポートの場合）

3 列目には、ポートの STP State が表示されます。ポートの状態に応じて、次のいずれかの値が表示されます。

- F：転送状態
- B：ブロック状態
- D：無効状態
- L：学習状態

4 列目には、Admin Mode が表示されます。この列には、次のいずれかの値が表示されます。

- Enable：ポートは有効です。
- Disable：ポートは無効です。

5 列目には、Physical Mode（Manual または Auto）が表示されます。

6 列目には、ポート速度と二重モードを示す Physical Status が表示されます。表示される値は、ピア間でネゴシエートされたもので、必ずしもポート自身の性能を示しているわけではありません。ネゴシエートによる値か、設定された値かに応じて、各ポートに次のいずれかが表示されます。

- 10 Half：10BASE-T/Half Duplex
- 10 Full：10BASE-T/Full Duplex
- 100 Half：100BASE-TX/Half Duplex
- 100 Full：100BASE-TX/Full Duplex
- 1000 Half：1000BASE-T/Half Duplex
- 1000 Full：1000BASE-T/Full Duplex

7 列目には、リンクが Up と Down のどちらであるかを示す Link Status が表示されます。

8 列目には、リンクステータスが変化した場合にスイッチがトラップを送信するかどうかを示す Link Trap モードが表示されます。この列に表示される値は、次のいずれかです。

- Enable：リンクステータスが変わると、トラップが送信されます
- Disable：リンクステータスが変わっても、トラップは送信されません

9 列目には、LACP Mode が表示されます。LACP Mode は、このポート上で LACP コントロールプロトコル（LACP）が有効か無効かを示します。この列に表示される値は、次のいずれかです。

- Enable：LACP プロトコルを有効にします
- Disable：LACP プロトコルを無効にします

10 列目には、ポートの物理的な接続性のタイプを示す Conn.Type が表示されます。サポートされているタイプは次のとおりです。

- RJ45
- LC
- MT-RJ

デフォルトではすべてのポートで、管理モードとオートネゴシエーションモードは有効になっています。

1000BASE-T モジュールは、ローカルで生成されたクロック（マスタモード）、または、そのピアから取得したクロック（スレーブモード）を使用して動作します。クロックモードは、手動で設定するか、オートネゴシエーション経由で設定することができます。1000BASE-T モジュール上の GE ポートのクロックステータスを表示するには、次のコマンドを実行します。

L3SW> show port clockmode

```
L3SW> show port clockmode
```

```
L3SW>show port clockmode
Slot. Port  Clock Mode Clock Status
 0.1        Auto        Master
 0.2        Auto        Slave
 0.3        Auto        Slave
 0.4        Auto        Slave
 0.5        Auto        Slave
 0.6        Auto        Slave
 0.7        Auto        Slave
 0.8        Auto        Master

 L3SW>
```

表 4-20：ポートのクロックモードの表示

1 列目には、Slot.port が表示されます。Slot フィールドには、次のいずれかの値が表示されます。

- 0：本体前面の 1000BASE-T ポート
- 1：本体前面の拡張スロット（1000BASE-T）
- Port フィールドには、次のいずれかの値が表示されます。
- 1～4：本体前面の 1000BASE-T ポート番号

2 列目には、このポート上で設定されているクロックモードを示す Clock Mode が表示されます。この列には、次のいずれかの値が表示されます。

- Master
- Slave
- Auto

3 列目には、Clock Status が表示されます。この列に表示される値は、次のいずれかです。

- Master
- Slave
- Fault

ポート統計には、ポート経由で送受信されたパケット数、送受信でエラーが発生したパケット数、衝突数などの詳細が表示されます。ポート統計は、要約形式または詳細形式で表示することができます。各ポートのポート統計を要約形式で表示するには、次のコマンドを実行します。

L3SW> show stats port summary <slot.port>

L3SW> show stats port summary 0.1

```
L3SW>show stats port summary 0.1
Packets Received Without Error ..................  0
Packets Received With Error .....................  0
Broadcast Packets Received ......................  0
Packets Transmitted Without Error ...............  0
Transmit Packets Errors .........................  0
Collisions Frames       .........................  0
Time Since Counters Last Cleared ................  0 day 0 hr 4 min
25 sec

L3SW>
```

表 4-21：ポートの要約の表示

L3SW> show stats port detailed <slot.port>

L3SW> show stats port detailed 0.1

```
L3SW>show stats port detailed 0.1

Total Packets Received (Octets) ..... 2088
Packets Received 64 Octets ..... 0
Packets Received 65-127 Octets ..... 9
Packets Received 128-255 Octets ..... 5
Packets Received 256-511 Octets ..... 0
Packets Received 512-1023 Octets ..... 0
Packets Received 1024-1518 Octets ..... 0
Packets Received 1519-1530 Octets ..... 0
Packets Received } 1530 Octets ..... 0

Total Packets Received Without Errors ..... 14
Unicast Packets Received ..... 0
Multicast Packets Received ..... 0
Broadcast Packets Received ..... 14

Total Packets Received with MAC Errors ..... 0
Jabbers Received ..... 0
Fragments/Undersize Received ..... 0
Alignment Errors ..... 0
FCS Errors ..... 0
Overruns ..... 0

—More— or (q)uit
Total Received Packets Mot Forwarded ..... 0
Local Traffic Frames,,,,,_ ..... 0
802, sk Pause Frames Received ..... 0
Unacceptable Frame Type ..... 0
VLAW Membership Mismatch. ..... 0
VLAW Viable Discards ..... 0
Multicast Tree Viable Discards ..... 0
Reserved Address Discards ..... 0
Broadcast Storm Recovery, ..... 0
CFI Discards ..... 0
Upstream Threshold ..... 0

Total Packets Transmitted (Octets) ..... 192
Packets Transmitted 64 Octets ..... 3
Packets Transmitted 65-127 Octets ..... 0
Packets Transmitted 128-255 Octets ..... 0
Packets Transmitted 256-511 Octets ..... 0
Packets Transmitted 512-1023 Octets ..... 0
Packets Transmitted 1024-1518 Octets ..... 0
Packets Transmitted 1519-1530 Octets ..... 0
Max Info ..... 1522

Total Packets Transmitted Successfully, ..... 3
—More— or (q)uit
```

表 4-22:ポート統計の表示

```
--More—or (q)uit
Unicast Packets Transmitted ..................  0
Multicast Packets Transmitted ................  3
Broadcast Packets Transmitted ................  0

Total Transmit Errors ........................  0
FCS Errors ...................................  0
Tx Oversized .................................  0
Underrun Errors ..............................  0

Total Transmit Packets Discarded .............  0
Single Collision Frames ......................  0
Multiple Collision Frames ....................  0
Excessive Collision Frames ...................  0
Port Membership Discards .....................  0
VLAN Viable Discards .........................  0

BPDUs received ...............................  0
BPDUs Transmitted ............................  0
802.3x Pause Frames Received .................  0
GVRP PDUs received ...........................  0
GVRP PDUs Transmitted ........................  0
GVRP Failed Registrations ....................  0
GMRP PDUs Received ...........................  0
—More— or (q)uit
GMRP PDUs Transmitted ........................  0
GMRP Failed Registrations ....................  0
Time Since Counters Last Cleared .............  0 day 0 hr
19 min 16 sec
L3SW>
```

表 4-23:ポート統計の表示

WBI は、ポート統計を表形式(CLI の場合と似た形式)またはグラフ形式で表示できます。

各ポートの WBI 統計をグラフィカルに表示するには、WBI にログインし、WBI ナビゲーションツリーで[Statistical Data]→[Monitor Individual Port]をクリックします。次に、モニタリングする[Slot.Port]を選択してから、[Polling Interval]を選択し(これで、WBI は自動的にポーリングし、統計表示をグラフィカルに更新するようになります)、[Submit]ボタンをクリックします。図 4-1 に、ポート 0.1 の WBI グラフィカル統計表示の画面例を示します。さまざまなタイプの棒グラフや折れ線グラフを選択することができます。[Presentation Type]から選択してください。

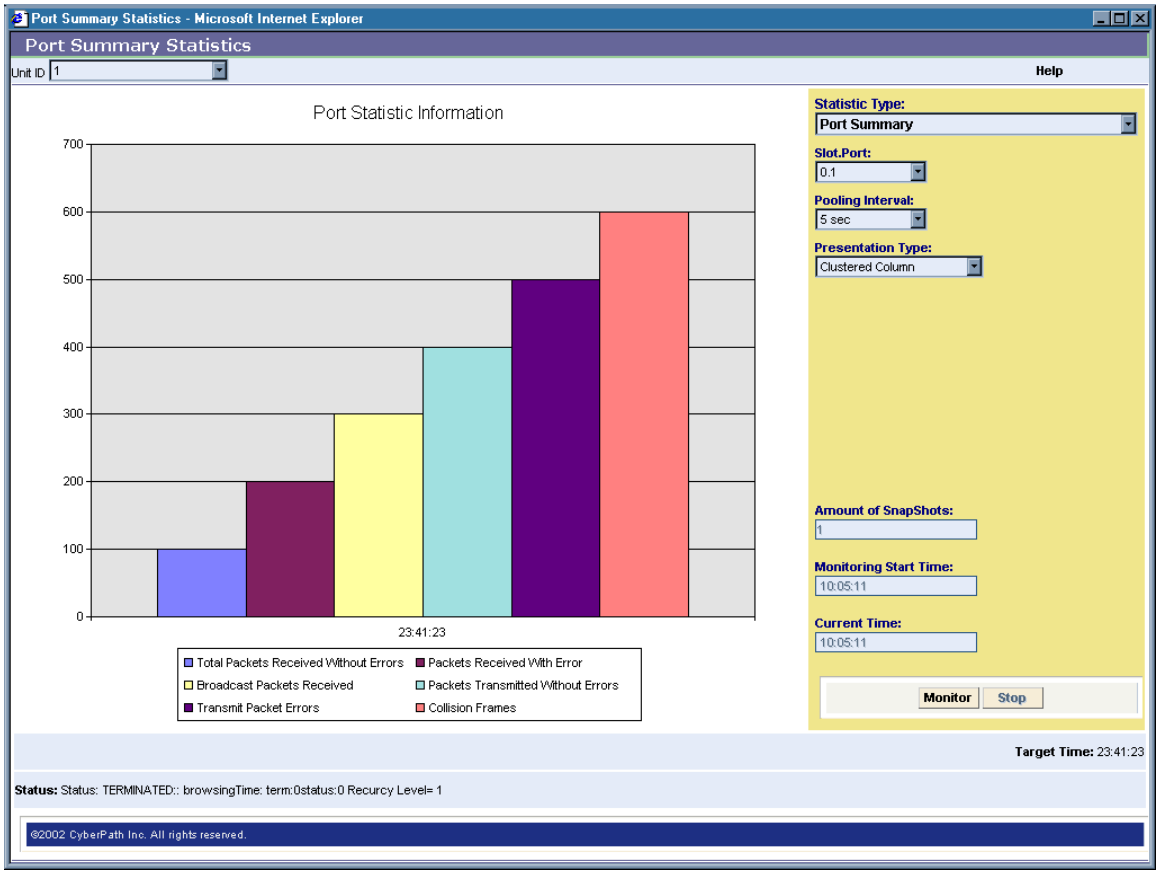

図 4-1：各ポートに対する WBI 統計のグラフィカル表示

全ポートの WBI 統計をグラフィカルに表示するには、WBI にログインし、WBI ナビゲーションツリーで[Statistical Data]→[Monitor All Ports]をクリックします。次に、[Polling Interval]を選択し（これで、WBI は自動的にポーリングし、統計表示をグラフィカルに更新するようになります）、[Submit]ボタンをクリックします。に、全ポートの WBI グラフィカル統計表示の画面例を示します。さまざまなタイプの棒グラフや折れ線グラフを選択することができます。[Presentation Type]から選択してください。

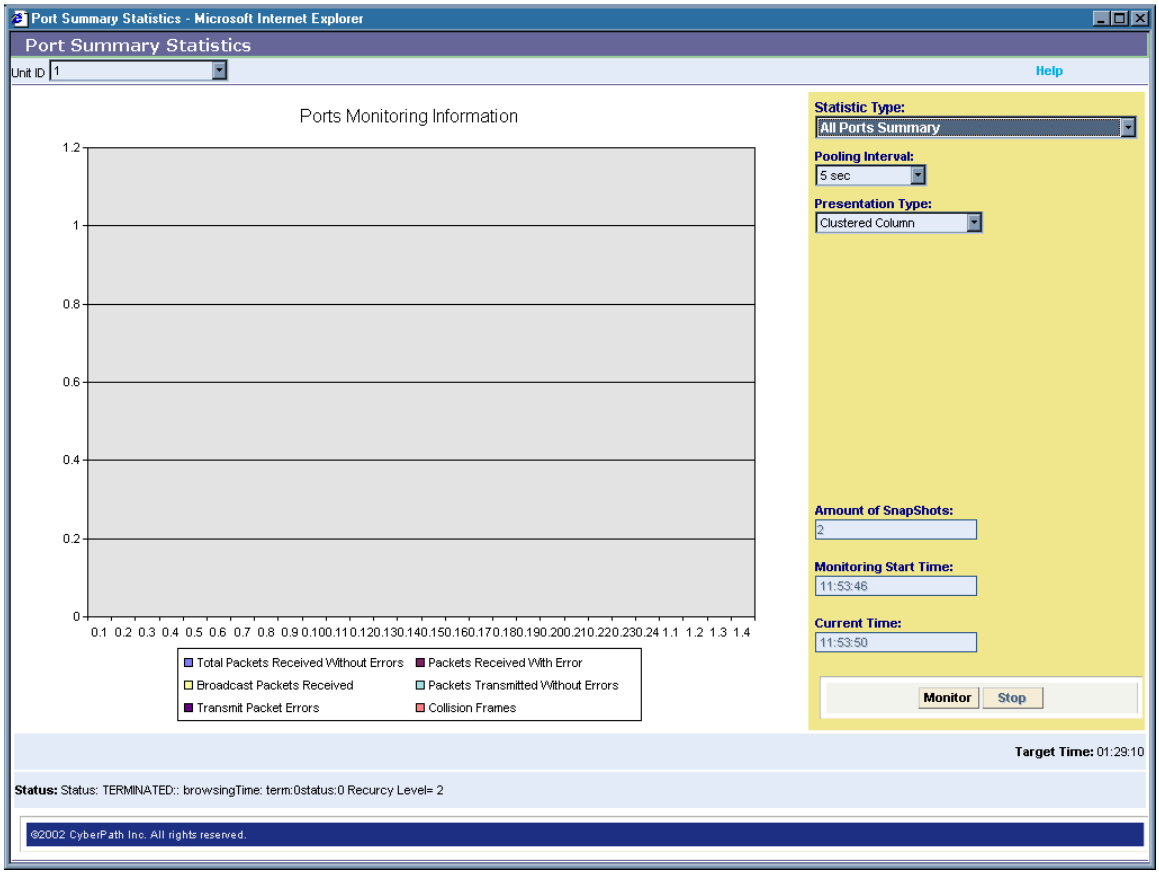

図 4-2：全ポートに対する WBI 統計のグラフィカル表示

4.5.2 ポート構成の設定

本製品で設定できるパラメータは次とおりです。

- ポートの管理モード
- オートネゴシエーションモード
- リンクアップ／ダウントラップ
- ポート速度および二重モード設定

各ポートの管理モードを有効または無効にするには、次のコマンドを実行します。ポートを無効にすると、すべてのトラフィックが転送されなくなります。ただし、そのポートに関するすべての設定値は保持されます。ポートの管理モードを有効または無効にするには、次のコマンドを実行します。

L3SW> config port adminmode <slot.port/all> <enable/disable>

```
L3SW> config port adminmode 0.1 enable
```

ポート速度や二重モードを設定したり、ピアポートとネゴシエートをする場合は、ポートのオートネゴシエーションを有効にする必要があります。ポート速度や二重モードを手動で設定する場合は、ポートのオートネゴシエーションは無効にします。オートネゴシエーションが有効な場合、手動による設定は上書きされます。オートネゴシエーションを有効または無効にするには、次のコマンドを実行します。

L3SW> config port autoneg <slot.port/all> <enable/disable>

```
L3SW> config port autoneg 0.1 enable
```

L3SW> config port linktrap <slot.port/all> <enable/disable>

```
L3SW> config port linktrap all enable
```

1000BASE-T ポートのクロックモードを手動で定義するには、次のコマンドを実行します。

L3SW> config port clockmode <slot.port> <auto/master/slave>

```
L3SW> config port clockmode 0.1 master
```

ポートの通信方式を Full Duplex または Half Duplex に、10BASE-T/100BASE-TX ポートの通信速度を 10Mbps または 100Mbps に、10BASE-T/100BASE-TX/1000BASE-T ギガビットポートの速度を 100Mbps または 1000Mbps にそれぞれ設定できます。1000BASE-SX ポートの通信速度と通信方式は、1000 Mbps/Full Duplex に固定されています。各ポートまたはすべてのポートの通信速度と通信方式を手動で設定するには、次のコマンドを実行します。

L3SW> config port physicalmode <slot.port/all> <100h/100f/10h/10f>

```
L3SW> config port physicalmode 0.1 10f
```

物理モード設定を有効にするには、オートネゴシエーションを無効にする必要があります。

ファストイーサネットポートのオートネゴシエーションが無効な場合、対応する PHY は MDI-X モードで動作するよう設定されており、関連付けられている RJ-45 コネクタのピン配列は MDI-X になります。このような状況で、ポートがオートネゴシエーションを実行している通信相手と適切な接続を確立できるのは、強制的に Half Duplex モードで動作している場合だけです。IEEE 802.3 によると、このような状況では、通信相手が Full Duplex モードを検出できないことが原因です。

ポートの管理モードが無効な場合、そのモードは PHY 層ではなく、MAC 層で無効ということです。その結果、ポートが別のスイッチに接続されている場合、「show port all」の応答として、リンク状態には「UP」が表示されます。ただし、そのポートを経由するトラフィックはブロックされます。

5. レイヤ 2 の設定

5.1 L2 転送データベース

5.1.1 転送データベースの表示

L2 転送データベースには、本製品が学習した MAC アドレスが保持されます。このデータベースに保存されているアドレスは、動的に学習され、保存期間経過後に削除されます。L2 転送データベースを要約形式で表示するには、次のコマンドを実行します。

L3SW> show forwardingdb summary
L3SW> show forwardingdb summary

```
L3SW>show forwardingdb summary
Slot.Port  iflndex  Static  Learned  Mgmt  GMRP  Self
0.1        1        0       0        1     0     1
0.2        2        0       0        0     0     1
0.3        3        0       1        0     0     1
0.4        4        0       0        0     0     1
0.5        5        0       0        0     0     1
0.6        6        0       0        0     0     1
0.7        7        0       0        0     0     1
0.8        8        0       0        0     0     1
0.9        9        0       0        0     0     1
0.10       10       0       0        0     0     1
0.11       11       0       0        0     0     1
0.12       12       0       0        0     0     1
0.13       13       0       0        0     0     1
0.14       14       0       0        0     0     1
0.15       15       0       0        0     0     1
0.16       16       0       0        0     0     1
0.17       17       0       0        0     0     1
0.18       18       0       0        0     0     1
0.19       19       0       0        0     0     1
0.20       20       0       0        0     0     1
—More— or  (q)uit
0.21       21       0       0        0     0     1
0.22       22       0       0        0     0     1
0.23       23       0       0        0     0     1
0.24       24       0       0        0     0     1
1.1        4097     0       0        0     0     1
1.2        4098     0       0        0     0     1
1.3        4099     0       0        0     0     1
1.4        4100     0       0        0     0     1
L3SW>
```

表 5-1:転送データベースの要約の表示

L2 転送データベースを詳細形式で表示するには、次のコマンドを実行します。

L3SW> show forwardingdb table

```
L3SW> show forwardingdb table
```

```
L3SW>show forwardimgdb table
Mac Address               Slot.Port  iflndex  Status
00:01:00:50:A8:00:31:00  0.1        1        Management
00:01:00:50:A8:00:31:02  0.1        1        Self
00:01:00:50:A8:00:31:03  0.2        2        Self
00:01:00:50:A8:00:31:04  0.3        3        Self
00:01:00:50:A8:00:31:05  0.4        4        Self
00:01:00:50:A8:00:31:06  0.5        5        Self
00:01:00:50:A8:00:31:07  0.6        6        Self
00:01:00:50:A8:00:31:08  0.7        7        Self
00:01:00:50:A8:00:31:09  0.8        8        Self
00:01:00:50:A8:00:31:0A  0.9        9        Self
00:01:00:50:A8:00:31:0B  0.10       10       Self
00:01:00:50:A8:00:31:0C  0.11       11       Self
00:01:00:50:A8:00:31:0D  0.12       12       Self
00:01:00:50:A8:00:31:0E  0.13         13       Self
00:01:00:50:A8:00:31:0F  0.14         14       Self
 — More — or (q)uit
Mac Address               Slot.Port    iflndex  Status
00:01:00:50:A8:00:31:10  0.15         15       Self
00:01:00:50:A8:00:31:11  0.16         16       Self
00:01:00:50:A8:00:31:12  0.17         17       Self
00:01:00:50:A8:00:31:13  0.18         18       Self
00:01:00:50:A8:00:31:14  0.19         19       Self
00:01:00:50:A8:00:31:15  0.20         20       Self
00:01:00:50:A8:00:31:16  0.21         21       Self
00:01:00:50:A8:00:31:17  0.22         22       Self
00:01:00:50:A8:00:31:18  0.23         23       Self
00:01:00:50:A8:00:31:19  0.24         24       Self
00:01:00:50:A8:00:31:1A  1.1          4097     Self
00:01:00:50:A8:00:31:1B  1.2          4098     Self
00:01:00:50:A8:00:31:1C  1.3          4099     Self
00:01:00:50:A8:00:31:1D  1.4          4100     Self
0F:FC:00:00:5E:00:01:03  0.3          3        Learned
L3SW>
```

表 5-2:転送データベースの詳細の表示

転送データベースのエージングタイムを表示するには、次のコマンドを実行します。

L3SW> show forwardingdb agetime

```
L3SW> show forwardingdb agetime
```

```
L3SW>show forwardingdb agetime
Address Aging Timeout.....................   300

L3SW>
```

表 5-3:転送データベースのエージングタイムの表示

5.1.2 転送データベースの設定

デフォルトで、転送データベースのエージングタイムは 300 秒（5 分）です。転送データベースのエージングタイムを設定するには、次のコマンドを実行します。

L3SW> config forwardingdb age <10-1000000>

```
L3SW> config forwardingdb age 100
```

5.2 バーチャル LAN（VLAN）

5.2.1 VLAN の概要

VLAN は、ネットワーク上の任意のノードをグループ化したものです。グループ化により、ネットワークリソースの使用効率が向上し、ネットワークに対する繰り返し処理が容易に実行できるようになります。理論的には、VLAN によって、ネットワーク管理者はネットワークを構成、分離、パーティション化することができます。例えば、既存の LAN 内のこのような構造として、IP ネットワーク内のサブネットや、ブリッジネットワーク内のブロードキャストドメインがあります。通常、これらの論理構造は、物理ネットワークエレメントに密接にリンクしています。単一の LAN セグメントは、1 つのブロードキャストドメインであり、そのセグメントがルータの LAN ポートに接続されると、IP サブネットアドレスが割り当てられます。

複数の LAN セグメントがブリッジされている場合でも、それらのブリッジセグメントは、ブリッジや共有メディアハブに物理的に接続されている各 LAN 上のすべてのブロードキャストやマルチキャストトラフィックを「受信」できます。LAN セグメント上で過度のブロードキャストトラフィックを作成せずにブリッジできるステーションまたは LAN セグメントの数には制限があります。過度のブロードキャストトラフィックを避けるには、ネットワークをサブネットに分割する必要がありますが、サブネットは物理的な LAN 構造に拘束されてしまいます。VLAN を使用すると、ネットワーク構成に伴うこのような制限の一部を解消できます。

1 つのノードは、複数の VLAN のメンバになることができます。この方法では、ノード同士を好きなように接続し、異機種混在ネットワークを形成できます。

5.2.2 VLAN の利点

ネットワークに VLAN を組み込むと、次のような利点があります。

- **VLAN により、トラフィックの制御が容易になります。**

従来のネットワークでは、ブロードキャストトラフィックがすべてのネットワークデバイスに向けて送信されるために、輻輳が発生する可能性があります。VLAN では、相互通信する必要があるデバイスだけを含んでセットアップするので、ネットワークの効率が向上します。

- **VLAN により、安全性が向上します。**

各 VLAN 内のデバイスは、同一 VLAN 内のデバイスとのみ通信することができます。異なる VLAN に接続されているノード（これらのノードは同じ物理的な LAN セグメント）が、相互に通信できるのは、VLAN 間のルータを介した場合だけです。例えば、Marketing という名前の VLAN 内のデバイスが Sales という VLAN 内のデバイスと通信する場合、そのトラフィックはルータを経由しなくてはなりません。

- **VLAN により、デバイスの変更と移動が容易になります。**

従来のネットワークの場合、ネットワーク管理者は、デバイスの移動と変更に多くの時間を取られてきました。複数のユーザが異なるサブネットワークに移動した場合、各エンドステーションのアドレスを手動でアップデートする必要があります。これに対して、VLAN（および VLAN 間のルーティング）では、ユーザは自身が接続されている LAN セグメントに関係なく、同じサブネットワークに接続できます。

5.2.3 VLAN の用語

ポートベースの VLAN の操作や設定を理解するには、いくつかの主要な用語の意味を知っておく必要があります。

- **VLAN ID**

VLAN ID は、VLAN を識別する一意の番号（1 から 4094 まで）です。VLAN ID 1 は、Default VLAN の ID として予約されています。

- **VLAN Name**

各 VLAN ID に付けられる 32 文字の英数字名です。VLAN Name を使用すれば、ユーザが定義した VLAN を簡単に識別したり、覚えることができます。

- **Tag Header (VLAN Tag)**

Tag Header はフレーム内のフィールドで、VLAN がどのフレームに分類されているかを識別します。送信元の MAC アドレスフィールドのすぐ後ろのフレームに Tag Header が挿入されます。Tag Header を構成する 12 ビットは VLAN ID で、残りのビットは他の制御情報を表します。

- **Tagged Frame**

Tagged Frame は、Tag Header があるデータフレームです。Tag Header は、VLAN 対応のスイッチによって、VLAN のメンバであるポートから受信したすべてのデータフレームに追加されます。

- **Untagged Frame**

Untagged Frame は、Tag Header がないデータフレームです。

- **Port VLAN ID (PVID)**

特定のスイッチポートの識別子（ポート 2、モジュール 1）を囲む識別子です。そのポートの VLAN メンバーを表すのが、PVID です。この識別子は、受信した Untagged Frame を分類して、これらのフレームがトランクポート経由で送信される際にタグを付けるために使用されます。

- **VLAN Participation**

VLAN participation は、ポートが特定の VLAN に参加する（つまり、特定の VLAN に属するフレームを受信する）かどうかを指定する際に必要です。ID は VLAN 識別番号で、interface はポート番号または all（すべてのポート）です。

- **Ingress Filter**

Ingress Filter は、スイッチポート経由で着信するトラフィックを制御します。有効にすると、着信

するトラフィックをスクリーニングして、ポートが参加している VLAN に属するフレームだけが許可されます。

- **Default VLAN**

Default VLAN は、初期化時にすべてのポートが割り当てられる VLAN です。デフォルト VLAN の VLAN ID は 1 です。

5.2.4 VLAN のタイプ

VLAN は、次の基準に従って作成します。

- **物理ポートベース**
- **IEEE802.1Q タグベース**
- **プロトコルベース**

5.2.4.1 ポートベース VLAN

ポートベース VLAN は、タグなし（Untagged）VLAN とも呼ばれます。ポートベース VLAN では、スイッチ上の 1 つまたは複数のポートから構成されるグループに対して、1 つの VLAN 名が付けられます。1 つのポートがメンバになれるポートベース VLAN は、1 つだけです。つまり、1 つのポートが複数のポートベース VLAN のメンバになることはできません。ポートベース VLAN の動作は、従来のスイッチベースのネットワークシステムの動作といくつかの点で異なります。異なる点は、各転送がスイッチ間またはスイッチ内のポート間を通過する際に、その VLAN メンバシップを常に追跡するかどうかです。

ポートベース VLAN 技術の利点は、VLAN メンバシップに基づいてポートにトラフィックをルーティングする点にあります。ポートベース VLAN では、VLAN に割り当てられたステーションのセキュリティとパフォーマンスが向上します。

VLAN を設定する場合、VLAN に割り当てられたすべてのネットワークスイッチデバイスが、ポートベース VLAN に関する IEEE 802.1Q の仕様を満たしている必要があります。VLAN の実装を始める前に、スイッチが IEEE802.1Q 仕様に完全に準拠していることを確認してください。

5.2.4.2 タグ付き（Tagged）VLAN

タグが最もよく使用されるのは、複数のスイッチにまたがる VLAN を作成する場合です。スイッチ－スイッチ接続は、一般的にはトランクと呼ばれています。タグを使用すると、2 つのスイッチ間の同じトランク上に複数の VLAN を作成できます。

ポートベース VLAN では、各 VLAN には専用のトランクポートのペアが必要です。タグを使用すると、1 つのトランクだけで 2 つのスイッチにまたがる複数の VLAN を作成できます。タグ VLAN のもう一つの利点は、1 つのポートを経由して複数の VLAN を使用できる点です。これは、複数の VLAN に属する必要があるデバイス（サーバなど）を使用する場合に特に便利です。

サーバまたは PC からタグ付きフレーム（Tagged Frame）を生成するには、IEEE802.1Q のタグ付けをサポートするネットワークインタフェースカード（NIC）を装備している必要があります。NIC は、フレームの優先度または QoS 値に基づいてフレームをタグ付けするように設定したり、ローカルのタグ付けポリシーに基づいて設定したりすることができます。このマニュアルでは、ホ

ストによるフレームのタグ付けを定義する方法については説明していません。スイッチ側から見ると、すべてのタグ付きフレームは、ホストが接続されているポートの VLAN メンバシップに応じて処理されます。ホストから送られるタグなしフレーム（Untagged Frame）は、ポートの PVID 値でタグ付けされてからスイッチの出力ポートに転送されます。

各 VLAN には、IEEE802.1Q VLAN タグを割り当てることができます。IEEE802.1Q タグを定義して VLAN にポートを追加する場合、そのポートを「タグ付き」または「タグなし」に設定する必要があります。

VLAN 内のすべてのポートをタグ付けする必要はありません。スイッチ内のポートからトラフィックが発信される際に、スイッチは、その VLAN に対して各宛先ポートが使用すべきパケット形式をタグ付きとタグなしのどちらにするかどうかをリアルタイムに決定します。VLAN のポート設定に基づいて、スイッチはタグを付けたり外したりします。受信したパケットが、ポート上に設定されていない VLAN ID でタグ付けされている場合、そのパケットは破棄されます。

デフォルトでは、すべてのポートが、IEEE802.1Q VLAN タグ（VLAN ID） 1 を持つ Default VLAN に割り当てられています。

5.2.4.3 プロトコルベース VLAN

プロトコルベース VLAN を使用すると、パケットフィルタを定義することができます。このパケットフィルタは、パケットが特定の VLAN に属するかどうかを識別する条件として使用されます。

プロトコルベース VLAN は、ネットワークセグメントに複数のプロトコルを実行しているホストが存在するような場合に使用されます。例えば、一部のホストが IP プロトコルを実行し、他のホストが IPX プロトコルを実行しているような場合、IP トラフィックと IPX トラフィックをプロトコルベース VLAN を使用して分離することができます。

5.2.4.4 デフォルト VLAN の概念

本製品のポートベース VLAN 分類機能では、タグなしフレームまたはプライオリティタグ付きフレーム（つまり、タグヘッダなしのフレームまたはヌルの VLAN ID が含まれるタグヘッダ付きのフレーム）に関連付けられた VLAN ID が、スイッチに入ってくるフレームの受信ポートに基づいて判別されます。この分類メカニズムでは、ポートの VLAN ID（PVID）をスイッチの各ポートに関連付ける必要があります。指定したポートの PVID は、そのポート経由で受信したタグなしフレームとプライオリティタグ付きフレームに VLAN ID を提供します。各ポートの PVID には、ヌルの VLAN ID の値ではなく、有効な VLAN ID 値が含まれます。

ポートに PVID 値が明示的に設定されていない場合は、そのポートの PVID として、デフォルト VLAN ID 1 が使用されます。

5.2.5 本製品での VLAN の設定

本製品では、IEEE802.1Q 互換の VLAN が設定できます。ポートベース VLAN は、同じブロードキャストドメインに属するスイッチによって指定されたスイッチポートのグループ（つまり、同じ PVID 値を持つポート）です。IEEE802.1Q 規格と互換性があるため、2 つ以上の VLAN にポートを割り当てることができるとともに、各 VLAN に個別のポートが必要な旧式のスイッチとの相互運用性も確保しています。

5.2.5.1 VLAN 設定の表示

VLAN 要約情報を表示するには、次のコマンドを実行します。

L3SW> show vlan summary

L3SW> show vlan summary

```
L3SW>show vlan summary
      VLAW ID   VLAW Name          VLAN Type
 -------  ----------------   ----------
 1          Default           Default
 10                           Static

 L3SW>
```

表 5-4:VLAN の要約の表示

VLAN ID や PVID に関連付けられている VLAN ポート番号を表示するには、次のコマンドを実行します。

L3SW> show vlan vlanport

L3SW> show vlan vlanport

```
L3SW>show  vlan ulanport
 List  of  VLANs per  Ports
 --------------------------
 Port:  0.1  PVID:  2
 Port:  0.2  PVID:  3
 Port:  0.3  PVID:  1
 Port:  0.4  PVID:  1
 Port:  0.5  PVID:  1
 Port:  0,6  PVID:  1
 Port:  0.7  PVID:  1
 Port:  0.8  PVID:  1
 Port:  0.9  PVID:  1
 Port:  0.10  PVID:  1
 Port:  0.11  PVID:  1
 Port:  0.12  PVID:  1
 Port:  0.13  PVID:  1
 Port:  0.14  PVID:  1
 Port:  0.15  PVID:  1
 Port:  0.16  PVID:  1
 Port:  0.17  PVID:  1
 Port:  0.18  PVID:  1
 Port:  0.19  PVID:  1
 Port:  0.20  PVID:  1
 —More-  or (q)uit
 Port:  0.21  PVID:  1
 Port:  0.22  PVID:  1
 Port:  0.23  PVID:  1
 Port:  0.24  PVID:  1
 Port:  1.1  PVID:  1
 Port:  1.2  PVID:  1
 Port:  1.3  PVID:  1
 Port:  1.4  PVID:  1
 Port:  2.1  PVID:  4

L3SW>
```

表 5-5:VLAN ポート番号の表示

VLAN 詳細情報を表示するには、次のコマンドを実行します。

L3SW> show vlan detailed <1-4094>

L3SW> show vlan detailed 2

```
L3SW>show vlan detailed 2
 VLAN ID: 2
 VLAN Name: CP
 VLAN Type: Static
Slot.Port  Current  Configured  Tagging
0.1        Include  Include     Untagged
0.2        Exclude  Autodetect  Untagged
0.3        Exclude  Autodetect  Untagged
0.4        Exclude  Autodetect  Untagged
0.5        Exclude  Autodetect  Untagged
0.6        Exclude  Autodetect  Untagged
0.7        Exclude  Autodetect  Untagged
0.8        Exclude  Autodetect  Untagged
0.9        Exclude  Autodetect  Untagged
0.10       Exclude  Autodetect  Untagged
0.11       Exclude  Autodetect  Untagged
0.12       Exclude  Autodetect  Untagged
0.13       Exclude  Autodetect  Untagged
0.14       Exclude  Autodetect  Untagged
0.15       Exclude  Autodetect  Untagged
0.16       Exclude  Autodetect  Untagged
 —More— or (q)uit
0.17       Exclude  Autodetect  Untagged
0.18       Exclude  Autodetect  Untagged
0.19       Exclude  Autodetect  Untagged
0.20       Exclude  Autodetect  Untagged
0.21       Exclude  Autodetect  Untagged
0.22       Exclude  Autodetect  Untagged
0.23       Exclude  Autodetect  Untagged
0.24       Exclude  Autodetect  Untagged
1.1        Exclude  Autodetect  Untagged
1.2        Exclude  Autodetect  Untagged
1.3        Exclude  Autodetect  Untagged
1.4        Exclude  Autodetect  Untagged
2.1        Include  Include     Untagged

L3SW>
```

表 5-6:VLAN の詳細の表示

ポートの VLAN 情報を表示するには、次のコマンドを実行します。

L3SW> show vlan port <slot.port/all>

L3SW> show vlan port 0.1

```
L3SW>show vlan port 0.1
            Port     Acceptable   Ingress
Slot.Port   VLAN ID  Frame Types  Filtering   GVRP
---------   -------  -----------  ---------   ----
0.1         2        Admit All    Disable     Disable

L3SW>
```

表 5-7:VLAN ポートの表示

5.2.5.2 VLAN の作成

新しい VLAN を追加し、その VLAN に VLAN ID を割り当てるには、次のコマンドを実行します。VLAN ID として、2 から 4094 までの任意の数値を使用できます。

VLAN ID 1 はデフォルト VLAN に予約されています。

L3SW> config vlan create <2-4094>

```
L3SW> config vlan create 10
L3SW> config vlan create 20
L3SW> config vlan create 30
L3SW> config vlan create 40
```

```
L3SW>show vlan summary
 VLAW ID  VLAM Name            VLAM Type
 -------  -------------------- ---------
 1        Default              Default
 10                            Static
 20                            Static
 30                            Static
 40                            Static

 L3SW>
```

表 5-8:作成された VLAN の表示

VLAN の識別に名前を使用する場合は、名前を割り当てるオプションを使用できます。名前には、最大 16 文字までの英数字を使用できます。

L3SW> config vlan name <"name"> <1-4094>

```
L3SW> config vlan name Sales 10
L3SW> config vlan name Accounts 20
L3SW> config vlan name Engineering 30
L3SW> config vlan name Systems 40
```

```
L3SW>show vlan summary
 VLAW ID  VLAM Name            VLAM Type
 -------  -------------------- ---------
 1        Default              Default
 10       Sales                Static
 20       Accounts             Static
 30       Engineering          Static
 40       Systems              Static

 L3SW>
```

表 5-9:作成された VLAN ID と VLAN 名の表示

既存の VLAN を削除するには、次のコマンドを実行します。

L3SW> config vlan delete <2-4094>

```
L3SW> config vlan delete 2
```

すべての VLAN を削除するには、次のコマンドを実行します。

L3SW> clear vlan config

```
L3SW> clear vlan config
Are you sure you want to restore all VLANs to default? (y/n) y
VLAN's Restored!
```

VLAN 設定を消去すると、ユーザが設定したすべての VLAN が削除され、すべてのポートがデフォルト VLAN (PVID=1)に割り当てられます。

5.2.5.3 ポートベース VLAN の設定

デフォルトで、すべてのポートはデフォルト VLAN(PVID=1)に属しています。デフォルト VLAN とは異なるポートベース VLAN を定義するには、次のコマンドを実行します。

L3SW> config vlan port add <2-4094> <slot.port>

```
L3SW> config vlan port add 2 0.1
```

このコマンドで PVID に新しく指定した VLAN ID を設定すると、デフォルト VLAN(PVID=1)から指定した VLAN にポートが移動します。

ポートベース VLAN からポートを削除するには、次のコマンドを実行します。

L3SW> config vlan port remove <2-4094> <slot.port>

```
L3SW> config vlan port remove 2 0.1
```

このコマンドで PVID 値に 1 を設定すると、ポートは指定した VLAN からデフォルト VLAN (PVID=1)に移動します。

すべての VLAN から指定したポートを削除してデフォルト VLAN に移動するには、次のコマンド

を実行します。

L3SW> clear vlan port <slot.port/all>

```
L3SW> clear vlan port 0.1
```

このコマンドは、指定したポートのプライマリ VLAN を 1 に設定します。「all」オプションを指定すると、すべてのポートに対してこの処理が実行されます。

5.2.5.4 タグベース VLAN の設定

タグベース VLAN を定義するには、次の手順を実行します。

手順 1:プライマリVLANをポートに割り当てる

タグなしフレームが送受信されると、プライマリ VLAN に関連付けられた VID がタグ付きポートで使用されます。ポートは、物理ポートまたは論理 LAG インタフェースのいずれかです。

L3SW> config vlan port add <2-4094> <slot.port>

```
L3SW> config vlan port add 2 0.1
```

手順 2:複数のVLANに参加する

VLAN ポートがプライマリ VLAN 以外の VLAN にも参加する必要がある場合は、次のコマンドを実行します。

L3SW> config vlan participation <exclude/include/auto> <1-4094> <slot.port>

```
L3SW> config vlan participation include 3 0.1
```

手順 3:ポートタギングを設定する

指定した VLAN の物理ポート上でタギングを有効または無効にするには、次のコマンドを実行します。

L3SW> config vlan port tagging <enable/disable> <1-4094> <slot.port/all>

```
L3SW> config vlan port tagging enable 2 0.1
```

手順 4:イングレスフィルタを適用する(オプション)

イングレスフィルタは、任意のスイッチポートに対して有効または無効にすることができます。イングレスフィルタが有効な場合、トラフィックの転送先は、このポート上に設定された VLAN に参加しているスイッチポートだけになります。イングレスフィルタが無効な場合は、すべてのポートに出力トラフィックが流れることになります。

L3SW> config vlan port ingressfilter <enable/disable> <slot.port/all>

```
L3SW> config vlan port ingressfilter enable 0.1
```

5.2.5.5 プロトコルベース VLAN の設定

本製品は、プロトコルベース VLAN をサポートしています。プロトコルベース VLAN を設定するには、次の手順を実行します。

手順 1:プロトコルグループ名を作成する

グループ名は、プロトコルベース VLAN 内に論理的にグループ化されたホストの識別子として使うことができます（例えば、red、marketing、development など）。プロトコルグループ名を作成するには、次のコマンドを実行します。

L3SW> config protocol create <groupname>

```
L3SW> config protocol create red
```

手順 2:プロトコルグループIDを表示する

数字の識別子を使用して、作成した VLAN を操作します。グループ名に関連付けられたプロトコルグループ ID を表示するには、次のコマンドを実行します。

L3SW> show protocol <groupid/all>

```
L3SW> show protocol all
```

```
L3SW>show protocol all
                Group
Group Name       ID    Protocol(s)  VLAN     Interface(s)
----------  --------  -----------  -----  -------------------
Red         1                      0

L3SW>
```

表 5-10:すべてのプロトコルの表示

手順 3:VLANを設定する

次のコマンドを実行すると、VLAN ID をプロトコルグループにリンクできます。

L3SW> config protocol vlan add <groupid> <vlan>

```
L3SW> config protocol vlan add 1 2
```

新しく作成した VLAN ID や作成済みの VLAN ID を使用することができます。また、新しい VLAN ID を選択して、将来の VLAN 設定用のプレースホルダを作成することもできます。ポートグループに別の VLAN ID が追加された場合は、以前の VLAN ID が新しい VLAN ID に置き換えられます。プロトコルグループ ID から既存の VLAN ID を削除するには、次のコマンドを実行します。

L3SW> config protocol vlan remove <groupid> <vlan>

```
L3SW> config protocol vlan remove 1 2
```

グループから VLAN を削除すると、プロトコルグループに 0 の VLAN ID が割り当てられます。

手順 4:プロトコルを設定する

プロトコルグループ ID にプロトコルを追加するには、次のコマンドを実行します。

L3SW> config protocol protocol add <groupid> <ip/arp/ipx>

```
L3SW> config protocol protocol add 1 ip
```

プロトコルグループから既存のプロトコルを削除するには、次のコマンドを実行します。

L3SW> config protocol protocol remove <groupid> <ip/arp/ipx>

```
L3SW> config protocol protocol remove 1 ip
```

手順 5:インタフェースを設定する

プロトコルグループ ID にインタフェースを追加するには、次のコマンドを実行します。

L3SW> config protocol interface add <groupid> <slot.port/all>

```
L3SW> config protocol interface add 1 0.1
```

プロトコルグループに関連付けられた VLAN メンバであるインタフェース(物理または論理ポート)は、自動的にプロトコルグループのメンバになるわけではありません。上記のコマンドを実行して、プロトコルグループにインタフェースを追加しなければなりません。

プロトコルグループからインタフェースを削除するには、次のコマンドを実行します。

L3SW> config protocol interface remove <groupid> <slot.port/all >

```
L3SW> config protocol interface remove 1 0.1
```

5.2.6 VLAN 設定

5.2.6.1 例 1:ポートベース VLAN 設定

図 5-1 では、すべてのワークステーションとサーバの NIC が、タギングなしでフレームを送受信するよう設定されています。

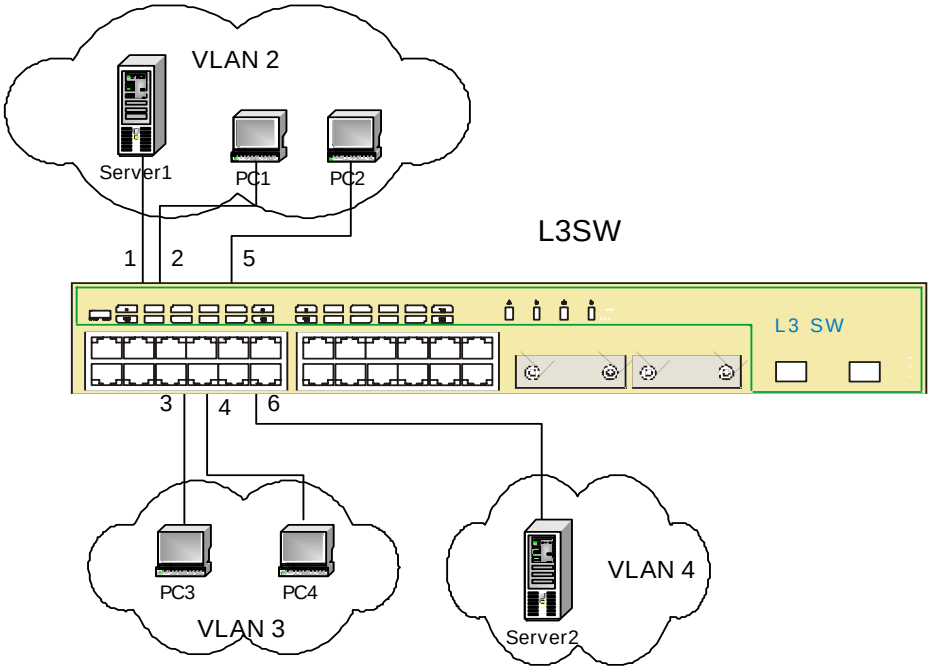

図 5-1:ポートベース VLAN 例

```
L3SW> config vlan create 2
L3SW> config vlan create 3
L3SW> config vlan create 4
L3SW> config vlan port add 2 0.1
L3SW> config vlan port add 2 0.2
L3SW> config vlan port add 2 0.5
L3SW> config vlan port add 3 0.3
L3SW> config vlan port add 3 0.4
L3SW> config vlan port add 4 0.6
```

上記の設定の結果は、次のとおりです。

- ワークステーション PC1、PC2、および Server1 が、相互に通信できるようになります。
- ワークステーション PC3 と PC4 が、相互に通信できるようになります。
- PC1、PC2、Server1 は、PC3 または PC4 と通信できません。
- Server2 は、他のデバイスと通信できません。

5.2.6.2 例 2:タグベース VLAN 設定

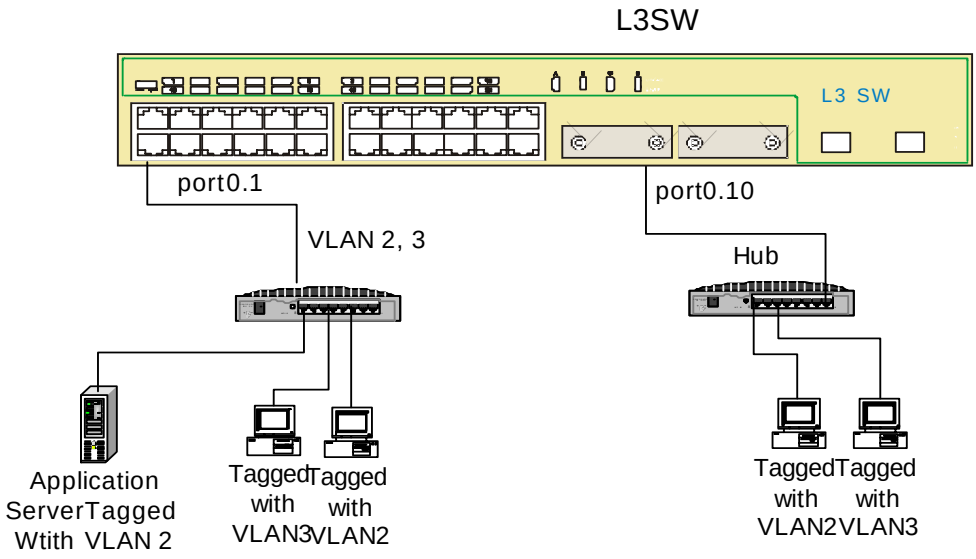

図 5-2:タグベース VLAN 例

図 5-2 に、VLAN タギングをサポートしている NIC がサーバやワークステーションにインストールされているネットワーク設定を示します。本製品上に、2 つの VLAN(VLAN 2 と VLAN 3)が作成されています。VLAN 2 でタグ付けされたワークステーションは相互に通信可能で、サーバとも通信できます。VLAN 3 でタグ付けされたワークステーションは相互に通信できますが、サーバとは通信できません。このように、1 つの物理ポートから 2 つ以上の VLAN に通信を提供できます。VLAN 2 および VLAN 3 をサポートするようにスイッチを設定するには、次のコマンドセットを実行します。

```
L3SW> config vlan create 2
L3SW> config vlan create 3
L3SW> config vlan port add 2 0.1
L3SW> config vlan port add 2 0.10
L3SW> config vlan participation include 3 0.1
L3SW> config vlan participation include 3 0.10
L3SW> config vlan port tagging enable 2 0.1
L3SW> config vlan port tagging enable 3 0.1
L3SW> config vlan port tagging enable 2 0.10
L3SW> config vlan port tagging enable 3 0.10
```

上記の設定では、参加しているすべてのノード上にベンダ提供のクライアント管理ソフトウェアがインストールされている IEEE802.1Q 対応の NIC が必要です。

5.2.6.3 例 3:プロトコルベース VLAN 設定

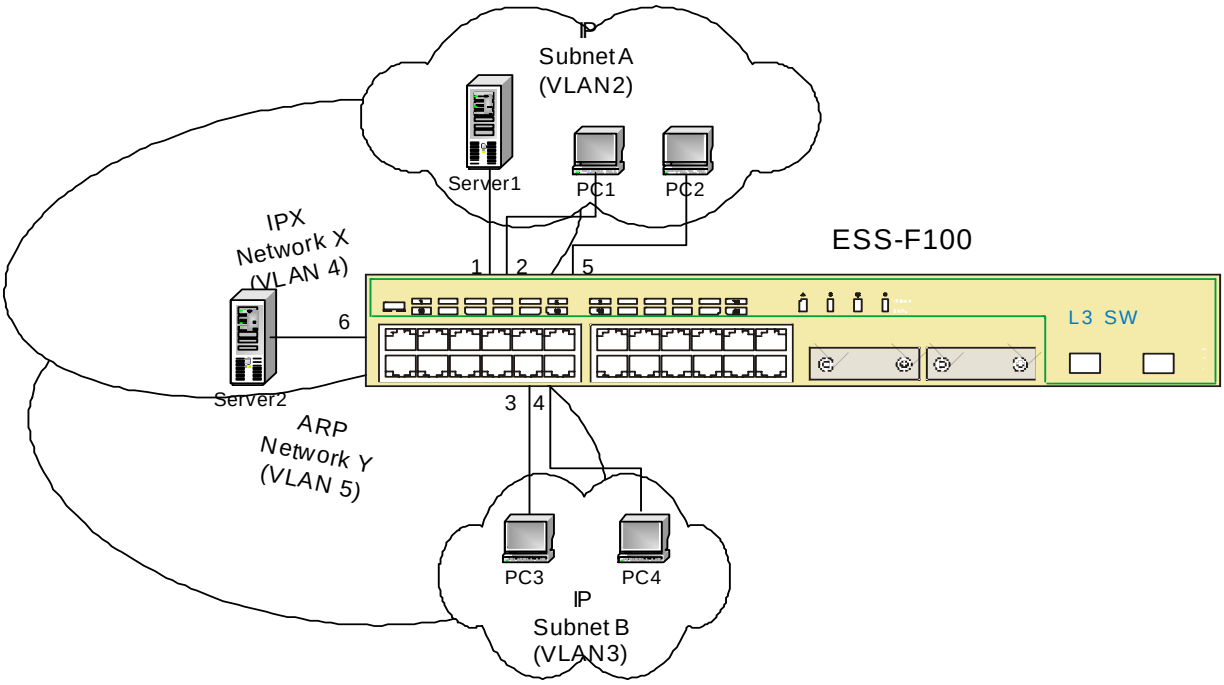

図 5-3:プロトコルベース VLAN 例

```
L3SW> config vlan create 10
L3SW> config vlan create 20
L3SW> config vlan create 30
L3SW> config vlan create 40
L3SW> config vlan create 50
L3SW> config vlan create 60
L3SW> config vlan port add 10 0.1
L3SW> config vlan port add 20 0.2
L3SW> config vlan port add 30 0.3
L3SW> config vlan port add 40 0.4
L3SW> config vlan port add 50 0.5
L3SW> config vlan port add 60 0.6
L3SW> config vlan create 2
L3SW> config vlan create 3
L3SW> config vlan create 4
L3SW> config vlan create 5
L3SW> config vlan participation include 2 0.1
L3SW> config vlan participation include 2 0.2
L3SW> config vlan participation include 2 0.5
L3SW> config vlan participation include 3 0.3
L3SW> config vlan participation include 3 0.4
L3SW> config vlan participation include 4 0.1
L3SW> config vlan participation include 4 0.6
L3SW> config vlan participation include 5 0.3
L3SW> config vlan participation include 5 0.6
L3SW> config protocol create red
L3SW> config protocol create blue
L3SW> config protocol create yellow
L3SW> config protocol create white
L3SW> config protocol protocol add 1 ip
L3SW> config protocol protocol add 2 ip
L3SW> config protocol protocol add 3 ipx
L3SW> config protocol protocol add 4 arp
L3SW> config protocol vlan add 1 2
L3SW> config protocol vlan add 2 3
L3SW> config protocol vlan add 3 4
L3SW> config protocol vlan add 4 5
```

```
L3SW> config protocol interface add 1 0.1
L3SW> config protocol interface add 1 0.2
L3SW> config protocol interface add 1 0.5
L3SW> config protocol interface add 2 0.3
L3SW> config protocol interface add 2 0.4
L3SW> config protocol interface add 3 0.1
L3SW> config protocol interface add 3 0.6
L3SW> config protocol interface add 4 0.3
L3SW> config protocol interface add 4 0.6
```

上記の設定の結果は、次のとおりです。

- IP プロトコルを実行している場合、PC1、PC2、および Server1 が、相互に通信できるようになります。PC3 と PC4 も、相互に通信できるようになります。
- IPX プロトコルを実行している場合、Server1 と Server2 が、相互に通信できるようになります。
- ARP プロトコルを実行している場合、PC3 と Server2 が、相互に通信できるようになります。
- 他のすべての状況では、通信は禁止されることになります。

5.3 汎用 VLAN Registration Protocol

5.3.1 GVRP の概要

GVRP により、LAN デバイスは、隣接する他のデバイスに対して、そこからのパケットの受信を要求する信号を送信できます。GVRP プロトコルは、IEEE 802.1Q VLAN 規格の一部として定義されています。このプロトコルの主な目的は、スイッチが VLAN 情報の一部を自動的に検出できるようにして、各スイッチ内で VLAN 情報を手動で設定しなくてすむようにすることです。GVRP は、ネットワークサーバでも実行できます。通常、これらのサーバは複数の VLAN に参加するように設定されており、参加している VLAN のネットワークスイッチに信号を送信しています。

GVRP によりスイッチは、手動で設定された IEEE 802.1Q VLAN を、GVRP をサポートしている他のデバイスにアドバタイズできます。VLAN がアドバタイズされるため、ネットワークの中核にある GVRP 対応のデバイスで、VLAN ID（VLAN タギング情報）を含めるように手動で設定する必要はありません。すべての GVRP 対応スイッチで使用される VLAN アドバタイズ機能には、アドレッシングされた PDU が含まれます。GVRP 対応デバイスは、各自のアップデートを既知（well-known）のマルチキャストアドレスに送信します。すべての GVRP 対応デバイスは、このアドレスを監視して、情報の変更状況をチェックします。

GVRP を有効にすると、VLAN 内の設定の変更に応じて、システムはアクティブなネットワークトポロジを動的に調整できます。GVRP は、各ブリッジの VLAN 変更をネットワーク内にあるその他すべての GVRP ブリッジにアドバタイズします。

5.3.2 GVRP 設定

最初に、次のコマンドを実行して、スイッチで GVRP をグローバルに有効にします。

L3SW> config garp gvrp adminmode <enable/disable>

```
L3SW> config garp gvrp adminmode enable
```

続いて、次のコマンドを実行して、必要なすべてのポート上で GVRP を有効にします。

L3SW> config garp gvrp interfacemode <slot.port/all> <enable/disable>

```
L3SW> config garp gvrp interfacemode 0.1 enable
```

次の 3 つのパラメータが設定できます。

- Join Time – VLANまたはマルチキャストグループのメンバシップを登録するGARPプロトコルデータユニットを転送する間隔です。デフォルト設定は、20 センチ秒です。[1].

  L3SW> config garp jointime <slot.port/all> <10-100>

  ```
  L3SW> config garp jointime 0.1 10
  ```

- Leave Time – VLAN またはマルチキャストグループに対する登録解除のリクエストを受信してから、その VLAN エントリを削除するまでの時間です。デフォルト設定は、60 センチ秒です。

  L3SW> config garp leavetimer <slot.port/all> <20-600>

  ```
  L3SW> config garp leavetimer 0.1 20
  ```

- Leave All Time – すべての登録が削除／解除されることを示す PDU を保持する時間です。デフォルト設定は、1000 センチ秒です。

  L3SW> config garp leavealltimer <slot.port/all> <200-6000>

  ```
  L3SW> config garp leavealltimer 0.1 200
  ```

GVRP の変更は、10 秒以内に適用されます。

ポート上で GVRP を有効にする前に、GVRP をグローバルに対して有効にしておいてください。

動的に学習される VLAN の最大数は、256 に制限されます。

5.3.3 GVRP の設定例

5.3.3.1 GVRP の有効化

L3SW> config garp gvrp adminmode enable

```
L3SW> show garp interface 0.1
```

[1] 1 センチ秒は 100 分の 1 秒を表します。つまり、20 センチ秒は 0.2 秒になります。

```
L3SW>show garp interface 0.1
             Join    Leave   LeaveAll   Port         Port
 Slot.Port   Timer   Timer    Timer   GMRP Mode   GVRP Mode
 ---------  -------  -------  -------  ---------  -----------
 0.1        20       60      1000     Disabled   Disabled

 L3SW>
```

表 5-11：ポート 0.1 の GARP 設定の表示

5.3.3.2　　VLAN タイプの変更

GVRP を使用して VLAN を作成したものの、後でスタティック VLAN 環境に変更するような場合、ダイナミック VLAN をスタティック VLAN に変更すれば、既存の動的設定を保持できます。

ダイナミック VLAN をスタティック VLAN に変更するには、次のコマンドを実行します。

L3SW> config vlan makestatic <2-4094>

L3SW> config vlan makestatic 3

5.4　スパニングツリープロトコル（STP）

STP は、IEEE によって定義されている IEEE802.1D ブリッジ仕様に含まれています。

5.4.1　STP の概要

STP は、ネットワークに障害が発生した場合に、ブリッジされたトラフィックの代替パスを決定することで、ネットワーク上にフォールトトレランス（耐障害性）を実現するブリッジベースのメカニズムです。STP により、ネットワークトラフィックに並列パスを実装し、次の点を保証します。

- **メインパスが動作している場合、サブパスは無効になります。**
- **メイントラフィックパスに障害が発生すると、サブパスが有効になります。**

VLAN や STP を設定する際の注意点は、次のとおりです。

- 各 VLAN は、独立したブロードキャストドメインを形成します。
- STP は、パスをブロックして、ループフリーの環境を作成します。
- STP がパスをブロックした場合、ブロックされたポート上でデータを送受信することはできなくなります。

STP には、次の 2 つのモードがあります。

- 802.1d：IEEE 規格に準拠しています。
- ファスト STP：ファスト STP は、STP を修正版です。このモードでは、ネットワーク収束時間が、STP で必要な時間の 3 分の 1 に短縮されます。約 30 秒以上かかる STP と比較して、ファスト STP によるネットワーク収束時間は、一般的

に約 10 秒です。

5.4.2 5.4.2 STP の開始

STP では、ネットワーク内の他のブリッジへの通信リンクが必要になります。STP では、これらの通信リンクを使用して、ブリッジ同士がブリッジプロトコルデータユニット（BPDU）を相互に交換して、有効なパスとブロックされるパスを判別します。

5.4.2.1 ルートブリッジ

ネットワークを一元的に設定するポイントでマスタとして識別されるブリッジは、ルートブリッジと呼ばれます。最小のブリッジ ID 値を持つブリッジが、ルートブリッジとして選択されます。ブリッジ ID 値は、ブリッジが持つ一意の MAC アドレスとそのブリッジに定義されたプライオリティコンポーネントを組み合わせたものです。ルートブリッジは、Hello Time と呼ばれる定期的な間隔で、すべてのポート上に BPDU を生成します。

5.4.2.2 ルートポート

ルートブリッジに最も近いポートは、ルートポートと呼ばれます。ルートポートは、ネットワーク内のすべてのブリッジにあります。

5.4.2.3 指定ブリッジ

複数のブリッジが同じ LAN に接続されている場合、1 つのブリッジが、その LAN の指定ブリッジとして選択されます。ルートブリッジと LAN の間のすべてのトラフィックは、指定ブリッジを経由することになります。

5.4.2.4 指定ブリッジポート

指定ポートとは、指定ブリッジと、そのブリッジが指定ブリッジとして機能している LAN を接続しているポートのことです。

5.4.2.5 STP タイマ

STP は、次のタイマを使用してブリッジを有効にし、ルートブリッジを選択したり、トポロジの変更について相互に通知し合ったりします。

- Hello Timers
- Hold Timer
- Topology Change Notification Timer
- Age Timer

これらのタイマに関する詳細は、IEEE802.1D 仕様を参照してください。

5.4.2.6 パスコスト（Path Cost）

この値は、ポートの速度と二重モードに基づいています。表 5-12 に、STP プロトコルで使用されるデフォルトのコストマトリックスを示します。これらの値は再設定できます。

ポートタイプ	コスト
10Mbps	**100**
100Mbps	**19**
1000Mbps	**4**

表 5-12：STP のコスト指標

各ルートポートは、そのポートからルートブリッジに向かうパスのコストに特定の値を設定します。ブリッジのルートパスコストには、ルートポートのコストと、指定したルートポートからネットワーク内のルートブリッジまでのパス内にあるすべてのルートポートのコストが含まれます。LAN セグメントの指定ポートは、そのセグメントで最小のルートパスコストを持ちます。

STP では、ネットワーク内のすべてのブリッジが、ルートブリッジ、指定ブリッジ、ルートポート、指定ポートに関する識別情報を確認できます。ネットワーク上のすべてのブリッジが、前述したような識別情報を確認した後、各ブリッジは、ルートポートとルートポートが接続されているネットワークセグメントの指定ブリッジポートの間のトラフィックだけを転送します。他のすべてのポートはブロックされます。つまり、ブリッジは、ブロックされたポートを経由したあらゆるトラフィックを送受信しなくなります。

5.4.3 STP の設定

STP をアクティブにするには、CLI の設定でスパニングツリープロトコルを選択します。STP のデフォルト設定は、すべてのスイッチポート上で“無効”です。

5.4.3.1 スイッチレベルの STP

ネットワーク上に接続されたスイッチで設定可能な STP パラメータは、次のとおりです。

- bridgepriority　STP ブリッジ優先度の値（0～65535）を設定します。デフォルト値は 32768 です。
- forwarddelay　STP ブリッジ転送遅延時間（4～30 秒）を設定します。デフォルト値は 15 秒です。
- hellotime　STP ハロータイムの値（1～10 秒）を設定します。デフォルト値は 2 秒です。
- maxage　STP ブリッジの最大エージの値（6～40 秒）を設定します。デフォルト値は 20 秒です。
- adminmode　スイッチ上のスパニングツリープロトコルを有効または無効にします。

スイッチ上で STP を有効にするには、次のコマンドを実行します。

```
L3SW> config spanningtree switch adminmode <enable/disable>

L3SW> config spanningtree switch adminmode enable
```

スイッチの STP パラメータを変更するには、次のコマンドを実行します。

```
L3SW> config spanningtree switch bridgepriority <0-65535>
```

```
L3SW> config spanningtree switch bridgepriority 0

L3SW> config spanningtree switch forwarddelay <4-30>
L3SW> config spanningtree switch forwarddelay 5

L3SW> config spanningtree switch hellotime <1-10>
L3SW> config spanningtree switch hellotime 3
```

スイッチレベルで STP が有効になったら、すべてのポートまたは各ポート単位で STP を有効にします。

5.4.3.2 ポートレベルの STP

以下は、ネットワーク上に接続されているスイッチポートや STP によってブリッジポートまたはルートポートとして指定された任意のポートで設定可能なパラメータです。

- **Mode** – off / IEEE802.1d / Fast

スイッチポートの STP モードとして、IEEE802.1d STP（標準 STP）またはファスト STP を選択できます。

- **Path cost** – Value from 1–65535 or Auto. The default value is 19
- **Priority** – Value can be from 0–255. The default value is 128

ポート 0.1 上で STP モードを有効するには、次のコマンドを実行します。

```
L3SW> config spanningtree port mode <off/802.1d/fast> <slot.port/all>

L3SW> config spanningtree port mode 802.1d 0.1
```

ポートの STP パラメータを変更するには、次のコマンドを実行します。

```
L3SW> config spanningtree port pathcost <1-65535/auto> <slot.port/all>
L3SW> config spanningtree port pathcost auto 0.1

L3SW> config spanningtree port priority <0-255> <slot.port>
L3SW> config spanningtree port priority 10 0.1
```

5.4.4 TP 設定の表示

特定のポートまたは本製品全体の STP 設定を表示するには、次のコマンドを実行します。

```
L3SW> show spanningtree switch

L3SW> show spanningtree switch
```

```
L3SW>show spanningtree switch

Spanning Tree Specification. .......  IEEE 802. ID
STP Base MAC Address ..............  00:50:A8:00:22:00
STP Topology Change Count .........  0
STP Time Since Topology Changed ....  0 day 0 hr 0 min 4 sec
STP Designated Root ...............  8000 OQ:5Q:A8:QO:22:OQ
STP Root Port .....................  0
STP Root Cost .....................  0
STP Max Age. (seconds) ............  20
STP Hello Time (seconds) ..........  2
STP Forward Delay (seconds) .......  15
STP Hold Time (seconds) ...........  1
Spanning Tree Algoritha ...........  Enable
STP Bridge Priority, ..............  32768
STP Bridge Maximum Age (seconds) ...  20
STP Bridge Hello Time (seconds) ....  2
STP Bridge Forward Delay (seconds) .  15

L3SW>
```

表 5-13:スイッチの STP 設定の表示

L3SW> show spanningtree port <slot.port>

L3SW> show spanningtree port 0.1

```
L3SW>show spanningtree port 0.1
STP Port ID. ..................... , 8001
STP Port Designated Root ..........  8000 00:50:A8:00:22:00
STP Port Designated Cost ..........  0
STP Port Designated Bridge ........  8000 00:50:A8:00:22:00
STP Port Designated Port ..........  8001
STP Port Forward Transitions Count .  1
STP Port State ....................  Forwarding
STP Port Administrative mode ......  802. ID
STP Port Priority. ................  128
STP Port Path Cost ................  4
STP Port Path Cost Mode ...........  Auto

L3SW>
```

表 5-14:ポート 0.1 の STP 設定の表示

5.4.5 STP の設定例

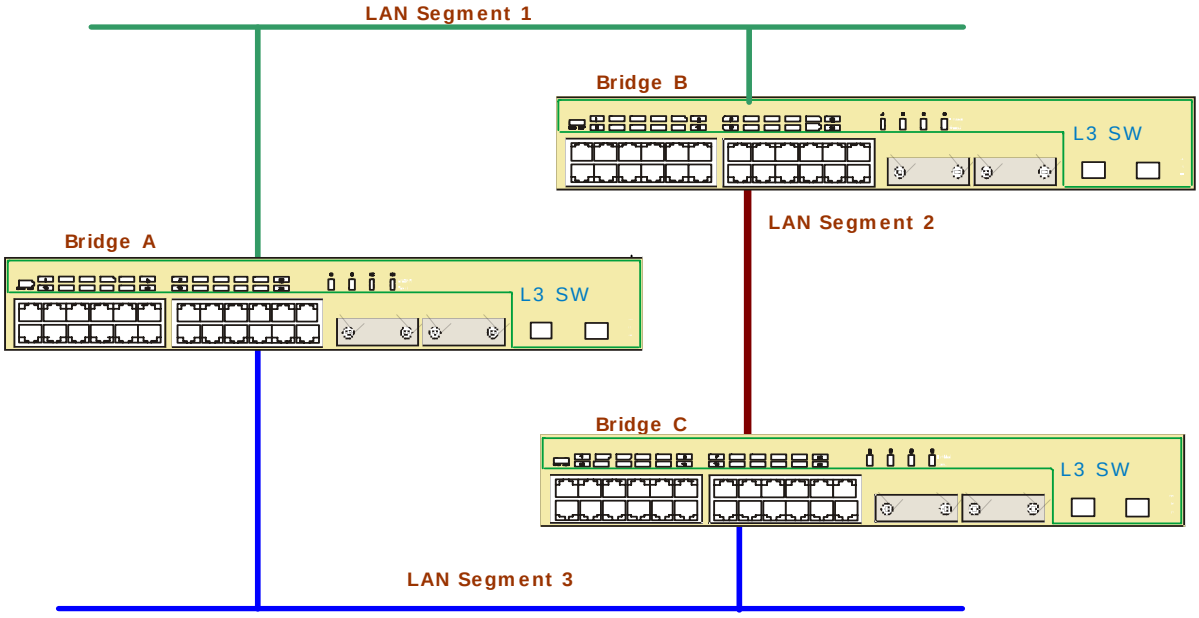

図 5-4:スパニングツリープロトコル(無効な場合)

例として、図 5-4 に、3 つのブリッジで分割された 3 つの LAN セグメントで構成されるネットワークを示します。この構成では、2 つのパスを使用して各セグメントが相互に通信できます。STP が無効な場合は、パケットがブロードキャストされると、ループが作成され、ネットワークが過負荷状態になるため、この構成は推奨できません。しかし、STP が有効な場合は、ブロードキャストストームの発生を心配しなくてすむため、この構成を採用できます。ネットワーク内で障害(リンク、ポート、またはスイッチの障害)が発生した場合、STP は、どのポートの転送をブロックまたはブロック解除すべきかをスイッチが決定するのを支援します。

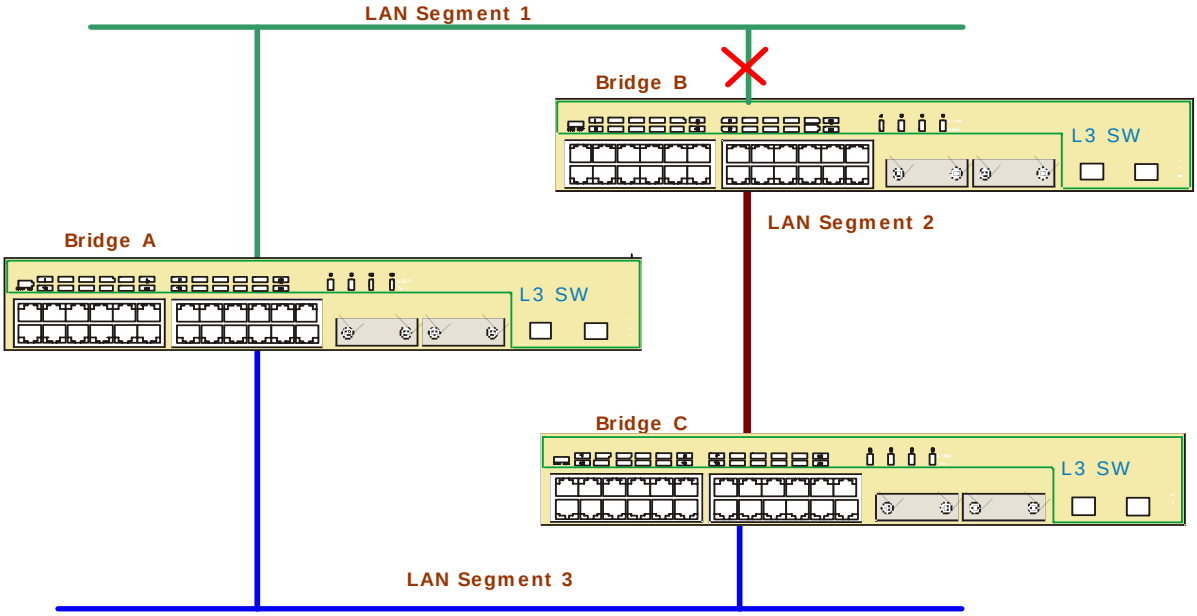

図 5-5:スパニングツリープロトコル(ポートがブロックされた場合)

図 5-5 に、同じ設定でブリッジ上の STP を有効にした結果を示します。この例の場合、ネットワーク内でループを避けるために、STP は、LAN セグメント 2 から LAN セグメント 1 へのトラフィックが、ブリッジ C とブリッジ A を経由した場合だけ流れることができるように指定しています。また、ブリッジ C 経由のリンクが失敗した場合、STP はネットワークを再設定して、LAN セグメント 2 からのトラフィックがブリッジ B 経由で流れるようにします。

5.4.6 ネットワーク内のポートコストの例

図 5-6 に、さらに大きな規模のネットワークを示します。この設定では、すべてのブリッジの各ポートにパスコスト値が割り当てられています。最小パスコスト原則に基づいて、STP はブリッジ A をルートブリッジに設定します。VLAN A の指定ブリッジポートは、ブリッジ A のポート 1 です。ルートブリッジ以外の 4 つの各ブリッジは、ルートポート(ルートブリッジに最も近いポート)を持ちます。ブリッジ X とブリッジ B は、LAN B に同じパスコストを提供できます。この場合、ブリッジ B のポートのブリッジ ID 値が最小であるため、指定ブリッジポートとして選択されます。ブリッジ C のポートが、最小のルートパスコストを提供しているため、LAN C の指定ブリッジポートとして選択されます(ブリッジ C とブリッジ B を経由したパスのコストは 200 で、ブリッジ Y とブリッジ B を経由したパスのコストは 300)。

ブリッジポートのパスコストを設定して、冗長パスを持つ任意のネットワークの構成に影響を与えることができます。

ネットワークトポロジが安定したら、すべてのブリッジは、ルートブリッジから転送される特殊な Hello BPDU を定期的に監視します。Hello BPDU を受信する前に STP 最大エージタイムが経過した場合、ルートブリッジとの通信が切断されたブリッジは、ルートブリッジまたはそのブリッ

ジ自体とルートブリッジの間のリンクがダウンしたと想定します。したがって、ブリッジは、適切な BPDU メッセージを送信して、ネットワークトポロジの再構成を開始します。

タイマを調整して、ネットワークを再設定するまでの時間（つまり、ネットワークがパス障害から回復するまでの時間）を指定できます。設定した値が低過ぎると、大量のトラフィックが発生した際にネットワークが不安定になります。

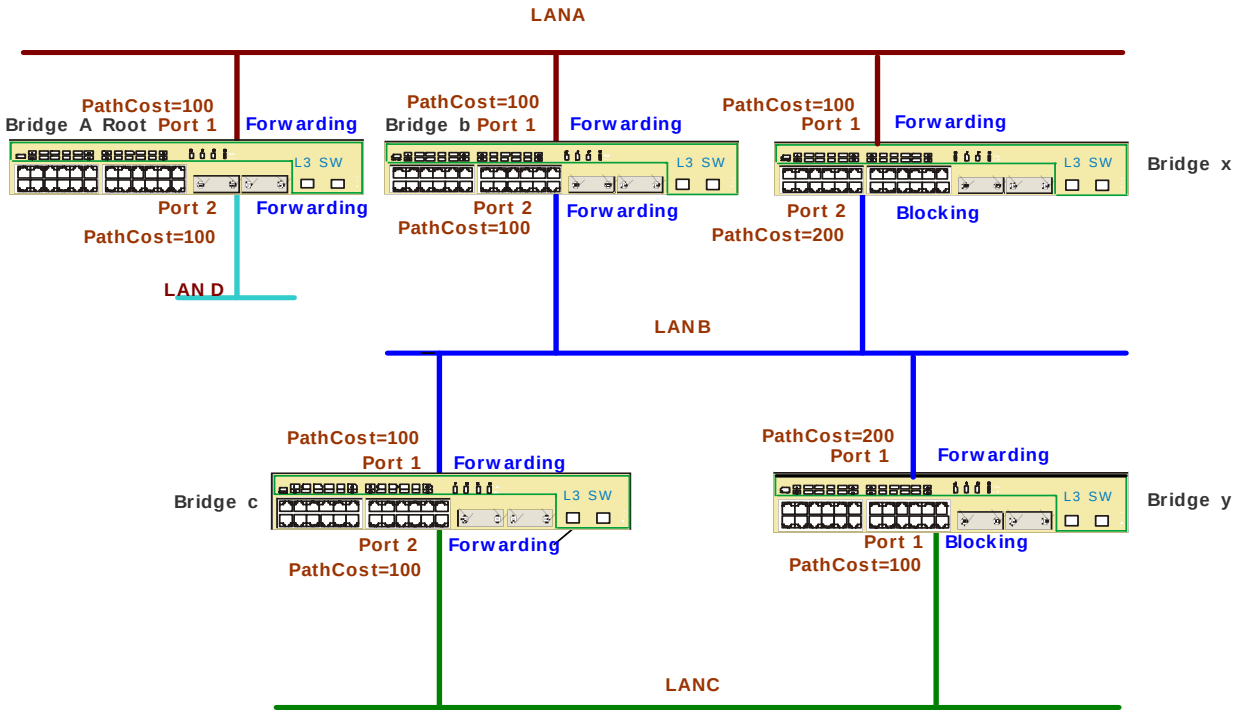

図 5-6：ネットワーク内の STP ポートコスト

5.4.7 ファスト STP

本製品のファスト STP モードでは、IEEE802.1D STP 収束時間（30 秒）より 3 倍速い STP の高速収束時間（10 秒）を実現します。この収束時間を実現するには、ポート状態を「ブロック」から「転送」に変更します。この場合、「Link Up」上の転送遅延時間は無視されます。

ファスト STP を設定するには、次のコマンドを実行します。

```
L3SW> config spanningtree port mode fast 0.1
L3SW> config spanningtree port mode fast 0.2
L3SW> config spanningtree port pathcost 100 0.1
L3SW> config spanningtree port pathcost 100 0.2
```

ファスト STP モードは、すべてのスイッチが本製品で構成されている環境でのみ使用できます。

5.5 トランク設定

5.5.1 概要

トランクポートを使用すると、2 つのスイッチ間で複数の VLAN からのトラフィックを転送できます。この目的で使用されるリンクを、トランクと呼びます。このリンクは、複数の本製品を使用した 2 つのファストまたはギガビットイーサネットポート間に設定できます。それぞれのスイッチ上にトランクポートを割り当てることで、スイッチ間に VLAN を拡張できます。

5.5.2 詳細設定

デフォルトの VLAN 1 だけを使用してスイッチ間の接続を確立した場合、追加の設定は必要ありません。トランク上で複数の VLAN をサポートする必要がある場合は、トランクポートに対してこれらの VLAN を設定する必要があります。

例えば、L3SW-1 と L3SW-2 のポート 1 がトランクポートとして設定されていて、これらのトランクポート上で 10 と 20 の VLAN ID を持つ VLAN をサポートする必要がある場合は、次のコマンドを実行します。

- (L3SW-1)VLAN 10 と VLAN 20 を作成します(作成済みの場合は不要)

```
L3SW-1> config vlan create 10
L3SW-1> config vlan create 20
```

- ポート 0.1 上で VLAN トランクを有効にします。

```
L3SW> config vlan port trunk <enable/disable> <slot.port/all>
L3SW> config vlan port trunk enable 0.1
```

- (L3SW-2)VLAN 10 と VLAN 20 を作成します(作成済みの場合は不要)

```
L3SW-2> config vlan create 10
L3SW-2> config vlan create 20
```

- (L3SW-2)ポート 0.1 上で VLAN トランクを有効にします。

```
L3SW> config vlan port trunk enable 0.1
```

ポートが VLAN トランクポートとして設定されると、そのポートでタギングが有効になり、設定されたすべての VLAN にそのポートが追加されます。無効に設定されると、ポートからすべての VLAN のタギングが削除され、デフォルト VLAN を除くすべての VLAN からそのポートが削除されます。特定のポート上でトランクを有効にして、このポートを参加させずに新しい VLAN を作成した場合、そのトランクには、それらのポートは参加していないことになります。したがって、config vlan participation コマンドを使用して、ポートを参加させる必要があります。

5.6 LACP

5.6.1 LAG の概要

LACP 機能を使用すると、2 つのスイッチ間で広い帯域幅の論理リンクを形成するためのファストイーサネットポートとギガビットイーサネットポートのグループを作成できます。LACP のためにグループ化されるポートを、LACP グループ(LAG)と呼びます。1 つの LAG は、スイッチ間またはスイッチとサーバ間を広い帯域幅で接続する論理ポートとして動作します。LAG の広い帯域

幅と Full Duplex 機能は、ファストイーサネットポートとギガビットイーサネットポートのセットで形成されており、スイッチ上の各ポートがサポートできる帯域幅より広い帯域幅が必要なアプリケーションを実行するような環境に適しています。LACP に適したアプリケーションには、次のものがあります。

- データセンタサーバ
- Web サーバ
- ストリーミングマルチメディアサーバ
- ハイエンドのグラフィックイメージングサーバやレンダリングサーバ

LAG には、フォールトトレランス機能が組み込まれています。1 つのリンクに障害が発生すると、トラフィック負荷が LAG 内の他のリンク上に分散され、管理者に問題の発生が通知されます。本製品がサポートする LAG 機能には、次のような特徴があります。

- 本製品の最大 8 個までのファストイーサネットポートまたは 8 個のギガビットイーサネットポートを LAG に割り当てることができます。
- 本製品内にある 4 個すべてのギガビットイーサネットポートを LAG に割り当てることができます。
- スイッチごとに、8 個までの LAG を設定できます。

5.6.2 LAG コマンド

LAG を作成または削除する際に使用するコマンドについて説明します。

5.6.2.1 LAG の作成

LAG を作成するには、次のコマンドセットを実行します。最初に、設定された LAG に追加する物理ポートのオートネゴシエーションモードを無効にします。次に、ポート 0.1 とポート 0.2 のオートネゴシエーションを無効にするコマンドのリストを示します。

```
L3SW> config port autoneg 0.1 disable
L3SW> config port autoneg 0.2 disable
L3SW> config port physicalmode 0.1 100f
L3SW> config port physicalmode 0.2 100f
```

LAG に参加するすべてのポートで、オートネゴシエーションを無効にして、二重モードを同じにする必要があります。

LAG を作成する（つまり、LAG の論理ポート番号と名前を関連付ける）には、次のコマンドを実行します。

```
L3SW> config lag create <name> [<slot.port> <slot.port> … <slot.port> (up to 8 interfaces)]
L3SW> config lag create Engg 0.1
```

name は、15 文字までの英数字で、Logical slot.port は LAG ポートの論理インタフェース番号です。LAG 機能に関連付けられた論理インタフェースのポート番号は、2.1 から 2.8 までです。

ポートを LAG に追加するには、config lag create コマンドでポートを指定するか、次のコマンドを実行します。

```
L3SW> config lag addport <name> [<slot.port> <slot.port> … <slot.port> (up to 8 interfaces)]
L3SW> config lag addport Engg 0.2
```

LAG に参加するすべてのポートで、LACP を有効にします。デフォルトでは、すべてのポートで LACP は有効であるため、それ以前に LACP が無効に設定されていない限り、特定のポート上で LACP を明示的に有効にする必要はありません。

作成された LAG は、デフォルトで有効になっています。LAG を有効または無効にするには、次のコマンドを実行します。

```
L3SW> config lag mode <name/all> <enable/disable>
L3SW> config lag mode Engg disable
```

LACP モードすべての LAG ポートメンバを無効にすると、対応する LAG リンクが自動的にダウンすることになります。

指定した LAG からポートを削除するには、次のコマンドを実行します。

```
L3SW> config lag removeport <name> [<slot.port> <slot.port> … <slot.port> (up to 8 interfaces)]
L3SW> config lag removeport Engg 0.1 0.2
```

作成した LAG の STP モードは、デフォルトで IEEE802.1D に設定されます。

LAG で STP モードを変更するには、次のコマンドを実行します。

```
L3SW> config lag stpmode <name/all> <off/802.1d/fast>
L3SW> config lag stpmode Engg fast
```

LAG リンクトラップモードは、デフォルトで有効になっています。ログ生成モードを有効または無効にするには、次のコマンドを実行します。

```
L3SW> config lag linktrap <name> <enable/disable>
L3SW> config lag linktrap Engg disable
```

5.6.2.2 LAG の表示

LAG の作成した後、LAG の情報を表示するには、次のコマンドを実行します。

```
L3SW> show lag <name/all>
L3SW> show lag all
```

```
L3SW>show lag all
                                                Link
Logical                 Link    Admin   Trap    STP     Mbr     Port
Slot.Port   Lag Name    State   Mode    Mode    Mode    Ports   Speed
---------   -------     ------  ------  -----   -----   ----    -----
2.1         Engg        Down    Enable  Enable  802.1d  0.1     100 Full
                                                        0.2     100 Full
L3SW>
```

表 5-15:設定されているすべての LAG の表示

このコマンドは、LAG 名、LAG に割り当てられている論理ポート番号、この LAG に参加しているスイッチポートとポート速度などの詳細情報を表示します。

5.6.2.3 LAG の削除

設定されている LAG を削除するには、次のコマンドを実行します。

```
L3SW> config lag delete <name>
L3SW> config lag delete Engg
```

5.6.3 LAG の設定例

次の例は、3 ポートを統合し、600Mbps(300MbpsFull Duplex)をサポートできる統合リンクを作成するように本製品を設定する方法を示しています。この例では、ポート 0.1、0.2、0.3 が使用されています。

```
L3SW> config port autoneg 0.1 disable
L3SW> config port autoneg 0.2 disable
L3SW> config port autoneg 0.3 disable
L3SW> config port physicalmode 0.1 100f
L3SW> config port physicalmode 0.2 100f
L3SW> config port physicalmode 0.3 100f
L3SW> config lag create Engg 0.1 0.2 0.3
L3SW> show lag all
```

```
L3SW>show lag all
                                                Link
Logical                 Link    Admin   Trap    STP     Mbr     Port
Slot.Port   Lag Name    State   Mode    Mode    Mode    Ports   Speed
---------   -------     ------  ------  -----   -----   ----    -----
2.1         Engg        Down    Enable  Enable  802.1d  0.1     100 Full
                                                        0.2     100 Full
                                                        0.3     100 Full

L3SW>
```

表 5-16:設定済みの LAG と参加しているポートの表示

5.7 プライオリティキューイング

5.7.1 プライオリティキューイングの概要

IEEE 802.1p 規格のプライオリティキューイングは、マルチメディアや遅延が許されないトラフィックの優先順位付けを有効にし、一般的なイーサネット上で音声、データ、ビデオトラフィックなどを転送できるようにします。

IEEE 802.1p では、相互接続しているネットワークハードウェアは、次の 3 つのグループに分類されます。

1. IEEE802.1p に完全準拠している。IEEE802.1p に完全準拠したハードウェアは、IEEE802.1p タギング機能をサポートし、IEEE802.1p 公開仕様に従ってパケットを転送します。ネットワーク内にあるすべてのハードウェアがこのカテゴリに適合している場合は、IEEE802.1p タギングのすべての利点を使用できます。
2. IEEE802.1p に準拠していないが、互換性はある。このタイプのハードウェアは、タグなしパケットを転送する場合と同じの方法でプライオリティタグ付きパケットを転送するだけになります。プライオリティタグを運ぶパケットに対して、特別な処理は行われません。Class I と Class II のリピータタイプのハブや一部のスイッチングハブは、このカテゴリに含まれます。ネットワーク内にあるハードウェアが、このカテゴリに含まれる場合は、IEEE802.1p タギングを有効にしても、ネットワーク上の問題は発生しませんが、パフォーマンスの向上は見込めません。
3. 互換性がない。このタイプのハードウェアは、プライオリティタグ付きパケットを解釈できないため、そのプライオリティタグ付きパケットを転送しません。ネットワーク内にあるご使用のハードウェアが、このカテゴリに含まれる場合は、その非互換ハードウェア上でタギングを有効にしないでください。

本製品は、IEEE 802.1p 仕様に完全に準拠しています。ネットワーク上の他のスイッチに関しては、必要に応じて、そのスイッチの製造元に問い合わせて、IEEE 802.1p 規格と互換性があるかどうかを確認してください。

同一セグメント上に互換性があるシステムと互換性がないシステムを混在させないでください。IEEE802.1p 互換のスイッチ上のポートが、非互換のスイッチ、ハードウェアまたはエンドノードが含まれるセグメントに接続されている場合は、パケットを転送する前にタギング情報を示す追加のバイトを削除するようにポートを設定する必要があります。

5.7.2 プライオリティキューイングの利点

- ソフトウェアベースのルータの場合、プライオリティキューイングでは、より精巧なキューイング方式と比較して、システムに与える計算負荷が軽減されます。
- プライオリティキューイングでは、ルータはバッファされたパケットを整理し、1 つのクラスのトラフィックを他のクラスのトラフィックとは別に処理できます。例えば、リアルタイムアプリケーション（双方向型のボイスやビデオなど）が、リアルタイムで動作しないアプリケーションよりも優先されるようにプライオリティを設定できます。

5.7.3 プライオリティキューイングの設定

デフォルトでは IEEE802.1p プライオリティキューイングは無効になっています。IEEE802.1p プライオリティキューイングを有効または無効にするには、次のコマンドを実行します。

```
L3SW> config switchconfig priority dot1p adminmode <enable/disable>
L3SW> config switchconfig priority dot1p adminmode enable
```

IEEE802.1p ユーザプライオリティは、出力キューにマッピングされます。マッピングエントリを使用するには、次のコマンドを実行します。

```
L3SW> show switchconfig priority dot1p
TOS Priority Mode     . . . . . .  Disable

L3SW>show switchconfig priority dotlp

 802.1p User Priority:   0 1 2 3 4 5 6 7
       Queue priority:   0 1 2 3 4 5 6 7
L3SW>
```

表 5-17:プライオリティキューマッピングの表示

プライオリティキューマッピングを変更するには、次のコマンドを実行します。

```
L3SW> config switchconfig priority dot1p map <DOT1P_priority(0-7)> <queue_priority(0-7)>
L3SW> config switchconfig priority dot1p map 0 1
```

プライオリティキュー機能が使用できるのは、ホスト上で IEEE802.1p 互換ネットワークアダプタが使用されている場合だけです。通常は、ホスト上でプライオリティを設定するアプリケーションが、NIC の製造元から提供されています。詳細は、NIC の製造元のマニュアルを参照してください。

5.8 フローコントロール

フローコントロールは、内部リソース（パケットバッファなど）の動作速度が低下した場合に、バックプレッシャーを利用して転送中の送信元からのトラフィックを削減する技術です。出力ポートに向かうトラフィック量が、そのポートの最大帯域幅を超えると、そのポートに対してパケットのキューイングが開始され、その内部バッファが一杯になると、パケットは破棄されます。ポート 1、2、3 が、10/100MBPS ポートであると仮定します。ポート 1 とポート 2 が 100Mbps のフル速度でポート 3 にトラフィックを転送している場合、ある時点でポート 3 に予約されている出力バッファでオーバーフローが発生することになります。データ損失を避けるために、Full Duplex リンクの場合は PAUSE フレーム、Half Duplex リンクの場合はジャバー（jabber）機能をそれぞれ使用して、ポート 1 とポート 2 上にバックプレッシャーを適用します。

5.8.1 Full Duplex フローコントロール

ポートに割り当てられたバッファ内のデータが特定のサイズを超えた場合、転送を停止する PAUSE フレームが転送中のポートに送信されます。

5.8.2 フローコントロールの設定

Full Duplex フローコントロールは、デフォルトでは無効になっています。

フローコントロールを有効または無効にするには、次のコマンドを実行します。

```
L3SW> config switchconfig flowcontrol <enable/disable>
L3SW> config switchconfig flowcontrol enable
```

フローコントロールでは、IEEE802.1p プライオリティキューイングを無効にする必要があります。フローコントロール用のポートは、Full Duplex モードで動作している必要があります。

5.8.3 フローコントロールの設定例

次の例は、Full Duplex フローコントロールを設定して、ポート 1 上で動作させる方法を示しています。

```
L3SW> config port autoneg 0.1 disable
L3SW> config port physicalmode 0.1 100f
L3SW> config switchconfig priority dot1p adminmode disable
L3SW> config switchconfig flowcontrol enable
```

5.9 ポートミラーリング

5.9.1 概要

ポートミラーリングは、ネットワークトラフィックをモニタリングする方法の一つです。ポートミラーリングでは、スイッチの任意のポート上で送受信される各パケットのコピーが、パケットをモニタリングする別のポートに転送されます。ネットワーク管理者は、ポートミラーリングを診断ツール

またはデバッグツールとして使用できます。

ミラーリングされたパケットを受信しているポート上にプロトコルアナライザを配置して、トラフィックをモニタリングすることができます。アナライザは、元のポート上で送受信されるトラフィックに影響を与えることなく、データのキャプチャと評価を実行できます。

ミラーリング元に設定されるポートは、モニタリング用に選択されたポートです。このポートに対するすべての入出力トラフィックは、コピーされてモニタリングポートに送信されます。ミラーリング元ポートをモニタリングするポートは、プローブポートと呼ばれます。スイッチ内で、ミラーリング用に選択できるポートは 1 つだけです。. ミラーリング元のポートが任意の VLAN のメンバである場合は、その VLAN を経由するすべてのトラフィックがモニタリングポート上で検査できます。ポートミラーリングモードは、デフォルトでは無効になっています。

現在、本製品がサポートしているのは、双方向型のポートミラーリングだけです。プローブポートで送受信されるトラフィック量が、ミラーリング元のポートの転送能力を超えると、ポートミラーリングは正常に動作しなくなります。

5.9.2 ポートミラーリングの設定

ポートミラーリングで設定可能なパラメータは、次のとおりです。

- mode：ポートミラーリングを有効または無効にします。
- create：スイッチポートをミラーリング用に設定します。
- elete：ミラーリング元のポートとプローブポートを削除します。

次の例は、ポートミラーリングの設定を示しています。

ポート 24 をミラーリング元のポート、ポート 23 をプローブポートとして設定するには、次のコマンドを実行します。

手順 1：ミラーリング元のポートとプローブポートを設定する

```
L3SW> config mirroring create <slot.port> <slot.port>
L3SW> config mirroring create 0.23 0.24
```

ポートミラーリングでは、デフォルト VLAN 1 からプローブポートが除外されます。したがって、ポートミラーリングを削除した場合、次のコマンドを実行して、プローブポートをデフォルト VLAN 1 に参加させる必要があります。

“config vlan participation include <vlanid> <slot.port>”

手順 2：スイッチでポートミラーリングを有効にする

```
L3SW> config mirroring mode <enable/disable>
L3SW> config mirroring mode enable
```

手順 3：ポートミラーリングの設定を確認する

```
L3SW> show mirroring
L3SW> show mirroring
```

```
L3SW>show mirroring

    Port Mirroring Mode ..................  Enable
    Probe Port Slot,Port .................  0.23
    Mirrored Port Slot.Port ..............  0.24
L3SW>
```

表 5-18:ポートミラーリングの表示

手順 4:ミラーリング後に物理ポートのタイプを確認する

```
L3SW> show port 0.23
```

```
L3SW>show port 0,23

Slot          STP    Admin   Physical   Physical   Link    Link   LACP   Conn
Port  Type  State  Mode     Mode       Status   Status   Trap   Mode   Type
----  ----  -----  ------  --------   --------  -------  -----  -----  ----
0.23  Probe  D     Enable   Auto      100 Full    Down    Enable Enable RJ45
                                        L3SW>
```

表 5-19:ポートミラーリング設定後のポート 0.23 の状態の表示

```
L3SW> show port 0.24
```

```
L3SW>show port 0.24

Slot          STP    Admin   Physical   Physical   Link    Link   LACP   Conn
Port  Type  State  Mode     Mode       Status   Status   Trap   Mode   Type
----  ----  -----  ------  --------   --------  -------  -----  -----  ----
0.24  Probe  D     Enable   Auto      100 Full    Down    Enable Enable RJ45
                                        L3SW>
```

表 5-20:ポートミラーリング設定後のポート 0.24 の状態の表示

次の例は、スイッチ内のポートミラーリングを削除する際に実行するコマンドを示しています。

手順 1:ミラーリングを無効にする

```
L3SW> config mirroring mode <enable/disable>
L3SW> config mirroring mode disable
```

手順 2:ポートミラーリングを削除する

```
L3SW> config mirroring delete
L3SW> config vlan participation include 1 0.23
L3SW> show mirroring
```

```
L3SW>show mirroring
Port Mirroring Mode ................. Disable
Probe Port Slot. Port ............... Not Configured
Mirrored Port Slot, Port ............ Not Configured
                                  L3SW>
```

表 5-21:ミラーリングを無効にした後のミラーリング状態の表示

本製品に設定できるポートミラーリングは、1 つだけです。

5.10 ブロードキャストストリームリカバリ(BSR)

BSR 機能を使用すると、ポートを経由して流れるブロードキャストとマルチキャストのトラフィック量を制限できます。ブロードキャストストームリカバリ機能が有効な場合、ブロードキャスト／マルチキャストトラフィックが使用する帯域幅を毎秒 4 回確認します。ブロードキャストトラフィック量がポート当たり 5M に達すると、ブロードキャストストームリカバリコントロールユニットがブロードキャストフレームのドロップを開始します。

ブロードキャストストームリカバリ機能は、L2 マルチキャストおよびブロードキャストのトラフィックや過度のトラフィックに対してサポートされています。

BSR は、次の目的で使用されます。

- スイッチが過度のブロードキャストトラフィックで溢れるのを防止する
- ブロードキャストトラフィックが使用している帯域幅をチェックする
- ブロードキャストトラフィックがしきい値に到達した場合に抑制する

本製品のブロードキャストストームリカバリ機能は、転送するブロードキャストトラフィックを特定のレートまたはしきい値に制限して、ストームの発生を防ぎます。転送したパケット数をチェックし、特定のタイムフレーム内で許可された数を超えたら、それ以降のパケットをドロップします。

本製品では、しきい値が設定できます。しきい値は、すべてのポートに対して VLAN 単位で適用され、各 VLAN に特定のブロードキャストトラフィック量が許可されることを意味します。また、しきい値は、パケット長がすべて 64 バイトであるという想定に基づいて、mbps 単位で計算されます。実際のパケットが 128 バイトである場合は、2 倍のレートのトラフィックが許可されます。

5.10.1 BSR の設定

ブロードキャストストームリカバリ機能は本製品上で設定します。BSR を設定するには、次のコマンドを実行します。

L3SW> config switchconfig broadcast <enable/disable>
L3SW> config switchconfig broadcast enable

ブロードキャストしきい値を設定するには、次のコマンドを実行します。

L3SW> config switchconfig broadcast theshold <1-1000>
L3SW> config switchconfig broadcast threshold 100

BSRは、マルチキャストパケットには影響しません。

BSR 設定を表示するには、show switchconfig summary コマンドを実行します。

```
L3SW>show switchconfig summary

Broadcast Storm Recovery Mode.................. Enable
Broadcast Storm Recovery Maximum Threshold... 100
802.3x Flow Control Mode....................... Disable
802.lp Priority Mode........................... Disable
Tos Priority Mode.............................. Disable
L3SW>
```

表 5-22:スイッチ設定情報の表示

5.11 Static MAC Filtering

5.11.1 スタティック MAC フィルタリングの概要

スタティック MAC フィルタリングを使用すると、一部のパケットが特定の物理ポートに送信されるのを防ぐことができます。設定された宛先または送信元の MAC アドレス、送信元または宛先の VLAN、送信元または宛先のポートと一致する任意のパケットが、フィルタリングされて破棄されます。スタティック MAC フィルタリング機能を使用するには、セキュリティ機能と帯域幅割り当て機能を無効にする必要があります。サポートされているスタティック MAC フィルタエントリは、最大 122 個までです。

5.11.2 スタティック MAC フィルタリングの設定

スタティック MAC フィルタリングは、デフォルトでは無効になっています。スタティック MAC フィルタリングを有効にするには、次のコマンドを実行します。

L3SW> config macfilter adminmode <enable/disable>
L3SW> config macfilter adminmode disable

スタティック MAC フィルタリングを作成するには、次のコマンドを実行します。

L3SW> config macfilter create <macaddr> <vlanid/all> <slot.port> <source/destination>
L3SW> config macfilter create 00:00:00:00:00:02 1 0.2 destination

注意

1.宛先の MAC フィルタでは、ユニキャストとマルチキャストの MAC アドレスが指定できますが、送信元の MAC フィルタで指定できるのはユニキャストの MAC アドレスだけです。

2.スタティック MAC フィルタリングでは、次の宛先 MAC アドレスは許可されません。

- 00:00:00:00:00:00
- 01:80:C2:00:00:00 to 01:80:C2:00:00:0F
- 01:80:C2:00:00:20 to 01:80:C2:00:00:21
- FF:FF:FF:FF:FF:FF

3. スタティック MAC フィルタリングでは、次の送信元 MAC アドレスは許可されません。

- 00:00:00:00:00:00
- 01:00:00:00:00:00 to FF:FF:FF:FF:FF:FF

既存のスタティック MAC フィルタエントリを削除するには、次のコマンドを実行します。

```
L3SW> config macfilter delete <macaddr> <vlanid/all> <slot.port> <source/destination>
L3SW> config macfilter delete 00:00:00:00:00:02 1 0.2 destination
```

すべての MAC フィルタ設定を消去するには、次のコマンドを実行します。

```
L3SW> clear macfilter
Are you sure you want to clear static MAC filter configuration? (y/n) Y
MAC Filter Configuration Cleared.
```

設定されたすべてのスタティック MAC フィルタを表示するには、次のコマンドを実行します。

```
L3SW> show macfilter <all/macaddr>
L3SW> show macfilter all
```

```
L3SW>show macfilter all

Static MAC Filtering Feature.................. Enable

MAC Address        VLAN ID   Desitnation Port
-----------------  -------  ------------------
00:00:00:00:00:02   1          0.2

L3SW>
```

表 5-23：すべてのスタティック MAC フィルタの表示

スタティック MAC フィルタリングを使用したブロードキャストパケット（不明な MAC アドレスを含む）とマルチキャストパケットのフィルタリングは、VLAN 単位でのみサポートされます。例えば、「config macfilter create 01:00:5e:01:01:01 2 0.6 destination」という macfilter コマンドは、宛先が「01:00:5e:01:01:01」のマルチキャストトラフィックを、コマンドで指定したポート 6 だけでなく、VLAN 2 に接続されたすべてのポートにフィルタリングします。

5.11.3 スタティック MAC フィルタの設定例

次の例は、送信元と宛先のポート、VLAN、MAC アドレスに対してスタティック MAC フィルタリングを設定する際に実行するコマンドを示しています。ポート 12 の MAC アドレスが、00:00:00:00:00:14、ポート 10 の MAC アドレスが、00:00:00:00:00:12 であり、これらのポートが VLAN 12 と VLAN 10 にそれぞれ参加していると仮定しています。設定後、ポート 10 以外の任意のポートが、ポート 10 の宛先 MAC アドレスを付けたトラフィックを送信した場合、ポート 10

はそのトラフィックを受信しません。同様に、送信元のポート 12、送信元の MAC アドレス、および送信元の VLAN 10 と一致するパケットは破棄されます。

```
L3SW> config bwprov disable
L3SW> config security disable
L3SW> config macfilter adminmode enable
L3SW> config macfilter create 00:00:00:00:00:12 10 0.10 destination
L3SW> config macfilter create 00:00:00:00:00:14 12 0.12 source
```

```
L3SW>show macfilter all

Static MAC Filtering Feature.................. Enable

MAC Address         VLAN ID   Desitnation Port
------------------  -------  ------------------
00:00:00:00:00:14   12           0.12

--More—or (q)uit

Destination MAC filter:
MAC Address         VLAN ID   Desitnation Port
------------------  -------  ------------------
00:00:00:00:00:12   10          0.10

L3SW>
```

表 5-24:送信元と宛先の MAC フィルタの表示

5.12 ポートセキュリティ

5.12.1 5.12.1 ポートセキュリティ機能の概要

ポートセキュリティを使用すると、一部のパケットを特定のポートに送信できます。デフォルトでは、すべての受信パケットは破棄されるように設定されています。設定された送信元の MAC アドレス、VLAN、ポートと一致するパケットだけが許可されます。ポートセキュリティ機能を使用するには、帯域幅割り当て機能を無効にする必要があります。最大 122 個までのポートセキュリティエントリがサポートされています。

5.12.2 ポートセキュリティの設定

ポートセキュリティ機能は、デフォルトでは無効になっています。有効にするには、次のコマンドを実行します。

```
L3SW> config secureport adminmode <enable/disable>
L3SW> config secureport adminmode enable
```

送信元の MAC アドレスを使用して、ポートセキュリティエントリにポートを追加するには、次のコマ

ンドを実行します。

```
L3SW> config secureport add <slot.port> <macaddr>
L3SW> config secureport add 0.1 00:00:00:00:00:02
```

注意

1. 設定できるのは物理ポートだけです。LAG または VLAN ルーティングで定義された論理インタフェースは設定できません。
2. ポートセキュリティ設定では、マルチキャスト MAC アドレス、ブロードキャスト MAC アドレス、次の宛先 MAC アドレスは設定できません。
    - 00:00:00:00:00:00
    - 01:00:00:00:00:00 to FF:FF:FF:FF:FF:FF

既存のポートセキュリティ設定を削除するには、次のコマンドを実行します。

```
L3SW> config secureport remove <slot.port> <macaddr>
L3SW> config secureport remove 0.2 00:00:00:00:00:02
```

すべてのポートセキュリティ設定を消去するには、次のコマンドを実行します。

```
L3SW> clear secureport
Are you sure you want to clear Port Security configuration? (y/n) y
Port Security Configuration Cleared.
```

すべてのポートセキュリティ設定を表示するには、次のコマンドを実行します。

```
L3SW> show secureport <slot.port/all>
L3SW> show secureport all
```

```
L3SW>show secureport all

Port Security Feature.....................Enable

  Slot Port        MAC Address
------------    -----------------
    0.1         00:00:00:00:00:02

L3SW>
```

表 5-25:すべてのポートセキュリティの表示

5.12.3 ポートセキュリティの設定例

次の例は、本製品でポートセキュリティを設定する際に実行するコマンドを示しています。ポート 1 の MAC アドレスが 00:00:00:00:00:02 で、すべてのポートが VLAN 1 にそれぞれ参加していると仮定しています。

```
L3SW> config bwprov disable
L3SW> config security disable
```

```
L3SW> config secureport adminmode enable
L3SW> config secureport add 0.1 00:00:00:00:00:02
```

5.13 IEEE802.1X

5.13.1 IEEE802.1x 機能の概要

IEEE 802.1x は、最小限の管理オーバーヘッドで、ほぼ無制限のスケーラビリティを実現できる新しい技術規格です。ネットワークの外縁でユーザアクセスを認証することで、不正なアクセスを防止し、一元化された認証サーバ上ですべてのユーザ認証が実行できます。クライアントと認証ポイントには、拡張可能認証プロトコル（EAP）を使用します。IEEE802.1x は、転送中の EAP メッセージのカプセル化を定義しているため、さまざまなメディアタイプ上でこれらのメッセージを転送できます。メディアタイプには、次のものが含まれます。

- EPA Over LAN (EPAOL)
- EPA Over Wireless.(EPAOW)

本製品がサポートしているのは、EPA Over LAN だけです。

IEEE802.1x 規格では、次の用語が使用されます。

- クライアント：IEEE802.1x 対応のクライアントとは、LAN サービスを要求しているネットワークアクセスデバイスのことです。
- 認証ポイント：IEEE802.1x 認証機能が有効なネットワークアクセスポイントのことです。このアクセスポイントには、本製品の LAN スイッチポートが含まれます。
- 認証サーバ：ユーザ名／パスワードに基づいてネットワークへのアクセスを許可または拒否する認証処理を実行するサーバです。02.1x では、リモート認証ダイヤルインユーザサービス（RADIUS）をサポートするサーバが使用されます。

5.13.2 IEEE802.1x 機能の設定

IEEE802.1x 機能で RADIUS サーバと通信するように本製品を設定するには、次のコマンドを実行します。

```
L3SW> config radius server addr <serverip>
L3SW> config radius server addr 10.10.10.2
```

本製品と RADIUS サーバの間で共有される秘密の鍵（パスワード）を設定します。このパスワードは、2 つのデバイス間のすべてのトランザクションの認証に使用されます。任意の英数字が含まれる 1 から 128 文字までの長さの文字列を指定できます。設定するには、次のコマンドを実行します。

```
L3SW> config radius server  <shared secret>
L3SW> config radius secret compcenter
```

RADIUS サーバサービスおよび RADIUS アカウンティングサービス用の UDP ポートを設定するには、次のコマンドを実行します。

```
L3SW> config radius server port  <1645/1812>
L3SW> config radius server port 1812
```

L3SW> config radius acct port <1646/1813>
L3SW> config radius acct port 1813

デフォルトの UDP ポート設定は、RADIUS サービスでは 1812、アカウンティングサービスでは 1813 です。

すべての RADIUS 設定を表示するには、次のコマンドを実行します。

L3SW> show radius info

```
L3SW>show radius info

Server IP.............................  10.10.10. 2
Server port...........................  1812
Server accounting port................  1813
Server shared secret key..............  compcenter
Idle Timeout..........................  30 minutes

L3SW>
```

表 5-26：RADIUS サーバ設定の表示

IEEE802.1x クライアント用にポートを設定するには、次のコマンドを実行します。

手順 1：IEEE802.1xの管理モードを有効または無効にする

IEEE802.1x 機能の管理モードは、デフォルトでは無効になっています。有効にするには、次のコマンドを実行します。

L3SW> config dot1x switch adminmode <enable/disable>
L3SW> config dot1x switch adminmode enable

手順 2：ポートコントロールモードを設定する

ポートコントロールには、次の 3 つのタイプがあります。

- ForceAuthorized:IEEE802.1x を無効にして、認証交換を要求せずに、ポートを認証済みの状態にします。これは、デフォルトのポートコントロール設定です。
- ForceUnauthorized:クライアントによるすべての認証試行を無視して、ポートを無条件に未認証の状態のままにします。
- Auto:IEEE802.1x を有効にします。これで、ポートは未認証の状態になります。

IEEE802.1x ポートコントロールを設定するには、次のコマンドを実行します。

L3SW> config dot1x port control <slot.port/all> <forceauthorized/forceunauthorized/auto>
L3SW> config dot1x port control all forceauthorized

IEEE802.1x 機能は、スイッチ上の MAC フィルタ機能を有効にする必要があります。

LAG または VLAN ルーティングで定義された論理インタフェースは、config dot1x コマンド内のポートパラメータとして指定できません。

IEEE802.1x クライアントが、異なるサブネット上の RADIUS サーバにアクセスできるようにするには、IEEE802.1x クライアントと RADIUS サーバが接続されるポート上に IP インタフェースを作成する必要があります。

IEEE802.1x スイッチ設定を表示するには、次のコマンドを実行します。

L3SW> show dot1x switch

```
L3SW>show dotlx switch

Switch administration mode.............  Enable
EAP re-transmission interval...........  30 seconds
EAP maximum re-transmissions...........  2
Re-authentication interval.............  3600 seconds
Quiet period.............................. 60 seconds
Maximum re-authentication attempts.....  2
Supplicant timeout interval............  30 seconds
Server timeout interval................  30 seconds

L3SW>
```

表 5-27：IEEE802.1x の状態表示

IEEE802.1x の物理ポートコントロール設定を表示するには、次のコマンドを実行します。

L3SW> show dot1x port <slot.port/all>

```
L3SW> show dot1x port all
```

```
L3SW>show dotlx port all
Slot. Admin   Control          Per.    Status
Port  Mode                     Re-auth
----- ------- ---------------- ------- ------------
0.1   Disable ForceAuthorized  Enable  UnAuthorized
0.2   Disable ForceAuthorized  Enable  UnAuthorized
0.3   Disable ForceAuthorized  Enable  UnAuthorized
0.4   Disable ForceAuthorized  Enable  UnAuthorized
0.5   Disable ForceAuthorized  Enable  UnAuthorized
0.6   Disable ForceAuthorized  Enable  UnAuthorized
0.7   Disable ForceAuthorized  Enable  UnAuthorized
0.8   Disable ForceAuthorized  Enable  UnAuthorized
0.9   Disable ForceAuthorized  Enable  UnAuthorized
0.10  Disable ForceAuthorized  Enable  UnAuthorized
0.11  Disable ForceAuthorized  Enable  UnAuthorized
0.12  Disable ForceAuthorized  Enable  UnAuthorized
0.13  Disable ForceAuthorized  Enable  UnAuthorized
0.14  Disable ForceAuthorized  Enable  UnAuthorized
0.15  Disable ForceAuthorized  Enable  UnAuthorized
0.16  Disable ForceAuthorized  Enable  UnAuthorized
0.17  Disable ForceAuthorized  Enable  UnAuthorized
0.18  Disable ForceAuthorized  Enable  UnAuthorized
0.19  Disable ForceAuthorized  Enable  UnAuthorized
—More— or (q)uit
0.20  Disable ForceAuthorized  Enable  UnAuthorized
0.21  Disable ForceAuthorized  Enable  UnAuthorized
0.22  Disable ForceAuthorized  Enable  UnAuthorized
0.23  Disable ForceAuthorized  Enable  UnAuthorized
0.24  Disable ForceAuthorized  Enable  UnAuthorized
1.1   Disable ForceAuthorized  Enable  UnAuthorized
1.2   Disable ForceAuthorized  Enable  UnAuthorized
1.3   Disable ForceAuthorized  Enable  UnAuthorized
1.4   Disable ForceAuthorized  Enable  UnAuthorized

L3SW>
```

表 5-28：IEEE802.1x ポート設定の表示

5.13.3 IEEE802.1x の設定例

次の例は、IEEE802.1x を設定する際に必要なコマンドのシーケンスを示しています。**図 5-7：IEEE802.1x クライアントと RADIUS サーバの設定**で示すネットワーク図には、3 つの IP サブネット（10.10.10.0/24、20.0.0.0/8、30.0.0.0/8）が含まれています。各サブネットには、1 つのポートが含まれます。10.10.10.0/24 サブネットにはポート 0.1、20.0.0.0/8 サブネットにはポート 0.2、30.0.0.0/8 サブネットにはポート 0.3 が、それぞれ設定されています。次の手順では、RADIUS サーバと IEEE802.1x クライアントを設定して本製品と接続する方法について説明します。

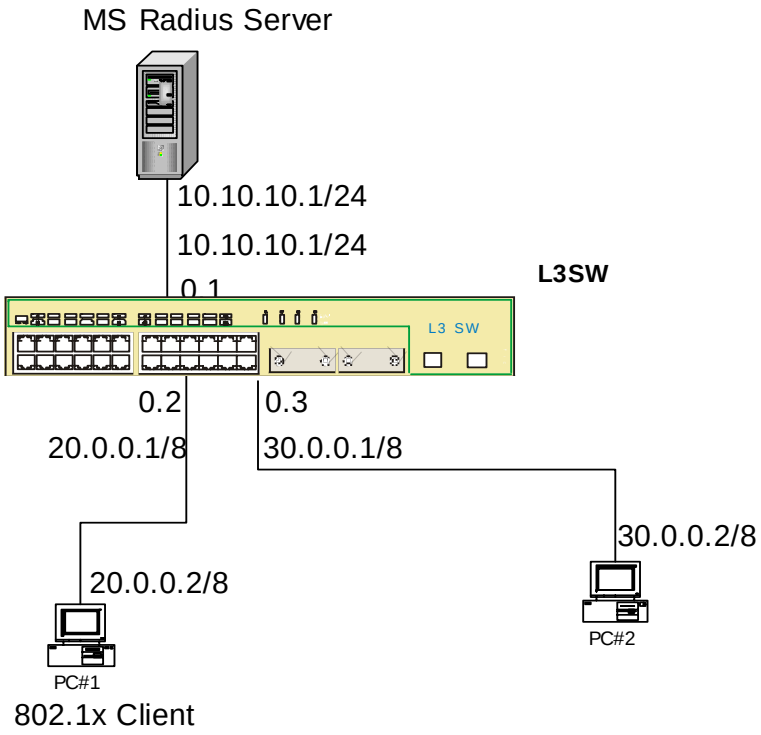

図 5-7：IEEE802.1x クライアントと RADIUS サーバの設定

1. *RADIUS サーバ*

a)この設定で使用される RADIUS サーバは、MS-IAS です

b)RADIUS サーバの IP アドレス：10.10.10.2/24

c)秘密鍵として、compcenter を設定します

d)アクティブディレクトリ内にユーザ名とパスワードを作成します（例えば、ユーザ名：raduser、パスワード：user）。

e)デフォルトドメインポリシー設定で、すべてのユーザに対する逆暗号化を有効にします。

f)IAS サーバ設定で EAP for MD5-Challenge を有効にします。

2. *IEEE802.1x クライアント（PC1）*

a）PC1 に AEGIS *IEEE802*.1x クライアントがインストールされていると仮定します。

b）PC1 の IP アドレス： 20.0.0.2

c）ユーザ名： raduser

d) パスワード： user

3. 本製品の設定詳細

手順 1：RADIUSサーバ、*IEEE802*.1xクライアント、非*IEEE802*.1xクライアントのIPインタフェースを設定する

a1) L3SW> config ip port create 0.1 10.10.10.1 255.255.255.0

a2) L3SW> config ip port create 0.2 20.0.0.1 255.0.0.0

a3) L3SW> config ip port create 0.3 30.0.0.1 255.255.255.0

手順 2：ルーティングを有効にする

a1) L3SW> config routing enable

手順 3：RADIUSを設定する

a1) L3SW> config radius server addr 10.10.10.2

a2) L3SW> config radius secret compcenter

手順 4：*IEEE802*.1xクライアントを設定する

a1) L3SW> config macfilter adminmode enable

a2) L3SW> config dot1x switch adminmode enable

a3) L3SW> config dot1x port adminmode 0.2 enable

手順 5：*IEEE802*.1xクライアントのポートコントロールをセットアップする

a1) L3SW> config dot1x port control 0.2 auto

上記のポートコントロール設定では、IEEE802.1x クライアントは、パスワードが正しい場合だけ認証され、PC1 は PC2 と通信できることになります。パスワードが正しくない場合、PC1 と PC2 は通信できません。

a2) L3SW> config dot1x port control 0.2 forceunauthorized

上記のポートコントロール設定では、IEEE802.1x クライアントは PC2 と通信できません。

a3) L3SW> config dot1x port control 0.2 forceauthorized

このコントロールモードでは、クライアントは常に認証され、PC2 と通信できます。

5.14 レイヤ2 マルチキャストサービス

5.14.1 レイヤ 2 マルチキャストの概要

本製品は、マルチキャストスイッチングのサポートを装備しています。マルチキャストトラフィックを通常のブロードキャストトラフィックとは別に処理する機能によって、マルチキャストストリームが、レイヤ 2 モードで動作しているスイッチを経由している場合のパフォーマンスが格段に向上します。マルチキャストスイッチングは、GARP マルチキャスト登録プロトコル（GMRP）とインターネットグループ管理プロトコル（IGMP）スヌーピングという 2 つの主な要素で構成されます。

GMRP では、ブリッジやエンドステーションが、同じ LAN セグメントに接続されている MAC ブリッジにマルチキャストグループメンバシップ情報を動的に登録したり、その登録を解除したりすることができるメカニズムが提供されており、その情報は、拡張フィルタリングサービスをサポートするブリッジ LAN 内のすべてのブリッジに伝播されることになります。GMRP の動作は、GARP が提供するサービスに依存します。

IGMP スヌーピングでは、スイッチが、ホストとルータの間の IGMP 通信を「監視」して、IGMP フレームを直接キャプチャできます。スイッチは、あるホストからの指定されたマルチキャストグループに対する IGMP レポートを受信すると、そのグループにホストのポート番号を追加します。また、IGMP LEAVE を受信すると、マルチキャストグループテーブルのエントリからホストのポートを削除します。グループメンバシップを保持するために、マルチキャストルータは IGMP クエリを 60 秒ごとに送信します。このクエリは、スイッチでインターセプトされ、スイッチ上のすべてのポートに転送されます。そのクエリに、グループのすべてのホストメンバが応答します。ホストは、他のホストのレポートを受信しないため、グループごとに 1 つのホストではなく、すべてのホストがレポートを送信します。その後、スイッチは、プロキシレポートを使用して、そのグループ用に受信したすべての応答に対してグループごとにレポートを 1 つだけ転送します。

5.14.2　GMRP 設定

L2 マルチキャスティングサポートをアクティブにするには、スイッチで GMRP をグローバルに有効にする必要があります。次のコマンドを実行して、GMRP をアクティブにします。

```
L3SW> config garp gmrp adminmode <enable/disable>
L3SW> config garp gmrp adminmode enable
```

続いて、次のコマンドを実行して、必要なポート上で GMRP を有効にする必要があります。

```
L3SW> config garp gmrp interfacemode <slot.port/all> <enable/disable>
L3SW> config garp gmrp interfacemode 0.1 enable
```

5.14.3　IGMP スヌーピングの設定

スイッチで IGMP スヌーピングをアクティブにするには、最初に次のコマンドを実行して、スイッチで IGMP スヌーピングをグローバルに有効にします。

```
L3SW> config igmpsnooping adminmode <enable/disable>
L3SW> config igmpsnooping adminmode enable
```

続いて、次のコマンドを実行して、必要なポート上で IGMP スヌーピングを有効にする必要があります。

```
L3SW> config igmpsnooping interfacemode <slot.port/all> <enable/disable>
L3SW> config igmpsnooping interfacemode 0.1 enable
```

次の 3 つのパラメータが設定できます。

- queryinterval（クエリ間隔）：エントリから特定のインタフェースが削除されるまでに、スイッチがそのインタフェース上で特定のグループからのレポートを待つ秒単位の時間です。この値は、最大応答時間の値より大きくする必要があります。デフォルト値は 125 秒です。この間隔を変更するには、次のコマンドを実行します。

```
L3SW> config igmpsnooping queryinterval <1-3600>
L3SW> config igmpsnooping queryinterval 180
```

- maxresponse（最大応答時間）：スイッチがインタフェース上でクエリを送信した後、その応答を待つ秒単位の時間です。この値は、クエリ間隔の値より小さくする必要があります。デフォルト値は 10 秒です。この間隔を変更するには、次のコマンドを実行します。

```
L3SW> config igmpsnooping maxresponse <1-3600>
L3SW> config igmpsnooping maxresponse 30
```

- mcrtrexpiretime（マルチキャストルータ存在時間）：インタフェース上でクエリが受信されるのをスイッチが待つ時間（秒単位）です。この時間が経過すると、マルチキャストルータが接続されているインタフェースのリストからそのインタフェースが削除されます。デフォルト値は 0（つまり、期限なし）です。この間隔を変更するには、次のコマンドを実行します。

```
L3SW> config igmpsnooping mcrtrexpiretime <0-3600>
L3SW> config igmpsnooping mcrtrexpiretime 1800
```

GMRP と IGMP スヌーピングの変更は、10 秒以内に適用されます。

ポート上で GMRP と IGMP スヌーピングを有効にする前に、スイッチに対してグローバルに有効にしておく必要があります。

IGMP スヌーピングモードが有効な場合、IGMP パケット（JOIN、LEAVE など）は、IGMP QUERY パケットを受信したポートのみを経由して転送されます。つまり、IGMP スヌーピングモードが有効な場合、IGMP パケットは、L3 マルチキャストルータに到達できるポートにだけ転送されます。

6. レイヤ 3 の設定

IP ルーティングとは、ネットワークトポロジを判定して、ネットワークでのパケット転送に使用する IP ルーティングテーブルを設定するプロセスのことです。一般に、パケットの宛先が発信元と異なるサブネットワークにある場合、パケットを指定された宛先に送るルート指定には1つ以上のルータが必要になります。ルーティングと転送の違いは、わずかなものです。本マニュアルでは、ルーティングと転送は同じ意味で使用しています。

IP パケットをルーティングするために、ルータではリモートネットワークのためのルーティングテーブルを設定管理する必要があります。ルートは隣接するルータから学習したり、ネットワーク管理者が設定したりします。本製品では、ルーティングテーブルのエントリを生成するために、次の方法を使用します。

- **スタティックルーティング**

  VLAN 間ルーティング

  スタティックルーティング

- **ダイナミックルーティング**

  RIP

  OSPF

  BGP

  DVMRP

  PIM-DM

6.1 一般的なレイヤ3 の設定

6.1.1 アドレス解決プロトコル（ARP）

本製品では ARP を使用して、ホストや他のルータの IP アドレスに対応する MAC アドレスを検出します。ARP テーブルのエントリには、ローカル、スタティック、ダイナミックの 3 種類があります。ローカル ARP エントリは、IP インタフェースによって生成されます。スタティック ARP エントリは、ユーザが生成します。ダイナミック ARP エントリは、ルーティングプロトコルによって学習されます。

6.1.1.1 ARP キャッシュサイズの設定

ARP キャッシュのサイズは、CAM のサイズによって決まります。ARP キャッシュサイズを最大に設定する場合は、show cam コマンドを実行します。

ARP キャッシュサイズを変更する場合は、次のコマンドを実行します。

```
L3SW> config arp cachesize <10-1256>
L3SW> config arp cachesize 1200
```

6.1.1.2 スタティック ARP エントリの生成

スタティックエントリの数は、ARP キャッシュサイズの半分以下に設定します。例えば、ARP キャッシュサイズが 1200 の場合、スタティック ARP エントリの数は 600 を超えることはできません。

ARP エントリを生成する場合は、次のコマンドを実行します。

```
L3SW> config arp create <arpentry> <macaddr>
L3SW> config arp create 10.1.1.10 00:00:00:01:01:01
```

6.1.1.3 ARP エントリの削除

ARP エントリを削除する場合は、次のコマンドを実行します。

```
L3SW> config arp delete <arpentry>
L3SW> config arp delete 10.1.1.10
```

6.1.1.4 ダイナミック ARP エントリの削除

学習済みのダイナミック ARP エントリを削除する場合は、次のコマンドを実行します。

```
L3SW> clear arp
L3SW> clear arp
```

6.1.1.5 ARP キャッシュテーブルの表示

ARP テーブルを表示する場合は、次のコマンドを実行します。

```
L3SW> show arp table
L3SW> show arp table
```

```
L3SW>show arp tab

     Age Time (seconds)........................  1200
     Response Time (seconds)...................  1
     Retries...................................  4
     Cache Size................................  1256

  IP Address      MAC Address      Interface     Type
--------------  ----------------  -----------  -------
10.1.1.1       00:50:A8:00:04:26  4.1          Local
10.1.1.10      00:00:00:00:01:01  4.1          Static
10.1.1.255     FF:FF:FF:FF:FF:FF  4.1          Static
10.2.1.1        00:50:A8:00:04:26  4.2          Local
10.2.1.255      FF:FF:FF:FF:FF:FF  4.2          Static
10.3.1.1        00:50:A8:00:04:26  4.3          Local
10.3.1.255      FF:FF:FF:FF:FF:FF  4.3          Static

L3SW>
```

表 6-1：ARP テーブルの表示

6.1.1.6 ARP 有効期間の設定

ダイナミックエントリを ARP キャッシュに保持しておく時間（秒）を設定します。デフォルトでは、保持期限を過ぎたエントリはキャッシュから消去されるように設定されています。保持期間は 15 から 3600 秒で指定します。デフォルト値は 1200 秒です。

```
L3SW> config arp agetime <15—3600 seconds>
L3SW> config arp agetime 200
```

6.1.1.7 ARP 応答時間の設定

ARP リクエストに対する待機時間（秒）を設定します。応答時間を過ぎると、本製品は ARP リクエストを再送信します。

```
L3SW> config arp resptime <1-10 seconds>
L3SW> config arp resptime 1
```

6.1.1.8 ARP 再試行回数の設定

特定の IP アドレスに宛てた ARP リクエストに応答がない場合に、ARP リクエストを再送信する回数を設定します。

```
L3SW> config arp retries <1-10>
L3SW> config arp retries 4
```

6.1.2 ルーティングモードの設定

デフォルトではルーティングモードは無効に設定されているため、本製品はレイヤ 2 スイッチとして動作します。本製品をルータとして利用するには、ルーティングモードを有効にする必要があります。ルーティングモード設定は、レイヤ 3 ルーティング設定の前に行ってください。

ルーティングモードを有効または無効にするには、次のコマンドを実行します。

```
L3SW> config routing <enable/disable>
L3SW> config routing enable
```

現在のルーティングモード設定を表示する場合は、次のコマンドを実行します。

```
L3SW> show ip summary
```

```
L3SW>show ip summary

Default Time to Live ..................... 64
Router ID ................................ 10.1.1.1
Routing Mode ............................. Enabled

L3SW>
```

表 6-2：ルーティングモードの表示

6.1.3 ルータ ID の設定

ルータ ID は、ルータを特定する識別子で、ルーティングプロトコルによるネットワーク内のプロトコルメッセージ生成元の識別に使用されます。ルータ ID は、仮想ポートに割り当てられた IP アドレスと同じである必要はありません。ただし、ネットワーク上に同一のルータ ID を割り当てることはできません。ルータインタフェースの 1 つの IP アドレスをルータ ID に指定することで、管

理者はネットワーク内でのルータ ID の二重割当を回避することができます。

ダイナミックルーティングプロトコルが有効な場合、ルータ ID を定義する必要があります。

ルータ ID を設定する場合は、次のコマンドを実行します。

L3SW> config router id <*routerid*>
L3SW> config router id 10.1.1.1

ルータ ID を表示する場合は、次のコマンドを実行します。

L3SW> show ip summary

☞ ***注意ルータ ID を変更した場合は、本製品を再起動してください。***

6.1.4 IP 統計データ

IP や ICMP パケットなどの IP 統計データを表示する場合は、次のコマンドを実行します。

L3SW> show ip stats
L3SW> show ip stats

```
L3SW>show ip stats

IpInReceives ..............................  67369
IpInHdrErrors .............................  0
IpInAddrErrors ............................  0
IpForwDatagrams ...........................  0
IpInUnknownProtos .........................  0
IpInDiscards ..............................  0
IpInDelivers ..............................  61766
IpOutRequests .............................  16493
IpOutDiscards .............................  0
IpOutWoRoutes .............................  0
IpReasmTimeout ............................  0
IpReasmReqds ..............................  0
IpReasmOKs ................................  0
IpReasmFails ..............................  0
IpFragOKs .................................  0
IpFragFails ...............................  0
IpFragCreates .............................  0
IpRoutingDiscards .........................  0
IcmpInMsgs ................................ 0
IcmpInErrors ..............................  0
—More— or (q)uit
IcmpInDestUnreachs ........................  0
IcmpInTimeExcds ...........................  0
IcmpInParmProbs ...........................  0
IcmpInSrcQuenchs ..........................  0
IcmpInReduects ............................  0
IcmpInEchos ...............................  0
IcmpInEchoReps ............................  0
IcmpInTimestamps ..........................  0
IcmpInTimestampReps .......................  0
IcmpInAddrllasks ..........................  0
IcmpInAddrllaskReps .......................  0
IcmpOutHsgs ...............................  0
IcmpOutErrors .............................  0
IcmpOutDestUnreachs .......................  0
IcmpOutTimeExcds ..........................  0
IcmpOutParmProbs ..........................0
IcmpOutSrcQuenchs .........................  0
IcmpOutReduects ...........................  0
IcmpOutEchoReps ...........................  0
IcmpOutTimestamps .........................  0
IcmpOutTimestampReps ......................  0
IcmpOutAddrMasks ..........................  0

—More— or (q)uit

L3SW>
```

表 6-3:統計データの表示

6.1.5 ルート優先度の設定

複数のルーティングプロトコルが有効な場合、ルーティングプロトコル優先度に従って最適ルートを選択します。最適ルートに使用されるのは、優先値が低いルートです。

ルート優先度情報を表示する場合は、次のコマンドを実行します（次の表は、各プロトコルに対するデフォルト優先値を示しています）。

L3SW> show router route preference
L3SW> show router route preference

```
L3SW>show router route preferences

Local.............................  0
Static............................  1
OSPF Intra........................  110
OSPF Inter........................  112
OSPF Type-1.......................  115
OSPF Type-2.......................  118
RIP...............................  120
BGP4..............................  200

L3SW>
```

表 6-4：ルータのルート優先度の表示

ローカルルート優先度を変更する場合は、次のコマンドを実行します。

L3SW> config router route preference local <0-254>
L3SW> config router route preference local 250

スタティックルート優先度を変更する場合は、次のコマンドを実行します。

L3SW> config router route preference static <0-254>
L3SW> config router route preference static 100

RIP ルート優先度を変更する場合は、次のコマンドを実行します。

L3SW> config router rip preference <0-254>
L3SW> config router rip preference 10

OSPF ルート優先度を変更する場合は、次のコマンドを実行します。

L3SW> config router ospf preference <intra/inter/type1/type2> <0-254>
L3SW> config router ospf preference intra 90

6.1.6 ルータルートテーブル

ルーティングテーブルを表示する場合は、次のコマンドを実行します。

L3SW> show router route table
L3SW> show router route table

```
L3SW>show router route ta

Network      Subnet                 Next Hop Intf   Next Hop
Address       Mask         Protocol   Intf    Status IP Address
-----------  ------------ --------- -------  ------ ----------
10.0.0.0     255.0.0.0    Local     4.1      Down   10.0.0.1
172.30.10.0  255.255.255.0 Static   4.2      Down   192.168.10.0
192.168.10.0 255.255.255.0 Local    4.2      Down   192.168.10.1

Total Number of Routes.............  3

L3SW>
```

表 6-5：ルータルートテーブルの表示

最適ルートを表示する場合は、次のコマンドを実行します。

L3SW> show router route bestroutes
L3SW> show router route bestroutes

ルーティングテーブルの特定のエントリを表示する場合は、次のコマンドを実行します。

L3SW> show router route entry 172.30.10.0
L3SW> show router route entry 172.30.10.0

```
L3SW>show router route entry 172.30.10.0

Network      Subnet                    Next Hop Next Hop
Address       Mask         Protocol    Intf    IP Address    Metric
-----------  ------------- --------- -------  ----------    ------
172.30.10.0  255.255.255.0 Static    4.2      192.168.10.0  1

Total Number of Routes.............  1

L3SW>
```

表 6-6:ルータルートエントリの表示

6.2 VLAN 間ルーティング

IP プロトコルを使用した VLAN 間ルーティングについて説明します。VLAN 間ルーティングは 1 台のルータの異なるサブネット間でのルート指定に使用され、ルーティングプロトコルは必要ありません。

6.2.1 概要

VLAN は、ブロードキャストドメインの大きさを制御し、同一 VLAN 内に配置されたデバイスへのトラフィックを維持するために使用されます。異なる VLAN 内の端末同士の通信には、VLAN 間通信を使用します。VLAN 間通信は、VLAN 間ルーティングで実現します。ネットワーク管理者は、宛先の VLAN に対するトラフィックのルートを指定するためにルータを設定します。

本製品には、複数のファストイーサネットポートとギガビットイーサネットポートがあります。それぞれのポートは、ブリッジポートや L3 ルーティングポートとして機能するように、個別に設定することができます。本製品では、仮想ルーティングインタフェースを設定することができます。仮想ルーティングインタフェースは VLAN と関連付けられており、VLAN と仮想ルーティングインタフェースは 1 対 1 の関係になっています。本マニュアルでは、仮想ルーティングインタフェースを論理インタフェースや L3(ルータ)ポートと呼ぶこともあります。

各物理ポートは、あるブリッジグループに属すると同時に、複数の仮想ルーティングインタフェースに属することもできます。したがって、各ポートはレイヤ 2 スイッチングもレイヤ 3 スイッチングも行えるように設定できます。例えば、ポート 10 が VLAN2 と VLAN3 に属しており、ポート 20 が VLAN2 と VLAN4 に属しているとします。また、VLAN3 と VLAN4 に対して仮想ルーティングインタフェースが設定されているとします。この場合、タグ値 2 でポート 10 に入るすべてのタグ付きフレームは、フレーム中のレイヤ 2 情報によってポート 20 にスイッチングされます。また、タグ値 3 とポート 20 にアタッチされたホストの IP アドレスを持ってポート 10 に入るすべてのタグ付きフレームは、パケット内のレイヤ 3 情報とスイッチに格納された IP 転送テーブルによって、

VLAN3 と VLAN4 に振り分けられます。このようなスイッチの仮想インタフェース間でのルーティングを、VLAN 間ルーティングと呼んでいます。

本製品のレイヤ 3 設定は、VLAN ルーティングを設定していなければ動作しないことに注意してください。仮想ルーティングインタフェースには、次のような特徴があります。

- IP アドレスー仮想ルーティングインタフェースに割り当てられた IPv4 アドレス。仮想ルーティングインタフェースに関連付けられた物理ポートが割り当てられたサブネットワークに属する必要があります。
- サブネットマスクーIP アドレスと同じ構成と表示法を持つ 32 ビットの値。サブネットマスクは、IP アドレスのどのビットがネットワーク番号、サブネット番号、ホスト番号を表すかを決定します。サブネットマスクの 1 は、IP アドレスのネットワーク／サブネットワーク部分に対応します。また、0 は IP アドレスのホスト部分に対応します。
- 論理インタフェースーレイヤ 3 ポートは、すべて論理ポートとして扱われます（仮想ルータポートと呼ばれることもあります）。論理ポートは、仮想ルーティングインタフェースに関連付けられた VLAN と同じ VLAN 上にある 1 つまたは複数の物理ポートから構成される場合もあります。論理ポートは、スロット番号とポート番号の組み合わせで識別されます。本製品では、どのレイヤ 3 ポートに対しても固定スロット番号、つまり 4 番が与えられています例えば、最初に生成されたレイヤ 3 ポートの論理ポート ID には 4.1 が、2 番目のポートには 4.2 が割り当てられます。
- 指向性ブロードキャスト（Net-directed Broadcast）ー指向性ブロードキャストのトラフィック転送の可／不可は、各レイヤ 3 ポートで個別に設定できます。

6.2.2 IP 設定

VLAN 間ルーティング設定用コマンドについて説明します。

6.2.2.1 物理ポート上の IP インタフェースの設定

物理ポートで IP インタフェースを設定するには、2 つの方法があります。1 つは簡易 IP インタフェース生成と呼ばれます。もう 1 つは VLAN 関連 IP インタフェース生成と呼ばれます。どちらを選択してもかまいません。ただし、簡易 IP インタフェース生成のほうが使いやすいので、こちらを推奨しています。

注意物理ポートや LAG ポートを含めたポートの IP インタフェース、サービスポート IP アドレス、ネットワークポート IP アドレスは、同一サブネットワーク上に設定する必要があります。

6.2.2.1.1 簡易 IP インタフェース生成

IP インタフェース設定を簡単にするため、VLAN コンセプトと関連設定を表示しない、簡易コマンドが実行できます。

```
L3SW> config ip port create <physical slot.port> <ipaddr> <subnetmask> [vlanId]
L3SW> config ip port create 0.1 173.30.10.1 255.255.0.0
```

このコマンドが問題なく実行されると、[Creation of IP interface for <slot port> also resulted in creation of <logical slot port> logical interface]という表示によって、VLAN と関連付けられた新たな論理インタフェースが生成されたことが示されます。VLAN ID が特定できない場合は、4094 から降順で ID が割り当てられます。

複数のポートでの同一 IP アドレス使用は、config ip port create コマンドによって禁止されています。同一の IP アドレスが複数のポートに共有されている場合は、詳しい設定について「6.2.2.3 既存のルーティングインタフェースへのポート追加と削除」(P.108)を参照してください。生成された IP アドレスを変更する場合は、「6.2.2.4 IP アドレスとルーティングインタフェースに対応するサブネットマスクの変更」(P.108)を参照してください。

6.2.2.1.2 VLAN に関連付けられた IP インタフェースの生成

この方法では、まず VLAN を生成してから VLAN と物理ポートを関連付け、さらに VLAN に関連付ける IP アドレスを生成します。設定は、次の順序で行います。

ステップ 1:VLANを作成します。

```
L3SW> config vlan create <2-4094>
L3SW> config vlan create 2
```

ステップ 2:VLANと物理ポートを関連付けます。

ポートがポートベース VLAN をサポートしている場合、次のコマンドを実行すると、ポートとプライマリ VLAN を関連付けられます。

```
L3SW> config vlan port add <2-4094> <slot.port>
L3SW> config vlan port add 2 0.1
```

複数の VLAN をポートがサポートしている場合、次のコマンドを実行すると、ポートとプライマリ VLAN 以外の VLAN を関連付けられます。

```
L3SW> config vlan participation include <1-4094> <slot.port>
L3SW> config vlan participation include 2 0.1
```

ステップ 3:VLANとIPインタフェースアドレスを関連付けます。

```
L3SW> config ip vlan create <vlanId> <ipaddr> <subnetmask>
L3SW> config ip vlan create 2 192.168.10.1 255.255.255.0
```

config ip vlan create コマンドは、デフォルト以外の VLAN にしか適用できません。デフォルト VLAN に対するこのコマンドによる IP インタフェース生成は、CLI によって拒否されます。

config ip vlan create コマンドが問題なく実行されると、[Creation of IP interface for VLAN <ID> also resulted in creation of <logical slot prt> logical interface]という表示によって、VLAN と関連付けられた新たな論理インタフェースが生成されたことが示されます。

複数の VLAN による IP インタフェース共有は、禁止されています。生成された IP アドレスを変更する場合は、6.2.2.4 節を参照してください。

6.2.2.2 LAG ポート上の IP インタフェースの設定

物理ポートの IP インタフェース設定と同様に、LAG ポートの IP インタフェース設定にも簡易 IP インタフェース生成と VLAN 関連 IP インタフェース生成の 2 つの方法があります。 簡易 IP インタフェース生成コマンドのほうが使いやすいので、通常はこちらを推奨します。LAG ポート上の VLAN 関連 IP インタフェース設定の詳細に関しては、6.2.2.1.2 節を参照してください。

LAG ポートの簡易 IP インタフェース設定には、LAG を生成してから次のコマンドを実行します。

```
L3SW> config ip lag create <lagName> <ipaddr> <subnetmask>
L3SW> config ip lag create red 173.30.10.1 255.255.0.0
```

コマンドが問題なく実行されると、次の表示によって新たに生成された論理インタフェースが示されます。

```
Creation of IP interface for LAG <LAG name> also resulted in creation of
<logical slot.port> logical interface
```

新しい論理インタフェースが生成されたことを示します。

複数のポートによる同一 IP アドレスの使用は、config ip port create コマンドによって禁じられています。同一の IP アドレスが複数のポートに共有されている場合は、詳しい設定については「6.2.2.3 既存のルーティングインタフェースへのポート追加と削除」(P.108)を参照してください。生成された IP アドレスを変更する場合は、「6.2.2.4 IP アドレスとルーティングインタフェースに対応するサブネットマスクの変更」(P.108)を参照してください。

6.2.2.3 既存のルーティングインタフェースへのポート追加と削除

IP インタフェースアドレスの生成が終わると、既存のルーティングインタフェースへのポートの追加や削除が可能になります。関連するコマンドは次のとおりです。config ip port コマンドでは、IP インタフェースに物理ポートだけを追加／削除します。config vlan port コマンドは、物理ポートと LAG ポートのどちらも追加／削除できます。

```
L3SW> config ip port add <physical slot.port> <logical slot.port>
L3SW> config ip port add 0.2 4.1

L3SW> config ip port remove <physical slot.port> <logical slot.port>
L3SW> config ip port remove 0.2 4.1

L3SW> config vlan port add <2-4094> < slot.port>
L3SW> config vlan port add 2 0.10

L3SW> config vlan port remove <2-4094> <slot.port>
L3SW> config vlan port remove 2 0.10
```

例えば、config ip port remove 0.1 4.1 コマンドによって IP インタフェースから最後の物理ポートを削除してしまうと、その後 show ip port コマンドを実行してもポート 0.1 やその他の IP ポートに関連付けられた IP インタフェースの存在は表示されません(0.1 は IP インタフェースに関連付けられた最後の物理ポートです)。この場合に IP インタフェース 4.1 に関する詳細情報を表示するには、config ip interface 4.1 コマンドを実行するのが唯一の方法です。

6.2.2.4 IP アドレスとルーティングインタフェースに対応するサブネットマスクの変更

IP インタフェースのアドレス生成が終了すると、次のコマンドによって既存のインタフェースの IP

アドレスやサブネットマスクを変更することができます。

```
L3SW> config ip interface networkid <logical slot.port> <ipaddr> <subnetmask>
L3SW> config ip interface networkid 4.1 10.1.1.1 255.255.255.0
```

既存の IP インタフェースを削除するには、次のコマンドを実行します。

```
L3SW> config ip interface delete <logical slot.port>
L3SW> config ip interface delete 4.1
```

6.2.3 IP インタフェース情報

VLAN、PVID、仮想スロットポート、IP アドレスなどのポート関連要約情報を表示する場合は、次のコマンドを実行します。

```
L3SW> show ip port
L3SW> show ip port
```

```
L3SW>show ip port

Physical  Type   LAG Name  PVID  Virtual   IP Address    Subnet Mask
Slot.Port                      Slot.Port
0.1                        2     4.1       173.30.10.1   255.255.0.0
0.2                        4094  4.2       192.168.10.1  255.255.255.0
0.3                        1
0.4                        1
0.5                        1
0.6                        1
0.7                        1
0.8                        1
0.9                        1
0.10                       1
0.11                       1
0.12                       1
0.13                       1
0.14                       1
0.15                       1
0.16                       1
0.17                       1
0.18                       1
0.19                       1
--More—or (q)uit
0.20                       1
0.21                       1
0.22                       1
0.23                       1
0.24                       1
1.1                        1
1.2                        1
1.3                        1
1.4                        1

L3SW>
```

表 6-7:IP ポートの表示

ルーティングインタフェースに関連した特定の論理ポート情報を表示する場合は、次のコマンドを実行します。

L3SW> show ip interface <slot.port>
L3SW> show ip interface 4.1

```
L3SW>show ip interface 4.1

IP Address..................................... 172.30.10.1
Subnet Mask.................................... 255. 255. 255. 0
Routing Mode................................... Enable
Administrative Mode............................ Enable
Forward Wet Directed Broadcasts................ Disable
Active State................................... Inactive
Link Speed Data Rate........................... 1000
MAC Address
.............................................. 00:50:A8:00:35:1
A
Maximum Transmission Unit...................... 1500
Encapsulation Type............................. Ethernet

L3SW>
```

表 6-8:仮想インタフェース設定の表示

デフォルトでは、指向性ブロードキャストの転送は無効になっています。転送を有効または無効にするには、次のコマンドを実行します。

L3SW> config ip interface netdirbcast <slot.port> <enable/disable>
L3SW> config ip interface netdirbcast 4.1 enable

6.2.4 VLAN 間ルーティングの例

VLAN 間ルーティングの設定に必要な一連のコマンドについて、図で説明します。図 6-1 に示したネットワークは、192.122.10.0/24 と 192.122.11.0/24、192.122.12.0/24 の 3 つの IP サブネットで構成されています。

サブネット間のトラフィックは、本製品でルートを指定されます。各サブネットにはポートが 2 つあり、ポート 1 と 2 はサブネット 192.122.10.0/24 に、ポート 15 と 16 はサブネット 192.122.11.0/24 に、ポート 10 と 11 はサブネット 192.122.12.0/24 に属しています。

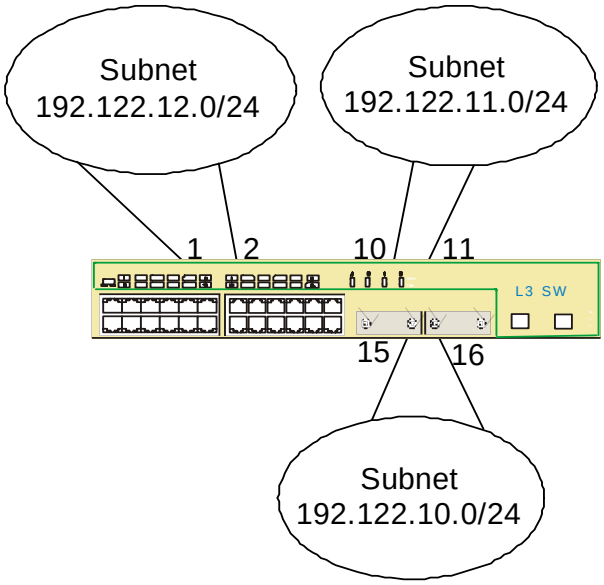

図 6-1：VLAN 間ルーティング

図の場合の設定コマンドは、次のようになります。

```
L3SW> config routing enable
L3SW> config ip port create 0.1 192.122.12.0 255.255.255.0
L3SW> config ip port create 0.15 192.122.10.0 255.255.255.0
L3SW> config ip port create 0.10 192.122.11.0 255.255.255.0
L3SW> config ip port add 0.2 4.1
L3SW> config ip port add 0.16 4.2
L3SW> config ip port add 0.11 4.3
```

6.3 スタティックルーティング

ネットワーク管理者によって、スタティックルーティングエントリを生成することができます。スタティックエントリは、削除されるまでルーティングテーブルに格納されます。

スタティックルートを設定する場合、最初に IP インタフェースを設定します。

特定の宛先 IP アドレスに宛てたスタティックルートを生成する場合は、次のコマンドを実行します。

```
L3SW> config router route create <ipaddr> <subnetmask> <nexthopip> [metric]
L3SW> config router route create 10.0.0.0 255.0.0.0 192.168.10.10
```

スタティックルートを削除する場合は、次のコマンドを実行します。

```
L3SW> config router route delete <ipaddr> <subnetmask> <nexthopip>
L3SW> config router route delete 10.0.0.0 255.0.0.0 192.168.10.10
```

どのルーティングエントリとも一致しない宛先 IP アドレス用にスタティックルートを設定する場合は、デフォルトルーティング設定を使用します。デフォルトのスタティックルートは、1 つのルータに 1 つしか存在できません。通常、デフォルトルートでは、インターネットに接続しているルータ

（または、そのサブネット内にあるルータ）が指定されます。

デフォルトルートを生成する場合は、次のコマンドを実行します。

```
L3SW> config router route default create <nexthopip>
L3SW> config router route default create 192.10.10
```

パケットの宛先アドレスに一致するエントリ（最大プレフィックスマッチング）がルーティングテーブルに見つからない場合、ルーティングテーブルへのデフォルトルートエントリの他に、パケットを転送するネクストホップ IP アドレスとして 192.168.10.10 を使用することもあります。

デフォルトルートを削除する場合は、次のコマンドを実行します。

```
L3SW> config router route default delete
L3SW> config router route default delete
```

パフォーマンスとセキュリティ上の理由から、本製品では[ICMP: Unreachable network]メッセージを送信しません。ただし、本製品に直接接続しているサブネットから到達できないホストがある場合は、[ICMP: unreachable host]のメッセージを送信します。

6.4 ルーティング情報プロトコル（RIP）

RIP は、管理ドメイン内での使用を目的に設計された距離ベクトルプロトコル（distance vector protocol）です。ルータで動作する RIP は、隣接ルータや、隣接ルータを通じて学習したルータとルート情報を交換します。隣接ルータからルーティング情報を受け取ると、それまでに受け取っていた情報に基づいたルーティングテーブルを更新します。この更新は、次のような単純な規則によって行われます。例えば、ルータ R が隣接ルータ S からルーティング情報を受け取ったとします。ルータ S を経由した宛先 Q までのホップ数が、ルーティングテーブル内の当該宛先に関するネクストホップエントリより小さければ、ルーティングテーブルのエントリは宛先 Q に関するネクストホップルータにルータ S を指定するよう変更されます。また、宛先 Q までのホップ数は新しい値に変更されます。ホップ値の範囲は、1 から 16 までです。宛先までのホップ数が 16 を超える場合は、当該宛先に対するホップ値は最大値 16 にリセットされます。このホップ数値は、距離メトリックと呼ばれることもあります。

RIP 設定は、次の 5 つの手順で行います。

ステップ 1：ルーティングモードを有効にします。

詳しい設定については、「6.1.2 ルーティングモードの設定」（P.101）を参照

ステップ 2：ルータIDを定義します。

詳しい設定については、「6.1.3 ルータ ID の設定」（P.101）を参照

ステップ 3：RIPポートに対するIPインタフェースを設定します。

詳しい設定については、「6.2.2.1 物理ポート上の IP インタフェースの設定」（P.106）を参照

ステップ 4：ルータでRIPを有効にします。

ステップ 5:インタフェースでRIPを設定します。

6.4.1 ルータ上での RIP 設定

デフォルトでは、RIP はルータで動作しません。RIP 有効または無効にするには、次のコマンドを実行します。

```
L3SW> config router rip adminmode <enable/disable>
L3SW> config router rip adminmode enable
```

ルータに関する RIP 情報を表示する場合は、次のコマンドを実行します。

```
L3SW> show router rip info
```

```
L3SW>show router rip info
Router ID   .........................10.1.1.1
RIP Admin Mode.......................Enable
Global route changes.................0
Global queries ......................0
Route redistribution,................
Connected    ........................Disable
Static       ........................Disable
OSPF.................................
Internal.      ......................Disable
External type 1......................Disable
External Type 2......................Disable
Redistribution default metric.........1
Connected      ......................1
Static         ......................1
OSPF.................................
Internal.     .......................1
External type 1......................1
External type 2..................1
  L3SW>
```

表 6-9:ルータ RIP 情報の表示

6.4.2 インタフェースでの RIP 設定

RIP プロトコルは物理ポートでも LAG ポートでも機能します。RIP インタフェース設定に関するすべてのコマンドでは、論理ポート番号や仮想ポート番号を使用します。インタフェースでのベーシックな RIP 設定では、インタフェース上で RIP モードを有効にするだけで十分です。拡張 RIP 設定を行う場合は、RIP インタフェース認証、デフォルトメトリック、RIP バージョンを設定します。

6.4.2.1 RIP インタフェースモードの設定

デフォルトでは、RIP はインタフェースで動作しません。RIP を有効または無効にするには、次のコマンドを実行します。

```
L3SW> config router rip interface mode <slot.port> <enable/disable>
L3SW> config router rip interface mode 4.1 enable
```

インタフェースに関する RIP 情報を表示する場合は、次のコマンドを実行します。

L3SW> show router rip interface summary

```
L3SW>show router rip interface summary

                          Send     Receive   RIP    Link
Slot.Port IP Address      Version  Version   Mode   State
--------- --------------- ------- --------  ------ -----
4.1       192.168.10.1    RIP-2    Both     Enable   Up
4.2       10.0.0.1        RIP-2    Both     Enable   Up

L3SW>
```

表 6-10：ルータ RIP インタフェースサマリの表示

特定のインタフェースに関する RIP 情報を表示する場合は、次のコマンドを実行します。

L3SW> show router rip interface detailed 4.1
L3SW> show router rip interface detailed 4.1

```
L3SW>show router rip interface detailed 4,1

Interface.................................  11
IP Address................................  192.168.10.1
Send version..............................  RIP-2
Receive version...........................  Both
RIP Admn Mode.............................  Enable
Link State................................  Down
Authentication Type.......................  None
Authentication Key........................
Default Metric............................  0
Bad Packets Received......................
Bad Routes Received.......................
Updates Sent..............................

L3SW>
```

表 6-11：インタフェース 4.1 に関するルータインタフェース詳細の表示

6.4.2.2 RIP インタフェース認証の設定

RIP メッセージは、ネットワークに対する偽ルーティング情報の流入やルータが交換するルーティング情報の改ざんを防ぐため、パスワード認証によって保護できます。ネットワーク管理者は近隣の RIP ルータ間での簡易パスワードを定義して、簡易パスワード認証を使う RIP を設定することができます。パスワードを設定するには、次のコマンドを実行します。

L3SW> config router rip interface authtypekey <slot.port> <none/simple> [key]
L3SW> config router rip interface authtypekey 4.1 simple password

6.4.2.3 RIP インタフェースのデフォルトメトリック

デフォルトルートエントリに関連した距離メトリックを設定する場合は、次のコマンドを実行します。

L3SW> config router rip interface defaultmetric <slot.port> <0-15>
L3SW> config router rip interface defaultmetric 4.1 2

デフォルトメトリック値 0 では、隣接ルータに RIP 更新を送る場合、デフォルトルートは 1 本しか存在しません。RIP がインタフェースで動作可能な場合、当該インタフェースのデフォルトメトリック値は 0 に設定されます。

6.4.2.4 RIP インタフェースのバージョン

RIP プロトコルには、バージョン 1 とバージョン 2 の 2 種類のバージョンがあります。本製品は、受信トラフィックでも送信トラフィックでも両方のバージョンに対応します。

ポートで RIP バージョンを設定する場合は、次のコマンドを実行します。

```
L3SW> config router rip interface version receive <slot.port> <rip1/rip2/both/none>
L3SW> config router rip interface version receive 4.1 both

L3SW> config router rip interface version send <slot.port> <rip1/rip1c/rip2/none>
L3SW> config router rip interface version send 4.1 rip2
```

このコマンドで同一のポートに対し「送信」と「受信」とで別々のバージョンの RIP プロトコルを指定することは可能ですが、同じバージョンのプロトコルを指定するように警告を受けます。

RIP における CIDR はつねに有効です。

6.4.3 RIP の例

図 6-2 では、L3SW-1 と L3SW-2 スイッチが RIP プロトコルで設定されています。図の設定では、すべてのサーバとワークステーションがネットワーク上で互いに通信可能です。

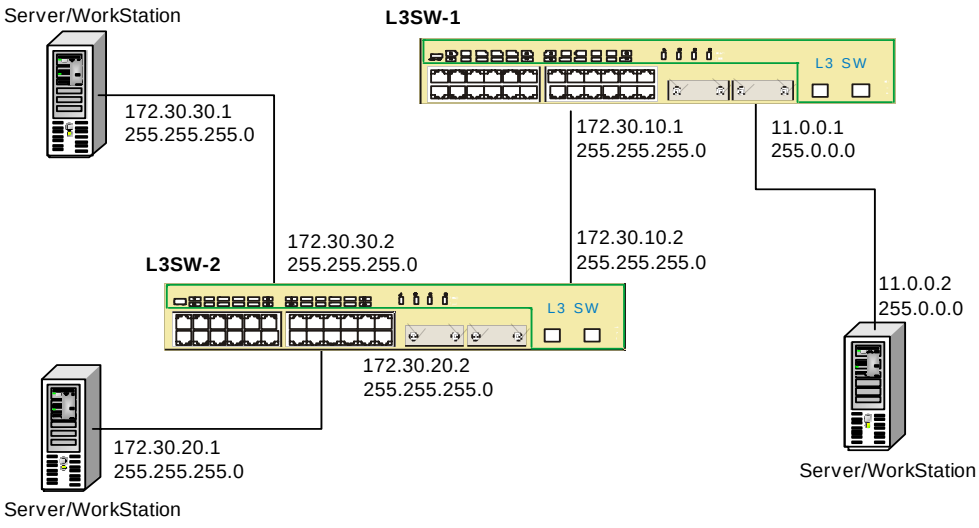

図 6-2：RIP の設定

本製品のスイッチ設定では、次のコマンドを実行します。

```
L3SW> config routing enable
L3SW> config router id 11.0.0.1
L3SW> config ip port create 0.4 172.30.10.1 255.255.255.0
L3SW> config ip port create 0.10 11.0.0.1 255.255.255.0
```

```
L3SW> config router rip adminmode enable
L3SW> config router rip interface mode 4.1 enable
```

本製品のスイッチ設定では、次のコマンドを実行します。

```
L3SW> config routing enable
L3SW> config router id 20.0.0.1
L3SW> config ip port create 0.1 172.30.30.2 255.255.255.0
L3SW> config ip port create 0.3 172.30.20.2 255.255.255.0
L3SW> config ip port create 1.1 172.30.10.2 255.255.255.0
L3SW> config router rip adminmode enable
L3SW> config router rip interface mode 4.3 enable
```

6.5 Open Short Path First (OSPF)

6.5.1 OSPF エリア

OSPF は、リンク状態ルーティングプロトコルの 1 つです。リンク状態データベースはネットワークトポロジ情報を収集したものです。リンクの隣接ルータ、リンクのコストメトリック、さらに最も重要な情報であるリンクのアップ／ダウンを示すリンク状態情報を格納します。OSPF などのリンク状態プロトコルは、各ルータに対してリンク状態データベースの生成と管理を可能にします。リンク状態データベースは、ネットワーク内のルータがアドバタイズしたリンク状態情報を元にルータにより生成されます。各ルータはリンクデータベース内の情報を利用して、管理ドメイン内外のすべての既知サブネットワークまでの最短パスを算出します。未知の宛先あてのパケットは、デフォルトルートを使用して転送します。

OSPF には距離ベクトルルーティングプロトコルにはない様々な機能があり、それらの機能により、大規模ネットワーク環境で幅広く利用されるルーティングプロトコルになっています。現在のバージョンは OSPFv2 で、RFC2328 で定義されています。

OSPF によって、自律システム（AS）は複数のエリアに分割されます。各エリアは 32 ビット ID で識別され、ネットワークセグメントとルータの集まりで構成されています。複数のエリアと接続しているルータは、エリア境界ルータ（ABR）と呼ばれます。エリアからエリアに宛てたパケットは、ABR を経由して送られます。外部リンク（外部 OSPF ルーティングドメインへのリンクのこと）を有する ABR は、自律システム境界ルータ（ASBR）と呼ばれます。

各 OSPF ルータは、ネットワークの他のルータからリンク状態アドバタイズ（LSA）を収集し作成した独自のリンク状態データベースを管理しています。エリアトポロジは互いに隠されており、各エリアは、サマリ LSA によって IP ルーティング情報を配送する ABR を介して相互に接続します。OSPF によるエリア定義は、次の 3 種類です。

- バックボーンエリア：すべての OSPF ネットワークには、少なくとも 1 つのエリアが含まれています。これが、バックボーンエリアです。バックボーンエリアは ID 0.0.0.0 として定義され、他のエリアと物理的に接続しています。すべてのエリアはバックボーンエリアに直接ルーティング情報を送り、バックボーンエリアから他のエリアのルーティング情報を受け取ります。すべての OSPF インタフェースがバックボーンエリアと関連しているルータは、イントラバックボーンルータであるとみなされます。バックボーンエリア関連インタフェースと非バックボーンエリア関連インタフェースを有するルータは、ABR であるとみなされます。本製品は、バックボーンルータとしても ABR としても、また両方を兼ねるようにも設定でき

ます。ネットワーク管理者は CLI コマンド show router ospf info を実行して、ルータが OSPF ABR であるかどうかを確認することができます。

- 非バックボーンエリア：0.0.0.0 以外のエリア ID を持つルーティングエリアを非バックボーンエリアといいます。通常、非バックボーンエリアは、バックボーンエリアに直接接続しています。非バックボーンエリアがバックボーンエリアと直接接続していない場合は、非バックボーンエリアの ABR と、バックボーンエリアと直接接続している別の非バックボーンエリアの ABR との間に仮想リンクを設定する必要があります。
- スタブエリア：　外部ルートは ASBR によって、ルーティングドメイン内のすべてのエリアに送信されます。ASBR によって公開された外部ルートは、エリア内のルータが管理しているルーティングテーブルで信頼されます。あるエリアのルーティングテーブルからすべての外部ルートを削除し、その代わりに単純にデフォルトエントリを挿入したい場合があります。こうした場合、ASBR から当該エリアに対して外部 LSA がフラッディングされないようにエリアの ABR を設定します。外部 LSA が ABR によって消去されたエリアは、スタブエリアと呼ばれます。

スタブエリア内ルータのリンク状態データベースには外部 LSA が存在しないため、スタブエリアの ABR は AS 外部の宛先に対してデフォルトルートを生成します。スタブエリアで管理される LSA は、イントラエリア LSA とエリア間 LSA だけです。スタブエリアは、外部 LSA だけでなくエリア間 LSA も排除するように設定することもできます。その場合、エリア間のパスには、同一のデフォルトルートを使用することができます。本製品では、一連の CLI コマンドによってデフォルトルートに対するメトリック値を設定し、スタブエリアを設定します。

6.5.2　OSPF の設定

OSPF の設定ベーシックな OSPF の設定は、次の 5 つの手順で行います。

ステップ 1：ルーティングモードを有効にします。

詳しい設定については、「6.1.2　ルーティングモードの設定」（P.101）を参照

ステップ 2：ルータIDを定義します。

詳しい設定については、「6.1.3　ルータ ID の設定」（P.101）を参照

ステップ 3：OSPFポートに対するIPインタフェースを設定します。

詳しい設定については、「6.2.2.1　物理ポート上の IP インタフェースの設定」（P.106）を参照

ステップ 4：ルータでのOSPFを有効にします。

ステップ 5：インタフェースでのOSPFの有効化とエリアIDを割り当てます。

本製品では、認証キーやメトリックコスト、RFC1583 互換性モードなどの追加パラメータ設定が可能です。OSPF に関連したこれらの追加パラメータ設定は、次のように行います。

ステップ 6：追加OSPFスイッチレベルパラメータを設定します。

ステップ 7：インタフェースに対する追加OSPFパラメータを設定します。

6.5.2.1 ルータでの OSPF の有効化

OSPF プロトコルは物理ポートでも LAG ポートでも機能します。OSPF インタフェース設定に関するすべてのコマンドでは、論理ポート番号や仮想ポート番号を使用します。

デフォルトでは、OSPF はルータで動作しません。OSPF を有効または無効にするには、次のコマンドを実行します。

```
L3SW> config router ospf adminmode <enable/disable>
L3SW> config router ospf adminmode enable
```

ルータに関する OSPF 情報を表示する場合は、次のコマンドを実行します。

```
L3SW> show router ospf info
```

```
L3SW>show router ospf info
Router ID....,.................................. 10,1.1.1
SPF Admin Mode.................................. Enable
RFC 1583 Compatibility.......................... Enable
ASBR Mode....................................... Disable
ABR Status...................................... Enable
Exit Overflow Interval.......................... 0
External LSA Count.............................. 0
External LSA Checksum........................... 0
New LSAs Originated............................. 0
LSAs Received................................... 0
External LSDB Limit ............................ No Limit
Route redistribution............................
      Connected.................................Disable
      Static ..................................... Disable
      RIP ........................................ Disable
Redistribution default metric................... 10,exttypel
Connected.....................................   10,exttypel
Static.......................................   10,exttypel
RIP ............................................ 10,exttypel
Default route redistribution.................... Disable
Default route redistribution metric............. 10,exttypel
L3SW>
```

表 6-12：OSPF 情報の表示

6.5.2.2 インタフェースでの OSPF の有効化

デフォルトでは、OSPF はインタフェースで動作しません。OSPF を有効または無効にするには、次のコマンドを実行します。

```
L3SW> config router ospf interface mode <slot.port> <enable/disable>
L3SW> config router ospf interface mode 4.1 enable
```

OSPF インタフェース情報を表示する場合は、次のコマンドを実行します。

L3SW> show router ospf interface info <slot.port>
L3SW> show router ospf interface info 4.4

```
L3SW>show router ospf interface info 4.4
IP Address ..................................... 192.168.1.1
Subnet Mask. ................................... 255. 255. 255. 0
OSPF Admin Mode ................................ Enable
OSPF Area ID ................................... 0. 0. 0.10
Router Priority.................................1
Retransmit Interval............................. 5
Hello Interval..................................  10
Dead Interval...................................  40
LSA Ack Interval................................1
Iftransit Delay Interval.......................  1
Authentication Type.............................  Wone
Metric Cost ....................................1
OSPF Interface Type.............................  broadcast
State...........................................  down
Designated Router ..............................0. 0. 0. 0
Backup Designated Router........................  0. 0. 0. 0
Number of Link Events...........................  0
L3SW>
```

表 6-13：OSPF インタフェース情報の表示

OSPF インタフェース統計データを表示する場合は、次のコマンドを実行します。

L3SW> show router ospf interface stats <slot.port>
L3SW> show router ospf interface stats 4.4

```
L3SW>show router ospf interface stats 4.4

OSPF AREA ID ..................  0.0.0.10
Spf Runs ......................  0
Area Border Router Count ......  0
AS Border Router Count ........  0
Area LSA Count ................  0
IP Address ....................  192.168.1.1
OSPF Interface Events .........  0
Victual Events ................  0
Neighbor Events ...............  0
External LSA Count ............  0
LSAs Received .................  0
Originated New LSAs ...........  0

L3SW>
```

表 6-14：OSPF インタフェース統計データの表示

6.5.2.3　　6.5.1.3　OSPF インタフェースエリア ID 設定

OSPF インタフェースは、エリア ID を割り当てて OSPF エリアにアタッチする必要があります。デフォルトでは、OSPF インタフェースはエリア ID 0.0.0.0 のバックボーンエリアにアタッチされています。OSPF インタフェースにバックボーンエリア以外のエリア ID を割り当てる場合は、次のコマンドを実行します。

L3SW> config router ospf interface areaid <slot.port> <areaid>
L3SW> config router ospf interface areaid 4.4 0.0.0.10

6.5.2.4 OSPF インタフェース認証の設定

OSPF メッセージは、ネットワークに対する偽ルーティング情報の流入やルータが交換するルーティング情報の改ざんを防ぐため、パスワード認証によって保護できます。ネットワーク管理者は、近隣の OSPF ルータ間における簡易パスワードを定義して、OSPF 認証を設定することができます。

OSPF インタフェース認証のタイプとキーを設定する場合は、次のコマンドを実行します。

```
L3SW> config router ospf interface authtypekey <slot.port> <none/simple > [key]
L3SW> config router ospf interface authtypekey 4.1 simple abcd
```

6.5.2.5 OSPF インタフェースのメトリックコスト設定

OSPF では、コストメトリックを使用して宛先までの最短パスを算出します。したがって、各ポートには、0～65535 の範囲でコストメトリックを割り当てる必要があります。コストメトリックの最小値は 0 で、アタッチされているネットワーク用に予約されています。

OSPF インタフェースメトリックを設定する場合は、次のコマンドを実行します。

```
L3SW> config router ospf interface cost <ipaddr> <slot.port> <1-65535>
L3SW> config router ospf interface cost 10.1.1.1 4.1 20
```

6.5.2.6 6.5.1.6 OSPF インタフェース優先度の設定

LAN セグメントに複数のルータが存在している場合は、指定ルータ(DR)とバックアップ指定ルータ(BDR)を決めます。DR は LAN セグメント内の他のルータから LSA を収集し、収集した LSA をセグメント内で他のルータのためにアドバタイズします。BDR は、既存の DR が到達不能になった場合や機能を停止している場合に DR に昇格します。DR と BDR の選出は、LAN セグメント内のルータが互いにアドバタイズしあう優先値に基づいて行われます。DR には優先度が最も高いルータが選出され、BDR には 2 番目に高いルータが選出されます。

OSPF インタフェース優先度を表示する場合は、次のコマンドを実行します。

```
L3SW> config router ospf interface priority <slot.port> <0-255>
L3SW> config router ospf interface priority 4.1 200
```

ルータに対する優先値 0 の割当は、当該ルータが DR にも BDR にもなれないことを示します。

6.5.2.7 OSPF インタフェースのトランジット遅延設定

特定のポートに対して OSPF トランジット遅延を設定する場合は、次のコマンドを実行します。

```
L3SW> config router ospf interface iftransitdelay <slot.port> <1-3600>
L3SW> config router ospf interface iftransitdelay 4.1 100
```

6.5.2.8 OSPF インタフェースインターバルの設定

特定のポートに対して OSPF デッドインターバルを設定する場合は、次のコマンドを実行します。

```
L3SW> config router ospf interface interval dead <slot.port> <1-2147483647>
L3SW> config router ospf interface interval dead 4.1 10
```

特定のポートに対して OSPF ハローインターバルを設定する場合は、次のコマンドを実行します。

```
L3SW> config router ospf interface interval dead <slot.port> <1-2147483647>
L3SW> config router ospf interface interval dead 4.1 10
```

特定のポートに対して OSPF 再送インターバルを設定する場合は、次のコマンドを実行します。

```
L3SW> config router ospf interface interval retransmit <slot.port> <0-3600>
L3SW> config router ospf interface interval retransmit 4.1 10
```

6.5.2.9 OSPF エリアの設定

OSPF ドメイン内の ABR は、エリア内のサブネットへのルートを集約し、各サブネットに個々のルートのかわりに 1 つのサマリをアドバタイズします。次に例をあげます。この例では、サブネットアドレスとサブネットマスクを持つ 32 のサブネットが存在しています。

- subnet 1: 128.1.64.0 255.255.255.0
- subnet 2: 128.1.65.0 255.255.255.0
- ……..
- ……
- subnet 32: 128.1.95.0 255.255.255.0

例の 32 のサブネットまでのルートはすべて、128.1.64.0 255.255.224.0 の 1 本のルートに集約して、ABR から他のエリアにサマリルートとしてアドバタイズできます。例のサマリルートを生成する場合は、次のコマンドを実行します。

```
L3SW> config router ospf area range create <areaid> <ipaddr> <subnetmask> [summ] <enable/disable>]
L3SW> config router ospf area range create 0.0.0.10 128.1.64.1 255.255.224.0
summ enable
```

例のコマンドでは、エリア 0.0.0.10 内の 128.1.64.0 から 128.1.95.0 までのサブネットに関連するルートを 1 本のサマリルータに集約できます。

パラメータ[summ]はオプションです。サマリルータは自動的に有効化されるので、enable オプションを明確に入力する必要はありません。ただし、サマリルータを動作不可にする場合は、複合パラメータ[summ disable]を入力します。

既存のサマリルートを削除するには、次のコマンドを実行します。

```
L3SW> config router ospf area range delete <areaid> <ipaddr> <subnetmask> [summ]
L3SW> config router ospf area range delete 0.0.0.10 128.1.64.1 255.255.224.0
```

あるエリアに不要なルートが送信されるのを防ぐには、エリアをスタブエリアとして設定します。通常、スタブエリアは外部ルートだけが送信されないように設定されます。しかし、「完全スタブエリア」の場合にはエリア間ルート（サマリ LSA）も送信できないように設定されています。スタブエリアの設定に関しては多くの制限があります。ネットワーク管理者はスタブエリアを設定する場合、それらの制限に注意する必要があります。この制限には、次のようなものがあります。

1. 通常、スタブエリアには出入口が一つしかありません。言い換えると、スタブエリアには ABR が 1 つしか存在しないということです。この ABR がエリア内の他のルータにデフォルトルートをアドバタイズします。ただし、スタブエリアに複数の ABR が存在している場

合は、各 ABR がデフォルトルートをアドバタイズします。スタブエリア内のルータによって選択された未知の宛先までのルートは、つねに最適なパスであるとは限りません。

2. スタブエリアは、仮想リンクのための転送エリアとして機能することはできません。
3. スタブエリアには外部ルートが許可されていないので、ASBR は存在できません。

あるエリアを「完全スタブエリア」として設定する場合、エリア間サマリ LSA が侵入できないようにする必要があります。

OSPF スタブエリアを生成する場合は、次のコマンドを実行します。

```
L3SW> config router ospf area stub create <areaid>
L3SW> config router ospf area stub create 0.0.0.10
```

OSPF スタブエリアを削除する場合は、次のコマンドを実行します。

```
L3SW> config router ospf area stub delete <areaid>
L3SW> config router ospf area stub delete 0.0.0.10
```

完全スタブエリアを設定する場合は、次のコマンドを実行します。

```
L3SW> config router ospf area stub summarylsa <areaid> <enable/disable>
L3SW> config router ospf area stub summarylsa 0.0.0.10 disable
```

スタブエリアが設定されると、ルータはデフォルトルートを生成してスタブエリア内のすべてのルータにアドバタイズします。メトリックタイプとメトリック値を設定する場合は、次のコマンドを実行します。

```
L3SW> config router ospf area stub metric type cost <areaid> <stub/comparable/noncomparable>
L3SW> config router ospf area stub metric type cost 0.0.0.10 comparable

L3SW> config router ospf area stub metric type monetary <areaid> <stub/comparable/noncomparable>
L3SW> config router ospf area stub metric type monetary 0.0.0.10 comparable
```

monetary types stub/comparable/noncomparable が意味しているのは、デフォルトルートに関するコストは内部 OSPF メトリックと外部タイプ 1 コストメトリック、外部タイプ 2 コストメトリックで定まるということです。これに関しては、ospfStubMetricType に関する RFC1850 で定義されています。

デフォルトルートに対してメトリック値を設定する場合は、次のコマンドを実行します。

```
L3SW> config router ospf area stub metric default monetary <areaid> <1-16777215>
L3SW> config router ospf area stub metric default monetary 0.0.0.10 225
```

6.5.2.10 OSPF ASBR モードの設定

本製品は、AS 外部ルーティングエントリ処理を有効／無効にするために、ASBR として設定することも非 ASBR として設定することもできます。この機能は、OSPF が外部ドメインについて学習するのに役立ちます。ASBR の有効／無効を設定する場合は、次のコマンドを実行します。

```
L3SW> config router ospf asbr <enable/disable>
L3SW> config router ospf asbr enable
```

6.5.2.11 OSPF 出口オーバフローインターバルの設定

OSPF 出口オーバフローインターバルを設定する場合は、次のコマンドを実行します。

```
L3SW> config router ospf exoverflowinterval <0-2147483647>
L3SW> config router ospf exoverflowinterval 10
```

6.5.2.12　OSPF RFC1583 互換モードの設定

OSPF RFC 1583 互換モードを設定する場合は、次のコマンドを実行します。

```
L3SW> config router ospf rfc1583compat <enable/disable>
L3SW> config router ospf exoverflowinterval 10
```

6.5.2.13　6.5.1.13 OSPF 外部 LSDB リミットの設定

OSPF 外部 LSDB リミットを設定する場合は、次のコマンドを実行します。

```
L3SW> config router ospf extlsdblimit <-1-2147483647>
L3SW> config router ospf extlsdblimit 10
```

6.5.2.14　OSPF 仮想リンクの設定

OSPF プロトコルでは、各エリアがバックボーンエリア、すなわち ID 0.0.0.0 エリアに直接接している必要があります。言い換えると、各エリア内の ABR のうち 1 台は、エリア ID 0.0.0.とのインタフェースを有する必要があります。しかし、ネットワーク構成によっては、エリア内の ABR がバックボーンエリアと直接接することできないこともあります。その場合には、離れたエリアとバックボーンエリアの間でルーティング情報を交換するパスとして仮想リンクを設定します。仮想リンクは 1 つの共通エリア（通過エリア）に接する 2 台の ABR 間に設定されます。その定義には、通過エリアに属するポート番号、通過エリア ID、隣接ルータ ID を使用します。

6.5.2.14.1　仮想（リンク）インタフェースの生成

OSPF プロトコルでは、各エリアがバックボーンエリア、すなわち ID 0.0.0.0 エリアに直接接していることが要求されます。言い換えると、各エリア内の ABR のうち 1 台は、エリア ID 0.0.0.とのインタフェースを有する必要があります。しかし、ネットワーク構成によっては、エリア内の ABR がバックボーンエリアと直接接することが不可能なこともあります。その場合には、離れたエリアとバックボーンエリアの間でルーティング情報を交換するパスとして仮想リンクを設定する必要があります。仮想リンクは 1 つの共通エリア（通過エリア）に接する 2 台の ABR 間に設定されます。その定義には、通過エリアに属するポート番号、通過エリア ID、隣接ルータ ID を使用します。

次の例は、本製品における仮想インタフェース設定を説明しています。ネットワーク構成は次の図のとおりです。

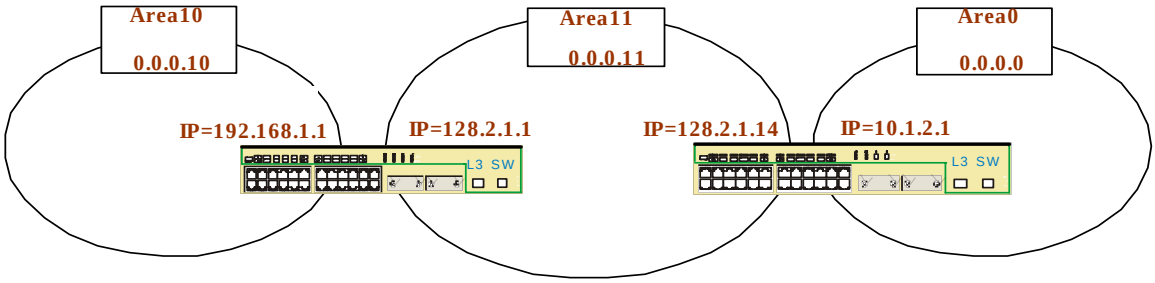

図 6-3：OSPF 仮想インタフェース

エリア 10 は非バックボーンエリアで、エリア 11 をバックボーンエリアに接続する「通過エリア」として利用します。ルータ A は、エリア 10 に接続する IP アドレス 192.168.1.1 のインタフェースと、エリア 11 に接続する IP アドレス 128.2.1.1 のインタフェースで、この 2 つのエリアに接続しています。ルータ B は、2 つのインタフェースを持っています。ルータ B は、IP アドレス 128.2.1.14 のインタフェースでエリア 11 に接続し、IP アドレス 10.1.2.1 のインタフェースでバックボーンエリア（アドレス 0 のエリア）に接続しています。したがって、上のネットワークのエリア 10 をバックボーンエリアに接続するには、ルータ A とルータ B の間に仮想リンクを設定する必要があります。次のコマンドは、ルータ A とルータ B 間の仮想リンク生成を説明しています。

L3SW> config router ospf virtif create <slot.id> <areaid> <neighbor-IPaddr>

ルータ A では、次のコマンドを実行します。

```
L3SW> config router ospf virtif create 4.3 0.0.0.11 128.2.1.14
```

ルータ B では、次のコマンドを実行します。

```
L3SW> config router ospf virtif create 4.2 0.0.0.11 128.2.1.1
```

仮想リンクの生成には、2 台のルータ、すなわちバックボーンエリアに接続するインタフェースと通過エリアに接続するインタフェースを持つルータ（上の例ではルータ B）と、非バックボーンエリアに接続するインタフェースと通過エリアに接続するインタフェースを持つルータ（上の例ではルータ A）で、それぞれ仮想インタフェースを設定する必要があります。

6.5.2.14.2 仮想（リンク）インタフェースの削除

設定した仮想インタフェースを削除する場合は、次のコマンドを実行します。

L3SW> config router ospf virtif delete <areaid> <neighbor-IPaddr>

ルータ A では、次のコマンドを実行します。:

```
L3SW> config router ospf virtif delete 0.0.0.11 128.2.1.14
```

ルータ B では、次のコマンドを実行します。

```
L3SW> config router ospf virtif delete 0.0.0.11 128.2.1.1
```

仮想リンクは、対応する 2 台のルータの仮想インタフェースが削除されなければ完全には削除されません。

6.5.2.14.3 仮想リンクのセキュリティ

仮想リンクへの不正な侵入を防ぐため、仮想リンクで交換されるルーティング情報はパスワードで保護することができます。これには、仮想リンクで送られるルーティング PDU にパスワードを組み込ます。有効なパスワードを持たないルーティング PDU は、仮想リンクで受信されても廃棄されます。仮想リンクへのパスワード設定には、次のコマンドを実行します。

```
L3SW> config router ospf virtif authtypekey <areaid> <neighbor-IPaddr> <none|simple> [key]
```

ルータ A では、次のコマンドを実行します。

```
L3SW> config router ospf virtif authtypekey 0.0.0.11 128.2.1.14 simple pass1
```

ルータ B では、次のコマンドを実行します。

```
L3SW> config router ospf virtif authtypekey 0.0.0.11 128.2.1.1 simple pass1
```

キーは最大 8 個の文字で構成されます。キーとなる文字列には、コントロールキー文字列は使用できません。

6.5.2.14.4 仮想リンクのタイマ設定

仮想リンクの動作に関しては、多数のタイマが存在します。仮想リンクが設定されると、それらのタイマにはデフォルト値が割り当てられます。仮想リンクの動作に使用されるタイマの一部と、そのデフォルト値を次に示します。

- ハロータイマ（Hello timer：1-65535 秒、デフォルトは 10 秒）
- デッドタイマ（Dead timer：1-65535 秒、デフォルトは 40 秒）
- 再送タイマ（Retransmission timer：1-3600 秒、デフォルトは 40 秒）
- トランジット遅延タイマ（Transit Delay timer：1-3600 秒、デフォルトは 60 秒）

仮想リンクの相手方も本製品で、仮想リンクでのトランジット遅延が小さい場合は、タイマのデフォルト値を変更する必要はありません。ただし、仮想リンクの適切な動作のためにタイマ値の変更が必要になった場合は、次の各コマンドによってタイマ値を変更することができます。タイマ値の変更には、次のコマンドを実行します。

- ハロータイマ設定コマンド

```
L3SW> config router ospf virtif interval hello <areaid> <neighbor> <1-65535>
L3SW> config router ospf virtif interval hello 0.0.0.10
   128.2.1.14 30
```

- デッドタイマ設定コマンド

```
L3SW> config router ospf virtif interval dead <areaid> <neighbor> <1-65535>
L3SW> config router ospf virtif interval dead 0.0.0.10
   128.2.1.14 80
```

- 再送タイマ設定コマンド

L3SW> config router ospf virtif interval rxmit <areaid> <neighbor> <1-3600>
L3SW> config router ospf virtif interval rxmit 0.0.0.10 128.2.1.14 80

- 再送タイマ設定コマンド

L3SW> config router ospf virtif transdelay <areaid> <neighbor> <1-3600>
L3SW> config router ospf virtif transdelay 0.0.0.10 128.2.1.14 120

6.5.2.15 OSPF 設定の表示

OSPF 対応のインタフェース設定終了後に設定を確認する場合は、show コマンドを実行します。エリア、インタフェース、LSDB、隣接ルータ、仮想リンクなど、OSPF 情報表示には複数のオプションが用意されています。次は、OSPF 設定表示に関連するコマンドとその表示の例です。

LSDB の検索コマンドに様々なオプションがあるのは、LSDB には多数の LSA エントリが存在する可能性があり、コマンドでタイプを指定する必要があるためです。

L3SW> show router ospf area info <areaid>
L3SW> show router ospf area info 0.0.0.10

```
L3SW> show router ospf area info 0,0,0,10


ArealD ..............................  0. 0. 0.10
Aging Interval. .....................  10
External Routing.....................Import External LS
As
Spf Runs.............................0
Area Border Router Count.............0
Area ISA Count ......................  0
Area ISA Checksum. ..................  0
Stub Mode ...........................  Disable
Import Summary LSAs..........................Enable

Type of Service Default Metric Metric Type
--------------- -------------- -----------
Monetary        10             Non-comparable Cost

L3SW>
```

表 6-15:OSPF エリア情報の表示

L3SW> show router ospf info

```
L3SW>show router ospf info
Router ID ..........................  10,1,1,1
OSPF Admin Mode ....................  Enable
RFC 1583 Compatibility. ............  Enable
ASBR Mode ..........................  Disable
ABR Status .........................  Enable
Exit Overflow Internal .............  0
External LSA Count .................  0
External LSA Checksum ..............  0
New LSAs Originated ................  0
LSAs Received ......................  0
External LSDB Limit ................  Mo Limit
Route redistribution.....................
   Connected.........................Disable
   Static............................Disable
   RIP ..............................  Disable
Redistribution default metric.........10,exttypel
Connected.............................10,exttypel
Static ...............................  10,exttypel
RIP ..................................  10,exttypel
Adefault route redistribution ........  Disable
Adefault route redistribution metric .  10,exttype1

L3SW>
```

表 6-16:OSPF 情報の表示

L3SW> show router ospf area info <areaid>
L3SW> show router ospf area info 0.0.0.10

```
L3SW> show router ospf area info 0.0.0.10


ArealD ..............................  0. 0. 0.10
Aging Interval.......................10
External Routing. ...................  Import External LS
As
Spf Runs ............................  0
Area Border Router Count ............  0
Area LSA Count ......................  0
Area LSA Checksum ...................  0
Stub Mode ...........................  Disable
Import Summary LSAs .................  Enable

Type of Service Default Metric Metric Type
--------------- -------------- -----------
Monetary        10             Non-coraparable Cost

L3SW>
```

表 6-17:OSPF エリア情報の表示

L3SW> show router ospf interface info <slot.port>
L3SW> show router ospf interface info 4.4

```
L3SW>show router ospf interface info 4.4

IP Address ..................................... 192. 168. 1. 1
Subnet Mask. ................................... 255. 255. 255.
OSPF Admin Mode ................................ Enable
OSPF Area ID ................................... 0. 0. 0. 10
Router Priority. ............................... 1
Retransmit Interval. ........................... 5
Hello Interval. ................................ 10
Dead Interval. ................................. 40
LSA Ack Interval ...............................  1
Iftransit Delay Interval. ...................... 1
Authentication Type. ........................... None
Metric Cost .................................... 1
OSPF Interface Type. ........................... broadcast
State. ......................................... down
Designated Router .............................. 0. 0. 0. 0
Backup Designated Router ....................... 0. 0. 0. 0
Number of Link Events. ......................... 0

L3SW>
```

表 6-18:OSPF インタフェース情報の表示

L3SW> show router ospf area range 0.0.0.10

```
L3SW>show router ospf area range 0.0.0.10

 Area ID  IP Address     Subnet Mask   Lsdb Type       Advertisement
--------- ------------  -------------  ---------------  ---------
0.0.0.10  192.168.0.0    255.255.0.0   Network summary  Enabled

L3SW>
```

表 6-19:OSPF レンジ 1 の表示

L3SW> show router ospf lsdb summary

```
L3SW> show router ospf lsdb su

 Area ID  Router       Network   Net-Summary  ASBR-Summary
--------- ---------    --------  -----------  ---------
0.0.0.0   2            1         1            0

AS-External LSAs.............. 1

L3SW>
```

表 6-20:OSPF リンク状態データベース要約情報の表示

```
L3SW> show router ospf lsdb detailed all
```

```
L3SW> show  router ospf Isdb detailed  all
LSA Type         Area ID
 Router ID       LS ID      Age     Sequence    Checksum  Options
 --------------  -------    -----   ----------- --------  -----------
Router links     0.0.0.0
 10.1.1.1        10.1.1.1   101     0x80000007  0x0010    - - - E -
Router links     0.0.0.0
 20.0.0.0        20.0.0.0   374     0x80000007  Oxf202    - - - E -
Network links    0.0.0.0
 20.0.0.0        10.1.1.10  374     0x80000003  Oxec20    - - - E -
Network summary   0.0.0.0
 20.0.0.0        10.30.1.0  316     0x80000002  0x8684    - - - E -
As external
20.0.0.0         10.20.1.0  255     0x80000002  Oxd5c9

L3SW>
```

表 6-21：OSPF リンク状態データベース詳細情報の表示

```
L3SW> show router ospf lsdb detailed router <network/netsummary, asbrsummary/asexternal>
```

```
L3SW> show  router ospf Isdb detailed router
 LSA Type         Area ID
  Router ID       LS ID      Age     Sequence    Checksum  Options
  --------------  -------    -----   ----------- --------  -----------
 Router links     0.0.0.0
  10.1.1.1        10.1.1.1   292     0x80000007  0x0010    - - - E -
 Router links     0.0.0.0
  20.0.0.0        20.0.0.0   566     0x80000007  Oxf202    - - - E –

 L3SW>
```

表 6-22：OSPF リンク状態データベースルータの表示

```
L3SW> show router ospf virtif summary
```

```
L3SW> show router ospf virtif su

                          Hello     Dead      Rxmt     Transit
 Area ID    Neighbor      Interval  Interval  Interval   Delay
 ---------  ------------  --------  --------  --------  --------
 0.0.0.10   192.168.1.100  10        40        5         1

L3SW>
```

表 6-23：仮想インタフェースサマリの表示

WBI は、OSPF インタフェース統計を表形式（CLI の場合と似た形式）またはグラフ形式で表示できます。

OSPF インタフェース統計をグラフィカルに表示するには、WBI にログインし、WBI ナビゲーションツリーで[Statistical Data]→[Monitor Interface]をクリックします。次に、[Polling Interval]を選択し(これで、WBI は自動的にポーリングし、統計表示をグラフィカルに更新するようになります)、[Submit]ボタンをクリックします。図 6-4 に、全ポートの WBI グラフィカル統計表示の画面例を示します。[Statistics Type]メニューを選択すると、Interface General、Interface Global、Event などの様々なインタフェース統計データが表示できます。さまざまなタイプの棒グラフや折れ線グラフを選択することができます。[Presentation Type]から選択してください。

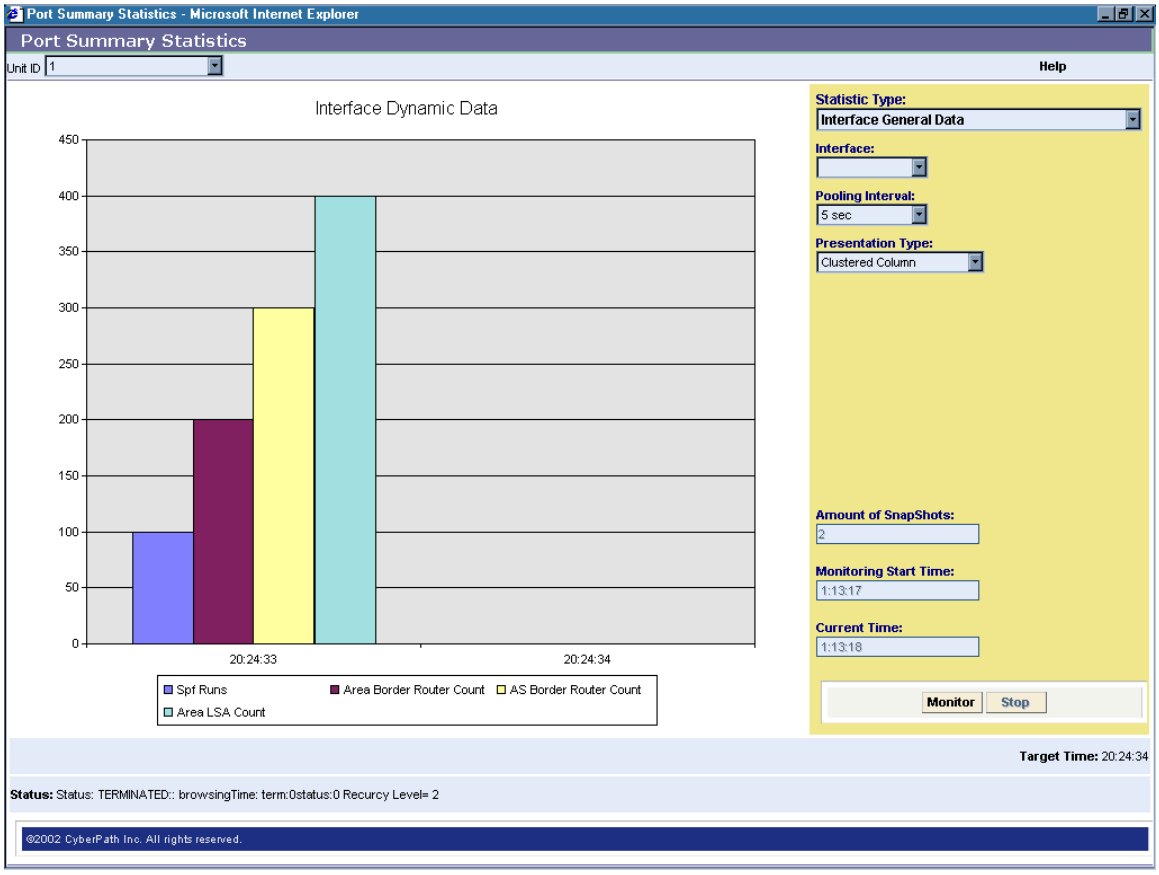

図 6-4：OSPF インタフェース統計データの WBI グラフ表示

6.5.2.16 OSPF 設定の例

図 6-5 では、OSPF 設定コマンドの使用法について説明しています。

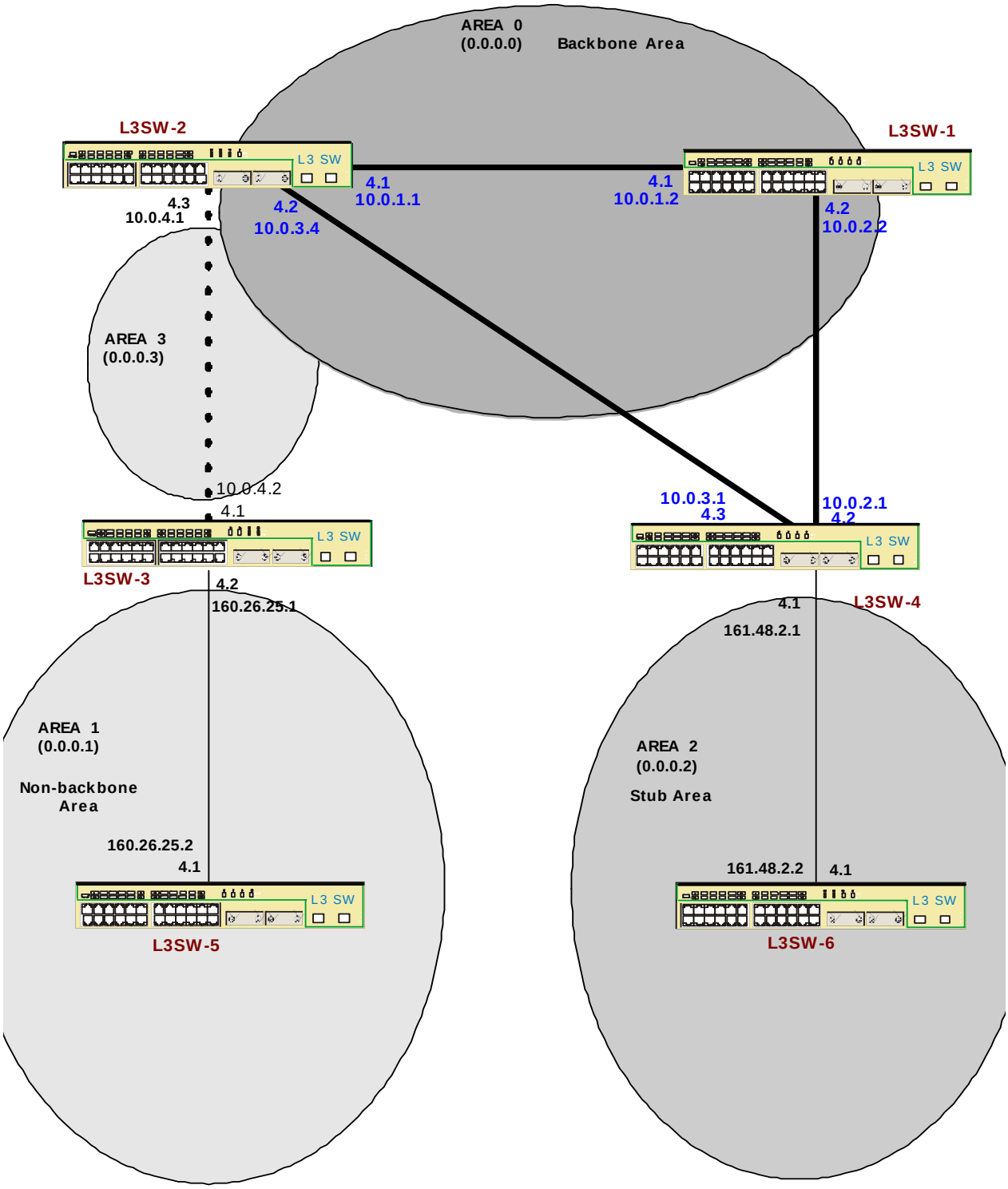

図 6-5：OSPF に基づいたネットワーク構成

このネットワーク構成例では、エリア 0、1、2、3 の 4 つの OSPF エリアが使用されています。エリア 0 はバックボーンエリア、エリア 2 はスタブエリアで、エリア 1 にはバックボーンエリアと直接接している ABR は存在しません。エリア 3 は、エリア 1 からバックボーンエリアへの仮想リン

クを設定する通過エリアとして機能しています。

このネットワークでは、6 台のルータが使用されています。各ルータのインタフェースには、4.1、4.2、4.3 の番号が付いています。各ルータポートの IP アドレスは、ルータポート番号の次に表示されています。L3SW-1 と L3SW-2、L3SW-3、L3SW-4 は、エリア境界ルータ(ABR)です。L3SW-5 と L3SW-6 は ABR ではありません。エリア 1 はバックボーンエリアに直接接していないので、エリア 1 のノードとネットワーク内の他のエリアとの円滑な通信のために仮想リンクを設定する必要があります。仮想リンクは、L3SW-3(ポート 4.1)と L3SW-2(ポート 4.3)の間に設定されています。

- **L3SW-1 の設定**

```
L3SW-1> config routing enable
L3SW-1> config router id 10.0.1.2
L3SW-1> config ip port create 0.1 10.0.1.2 255.255.255.0
L3SW-1> config ip port create 0.2 10.0.2.2 255.255.255.0
L3SW-1> config router ospf adminmode enable
L3SW-1> config router ospf interface areaid 4.1 0.0.0.0
L3SW-1> config router ospf interface areaid 4.2 0.0.0.0
L3SW-1> config router ospf interface mode 4.1 enable
L3SW-1> config router ospf interface mode 4.2 enable
```

- **L3SW-2 の設定**

```
L3SW-2> config routing enable
L3SW-2> config router id 10.0.1.1
L3SW-2> config ip port create 0.1 10.0.1.1 255.255.255.0
L3SW-2> config ip port create 0.2 10.0.3.4 255.255.255.0
L3SW-2> config ip port create 0.3 10.0.4.1 255.255.255.0
L3SW-2> config router ospf adminmode enable
L3SW-2> config router ospf interface areaid 4.1 0.0.0.0
L3SW-2> config router ospf interface areaid 4.2 0.0.0.0
L3SW-2> config router ospf interface areaid 4.3 0.0.0.3
L3SW-2> config router ospf interface mode 4.1 enable
L3SW-2> config router ospf interface mode 4.2 enable
L3SW-2> config router ospf interface mode 4.3 enable
L3SW-2> config router ospf virtif create 4.3 0.0.0.3 10.0.4.2
L3SW-2> config router ospf virtif authtypekey 0.0.0.3 10.0.4.2 simple
goldkey
```

- **L3SW-3 の設定**

```
L3SW-3> config routing enable
L3SW-3> config router id 10.0.4.2
L3SW-3> config ip port create 0.1 10.0.4.2 255.255.255.0
L3SW-3> config ip port create 0.2 160.26.25.1 255.255.255.0
L3SW-3> config router ospf adminmode enable
L3SW-3> config router ospf interface areaid 4.1 0.0.0.3
L3SW-3> config router ospf interface areaid 4.2 0.0.0.2
L3SW-3> config router ospf interface mode 4.1 enable
L3SW-3> config router ospf interface mode 4.2 enable
L3SW-3> config router ospf virtif create 4.1 0.0.0.3 10.0.1.1
L3SW-3> config router ospf virtif authtypekey 0.0.0.3 10.0.1.1 simple
goldkey
```

- **L3SW-4 の設定**

```
L3SW-4> config routing enable
L3SW-4> config router id 10.0.2.1
L3SW-4> config ip port create 0.1 161.48.2.1 255.255.255.0
```

```
L3SW-4> config ip port create 0.2 10.0.2.1 255.255.255.0
L3SW-4> config ip port create 0.3 10.0.3.1 255.255.255.0
L3SW-4> config router ospf adminmode enable
L3SW-4> config router ospf interface areaid 4.1 0.0.0.2
L3SW-4> config router ospf interface areaid 4.2 0.0.0.0
L3SW-4> config router ospf interface areaid 4.3 0.0.0.0
L3SW-4> config router ospf interface mode 4.1 enable
L3SW-4> config router ospf interface mode 4.2 enable
L3SW-4> config router ospf interface mode 4.3 enable
L3SW-4> config router ospf area stub summarylsa 0.0.0.2 disable
```

- L3SW-5 の設定

```
L3SW-5> config routing enable
L3SW-5> config router id 160.26.25.2
L3SW-5> config ip port create 0.1 160.26.25.2 255.255.255.0
L3SW-5> config router ospf adminmode enable
L3SW-5> config router ospf interface areaid 4.1 0.0.0.1
L3SW-5> config router ospf interface mode 4.1 enable
```

- L3SW-6 の設定

```
L3SW-6> config routing enable
L3SW-6> config router id 161.48.2.2
L3SW-6> config ip port create 0.1 161.48.2.2 255.255.255.0
L3SW-6> config router ospf adminmode enable
L3SW-6> config router ospf interface areaid 4.1 0.0.0.2
L3SW-6> config router ospf interface mode 4.1 enable
```

6.6 仮想ルーティング冗長プロトコル（VRRP）

6.6.1 概要

VRRP は RFC 2338 に定義されており、LAN 内の複数の IP ルータが即時かつ自動的に互いにバックアップできるグループとしての動作を可能にします。VRRP は、バックアップルータによるマスタルータの状況のモニタと、マスタルータに障害が起きたときの役割引き継ぎについて定義されています。

本製品は、ポートレベルで VRRP に対応しています。ルータポートとして設定されているどのスイッチポートでも VRRP は動作します。VRRP に対応するルータは、アドバタイズパケットの定期的送信によって LAN セグメント上でお互いを見つけ出します。この定期的な VRRP アドバタイズ送信には、他の VRRP ルータに自分自身が動作中であることを知らせるという意味もあります。それまで VRRP パケットを送信していたルータからのアドバタイズ受信が無くなると、ルータは（サブ）ネットワークの他のルータによってダウンしたとみなされます。ダウンしたルータが回復すると、自動的にバックアップルータと交代して活動を再開します。

6.6.2 VRRP の設定

ベーシックな VRRP の設定は、次の 4 つの手順で行います。

ステップ 1：ルーティングモードを有効にします。

詳しい設定については、「6.1.2　ルーティングモードの設定」(P.101)を参照

ステップ 2:VRRPポートに対するIPインタフェースを設定します。

詳しい設定については、「6.2.2.1　物理ポート上の IP インタフェースの設定」(P.106)を参照

ステップ 3:ルータでのVRRPを有効にします。

ステップ 4:インタフェースでのVRRPを設定します。

6.6.2.1　ルータ上での VRRP 設定

デフォルトでは、VRRP はルータで動作しません。VRRP を有効または無効にするには、次のコマンドを実行します。

```
L3SW> config router vrrp adminmode <enable/disable>
L3SW> config router vrrp adminmode enable
```

6.6.2.2　インタフェース上での VRRP 設定

ベーシック VRRP インタフェースを設定するには、VRRP ルータ ID と VRRP IP アドレスを設定してインタフェースで VRRP が動作できるようにする必要があります。

VRRP のルータ ID を設定する場合は、次のコマンドを実行します。

```
L3SW> config router vrrp interface routerid <slot.port> <vrid>
L3SW> config router vrrp interface routerid 4.1 1
```

VRRP インタフェースの IP アドレスを設定する場合は、次のコマンドを実行します(マスタルータには、VRRP インタフェースの IP アドレスと同じ実 IP アドレスを持つルータがなります)。

```
L3SW> config router vrrp interface ipaddress <slot.port> <vrid> <ipaddr>
L3SW> config router vrrp interface ipaddress 4.1 1 10.1.1.1
```

インタフェースで VRRP が動作できるようにするには、次のコマンドを実行します。

```
L3SW> config router vrrp interface adminmode <slot.port> <vrid> <enable/disable>
L3SW> config router vrrp interface adminmode 4.1 1 enable
```

VRRP マスタルータがダウンした場合、次のマスタルータは VRRP グループで各ルータが互いにアドバタイズしあう優先値に基づいて決められます。各 VRRP ルータに優先値を割り当てるには、次のコマンドを実行します。

```
L3SW> config router vrrp interface priority <slot.port> <vrid> <1-254>
L3SW> config router vrrp interface priority 4.1 1 100
```

VRRP ルータ間で交換される VRRP メッセージは、改ざん防止のため最大 8 文字の ASCII ストリングを使用したパスワードで保護できます。次のコマンドで実行します。

```
L3SW> config router vrrp interface authdetails <slot.port> <vrid> <none/simple> [key]
L3SW> config router vrrp interface authdetails 4.1 1 simple keygroup1
```

VRRP プロトコルによって定義されるプリエンプト(preempt)モードでは、優先度の高いルータが低いルータに優先します。この機能により、ダウンしたルータは復旧後にバックアップルータからルーティング機能を引き継ぐことができます。プリエンプトモードを有効／無効は、次のコマン

ドで実行します。

L3SW> config router vrrp interface preemptmode <slot.port> <vrid> <enable/disable>
L3SW> config router vrrp interface preemptmode 4.1 1 enable

6.6.2.3 VRRP 設定の表示

VRRP 関連の設定を表示する場合は、次のコマンドを実行します。

L3SW> show router vrrp info

```
L3SW>show router vrrp info

VRRP Admin mode.......................... Enable
Router Checksum Errors................... 0
Router Version Errors.................... 0
Router VRID Errors....................... 0

L3SW>
```

表 6-24:VRRP 情報の表示

特定のインタフェースに関する VRRP データを表示する場合は、次のコマンドを実行します。

L3SW> show router vrrp interface detailed <slot.port> <vrid>
L3SW> show router vrrp interface detailed 4.1 1

```
L3SW>show router vrrp interface detailed 4.1 1

IP Address.............................. 10.1.2.1
UMAC Address............................ 00:00:5e:00:01:01
Authentication Type..................... None
Priority................................ 255
Advertisement Interval.................. 1
Pre-Empt Node........................... Enable
Administrative Node..................... Enable
State................................... Initialized

L3SW>
```

表 6-25:インタフェースに対する VRRP 要約情報の表示

特定のインタフェースに関する VRRP 統計データを表示する場合は、次のコマンドを実行します。

L3SW> show router vrrp interface stats <slot.port> <vrid>
L3SW> show router vrrp interface stats 4.1 1

```
L3SW>show router vrrp interface stats 4.1 1

UpTime.............................. 0 days 0 hrs 0 mins 0 secs
Protocol............................ IP
State Transitioned to Master........ 0
Advertisement Received.............. 0
Advertisement Interval Errors....... 0
Authentication Failure.............. 0
PIP TTL Errors...................... 0
Zero Priority Packets Received...... 0
Zero Priority Packets Sent.......... 0
Invalid Type Packets Received....... 0
Address List Errors................. 0
Invalid Authentication Type......... 0
Authentication Type Mismatch........ 0
Packet Length Errors................ 0

                                L3SW>
```

表 6-26:VRRP インタフェース統計データの表示

VRRP インタフェース要約情報を表示する場合は、次のコマンドを実行します。

L3SW> show router vrrp interface summary

```
L3SW>show router vrrp interface summary
Slot.Port  VRID  IP Address      Mode      State
---------  ----  -------------   -------   ---------
4.1        1     10.1.2.1        Enable    Initialize
4.2        2     128.2.1.4       Enable    Master

L3SW>
```

表 6-27:すべてのインタフェースに対する VRRP 要約情報の表示

6.6.3 VRRP のサンプル

次の例では、2 台の本製品が 2 つのネットワークに接続されています。VRRP がサポートされているので、2 台のうち 1 台がダウンしても、Network-1 に接続しているホストは Network-2 と通信できます。

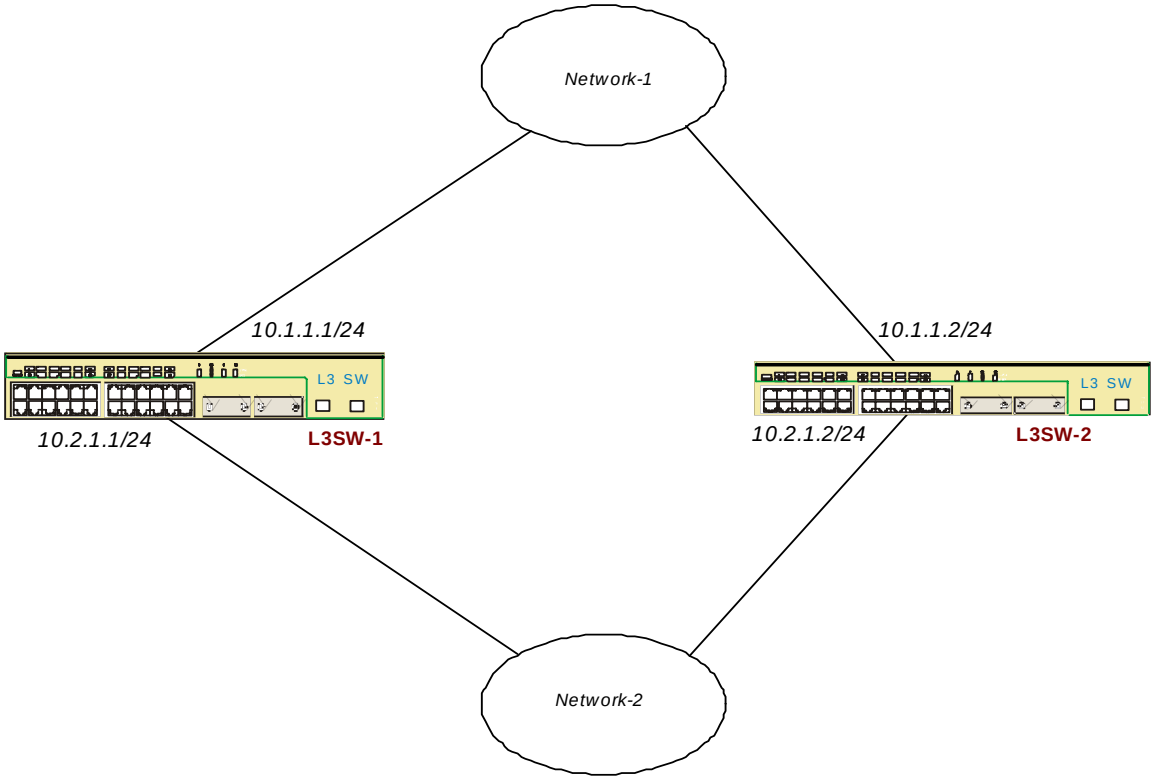

図 6-6：VRRP 構成図

L3SW-1 を、Network-1 と Network-2 のマスタルータにする場合、次のように設定します。

- L3SW-1 の設定

```
L3SW-1> config routing enable
L3SW-1> config ip port create 0.1 10.1.1.1 255.255.255.0
L3SW-1> config ip port create 0.2 10.2.1.1 255.255.255.0
L3SW-1> config router vrrp adminmode enable
L3SW-1> config router vrrp interface routerID 4.1 1
L3SW-1> config router vrrp interface routerID 4.2 2
L3SW-1> config router vrrp interface adminmode 4.1 1 enable
L3SW-1> config router vrrp interface adminmode 4.2 2 enable
L3SW-1> config router vrrp interface ipaddress 4.1 1 10.1.1.1
L3SW-1> config router vrrp interface ipaddress 4.2 2 10.2.1.1
```

- L3SW-2 の設定

```
L3SW-2> config routing enable
L3SW-1> config router vrrp interface priority 4.1 1 50
L3SW-2> config ip port create 0.1 10.1.1.2 255.255.255.0
L3SW-2> config ip port create 0.2 10.2.1.2 255.255.255.0
L3SW-2> config router vrrp adminmode enable
L3SW-2> config router vrrp interface routerID 4.1 1
L3SW-2> config router vrrp interface routerID 4.2 2
L3SW-2> config router vrrp interface adminmode 4.1 1 enable
L3SW-2> config router vrrp interface adminmode 4.2 2 enable
L3SW-2> config router vrrp interface ipaddress 4.1 1 10.1.1.1
L3SW-2> config router vrrp interface ipaddress 4.2 2 10.2.1.1
```

6.7 ルータ通知(Router Discovery)

6.7.1 ルータ通知の概要

ICMP ルータ通知メッセージ(IRDM)は、RFC 1256 で定義されているとおり、サブネットワークのホストに隣接ルータの IP アドレスを通知します。そのため、IRDM は ICMP ルータ通知プロトコル(IRDP)と呼ばれることもあります。これにより、ネットワーク内の各ホストのデフォルトゲートウェイ(隣接ルータ)IP アドレスをネットワーク管理者が手動で設定する必要がなくなります。また、プライマリルータがダウンまたは機能停止した場合には、このプロトコルを利用して代替ルータの IP アドレスを自動的に通知することができます。

一般に IRDP に対応しているルータは、マルチキャストやブロードキャストで定期的にルータアドバタイズを送信します。ネットワーク上のホストは、ルータのアドバタイズや自分自身が送信したルータ要求メッセージへの応答を受信して、デフォルトゲートウェイの IP アドレスのリストを維持します。ただし、ホストによるルータ通知やアドバタイズへの対応を可能にするには、ホストに独自の IP アドレスとサブネットマスクを設定する必要があります。ホストが BOOTP/DHCP サーバからの IP アドレス割当を待っている場合、ホストが受信した IRDP アドバタイズはすべて無視されます。

IRDP に対応しているルータは、マルチキャストグループのアドレス 224.0.0.1 を使って自身の IP アドレスをアドバタイズします。このマルチキャストグループには、IRDP に対応するルータのインタフェースがすべて含まれます。ホストはマルチキャストアドレス 224.0.0.2 によってルータ要求メッセージを送り、ルータはマルチキャストアドレス 224.0.0.1 によってアドバタイズメッセージを送ります。本製品では、次の IRDP 設定オプションが可能です。

- IRDP の有効／無効
- Lifetime:ルータアドバタイズのライフタイムフィールドの値(最大間隔値:9000)で、デフォルト値は 1800
- Max interval:アドバタイズ送信間隔の最大時間(4～1800)で、デフォルト値は 600
- Min interval:アドバタイズ送信間隔の最小値(3～最大間隔値)で、デフォルト値は 450
- Preference:ホストによってルータがサブネットへのデフォルトゲートウェイ(ルータ)に決められる可能性の度合いを定義します。この値が高いほど、サブネット内のホストによってデフォルトゲートウェイに決められる可能性が高くなります。ホストは、デフォルトゲートウェイの IP アドレスを優先度に応じて格納したリストを管理しています。IP パケットの送信後に ICMP の宛先変更メッセージを受信すると、優先度リストの次順位ゲートウェイに宛てて IP パケットを再送信します。

6.7.2 ルータ通知の設定

ルータ通知の設定は、次の 4 つの手順で行います。

ステップ 1:ルーティングモードを有効にします。

詳しい設定については、「6.1.2　ルーティングモードの設定」(P.101)を参照

ステップ 2:ルータ通知ポートに対するIPインタフェースを設定します。

詳しい設定については、「6.2.2.1　物理ポート上の IP インタフェースの設定」(P.106)を参照

ステップ 3:インタフェースでのルータ通知を有効にします。

ステップ 4:インタフェースでのルータ通知パラメータを設定します。

インタフェースでのルータ通知を動作可能にする場合は、次のコマンドを実行します。

```
L3SW> config router rtrdiscovery adminmode <slot.port> <enable/disable>
L3SW> config router rtrdiscovery adminmode 4.1 enable
```

ポートでのルータ通知機能を動作可能に設定すると、そのポートに対して最大、最小、アドバタイズライフタイム設定などすべてのパラメータのデフォルト値が自動的に設定されます。これらのデフォルト値は、コマンドを使って変更できます。値を再設定する方法については、後で例をあげて説明します。パラメータの値を表示する場合は、次のコマンドを実行します。

```
L3SW> show router rtrdiscovery <slot.port/all>
L3SW> show router rtrdiscovery 4.1
```

```
L3SW>show router rtrdiscovery 4.1

Intf Ad Mode Advertise Address Max Int Min Int Adv Life Preference
---- ------- ----------------- ------- ------- -------- ----------
4.1  Enable  244.0.0.1         600     450     1800     0
L3SW>
```

表 6-28:ルータ通知テーブルの表示

6.7.3　ルータ通知の例

次の図では、ネットワークが 2 台のルータに接続されています。このネットワークでは、ルータ通知プロトコルによりデフォルトゲートウェイが自動的に検索されます。

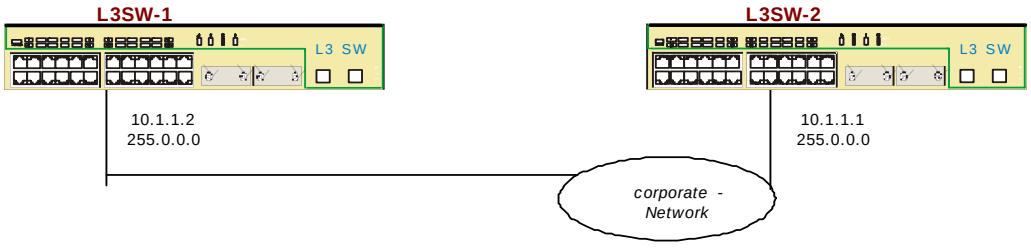

図 6-7:ルータ通知の構成図

- L3SW-1

```
L3SW-1> config ip port create 0.1 10.1.1.2 255.255.255.0
L3SW-1> config routing enable
L3SW-1> config router rtrdiscovery adminmode 4.1 enable
```

```
L3SW-1> config router rtrdiscovery preference 4.1 20
```

- L3SW-2

```
L3SW-2> config ip port create 0.1 10.1.1.1 255.255.255.0
L3SW-2> config routing enable
L3SW-2> config router rtrdiscovery adminmode 4.1 enable
L3SW-2> config router rtrdiscovery preference 4.1 2
```

6.8 ルート再配布

6.8.1 ルート再配布の概要

ルーティング機能は、ルーティングテーブルに基づいて動作します。本製品は、ルーティングテーブルへの手動によるスタティックルーティングエントリ生成と、ルーティングプロトコルによる動的なルーティング情報の学習をサポートしています。ルート再配布は、ルーティングドメインを越えた学習に役立ちます。違うプロトコルを使っていて宛先までのコストについてのメソッドとメトリックが異なる場合、別々のルーティングドメイン間で慎重にルートを再配布することでルーティングループを回避できます。本製品では、次のルーティングドメイン間でのルート再配布に対応しています。

- スタティックルーティング
- 直接接続ルーティング
- OSPF（OSPF 内部ルート、AS 外部ルートタイプ 1、AS 外部ルートタイプ 2）
- RIP

本製品では、2 種類のルーティングテーブルを管理しています。1 つは、スタティックルートと直接ルータに接続しているルート、ルーティングプロトコルで学んだルートのエントリをすべて含むテーブルです。もう 1 つはトラフィック転送に使用される最適ルーティングテーブルです。最適ルーティングテーブルはルーティングテーブルのサブセットで、同じ宛先までの複数のルーティングエントリの中から、特定タイプのルート向けに定義された優先度に従ってルートが選出されています。ルート再配布は、この最適ルーティングテーブルのエントリに基づいて実行されます。したがって、最適ルーティングテーブルに選ばれなかったルーティングテーブルのエントリは、それが再配布可能なルートタイプであっても再配布されません。

例えば、あるルータが RIP と OSPF（ASBR）に対応するように設定されていて、RIP で宛先 N までのルートを学習し、また N までのスタティックルートも存在するとします。この場合、この 2 つのエントリはルーティングテーブルに表示されます。優先度設定により、スタティックルートは RIP ルートよりも上になっているため、最適ルーティングテーブルではスタティックルートが転送エントリに選択されます。しかし、RIP から OSPF へのルート再配布を可能にすれば（スタティックから OSPF への再配布は不可能）、N までの RIP ルーティングエントリはルータにより OSPF ドメインに再配布されます。どのルーティングエントリが再配布されるかを確認したい場合は、次のコマンドを実行して最適ルーティングテーブルを検索します。

6.8.2 他のドメインから RIP へのルート再配布

6.8.2.1 他のドメインから RIP へのルート再配布の有効／無効

RIP に対しては、スタティックルート、OSPF 内部ルート、AS 外部ルートのタイプ 1 とタイプ 2 が

それぞれ再配布できます。次のコマンドをオプション「all」で実行すれば、これらのルート再配布が一度で可能です。

```
L3SW> config router rip redistribute enable <connected/static/ospf/ospfint/ospfexttype1/ospfexttype2/all>
[redistribute-metric]
L3SW> config router rip redistribute enable connected 2
```

メトリック値を指定する場合は、次のコマンドを実行します（それ以外のときは、デフォルト値が用いられます）。

```
L3SW-1> config router rip redistribute disable
<connected/static/ospf/ospfint/ospfexttype1/ospfexttype2/all>
L3SW-1> config router rip redistribute disable connected
```

enable/disable ospf オプションでは、ospfint、ospfexttype1、ospfexttype2 オプションをまとめて実行できます。

6.8.2.2 再配布エントリに対するデフォルトメトリック値の設定

次のコマンドを実行すると、特定のルートエントリ再配布を可能にする前にデフォルトメトリック値を変更することができます。

```
L3SW> config router rip redistribute defaultmetric <redistribute-defaultmetric>
L3SW> config router rip redistribute defaultmetric 10
```

デフォルトメトリック値の変更は、実行可能になっていない再配布タイプにのみ影響します。

再配布可能なタイプに対するメトリックをデフォルト値に戻す場合は、再配布の有効／無効をやり直す必要があります。

再配布可能なタイプに対するメトリックを他の値に戻す場合は、再配布の有効／無効をやり直す必要があります。

6.8.2.3 RIP ルート再配布構成の表示

ルート再配布の設定を表示する場合は、次のコマンドを実行します。

```
L3SW-1> show router rip info
L3SW-1> show router rip info
```

```
L3SW>show router rip info

Router ID.....................................  10.1.1.1
RIP Admin Mode................................  Disable
Global route changes..........................  0
Global queries................................  0
Route redistribution..........................
   Connected.....................................Disable
   Static  ..................................... Disable
   OSPF ..........................................
     Internal.....................................Enable
     External type 1..............................Enable
     External type 2..............................Enable
Redistribution default metric..................10
  Connected..................................... 10
  Static       .................................10
  OSPF ..............................
     Internal..................................... 5
     External type 1.............................. 5
     External type 2.............................. 5

L3SW>
```

表 6-29:RIP 構成の表示

6.8.3 他のドメインから OSPF へのルート再配布

他のドメイン内のルートは、AS 外部 LSA を使って OSPF に挿入することができます。これは、OSPF 内の ASBR によって実行されます。AS 外部 LAS には、演算メトリックの手法の違いによって 2 つのタイプがあります。タイプ 1 では、ASBR までの内部 OSPF コストに外部メトリックをプラスしてパスコストを算出します。一方、タイプ 2 では、外部メトリックのみをパスコストとします。通常、外部メトリックが内部コストよりはるかに大きいと予想される場合は、タイプ 2 を設定します。

6.8.3.1 ルート再配布の有効／無効

OSPF は、スタティックルート、直接接続ルート、RIP ルートについて、個別指定または全部のルート再配布によって学習することができます。スタティックルートから OSPF ドメインへのルート再配布を有効にする場合は、次のコマンドを実行します。

L3SW> config router ospf redistribute enable <connected/static/rip/all> [<redistribute-default-metric> [<exttype1/exttype2>]]
L3SW> config router ospf redistribute enable static

ルート再配布を無効にする場合は、次のコマンドを実行します。

L3SW> config router ospf redistribute disable <connected/static/rip/all>
L3SW> config router ospf redistribute disable static

6.8.3.2 ルート再配布のデフォルトメトリック

ルート再配布を有効にした場合、メトリックが指定されていないときに使用するデフォルトメトリック値を定義できます。すでに再配布が有効になっているルートは、デフォルトメトリックの変更による影響は受けません。デフォルトメトリックを変更するには、次のコマンドを実行します。

L3SW> config router ospf redistribute defaultmetric <redistribute-defaultmetric>
L3SW> config router ospf redistribute defaultmetric 10 exttype1

再配布可能なタイプのデフォルトメトリックを変更する場合は、ルート再配布の特定のタイプに関して再配布の有効／無効をやり直す必要があります。

タイプ1／タイプ2 を変更する場合は、デフォルトメトリック設定コマンドを実行するか、またはタイプ1／タイプ2 を指定して再配布有効／無効をやり直します。デフォルトでは、タイプ1 が指定されています。

6.8.3.3 OSPF ルート再配布設定の表示

OSPF ルート再配布の設定を表示する場合は、次のコマンドを実行します。

L3SW> show router ospf info

```
L3SW>show router ospf info

Router ID ..............................  10.1.1.1
OSPF Admin Mode ........................  Enable
RFC 1583 Compatibility. ................  Enable
ASBR Mode ..............................  Disable
ABR Status .............................  Enable
Exit Overflow Interval.....................0
External ISA Count.........................0
External LSA Checksum......................0
iw LSAs Originated.........................0
LSAs Received..............................0
External LSDB Limit........................No Limit
Route redistribution.......................
  Connected.............................  Disable
  Static................................    Disable
  RIP ..................................  Enable
Redistribution default metric..............8,exttype1
  Connected.............................  8,exttype1
  Static................................    8,exttype1
  RIP  ................................... 10,exttypel
Default route redistribution...............Disable
Default route redistribution metric........10,exttypel

L3SW>
```

表 6-30：OSPF 設定の表示

6.8.4 ルート再配布の例

プロトコル間でのルート再配布が理解しやすいように、システム設定の例を使って説明します。この例では、ルータ R1 は OSPF ASBR として設定され、RIP と OSPF 間のルーティングエントリ再配布に対応しています。RIP ドメインでは、ルータ R2 とネットワーク N1、N2 が接続され、OSPF ドメインでは、ルータ R3 とネットワーク N3、N4 がバックボーンで設定されています。この構成では、複数のエリアへの拡張や、再配布の一方向への制限を簡単に行えます。

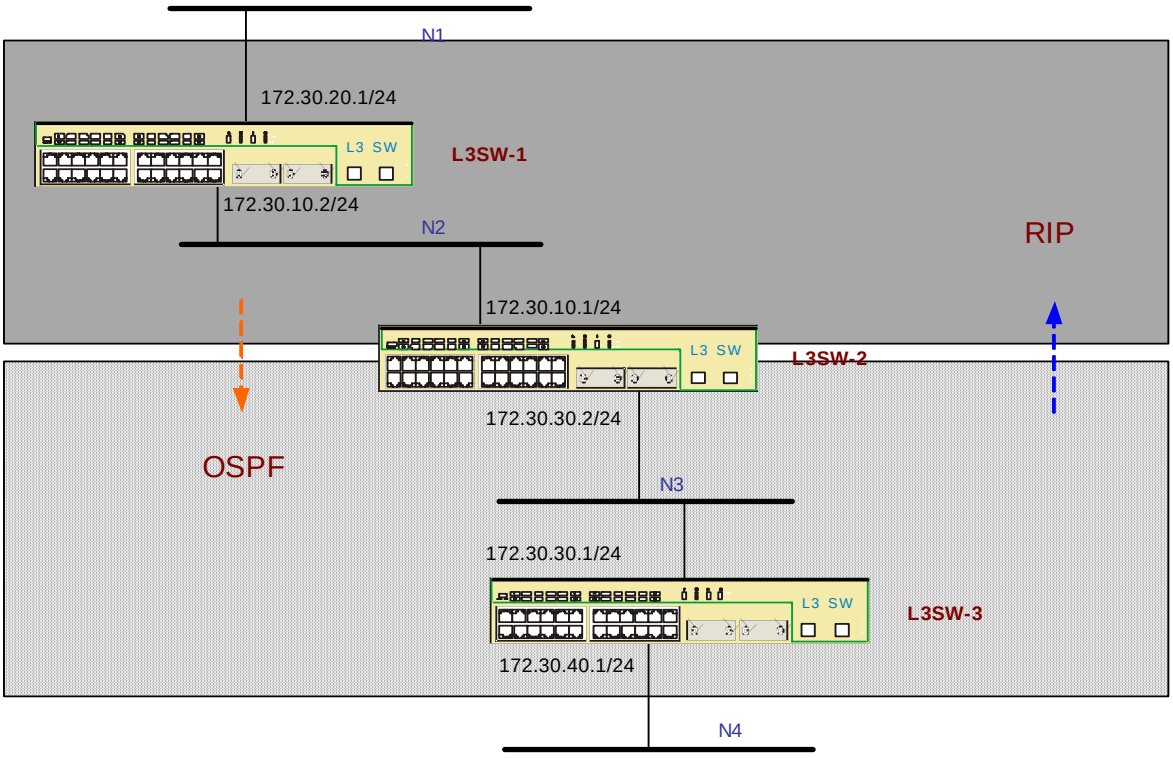

図 6-8:ルート再配布の例

この例でのルータ設定では、次のコマンドを実行します。

- スイッチ R1

```
L3SW-1> config ip port create 0.1 172.30.10.2 255.255.255.0
L3SW-1> config ip port create 0.2 172.30.20.1 255.255.255.0
L3SW-1> config routing enable
L3SW-1> config router id 172.30.10.2
L3SW-1> config router rip adminmode enable
L3SW-1> config router rip interface mode 4.1 enable
L3SW-1> config router rip interface mode 4.2 enable
```

- スイッチ R2

```
L3SW-2> config routing enable
L3SW-2> config router id 172.30.10.1
L3SW-2> config ip port create 0.1 172.30.10.1 255.255.255.0
L3SW-2> config ip port create 0.2 172.30.30.2 255.255.255.0
L3SW-2> config router rip adminmode enable
L3SW-2> config router ospf adminmode enable
L3SW-2> config router ospf asbr enable
L3SW-2> config router rip interface mode 4.1 enable
L3SW-2> config router ospf interface areaid 4.2 0.0.0.0
L3SW-2> config router ospf interface mode 4.2 enable
L3SW-2> config router rip redistribute defaultmetric ospf 5
L3SW-2> config router ospf redistribute defaultmetric rip 100
L3SW-2> config router rip redistribute enable ospf
L3SW-2> config router ospf redistribute enable rip
```

- スイッチ R3

```
L3SW-3> config routing enable
L3SW-3> config router id 172.30.30.1
L3SW-3> config ip port create 0.1 172.30.30.1 255.255.255.0
L3SW-3> config ip port create 0.2 172.30.40.1 255.255.255.0
L3SW-3> config router ospf adminmode enable
L3SW-3> config router ospf interface areaid 4.1 0.0.0.0
L3SW-3> config router ospf interface mode 4.1 enable
L3SW-3> config router ospf interface areaid 4.2 0.0.0.0
L3SW-3> config router ospf interface mode 4.2 enable
```

6.9 ボーダーゲートウェイプロトコル（BGP）

BGP と本製品でのその用法および設定について説明します。関連コマンドの使用法については例で説明します。

6.9.1 BGP の概要

OSPF プロトコル説明でも触れたように、BGP は自律システム間でのルーティング情報のやり取りに使われます。BGP ルータは外部／内部 BGP スピーカを介して複数のパスについて学習し、ネットワーク管理者が定義したポリシーに従ってその中から最適パスを選択します。BGP スピーカ間のすべてのセッションは、IGP から動的に取得した情報や静的に設定された BGP 隣接ルータから得た情報に基づいて設定されます。

本製品では、次にあげる BGP パラメータを設定するコマンドが実行できます。

- 一般的な BGP 設定
- ピアとセッションの設定
- スタティック NLRI 設定
- BGP オプションの設定
- コミュニティ設定
- ルータリフレクタ設定
- ポリシー設定
- アドレス集約設定

本製品では、次にあげる BGP パラメータを表示するコマンドも実行できます。

- 一般的な BGP 情報
- ピアとセッションの状況および情報
- NLRI テーブル
- NLRI 属性
- BGP ルーティングテーブル
- ポリシーリスト
- アドレス集約リスト

IGP と BGP 間のルート再配布は、今後のリリースで対応予定です。

6.9.2 BGP の設定

6.9.2.1 一般的な BGP 設定

一般的設定には、BGP の有効／無効、AS 番号の定義、BGP ルータ ID の定義が含まれます。これらのコマンドは BGP 環境に関する高度なコマンドで、BGP の適切な動作を目的として実行されます。BGP 環境の一般的な設定には、次のコマンドを実行します。

```
L3SW> config router bgp4 adminmode <enable/disable>
L3SW> config router bgp4 adminmode enable

L3SW> config router bgp4 asnumber <asnumber>
L3SW> config router bgp4 asnumber 10

L3SW> config router bgp4 localid <localid>
L3SW> config router bgp4 localid 10.1.1.1
```

BGP ルータ ID は、config router id コマンドで定義され IGP プロトコルで使用するルータ ID と同じでもかまいません。

6.9.2.2 ピアとセッションの設定

BGP では、2 地点間 TCP 接続を行うピアでルーティング情報を交換するため、ピアに関する詳細を設定する必要があります。ピア設定コマンドには、ピアの生成／削除、ピアの有効／無効、ピア認証、ピアパラメータの変更、セッションパラメータ、BGP セッション制御があります。

基本的なピア設定は、次のステップで行います。

- ピア生成
- ローカルインタフェースのピアへの関連付け
- ピアの有効化

また、BGP ピアやセッションに関連したパラメータは変更が可能です。

- ピアパラメータの変更
- セッションパラメータの変更
- BGP セッションの制御

6.9.2.2.1 ピアの生成と削除

ピアを生成するには、ピア IP アドレス、AS 番号、ピアルータ ID を指定します。ピアの AS 番号とローカル AS 番号を比較することで、生成されたピアが AS 外部ピアか内部ピアか識別され、それに従って操作されます。ピアを生成する場合は、次のコマンドを実行します。

```
L3SW> config router bgp4 peer create <peeripaddr> <peerasnumber> <peerlocalid>
L3SW> config router bgp4 peer create 10.1.1.3 2 10.1.1.2
```

peerlocalid には、config router bgp4 localid コマンドで設定したピアの BGP ルータ ID を入

力します。

本製品は、最大 10 個の BGP ピアをサポートします。

いったんピアを生成すると、その後の操作ではピアの IP アドレスをピア識別に使用します。このアドレスは、ピア ID として利用できます。ピアを削除する場合は、次のコマンドを実行します。

```
L3SW> config router bgp4 peer delete <peeripaddr>
L3SW> config router bgp4 peer delete 10.1.1.3
```

6.9.2.2.2 ローカルインタフェースとの関連付け

ピアセッションを有効にしたり起動する場合は、ピアの IP アドレスを使ってローカルインタフェースをピアに関連付ける必要があります。新しいローカルパスが生成されると、ローカル IP アドレスがピアに対するネクストホップとして使用されます。いったん、このローカルインタフェースが設定されると、BGP セッション設定に使用されたパケットはすべて、そのインタフェースを経由して転送されます。インタフェースとの関連付けには、次のコマンドを実行します。

```
L3SW> config router bgp4 peer localintf <peeripaddr> <localipaddr>
L3SW> config router bgp4 peer localintf 10.1.1.3 10.1.1.1
```

ピアの IP アドレスとローカル IP アドレスは、異なるサブネットに属していてもかまいません。その場合には、IGP から学習したルート情報やスタティックルートに基づいて、BGP セッションが設定されます。

6.9.2.2.3 ピアの有効／無効

設定したピアを有効または無効にする場合は、start または stop オプションを使って次のコマンドを実行します。

```
L3SW> config router bgp4 peer adminstatus <start/stop>
L3SW> config router bgp4 peer adminstatus start
```

6.9.2.2.4 ピア認証

BGP では、簡易パスワード（クリアテキスト）や暗号化パスワードによってピアセッションの認証を行うことができます。ただし、現在の本製品は、簡易パスワードしか対応していません。暗号化パスワードは、今後のリリースで対応する予定です。パスワード設定には、次のコマンドを実行します。

```
L3SW> config router bgp4 peer authtypekey <peeripaddr> <type> <key>
L3SW> config router bgp4 peer authtypekey 10.0.0.3 simple peer1
```

type に none を指定してこのコマンドを実行すると、ピア認証を解除できます。

6.9.2.2.5 ピアパラメータの変更

ピア ID や AS 番号、ポート番号などのピアパラメータは、変更できます。デフォルトでは TCP ポート 179 を使用していますが、スピーカ間での TCP セッションが設定されているポートであれば、その他の TCP ポートを利用することも可能です。ピアパラメータを変更する場合は、次のコマンドを実行します。

```
L3SW> config router bgp4 peer peerid <peeripaddr> <peerlocalid>
L3SW> config router bgp4 peer peerid 10.0.0.3 10.0.0.2
```

```
L3SW> config router bgp4 peer remoteas <peeripaddr> <peerasnumber>
L3SW> config router bgp4 peer remoteas 10.0.0.3 1

L3SW> config router bgp4 peer remoteport <peeripaddr> <peertcpport>
L3SW> config router bgp4 peer remoteport 10.0.0.3 2000
```

これらのピアパラメータは、BGP セッションに強く関連付けられているため、reset か stop コマンドの実行後にパラメータを変更して、start コマンドを実行することを推奨します。

```
L3SW> config router bgp peer reset 10.0.0.3
```

または

```
L3SW> config router bgp peer adminstatus 10.0.0.3 stop
.....
L3SW> config router bgp peer adminstatus 10.0.0.3 start
```

ピアルータID、AS 番号、ピアポート番号の設定は、両方のスピーカ間で同期させる必要があります。同期を行わないと、ピアによる TCP 接続がダウンすることがあります。

6.9.2.2.6 セッションパラメータ

本製品では、次の TCP セッションパラメータの変更が可能です。

- Hold time

Hold Time 値は、2 つの連続する KEEPALIVE または UPDATE メッセージ経過時間（秒）を定義します。ローカルの値がピアに送られた OPEN パケットで伝わると、ルータはローカル「Hold Time」と受信した「Hold Time」のうち小さい数を選択します。Hold Time が経過すると、TCP セッションはリセットされ再起動します。

- Keep-alive interval

Keep-alive タイマは、ピアに送られる KEEPALIVE メッセージの間隔（秒）を定義します。

- Connection retry interval

Connection retry interval は、ピアに対する BGP セッション設定の再試行間隔（秒）を定義します。

- Minimum AS Origination Interval

このタイマは、BGP スピーカが属する AS 内での変更を報告する UPDATE アドバタイズの最小送信間隔を設定します。

- Minimum Route Advertise Interval

このタイマは、1 つの BGP スピーカから特定の宛先までのルートに関するアドバタイズの最小送信間隔を設定します。

1） ピア伝送キューに格納可能な最大メッセージ数

2） msgSendLimit パケットの伝送セッション間の遅延インターバル

本製品では、RFC1771 で定められた推奨値をデフォルト値にしています。また、RFC1771 の規

定に基づいて、タイマを変更するコマンドを用意しています。ただし、通常はタイマを頻繁に変更する必要はありません。パラメータを変更する場合は、次のコマンドを実行します。

L3SW> config router bgp4 peer holdtime <peeripaddr> <seconds>
```
L3SW> config router bgp4 peer holdtime 100
```

L3SW> config router bgp4 peer keepalive <peeripaddr> <seconds>
```
L3SW> config router bgp4 peer keepalive 40
```

L3SW> config router bgp4 peer msgsendlimit <peeripaddr> <sendlimit>
```
L3SW> config router bgp4 peer msgsendlimit 120
```

L3SW> config router bgp4 peer txdelayint <peeripaddr> <seconds>
```
L3SW> config router bgp4 peer txdelayint 4
```

L3SW> config router bgp4 peer connretryint <peeripaddr> <seconds>
```
L3SW> config router bgp4 peer connretryint 120
```

L3SW> config router bgp4 interval minasorigin <seconds>
```
L3SW> config router bgp4 interval minasorigin 2
```

L3SW> config router bgp4 minrouteadvint <seconds>
```
L3SW> config router bgp4 minrouteadvint 3
```

ピア側のタイマ値は、ローカルでの変更に合わせて変更することを推奨します。

6.9.2.2.7 ピア情報の表示

ピア情報を表示する場合は、次のコマンドをそれぞれ実行します。

- ピアの詳細:このコマンドでは、特定のピアに関する設定の詳細とセッション状況を表示します。ピアの設定確認と状況のモニタが可能です。

  ```
  L3SW> show router bgp4 peer info 10.1.1.10
  ```

```
L3SW>show router bgp4 peer info 10.1.1.10

Remote Address..................... 10.1.1.10
Peer ID............................ 10.1.1.1
Peer Admin Status.................. START
Peer State......................... OPEN-SENT
Local Port......................... 179
Remote AS.......................... 2
Remote Port........................ 179
Connection Retry Interval........ 120
Confederation Member.............. Disable
Optional Capabilities............. None
Route Reflector Mode.............. Disable
Next Hop Self Mode................ Disable
Authentication Code............... No Authentication
Local Interface Address.......... 10.1.1.10
Message Send Limit................ 100
Transmission Delay Interval...... 5
Negotiated Version................ 0
Configured Hold Time.............. 90
Configured Keep Alive Time....... 30

L3SW>
```

表 6-31:BGP ピア情報の表示

- ピアのリスト:BGP でのピアをすべて表示する場合は、次のコマンドを実行します。

```
L3SW> show router bgp4 peer list
```

```
L3SW>show router bgp4 peer list

S.No Peer Address
---- ------------
 1   10.1.1.10
 2   11.1.1.10

L3SW>
```

表 6-32:BGP ピアリストの表示

- ピアの統計情報:ピア ID や管理状況、アップデートパケットの送受信、メッセージ送受信数のサマリ、イベントなどのピアに関する統計データを表示します。

```
L3SW> show router bgp4 peer stats 10.1.1.10
```

```
L3SW>show router bgp4 peer stats 10.1.1.10

Remote Address ..................  10.1.1.10
Peer Admin Status ...............  START
Updates Received ................0
Updates Sent ....................  0
Total Messages Received .........0
Total Messages Sent .............  21
Last Error ......................  None
Established Transitions .........  0
Established Time ................  0 day 0 hr 0 min 0 sec
Time Elapsed since Last Update ..  0 day 0 hr 0 min 0 sec

L3SW>
```

表 6-33:BGP ピア統計データの表示

6.9.2.3 BGP NLRI 設定

現在、IGP と BGP 間のルート再配布には対応していません。したがって、AS 内部のルータに対する NLRI(ネットワーク層到達可能性情報)を設定して、BGP ルータから他の BGP ピアにスタティック NLRI をアドバタイズ可能にする必要があります。

6.9.2.3.1 スタティック NLRI の追加

スタティック NLRI を NLRI リストに追加する場合は、次のコマンドを実行します。

```
L3SW> config router bgp4 nlri add <prefix> <prefixlen> <vpncos> <nexthop> <send/donotsend>
L3SW> config router bgp4 nlri add 20.0.0.0 8 0 10.0.0.1 send
```

現行のリリースは、VPN/COS 識別子の定義に使用する<vpncos>オプションに対応していません。したがって、このフィールドには 0 を指定してください。

BGP は CIDR に対応しているので、prefixlen フィールドには 8/16/24 以外の値を入力することもできます。

6.9.2.3.2 スタティック NLRI の削除

スタティック NLRI を削除する場合は、次のコマンドを実行します。

```
L3SW> config router bgp4 nlri delete <prefix> <prefixlen>
L3SW> config router bgp4 nlri delete 20.0.0.0 8
```

6.9.2.3.3 NLRI リストの表示

BGR NLRI リスト(ピアから学習したエントリとスタティックに設定されたエントリをすべて含む)を表示する場合は、次のコマンドを実行します。

```
L3SW> show router bgp4 nlrilist
```

```
L3SW>show router bgp4 nlrilist

Prefix/len    NextHop     VpnCosId  Send Now
------------ ------------ --------- ---------
20.0.0.0/8    10.0.0.1      0      send

L3SW>
```

表 6-34:BGP NLRI リストの表示

6.9.2.4 パス属性

6.9.2.4.1 BGP ローカルパス設定の表示

ルートオリジン、MED、ローカル優先度、サプレスモード、コミュニティ、ネクストホップアドレス長、パス集約モード、アドレス集約モードなどのローカルパス設定は、すべて次のコマンドによって検索できます。

```
L3SW> show router bgp4 pathlocalparms
```

```
L3SW>show router bgp4 pathlocalparms

Route Origin ..................................  None
Route MED .....................................N/A
Route Local Preference ........................  N/A
Suppress Mode .................................  Disable
Route Community ...............................  N/A
Wext Hop Address Length .......................32
Path Attribute Aggregation Mode ...............  Disable
Address Aggregation Mode ......................  Enable

L3SW>
```

表 6-35:BGP ローカルパス設定の表示

6.9.2.4.2 BGP パス属性の表示

各 NLRI に格納された、Peer ID、Prefix、Prefix Length、Origin、AS-PATH、MED、NextHop、Local Preference、AtomicAggr、AggrAs、Aggregator、CalcLocalPref、Best などのパス属性を検索する場合は、次のコマンドを実行します。

```
L3SW> show router bgp4 pathattrtable
```

```
L3SW>show router bgp4 pathattrtable
Peer ..........................  10.1.1.3
Prefix/Length ................  10.1.5.0/24
Origin. .......................  egp
AsPath. .......................
NextHop .......................  10.1.1.3
MultiExitDiEsc ................  -1
LocalPref. ....................  -1
AtomicAggr. ...................  Less Specific Route Not Selected
AggrAS ........................  0
Aggregator ....................  0.0.0.0
CalcLocalPref .................  0
Best ..........................  False
Unknown .......................

—More— or (q)uit
Peer ..........................  10.1.1.3
Prefix/Length ................  10.1.6.0/24
Origin.........................egp
AsPath. .......................
NextHop .......................  10.1.1.3
MultiExitDisc .................  -1
LocalPref. ....................  -1
AtomicAggr ....................  Less Specific Route Mot Selected
AggrAS ........................  0
gregator ......................  0.0.0.0
CalcLocalPref. ................  0
Best...........................False
Unknown. ......................

L3SW>
```

表 6-36：BGP パス属性テーブルの表示

6.9.2.4.3　　ローカルルートオリジンの設定

NLRI ローカルルートオリジンに対する ORIGIN 属性を設定する場合は、次のコマンドを実行します。

```
L3SW> config router bgp4 localorigin <origin>
L3SW> config router bgp4 localorigin igp
```

6.9.2.4.4　　ルート MED の設定

NLRI ローカルオリジンに対する MED 属性を設定する場合は、次のコマンドを実行します。

```
L3SW> config router bgp4 localmed <localmed>
L3SW> config router bgp4 localmed 80
```

6.9.2.4.5　　ローカル優先度の設定

NLRI ローカルオリジンに対する LOCAL PREFERENCE 属性を設定する場合は、次のコマンドを実行します。

L3SW> config router bgp4 localpref <localpref>
L3SW> config router bgp4 localpref 100

6.9.2.4.6 パス属性集約モードの有効／無効

NLRI ローカルオリジンに対する path aggregation 属性を設定する場合は、次のコマンドを実行します。

L3SW> config router bgp4 pathattraggr <enable/disable>
L3SW> config router bgp4 pathattraggr enable

6.9.2.5 BGP ルート集約

BGP は AS 間ルーティングプロトコルなので、CIDR にも対応しています。 BGP トラフィックのオーバーヘッドを防ぐには、ルート集約が有効であり、すべての BGP ルータが対応しています。ルート集約には、操作が適切に行われないとルーティングループが生じかねないという問題があります。BGP NLRI ではパスが通過するすべての AS を AS-PATH で記録しますが、AS-PATH では非集約ルートでのルーティングループしか防止できません。したがって、ルート集約はネットワーク管理者によって慎重に行われる必要があります。その他に、ルート集約活動を記録するために次の属性があります。

- AGGREGATOR:集約が行われる AS 番号とルータを表示します。
- ATOMIC_AGGREGATE:自分自身のピアの 1 つから重複ルートの組を受け取り、限定性の低いルートを選択した BGP ルータを表示します。

本製品では、ルータは集約モードでも非集約モードでも動作できます。集約モードでは、集約ルートでまとめることができる、特定のルートに一致する各ルートすべてを集約ルートで置き換えるように定義することができます。

6.9.2.5.1 ルート集約設定の表示

ルート集約設定を表示する場合は、次のコマンドを実行します。

L3SW> show router bgp4 aggrlist

```
L3SW>show router bgp4 aggrlist
Address Aggregation Mode ......................  Enable
   Prefix/Len     Aggr Effect  Adv Unfeasible
   ------------  ------------ ---------------
   10.1.0.0/16   advertise    feasible
L3SW>
```

表 6-37:BGP 集約リストの表示

6.9.2.5.2 ルート集約モードの有効化

デフォルトでは、ルート集約モードは無効になっています。集約モードが無効になっている場合、入力パスについてはいかなる集約も実行されません。ルート集約設定を有効にする場合は、次のコマンドを実行します。

L3SW> config router bgp4 addraggr mode <enable/disable>

```
L3SW> config router bgp4 addraggr mode enable
```

6.9.2.5.3 集約アドレスの生成

ルート集約は、ネットワーク管理者が実行します。集約ルートの設定では、ルート集約の範囲を制限する必要があります。集約ルートが設定されて他のピアにアドバタイズされる場合でも、集約ルータでは集約ルートの一部である非集約ルートを維持する必要があります。

例えば、ルータ A に集約可能ルート 10.1.0.0/16 が設定され、アドバタイズ可能であるとします。また、ルータ A のピアの 1 つであるルータ B は、パス 10.1.1.0/24 をアドバタイズし、もう 1 つのピアルータ C はパス 10.1.2.0/24 をアドバタイズするとします。その結果、ルータ A は自分自身の NLRI データベースに、10.1.1.0/24 と 10.1.2.0/24、10.1.0.0/16 の 3 本のパスを維持することになります。以上の条件で、ルータ A はルータ D には集約パス 10.1.0.0/16 を、ルータ C にはルータ B から学習した非集約パス 10.1.1.0/24 を、ルータ B にはルータ C から学習した非集約パス 10.1.2.0/24 を伝えます。アドレス集約を利用する場合は、次のコマンドを実行します。

```
L3SW> config router bgp4 addraggr create <prefix> <prefixlen> <advertise/donotadvertise>
<feasible/unfeasible>
L3SW> config router bgp4 addraggr create 10.1.0.0 16 advertise feasible
```

6.9.2.5.4 集約アドレスの削除

集約アドレスを削除するには、次のコマンドを実行します。

```
L3SW> config router bgp4 addraggr delete <prefix> <prefixlen>
L3SW> config router bgp4 addraggr delete 10.1.0.0 16
```

6.9.2.5.5 アドバタイズの有効／無効

集約アドレスのアドバタイズを有効または無効にするには、次のコマンドを実行します。

```
L3SW> config router bgp4 addraggr update <prefix> <prefixlen> <advertise/donotadvertise>
L3SW> config router bgp4 addraggr update 10.1.0.0 16 advertise
```

6.9.2.6 BGP コミュニティの設定

本製品では BGP コミュニティに対応して、ルーティング決定が適用可能な宛先をグループに分けています。デフォルトでは、ルートはインターネットコミュニティに属していますが、さらに複数のコミュニティに属することも可能です。

COMMUNITY は NLRI 属性についてのオプションです。show router bgp4 pathlocalparms コマンドによって確認や検索ができます。また、ローカル AS 番号でコミュニティ番号を指定し、コミュニティでのオプション機能を有効にする必要があります。

6.9.2.6.1 コミュニティの設定

LOCAL COMMUNITY 属性を設定する場合は、次のコマンドを実行します。

```
L3SW> config router bgp4 routecomm <community>
L3SW> config router bgp4 routecomm 10
```

6.9.2.6.2 コミュニティの有効／無効

COMMUNITY 属性を有効にする場合は、次のコマンドを実行します（オプション設定を表示する

場合は、show router bgp4 info コマンドを実行します）。

```
L3SW> config router bgp4 optionalcap <option> <enable/disable>
L3SW> config router bgp4 optionalcap community enable
```

1 台のルータが複数のコミュニティに属することはできません。コミュニティ番号に関する新たな設定は、以前の番号にも影響します。

6.9.2.7 BGP コンフェデレーション

本製品では BGP コンフェデレーションに対応することで AS をより小さなドメインに分割し、IBGP ピア間の完全なメッシュセッションを減少させています。コンフェデレーションは CONFEDERATION ID で識別されます。コミュニティの場合と同様に、コンフェデレーションでのオプション機能を有効にする必要があります。

show router bgp4 pathlocalparms コマンドは、設定の確認や検索を行います。show router bgp4 info コマンドは、スイッチによって定義されたオプション機能の確認や検索を行います。

6.9.2.7.1 コンフェデレーション ID の設定

コンフェデレーション ID を設定する場合は、次のコマンドを実行します。

```
L3SW> config router bgp4 confedid <confedid>
L3SW> config router bgp4 confedid 100
```

6.9.2.7.2 コンフェデレーションの有効／無効

コンフェデレーションを有効にする場合は、次のコマンドを実行します。

```
L3SW> config router bgp4 optionalcap <option> <enable/disable>
L3SW> config router bgp4 optionalcap confed enable
```

1 台のルータが複数のコンフェデレーションに属することはできません。新たな設定は、以前の番号にも影響します。

6.9.2.8 BGP ルートリフレクタ設定

本製品では BGP ルートリフレクタに対応することで、IBGP ピア間での完全なメッシュセッションを回避します。ルートリフレクタは、IBGP ピアをクライアントピアと非クライアントピアに分割します。ルートリフレクタは、クライアントピアから他のクライアントピアや非クライアントピアに NLRI 受信を伝えます。ルートリフレクタはクライアントピアとともに、クラスタ ID で識別されるクラスタを形成します。

6.9.2.8.1 クラスタ ID の設定

クラスタ ID を設定する場合は、次のコマンドを実行します。

```
L3SW> config router bgp4 clusterid <clusterid>
L3SW> config router bgp4 clusterid 0.0.0.2
```

6.9.2.8.2 ルートリフレクトの有効／無効

ルートリフレクトを有効にする場合は、次のコマンドを実行します。

L3SW> config router bgp4 routereflect <enable/disable>
L3SW> config router bgp4 routereflect enable

6.9.2.8.3 オプション機能の有効化

オプション機能を有効にする場合は、次のコマンドを実行します。

L3SW> config router bgp4 optionalcap <option> <enable/disable>
L3SW> config router bgp4 optionalcap routereflect enable

クライアントサイドの設定では、ルートリフレクトを有効にする必要はありません。

6.9.2.9 BGP ポリシーの設定

本製品の BGP ポリシーは、<matchtype>というオブジェクトに関して次の操作を実行する場合に使用されます。

- Route filtering
- Route mapping
- Route attribute modification
- NLRI filtering

6.9.2.9.1 ポリシーの表示

本製品で利用可能なポリシーを表示する場合は、次のコマンドを実行します（ポリシインデックス番号、プロトコルタイプ、アクセスモード、マッチタイプが表示されます）。

L3SW> show router bgp4 policy summary

```
L3SW>show router bgp4 policy summary

                                    Permit
Index    Protocol     MatchType     Deny
------ ------------- ----------- --------
1      bgpinternalin  Peer         Permit

L3SW>
```

表 6-38：BGP ポリシーの表示

特定のポリシ番号に関する詳細情報を表示する場合は、次のコマンドを実行します。

L3SW> show router bgp4 policy detailed 1

```
L3SW>show router bgp4 policy detailed 1

Policy Index..................................... 1
Protocol ID...................................... bgpinternalin
Access Mode...................................... permit
Match Type....................................... Peer
Range IP Address.................  10.1.1.10/255.255.255.255

Action Type    MatchType        Value
------------  -----------------  ------
Add           Multi Exit Disc    100
L3SW>
```

表 6-39:BGP ポリシーの詳細表示

6.9.2.9.2 ポリシーの生成

ポリシーの生成は、次の 3 つのステップで行います。

- ポリシーの生成
- ポリシーの<matchtype>に対して、範囲を関連付け
- ポリシーに対するアクションの定義

最初の 2 つのステップでは BGP データベースから適格ルートや NLRI を選択し、最後のステップでは選択したルートや NLRI での操作とアクションを定義します。これを要約すると、次のようになります。

- ポリシーインデックスの作成とパケットフローの定義(インおよびアウト)
- <matchtype>条件一致の定義
- 一致した場合のアクションの定義

ポリシーを生成する前に、show router bgp4 policy summary コマンドを実行して既存のポリシーをチェックし、既存のポリシーで使用されていないインデックス番号の取得を促すメッセージが表示されます。このインデックス番号は、その後の設定や確認の際にポリシ ID として使用できます。

L3SW> config router bgp4 policy create <index> <access> <protocol> <matchtype>
L3SW> config router bgp4 policy create 1 permit bgpinternalin peer

access モードとして、“許可”または“拒否”を設定します。protocol は、bgpinternalin か bgpinternalout のどちらかを設定します。bgpinternalin は受信 matchtype に対するフィルタで、bgpinternalout は送信 matchtype に対するフィルタです。matchtype は、フィルタのためのキータイプを定義します。

6.9.2.9.3 ポリシーに対する範囲の関連付け

ポリシーが生成されると、policy ID、access mode、matchType が定義されます。すでに説明したように、matchtype で定義されるのはフィルタリングのキータイプだけです。実際のキー値は範囲で定義します。異なる matchtype に対しては、別々の範囲設定コマンドを使用します。例えば、IP アドレスで識別する matchtype を設定した場合は、config router bgp4 policy range address コマンドを実行します。整数値で識別する場合は、config router bgp4 policy between

(equal, greatthan, lessthan)コマンドを実行します。BGP ポリシー設定コマンドの使い方については、次の例を参照してください。

```
L3SW> config router bgp4 policy range address <index> <peerlocalid> <mask>
L3SW> config router bgp4 policy range address 1 10.1.1.10 255.255.255.255

L3SW> config router bgp4 policy range between <index> <minvalue> <maxvalue>
L3SW> config router bgp4 policy range between 1 5 10

L3SW> config router bgp4 policy range equal <index> <value>
L3SW> config router bgp4 policy range equal 1 equal 5

L3SW> config router bgp4 policy range greaterthan <index> <value>
L3SW> config router bgp4 policy range greaterthan 1 5

L3SW> config router bgp4 policy range lessthan <index> <value>
L3SW> config router bgp4 policy range lessthan 1 10
```

6.9.2.9.4 ポリシーに対するアクションの定義

ポリシーによりルートのフィルタリングに使用される、ルートや NLRI エントリに対するアクション（特定の属性の追加、削除、変更）の定義を定義することができます。ポリシーアクションを追加／削除する場合は、次のコマンドを実行します。

```
L3SW> config router bgp4 policy action addip add <index> <matchtype> <ipaddr>
L3SW> config router bgp4 policy action addip add 1 nexthop 10.1.1.9

L3SW> config router bgp4 policy action addip delete <index> <matchtype> [ipaddr]
L3SW> config router bgp4 policy action addip delete 1 nexthop 10.1.1.9

L3SW> config router bgp4 policy action addip modify <index> <matchtype> [ipaddr]
L3SW> config router bgp4 policy action addip modify 1 nexthop 10.1.1.8
```

addip の場合の matchtype としては、clusternumber、destippref、nexthop、per、aggregatorid が使用できます。

```
L3SW> config router bgp4 policy action addint add <index> <matchtype> <value>
L3SW> config router bgp4 policy action addint add 1 localpreference 100

L3SW> config router bgp4 policy action addint delete <index> <matchtype> [value]
L3SW> config router bgp4 policy action addint delete 1 localpreference

L3SW> config router bgp4 policy action addint modify <index> <matchtype> [value]
L3SW> config router bgp4 policy action addint add 1 localpreference 90
```

addint の場合の matchtype には、aspath、origin、localpreference、multiexitdisc、community、cofederationid、aspathlen、protocolid、ospfdestinationtype、atomicaggregate、aggregators が使用できます。

アクション定義の際の matchtype は、ポリシー生成の際の matchtype 定義と異なっていてもかまいません。

```
L3SW> config router bgp4 policy action remove <index> <matchtype>
L3SW> config router bgp4 policy action remove 1 localpreference
```

6.9.2.9.5 ポリシーの例

1) トラフィック内のピアを拒否する場合は、次のコマンドを実行します。

```
L3SW-1> config router bgp4 policy create 124 permit bgpinternalin peer
L3SW-1> config router bgp4 policy range address 124 10.1.1.20
255.255.255.255
```

2) ピアの外側のローカル優先度に 160 を追加する場合は、次のコマンドを実行します。

```
L3SW-1> config router bgp4 policy create 124 permit bgpinternalout peer
L3SW-1> config router bgp4 policy range address 124 10.1.1.20
255.255.255.255
L3SW-1> config router bgp4 policy action addint add 124 localpreference
160
```

3) ミュニティの範囲をピアから 100 までに変更する場合は、次のコマンドを実行します。

```
L3SW-1> config router bgp4 policy create 123 permit bgpinternalin peer
L3SW-1> config router bgp4 policy range address 123 10.1.1.30
255.255.255.255
L3SW-1> config router bgp4 policy action addint modify 123 community 100
```

4) 50 以上 500 未満のコミュニティで、パケットに対するローカル優先度を削除する場合は、次のコマンドを実行します。

```
L3SW-1> config router bgp4 policy create 123 permit bgpinternalin
community
L3SW-1> config router bgp4 policy range greaterthan 123 50
L3SW-1> config router bgp4 policy range lessthan 123 500
L3SW-1> config router bgp4 policy action addint delete 123
localpreference
```

6.9.3 BGP の例

6.9.3.1 BGP の例 1

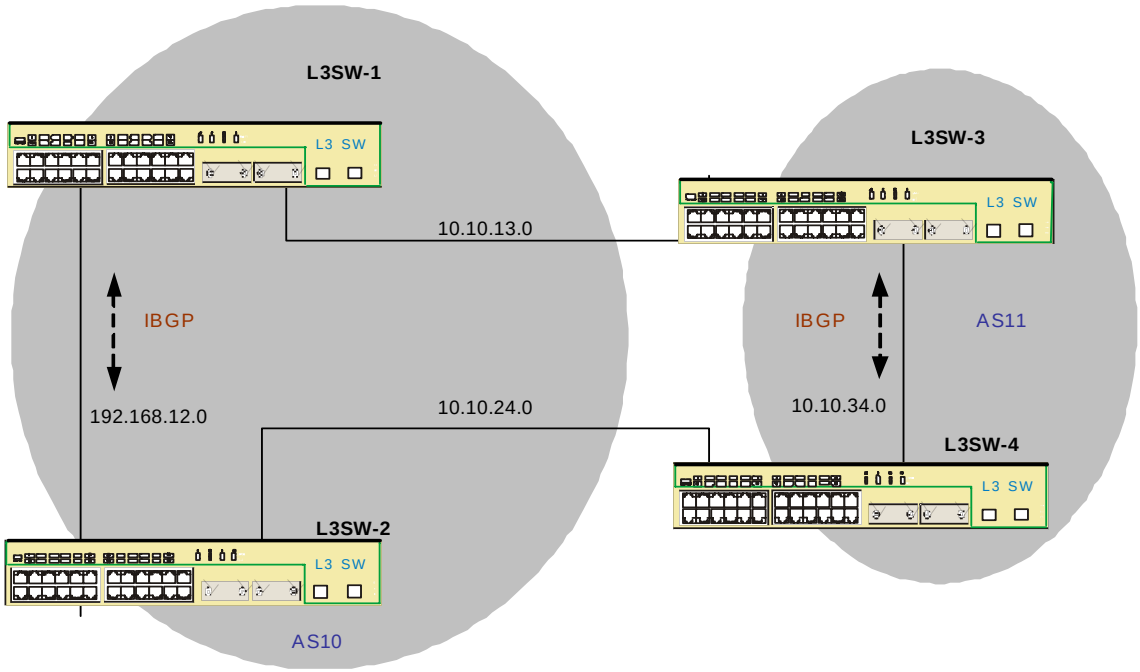

図 6-9:本製品 4 台による BGP 構成

例では、AS10 と AS11 のどちらでも 2 台の BGP ルータが IBGP セッションで接続しています。また、この 2 つの AS 間では、ルータ 1 が EBGP セッションでルータ 3 に、ルータ 2 が同じく EBGP セッションでルータ 4 に接続しています。この 2 つの EBGP セッションによって、一方の接続ポイントがダウンした場合に備えた冗長リンクが設定されています。

ルータ 1

- インタフェースを設定する

```
L3SW-1> config ip port create 0.1 192.168.12.1 255.255.255.0
L3SW-1> config ip port create 0.2 10.10.13.1 255.255.255.0
```

- ルータ ID 設定とルーティングの有効化

```
L3SW-1> config router id 10.10.13.1
L3SW-1> config routing enable
```

- BGP ルータ ID、AS 番号の定義と BGP の有効化

```
L3SW-1> config router bgp4 localid 10.10.13.1
L3SW-1> config router bgp4 asnumber 10
L3SW-1> config router bgp4 adminmode enable
```

- BGP ピアの定義

```
L3SW-1> config router bgp4 peer create 192.168.12.2 10 10.10.24.1
L3SW-1> config router bgp4 peer localintf 192.168.12.2 192.168.12.1
L3SW-1> config router bgp4 peer create 10.10.13.2 11 10.10.13.2
L3SW-1> config router bgp4 peer localintf 10.10.13.2 10.10.13.1
```

- NLRI の定義

```
L3SW-1> config router bgp4 nlri add 192.168.12.0 24 0 10.10.13.1
```

- 設定の確認

```
L3SW-1> show router bgp4 peer info 192.168.12.2
L3SW-1> show router bgp4 peer info 10.10.13.2
L3SW-1> show router bgp4 info
L3SW-1> show router bgp4 nlrilist
```

- ピアの起動

```
L3SW-1> config router bgp4 peer adminstatus 192.168.12.2 start
L3SW-1> config router bgp4 peer adminstatus 10.10.13.2 start
```

ルータ 2

- インタフェースを設定する

```
L3SW-2> config ip port create 0.1 192.168.12.2 255.255.255.0
L3SW-2> config ip port create 0.2 10.10.24.1 255.255.255.0
```

- ルータ ID の変更とルーティングの有効化

```
L3SW-2> config router id 10.10.24.1
L3SW-2> config routing enable
```

- BGP ルータ ID、AS 番号の定義と BGP の有効化

```
L3SW-2> config router bgp4 localid 10.10.24.1
L3SW-2> config router bgp4 asnumber 10
L3SW-2> config router bgp4 adminmode enable
```

- BGP ピアの定義

```
L3SW-2> config router bgp4 peer create 192.168.12.1 10 10.10.13.1
L3SW-2> config router bgp4 peer localintf 192.168.12.1 192.168.12.2
L3SW-2> config router bgp4 peer create 10.10.24.2 11 10.10.24.1
L3SW-2> config router bgp4 peer localintf 10.10.24.2 10.10.24.1
```

- NLRI の定義

```
L3SW-2> config router bgp4 nlri add 192.168.12.0 24 0 10.10.24.1
```

- 設定の確認

```
L3SW-2> show router bgp4 peer info 192.168.12.1
L3SW-2> show router bgp4 peer info 10.10.24.2
L3SW-2> show router bgp4 info
L3SW-2> show router bgp4 nlrilist
```

- ピアの起動

```
L3SW-2> config router bgp4 peer adminstatus 192.168.12.1 start
L3SW-2> config router bgp4 peer adminstatus 10.10.24.2 start
```

ルータ 3

- インタフェースを設定する

```
L3SW-3> config ip port create 0.1 10.10.34.1 255.255.255.0
L3SW-3> config ip port create 0.2 10.10.13.2 255.255.255.0
```

- ルータ ID 設定とルーティングの有効化

```
L3SW-3> config router id 10.10.13.2
L3SW-3> config routing enable
```

- BGP ルータ ID、AS 番号の定義と BGP の有効化

```
L3SW-3> config router bgp4 localid 10.10.13.2
L3SW-3> config router bgp4 asnumber 11
L3SW-3> config router bgp4 adminmode enable
```

- BGP ピアの定義

```
L3SW-3> config router bgp4 peer create 10.10.13.1 10 10.10.13.1
L3SW-3> config router bgp4 peer localintf 10.10.13.1 110.10.13.2
L3SW-3> config router bgp4 peer create 10.10.34.2 11 10.10.24.2
L3SW-3> config router bgp4 peer localintf 10.10.34.2 10.10.34.1
```

- NLRI の定義

```
L3SW-3> config router bgp4 nlri add 10.10.34.0 8 0 10.10.34.1
```

- 設定の確認

```
L3SW-3> show router bgp4 peer info 10.10.13.1
L3SW-3> show router bgp4 peer info 10.10.34.2
L3SW-3> show router bgp4 info
L3SW-3> show router bgp4 nlrilist
```

- ピアの起動

```
L3SW-3> config router bgp4 peer adminstatus 10.10.13.1 start
L3SW-3> config router bgp4 peer adminstatus 10.10.34.2 start
```

ルータ 4

- インタフェースを設定する

```
L3SW-4> config ip port create 0.1 10.10.24.2 255.255.255.0
L3SW-4> config ip port create 0.2 10.10.34.2 255.255.255.0
```

- ルータ ID 設定とルーティングの有効化

```
L3SW-4> config router id 10.10.24.2
L3SW-4> config routing enable
```

- BGP ルータ ID、AS 番号の定義と BGP の有効化

```
L3SW-4> config router bgp4 localid 10.10.24.2
L3SW-4> config router bgp4 asnumber 11
L3SW-4> config router bgp4 adminmode enable
```

- BGP ピアの定義

```
L3SW-4> config router bgp4 peer create 10.10.24.1 10 10.10.24.1
L3SW-4> config router bgp4 peer localintf 10.10.24.1 10.10.24.2
L3SW-4> config router bgp4 peer create 10.10.34.1 11 10.10.13.2
L3SW-4> config router bgp4 peer localintf 10.10.34.1 10.10.34.2
```

- NLRI の定義

```
L3SW-4> config router bgp4 nlri add 10.10.34.0 8 0 10.10.34.2
```

- 設定の確認

```
L3SW-4> show router bgp4 peer info 10.10.34.1
```

```
L3SW-4> show router bgp4 peer info 10.10.24.1
L3SW-4> show router bgp4 info
L3SW-4> show router bgp4 nlrilist
```

- **ピアの起動**

```
L3SW-4> config router bgp4 peer adminstatus 10.10.34.1 start
L3SW-4> config router bgp4 peer adminstatus 10.10.24.1 start
```

6.9.3.2 BGP Example 2

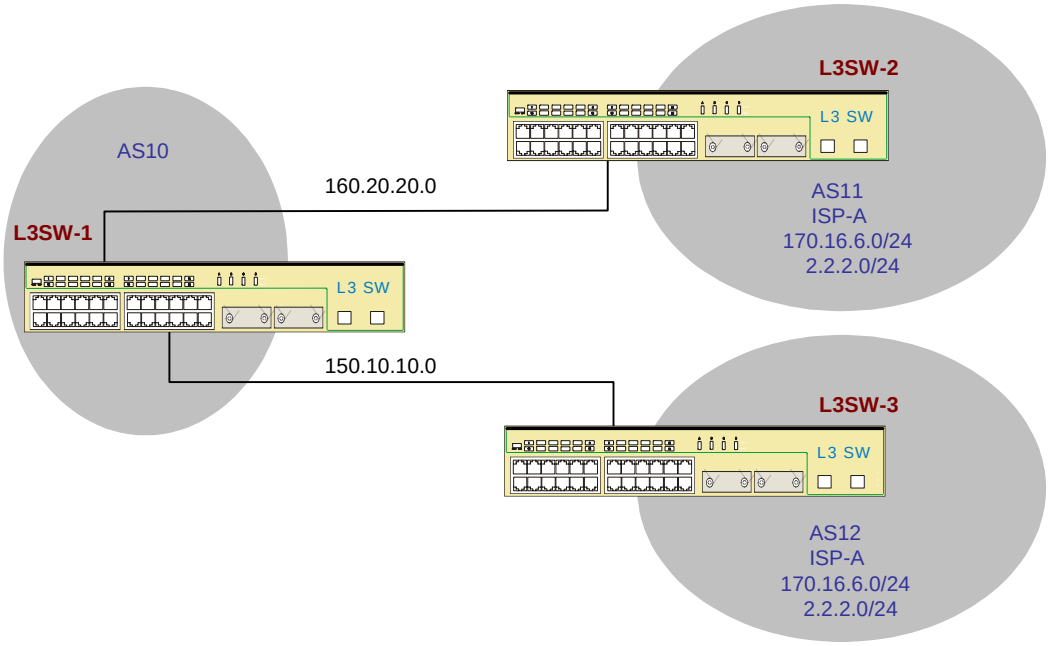

図 6-10:本製品 3 台による BGP 構成

この例では、ルータ 1 は別々の ISP に属している 2 つの EBGP ピアに接続しています。ルータ 1 とルータ 2 は、宛先 170.16.6.0/24 と 2.2.2.0/24 に宛ててルーティング情報を送ります。

ポリシーにより、ルータ 2 はインターネットにアクセスする一次ルータとして他のルータに優先します。ルータ 2 から学習したルートに対してより低い MED 番号を設定することで可能です。ルータ 1 とルータ 2 の間のリンクがダウンした場合、ルータ 1 はインターネットへのアクセスをルータ 3 に切り替えます。

例で使用したルータの設定には、次のコマンドを実行します。

ルータ 1

- **ルータ ID 設定とルーティングの有効化**

```
L3SW-1> config ip port create 0.1 160.20.20.1 255.255.255.0
L3SW-1> config ip port create 0.2 150.10.10.1 255.255.255.0
```

- **ルータ ID 設定とルーティングの有効化**

```
L3SW-1> config router id 150.10.10.1
L3SW-1> config routing enable
```

- BGP ルータ ID、AS 番号の定義と BGP の有効化

```
L3SW-1> config router bgp4 localid 150.10.10.1
L3SW-1> config router bgp4 asnumber 10
L3SW-1> config router bgp4 adminmode enable
```

- BGP ピアの定義

```
L3SW-1> config router bgp4 peer create 160.20.20.2 11 160.20.20.2
L3SW-1> config router bgp4 peer localintf 160.20.20.2 160.20.20.1
L3SW-1> config router bgp4 peer create 150.10.10.2 12 150.10.10.2
L3SW-1> config router bgp4 peer localintf 150.10.10.2 150.10.10.1
```

- Step 5:NLRI の定義

```
L3SW-1> config router bgp4 policy create 1 permit bgpinternalin peer
L3SW-1> config router bgp4 policy range address 1 160.20.20.2
255.255.255.255
L3SW-1> config router bgp4 policy action addint add multiexitdisc 1 90
L3SW-1> config router bgp4 policy create 2 permit bgpinternalin peer
L3SW-1> config router bgp4 policy range address 2 150.10.10.2
255.255.255.255
L3SW-1> config router bgp4 policy action addint add multiexitdisc 2 100
```

- 設定の確認

```
L3SW-1> show router bgp4 peer info 160.20.20.2
L3SW-1> show router bgp4 peer info 150.10.10.2
L3SW-1> show router bgp4 policytable
L3SW-1> show router bgp4 nlrilist
L3SW-1> show router bgp4 pathattrtable
L3SW-1> show router bgp4 info
```

- ピアの起動

```
L3SW-1> config router bgp4 peer adminstatus 160.20.20.2 start
L3SW-1> config router bgp4 peer adminstatus 150.10.10.2 start
```

ルータ 2

- インタフェースを設定する

```
L3SW-2> config ip port create 0.1 160.20.20.2 255.255.255.0
L3SW-2> config ip port create 0.2 10.10.10.1 255.255.255.0
```

- ルータ ID 設定とルーティングの有効化

```
L3SW-2> config router id 160.20.20.2
L3SW-2> config routing enable
```

- BGP ルータ ID、AS 番号の定義と BGP の有効化

```
L3SW-2> config router bgp4 localid 160.20.20.2
L3SW-2> config router bgp4 asnumber 11
L3SW-2> config router bgp4 adminmode enable
```

- BGP ピアの定義

```
L3SW-2> config router bgp4 peer create 160.20.20.1 10 150.10.10.1
L3SW-2> config router bgp4 peer localintf 160.20.20.1 160.20.20.2
```

- NLRI の定義

```
L3SW-2> config router bgp4 nlri add 170.16.6.0 24 0 10.10.10.1
L3SW-2> config router bgp4 nlri add 2.2.2.0 24 0 10.10.10.1
```

- 設定の確認

```
L3SW-2> show router bgp4 peer info 160.20.20.1
L3SW-2> show router bgp4 info
L3SW-2> show router bgp4 nlrilist
```

- ピアの起動

```
L3SW-2> config router bgp4 peer adminstatus 160.20.20.1 start
```

ルータ 3

- インタフェースを設定する

```
L3SW-3> config ip port create 0.1 150.10.10.2 255.255.255.0
L3SW-3> config ip port create 0.2 11.11.11.1 255.255.255.0
```

- ルータ ID 設定とルーティングの有効化

```
L3SW-3> config router id 150.10.10.2
L3SW-3> config routing enable
```

- BGP ルータ ID、AS 番号の定義と BGP の有効化

```
L3SW-3> config router bgp4 localid 150.10.10.2
L3SW-3> config router bgp4 asnumber 12
L3SW-3> config router bgp4 adminmode enable
```

- BGP ピアの定義

```
L3SW-3> config router bgp4 peer create 150.10.10.1 10 150.10.10.1
L3SW-3> config router bgp4 peer localintf 150.10.10.1 150.10.10.2
```

- NLRI の定義

```
L3SW-3> config router bgp4 nlri add 170.16.6.0 24 0 11.11.11.1
L3SW-3> config router bgp4 nlri add 2.2.2.0 24 0 11.11.11.1
```

- 設定の確認

```
L3SW-3> show router bgp4 peer info 150.10.10.1
L3SW-3> show router bgp4 info
L3SW-3> show router bgp4 nlrilist
```

- ピアの起動

```
L3SW-3> config router bgp4 peer adminstatus 150.10.10.1 start
```

7. セカンダリ IP アドレス

本製品のセカンダリ IP アドレス機能について説明します。

7.1 概要

セカンダリ IP アドレスは、さまざまな状況で利用できます。次にあげるのは、その最も典型的な例です。

- 特定のネットワークセグメントに十分なホストアドレスがない場合。例えば、ポート上のサブネット化で最大 254 のホストが接続可能だが、そのポートで 300 のホストアドレスをサポートできるようにしたい場合があります。この場合、ルータかアクセスサーバでセカンダリ IP アドレスを使用すると、1 つの物理ポートに 2 つの論理サブネットを設定することができます。
- 多数の古いネットワークが、レベル 2 のブリッジで構築されている場合。セカンダリ IP アドレスをうまく利用すれば、サブネット化されたルータベースのネットワークに移行することができます。ブリッジされた古いセグメント上のルータは、セグメントに存在する複数のサブネットを認識します。
- 1 つのネットワークの 2 つのサブネットが、別のネットワークにより分離される可能性がある場合。このような状況は、サブネットが使用中であれば起こりません。この場合、最初のネットワークを拡張するか、セカンダリ IP アドレスを使用する二次ネットワークの最上位にレイヤ化します。

7.2 セカンダリIP の設定

本製品の IP インタフェースにセカンダリ IP アドレスを設定するコマンドについて説明します。

- 次のコマンドを実行して、物理ポートに IP インタフェースを設定します。

  L3SW> config ip port create <physical slot.port> <ipaddr> <subnetmask> [vlanId]
  L3SW> config ip port create 0.1 172.10.1.1 255.255.255.0

- IP インタフェースに対してセカンダリ IP アドレスを割り当てるには、次のコマンドを実行します。

  L3SW> config ip interface networkid <virtual slot.port> <ipaddr> <subnetmask> <primary/secondary> [<add/remove> <routing-ignore/routing-passive>]
  L3SW> config ip interface networkid 4.1 172.10.2.1 255.255.255.0 secondary add

- セカンダリ IP インタフェースを削除する場合は、次のコマンドを実行します。

  L3SW> config ip interface networkid 4.1 172.10.2.1 255.255.255.0 secondary remove

パラメータの説明

- virtual slot port：論理インタフェースのスロットとポートの番号

- ipaddr: IP アドレス
- subnetmask – サブネットマスク
- primary/secondary:プライマリ IP アドレスとセカンダリ IP アドレスに対する設定入力オプションの選択に使用します。最大 128 のセカンダリサブネットを設定できます。
- add/remove:セカンダリ IP アドレスを追加または削除します。このオプションは、セカンダリ IP アドレス設定の場合にのみ必要です。
- routing-ignore/routing-passive:セカンダリ IP アドレスで動作させるルーティングの制限を追加するオプションです。このオプションは、セカンダリ IP アドレス設定に対してのみ有効です。なお、セカンダリ IP アドレスでのルーティングは、OSPF ルーティングドメインでしか実行できません。
- Routing-ignore:設定したセカンダリ IP アドレスに対して、ダイナミックルーティングを無効にします。
- Routing passive:セカンダリ IP アドレスでダイナミックルーティングは実行しないが、他のアクティブサブネットに対するアドバタイズは行います。

7.3 セカンダリIP 設定の表示

7.3.1 ルータ IP インタフェース要約情報の表示

プライマリアドレスとセカンダリアドレスを含む、すべての IP アドレスに対するルータインタフェースの要約情報を表示する場合は、次のコマンドを実行します。最初の行は次のように指定します。

L3SW> show router ip interface summary

```
L3SW>show router ip interface summary

                                        Netdir   Multi    InAccess OutAccess
Slot.Port IP Address      IP Mask       Bcast    CastFwd  Mode     Mode
--------- --------------- ------------- -------- -------- -------- -------
4.1       172.10.1.1      255.255.255.0 Disable  Disable  Disable  Disable
          172.10.2.1      255.255.255.0 Disable  Disable  Disable  Disable

L3SW>
```

表 7-1:ルータ IP インタフェース要約情報の表示

7.3.2 IP インタフェースの表示

すべての IP アドレス(論理ポートに割り当てられたプライマリアドレスとすべてのセカンダリアドレス)に加えて、IP インタフェースの詳細情報を表示する場合は、次のコマンドを実行します。

L3SW> show ip interface <slot.port>
L3SW> show ip interface 4.1

```
L3SW>show ip interface 4.1

Administrative Mode............................ Enable
Link Speed Data Rate........................... 100
MAC Address.................................... 00:50:A8:00:32:26
Maximum Transmission Unit...................... 1500
Encapsulation Type............................. Ethernet

IP               Subnet          Routing Forward Net  Active
Address           Mask            Mode   Direct BCST  State
---------------- --------------- -------- ----------- -------
172.10.1.1       255.255.255.0   Enable   Disable     Active
172.10.2.1       255.255.255.0   Enable   Disable     Active

L3SW>
```

表 7-2:IP インタフェースの表示

7.4 使用例

図 7-1 は、本製品 2 台が互いに物理ポート 0.1 で接続しています。この 2 台の設定は、次の各ステップで行います。

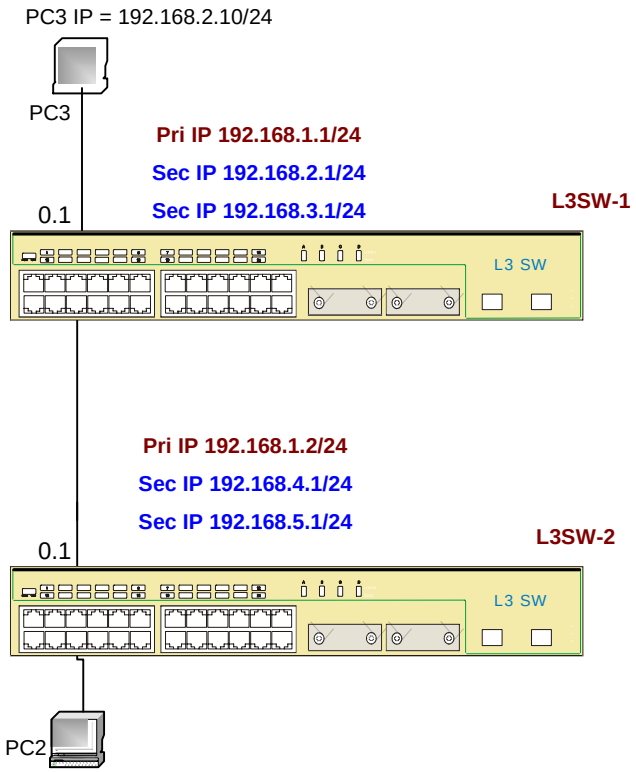

図 7-1:セカンダリ IP の設定例

- 本製品でルーティングを有効にする

```
L3SW-1> config routing enable
```

- 物理ポート 0.1 での IP インタフェース設定

```
L3SW-1> config ip port create 0.1 192.168.1.1 255.255.255.0
```

- 生成した IP インタフェースへのセカンダリ IP 追加

```
L3SW-1> config ip interface networkid 4.1 192.168.2.1 255.255.255.0
secondary add
L3SW-1> config ip interface networkid 4.1 192.168.3.1 255.255.255.0
secondary add
```

```
L3SW>show router ip interface summary

                                        Netdir   Multi    InAccess OutAccess
Slot.Port IP Address      IP Mask       Bcast    CastFwd  Mode     Mode
--------- --------------- ------------- -------- -------- -------- -------
4.1       192.168.1.1      255.255.255.0 Disable  Disable  Disable  Disable
          192.168.2.1      255.255.255.0 Disable  Disable  Disable  Disable
          192.168.3.1      255.255.255.0 Disable  Disable  Disable  Disable


L3SW>
```

表 7-3:IP インタフェース要約情報

- ルータ 2 のセカンダリインタフェースのためのスタティックルーティング生成

```
L3SW-1> config route route create 192.168.4.0 255.255.255.0 192.168.1.2
L3SW-1> config route route create 192.168.5.0 255.255.255.0 192.168.1.2
```

```
L3SW>show ip interface 4.1

Administrative Mode............................ Enable
Link Speed Data Rate........................... 100
MAC Address.................................... 00:50:A8:00:32:26
Maximum Transmission Unit...................... 1500
Encapsulation Type .............................Ethernet

IP              Subnet          Routing Forward Net  Active
Address          Mask            Mode   Direct BCST  State
--------------- --------------- -------- ----------- -------
192.168.1.1    255.255.255.0   Enable   Disable     Active
192.168.2.1    255.255.255.0   Enable   Disable     Active
192.168.3.1    255.255.255.0   Enable   Disable     Active

L3SW>
```

表 7-4:IP インタフェース詳細情報

- L3SW-2 でルーティングを有効にする

```
L3SW-2> config routing enable
```

- 物理ポート 0.1 での IP インタフェース設定

```
L3SW-2> config ip port create 0.1 192.168.1.2 255.255.255.0
```

- 生成した IP インタフェースへのセカンダリ IP 追加

```
L3SW-2> config ip interface networkid 4.1 192.168.4.1 255.255.255.0
secondary add
L3SW-2> config ip interface networkid 4.1 192.168.5.1 255.255.255.0
secondary add
```

- ルータ 2 のセカンダリインタフェースのためのスタティックルーティング生成

```
L3SW-2> config route route create 192.168.2.0 255.255.255.0 192.168.1.1
L3SW-2> config route route create 192.168.3.0 255.255.255.0 192.168.1.1
```

8. IP マルチキャストルーティング

IP マルチキャスティングは、ネットワークでの音声や画像のストリーム伝送に使用され、帯域幅とネットワークリソースを効率的に利用できます。IP マルチキャストストリームの配信は、IP マルチキャストグループのアドレスで定義されます。IP マルチキャストでは、マルチキャストサーバは指定したマルチキャストグループアドレス宛てのストリーム内部の各パケットに宛先アドレスを付けて、マルチキャストストリームを送信します。マルチキャストストリームは、ネットワークのマルチキャストルータによって、ストリームのグループアドレスを付けた sending out JOIN メッセージを使ってマルチキャストストリームの受信を表明しているクライアントやホストまでルーティングされます。

IPマルチキャストアドレスは、IANAに予約されている 224.0.0.0 から 239.255.255.255 までのクラスDアドレス空間に属します。IPマルチキャストグループアドレスの中には、224.0.0.0 や 224.0.0.1、224.0.0.2 のように、サブネット内のすべてのマルチキャストルータとグループに属するホストへのアドレッシングなど特別な使用のために予約されているものもあります。マルチキャストグループの予約アドレスのリストは、IANAのウェブサイトwww.iana.orgで参照できます。

IP マルチキャストプロトコルは、マルチキャストトラフィックを発信元からネットワーク内のトラフィック受信先に送信するため、ルータにより使用されます。本製品が対応するマルチキャストルーティングプロトコルは、次のとおりです。

- **インターネットグループ管理プロトコル（IGMP：Internet Group Management Protocol ）**
- **距離ベクトル型マルチキャストルーティングプロトコル（DVMRP：Distance Vector Multicast Routing Protocol）**
- **プロトコル非依存型マルチキャスト（PIM：Protocol Indepdendent Multicast）**

以下の項では、プロトコルの概要と本製品での設定について説明します。.

8.1 IGMP

インターネットグループ管理プロトコルは、LAN のホストとルータによって、LAN 内のホストが有するマルチキャストグループメンバー資格情報の交換に利用されます。LAN 上のルータは、ホストから送信される IGMP JOIN メッセージによって、ホストのマルチキャストグループメンバー資格を学習します。ホストから IGMP メッセージを受け取ったルータは、少なくとも 1 台のアクティブメンバーが存在すればマルチキャストグループアドレスのリストを維持します。IGMP プロトコルには、IGMPv1、IGMPv2、IGMPv3 の 3 種類のバージョンがあります。本製品では、IGMPv1 と IGMPv2 に対応しています。IGMPv3 については、将来のリリースで対応する予定です。

IGMPv1 では、ルータはすべてのマルチキャストグループのホスト宛てに、あるグループのアクティブメンバーが存在するかどうかを問うクエリを定期的に送信します。ホストはこのクエリを受け取ると、メンバー資格報告を送信して、自身が属するマルチキャストグループのグループアドレスを表示します。ルータ／スイッチ内のマルチキャストグループテーブルは、このメンバー資格報告を利用して更新されます。IGMPv1 と IGMPv2 の主要な違いは、IGMPv2 の場合、ホストは IGMP LEAVE メッセージを送信することで、自分自身が属するサブネットのルータ／スイッチに対して、グループからの脱退意思を伝えることができる点にあります。また、IGMPv2 では、同

じサブネットに属するルータの中から指名ルータとして定期的にクエリを送信するクエリの選出が行われます。

8.1.1 IGMP の設定

IGMP を設定します。

次の 5 つのステップで行います。

ステップ 1：ルーティングモードを有効にします。

詳しい設定については、「6.1.2 ルーティングモードの設定」(P.101)を参照

ステップ 2：物理ポート上のIPインタフェースを設定します。

詳しい設定については、「6.2.2.1 物理ポート上の IP インタフェースの設定」(P.106)を参照

ステップ 3：IGMP管理モードを有効にします。

ステップ 4：対象となる論理インタフェースポートでのIGMPを有効にします。

ステップ 1 と 2 は、他の機能における設定と同じです。ここでは IP インタフェース 4.1 と 4.2 がすでに設定済みという前提で、IGMP の設定について例をあげて説明します。

- **IGMP 管理モードの有効化**

```
L3SW> config router igmp adminmode <enable/disable>
L3SW> config router igmp adminmode enable
```

- **対象となる論理インタフェースポートでの IGMP の有効化**

```
L3SW> config router igmp interface mode <slot.port> <enable/disable>
L3SW> config router igmp interface mode 4.1 enable
L3SW> config router igmp interface mode 4.1 enable
```

次のコマンドを実行すると、スイッチのすべての論理インタフェースでの IGMP 管理状況を表示できます。

```
L3SW> show router igmp info
```

```
L3SW>show router igmp info


IGMP Admin Mode.............................  Disable

    IGMP INTERFACE STATUS
Slot.Port Interface Mode  Protocol State
--------- --------------- ---------------
4.1       Enable          Non-operational
4.2       Enable          Non-operational
4.3       Enable          Non-operational

L3SW>
```

表 8-1:IGMP スイッチ情報

IGMP インタフェースの関連情報は、次のコマンドによっても表示できます。

L3SW> config router igmp interface info <slot.port>
L3SW> show router igmp interface info 4.1

```
L3SW>show router igmp info


 Slot.Port     .............................  4.1
 IGMP Admin Mode............................. Disable
 Interface Mode.............................  Enable
 IGMP Version  .............................  2
 Query Interval (secs)..................... 125
 Query Max Resonse Time (1/10 of a second).. 100
 Robustness    .............................  2
 Startup Query Interval (secs)..............  31
 Startup Query Count........................ 2
 Last Member Query Interval(1/10 of a second)10
 Last Member Query Count     ..............  2

 L3SW>
```

表 8-2:IGMP インタフェース情報

本製品では、ネットワーク管理者が IGMP プロトコルに関連した数値パラメータを設定できます。次の 2 つは、その中でも最も多く利用されるパラメータです。

- queryinterval:インタフェースに接続しているホストに対して、マルチキャストグループのメンバー情報資格クエリを送信する間隔を定義します。パラメータの範囲は 1～3600 秒までで、デフォルト値は 125 秒です。
- maxresptime:インタフェース上にマルチキャストグループのメンバーホストが存在しないと判断するまでの時間(秒)を定義します。パラメータの範囲は 1～255(単位 1/10 秒)で、デフォルト値は 100(10 秒)です。

queryinterval 値を設定する場合は、IGMP を論理インタフェースで有効にしてから、次のコマンドを実行します。

L3SW> config router igmp interface <queryinterval/…> <slot.port> <1-3600>
L3SW> show router igmp interface queryinterval 4.1 200

maxresponse 時間を設定する場合は、次のコマンドを実行します。

L3SW> config router igmp interface <maxresptime/…> <slot.port> <1-255>
L3SW> show router igmp interface queryinterval 4.1 150

次の表は、queryinterval と maxresponse の値を変更した後に新たに割り当てられた値を表示しています。

```
L3SW>show router igmp interface info 4.1


 Slot.Port     .............................  4.1
 IGMP Admin Mode............................. Disable
 Interface Mode..............................  Enable
 IGMP Version  ..............................  2
 Query Interval (secs)....................... 125
 Query Max Resonse Time (1/10 of a second).. 100
 Robustness    ..............................  2
 Startup Query Interval (secs)............... 31
 Startup Query Count......................... 2
 Last Member Query Interval(1/10 of a second)10
 Last Member Query Count     ..............  2


 L3SW>
```

表 8-3:変更 IGMP パラメータ値

8.2 DVMRP

距離ベクトル型マルチキャストルーティングプロトコル(DVMRP)は、ネットワーク内の目的のホストすべてにマルチキャストトラフィックを効果的に配信するために、マルチキャストルータによって使用されます。このプロトコルに対応したルータは、ネットワークにトラフィックをブロードキャストし、マルチキャストグループに属するホストが存在しないパスを除去して、発信元であるルータ自身から個々のマルチキャストグループまでのマルチキャストツリーを構築します。DVMRPでは、「リバースパス転送」とプルーニングを使用して、マルチキャストグループのすべてのホストに対し、特定の発信元からの枝の数を最少にしたツリーを維持します。

8.2.1 DVMRP の設定

DVMRP の設定は、次の各ステップで行います。

ステップ 1:ルーティングモードを有効にします。

詳しい設定については、「6.1.2 ルーティングモードの設定」(P.101)を参照

ステップ 2:すべての関連ポートに対するIPインタフェースを設定します。

詳しい設定については、「6.2.2.1 物理ポート上の IP インタフェースの設定」(P.106)を参照

ステップ 3:IGMPの有効化と設定をします。

IGMP は、ホストとルータが接続するインタフェースで設定する必要があります。

ステップ 4:ルータIDを設定します。

ステップ 5:マルチキャスト(ルーティング)管理モードを有効にします。

ステップ 6:DVMRP管理モードを有効にします。

ステップ 7：対象となる論理インタフェースでのDVMRPを有効にします。

ステップ 1、2、3 については、すでに説明しています。ここでは、DVMRP プロトコルの設定に必要なその後のステップを中心に説明します。IP インタフェース 4.1 と 4.2 がすでに生成済みで、他の DVMRP ルータとの接続に利用されているという前提で、DVMRP の設定について例をあげて説明します。

- **ルータ ID の設定**

```
L3SW> config router id <router-ID>
L3SW> config router id 20.0.0.1
```

- **マルチキャスト（ルーティング）管理モードの有効化**

```
L3SW> config router mcast adminmode <enable/disable>
L3SW> config router mcast adminmode enable
```

- DVMRP 管理モードの有効化

```
L3SW> config router dvmrp adminmode <enable/disable>
L3SW> config router dvmrp adminmode enable
```

- 対象となるインタフェースでの DVMRP の有効化

```
L3SW> config router dvmrp interface mode <slot.port> <enable/disable>
L3SW> config router dvmrp interface mode 4.1 enable
```

すべての論理インタフェースに対する DVMRP 管理状況を表示する場合は、次のコマンドを実行します。表 8-4 はその結果を示しています。

```
L3SW> config router dvmrp adminmode
```

```
L3SW>show router dvmrp info


 Admin Mode    ............................  Enable
 Version       ............................  3
 Total Number of Routes..................... 0
 Reachable Routes........................... 0

    DVMRP INTERFACE STATUS
Slot.Port Interface Mode  Protocol State
--------- --------------- ---------------
4.1       Enable          Non-operational
4.2       Disable         Non-operational

 L3SW>
```

表 8-4：DVMRP 管理モード状況

次のコマンドでも、DVMRP 関連設定パラメータと論理インタフェースに関係した管理モード状況を表示できます。次の表は、その結果の一例です。

```
L3SW> config router dvmrp interfaceinfo 4.1
```

```
L3SW>show router dvmrp interface info 4.1


 Interface Mode ............................. Enable
 Interface Metric............................ 3
 Local Address .............................  60.0.0.1
 Received Bad Packets........................ 0
 Received Bad Routes......................... 0
 Sent Routes   .............................  0


 L3SW>
```

表 8-5:DVMRP インタフェース情報

8.2.2 IGMP と DVMRP の複合設定の例

図 8-1 は、3 台のマルチキャストルータと 6 台のマルチキャストクライアント、2 台のマルチキャストサーバによるネットワーク構成を表示しています。図では、ホスト 1、2、5 はサーバ#1 がサポートしているマルチキャストグループ#1 のメンバーであり、ホスト 3、4、6 はサーバ#2 がサポートしているグループ#2 のメンバーであるとします。それぞれの物理ポートに割り当てられているポート番号と IP アドレスも図に表示されています。 サーバ#1 からのトラフィックは、ルータ#3 によってホスト 1 と 2 が接続しているルータ#2 と、ルータ#5 が接続しているルータ#1 に転送されます。サーバ#1 から受信したトラフィックがルータ#1 によってルータ#2 に転送されると、ルータ#2 は、自身から別のルータを通って発信元(サーバ#1)まで到達可能であることが「リバースパス転送チェック」によって知らされるので、PRUNE メッセージを送信します。そこで、ルータ#1 はグループ#1 にあてたトラフィックのルータ#2 への転送を停止し、サーバ#1 を発信元とするグループ#1 のためのマルチキャストツリーを設定します。各ルータで必要な設定については、次を参照してください。

ルータ #1

- **手順 1:ルーティングの有効化**

```
L3SW-1>config routing enable
```

- **手順 2: 物理ポート上のIPインタフェースの設定**

```
L3SW-1>config ip port create 0.1 60.0.0.1 255.255.255.0
L3SW-1>config ip port create 0.2 70.0.0.1 255.255.255.0
L3SW-1>config ip port create 0.3 80.0.0.1 255.255.255.0
L3SW-1>config ip port create 0.4 20.0.0.1 255.255.255.0
L3SW-1>config ip port create 0.5 40.0.0.1 255.255.255.0
```

このコマンドにより、論理インタフェース 4.1、4.2、4.3、4.4、4.5 がそれぞれ生成されます。

- **手順 3:ルータIDの設定**

```
L3SW-1>config router id 20.0.0.1
```

- **手順 4:対象となる論理インタフェースでのIGMP設定**

```
L3SW-1>config router igmp adminmode enable
L3SW-1>config router igmp interface mode 4.1 enable
L3SW-1>config router igmp interface mode 4.2 enable
L3SW-1>config router igmp interface mode 4.3 enable
L3SW-1>config router igmp interface mode 4.4 enable
L3SW-1>config router igmp interface mode 4.5 enable
```

- **手順 5:対象となる論理インタフェースでのDVMRPの設定**

```
L3SW-1>config router mcast adminmode enable
L3SW-1>config router dvmrp adminmode enable
L3SW-1>config router dvmrp interface mode 4.4 enable
L3SW-1>config router dvmrp interface mode 4.5 enable
```

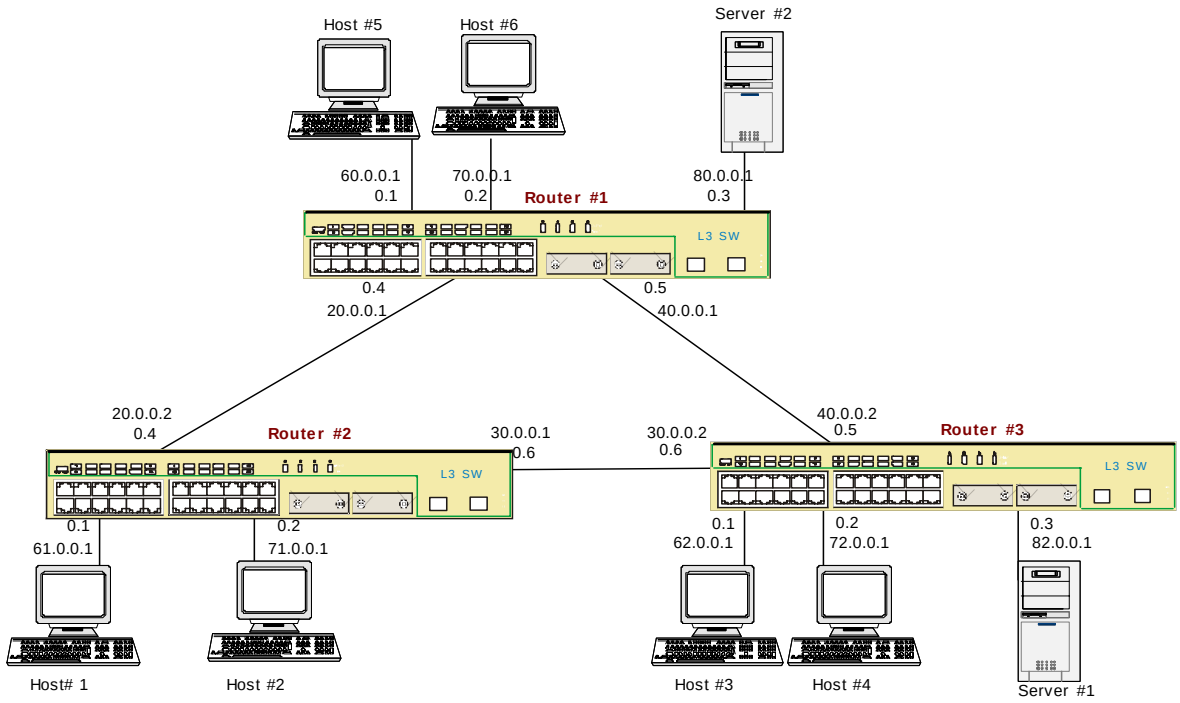

図 8-1:IGMP+DVMRP Configuration Example

ルータ#2

```
L3SW-2>config routing enable
L3SW-2>config ip port create 0.1 61.0.0.1 255.255.255.0
L3SW-2>config ip port create 0.2 71.0.0.1 255.255.255.0
L3SW-2>config ip port create 0.4 20.0.0.2 255.255.255.0
L3SW-2>config ip port create 0.6 30.0.0.1 255.255.255.0
L3SW-2>config router id 20.0.0.2
L3SW-2>config router igmp adminmode enable
L3SW-2>config router igmp interface mode 4.1 enable
L3SW-2>config router igmp interface mode 4.2 enable
L3SW-2>config router igmp interface mode 4.2 enable
L3SW-2>config router igmp interface mode 4.2 enable
L3SW-2>config router mcast adminmode enable
L3SW-2>config router dvmrp adminmode enable
L3SW-2>config router dvmrp interface mode 4.3 enable
L3SW-2>config router dvmrp interface mode 4.4 enable
```

ルータ#3

```
L3SW-3>config routing enable
L3SW-3>config ip port create 0.1 62.0.0.1 255.255.255.0
L3SW-3>config ip port create 0.2 72.0.0.1 255.255.255.0
L3SW-3>config ip port create 0.3 82.0.0.1 255.255.255.0
L3SW-3>config ip port create 0.5 40.0.0.2 255.255.255.0
```

```
L3SW-3>config ip port create 0.6 30.0.0.2 255.255.255.0
L3SW-3>config router id 30.0.0.2
L3SW-3>config router igmp adminmode enable
L3SW-3>config router igmp interface mode 4.1 enable
L3SW-3>config router igmp interface mode 4.2 enable
L3SW-3>config router igmp interface mode 4.3 enable
L3SW-3>config router igmp interface mode 4.4 enable
L3SW-3>config router igmp interface mode 4.5 enable
L3SW-3>config router mcast adminmode enable
L3SW-3>config router dvmrp adminmode enable
L3SW-3>config router dvmrp interface mode 4.4 enable
L3SW-3>config router dvmrp interface mode 4.5 enable
```

8.3 PIM-DM

プロトコル非依存型マルチキャスト（PIM）ルーティングでは、RIP や OSPF などのユニキャストルーティングプロトコルで生成したルーティングテーブルをもとに「リバースパスチェック」を行い、マルチキャストパケットを受信対象者に宛てて転送します。これが、プロトコル非依存型マルチキャストと呼ばれているのは、ユニキャストルーティングプロトコルに依存せずに動作するからです。PIM には、PIM-Dense モード（DM）と Sparse モード（SM）の 2 種類があります。

PIM-DM はリバースパス転送技術によってマルチキャストツリーを構築するマルチキャストプロトコルであり、RIP や OSPF などのユニキャストルーティングプロトコルで生成した既存のルーティングテーブルを利用して、リバースパス転送を行います。PIM-DM はブロードキャストプルーニングプロトコルであるため、ネットワーク全体に少数のマルチキャストクライアントしか存在しない場合はとくに、不要なトラフィックを生成することがあります。

8.3.1 PIM-DM の設定

本製品でのベーシック PIM-DM 動作設定は、次の手順で行います。この設定では、その他の設定可能な PIM-DM パラメータにはすべてデフォルト値を割り当てます。

ステップ 1：ルーティングモードを有効にします。

詳しい設定については「6.1.2　ルーティングモードの設定」（P.101）を参照

ステップ 2：すべての関連ポートに対するIPインタフェースを設定します。

詳しい設定については「6.2.2.1　物理ポート上の IP インタフェースの設定」（P.106）を参照

ステップ 3：インタフェースでのIGMPの有効化と設定をします。

ホストとルータが接続しているすべての論理インタフェースでの IGMP の有効化

ステップ 4：ルータIDを設定します。

ステップ 5：ユニキャストルーティングプロトコルを設定します。

RIP や OSPF などのユニキャストプロトコルが使用できます。ネットワーク構成によっては、必要

なルートをスタティックに設定することも可能です。

ステップ 6：マルチキャスト（ルーティング）管理モードを有効にします。

ステップ 7：PIM—DM管理モードを有効にします。

ステップ 8：関連する論理インタフェースでPIM-DMを有効にします。

ルータだけでなくマルチキャストクライアントが接続するインタフェースで、PIM-DM を有効にする必要があります。

ステップ 1 からステップ 5 までは前の説明と同じです。ここの節では、PIM-DM プロトコルの設定に必要なステップ 6 以降の手順を中心に説明します。次では、IP インタフェース 4.1 と 4.2 の生成がすでに終わり、他の PIM-DM ルータとの接続に使用されているという前提で、PIM-DM の設定について例をあげて説明します。

- マルチキャスト（ルーティング）管理モードの有効化

```
L3SW> config router mcast adminmode <enable/disable>
L3SW> config router mcast adminmode enable
```

- PIM-DM 管理モードの有効化

```
L3SW> config router pimdm adminmode <enable/disable>
L3SW> config router pimdm adminmode enable
```

- 関連する論理インタフェースでの PIM-DM の有効化

```
L3SW> config router pimdm interface mode <slot.port> <enable/disable>
L3SW> config router pimdm interface mode 4.1 enable
```

PIM-DM は、クライアントとルータが接続しているすべてのインタフェースで有効化してください。また、PIM-DM の適切な動作には、ルータだけが接続しているインタフェースで IGMP プロトコルに対応する必要があります。

次のコマンドを実行すると、すべての論理インタフェースについて PIM-DM 管理モード状況を表示します。表はその結果です。

L3SW> show router pimdm interface info

```
L3SW>show router pimdm info

PIMDM Admin Mode.............................. Enable

    PIM-DM INTERFACE STATUS
Slot.Port Interface Mode  Protocol State
--------- --------------- ---------------
4.1       Enable          Operational
4.2       Enable          Operational
4.3       Enable          Operational
4.4       Enable          Operational
4.4       Enable          Operational


L3SW>
```

表 8-6：PIM-DM 設定の詳細

次のコマンドを実行すると、スイッチの特定のインタフェースについて PIM-DM 設定の詳細を表示できます。次の表はこのコマンドを実行した結果の一例です。

```
L3SW>show router pimdm interface info 4.1

Interface Mode.............................. Enable
Interface Hello Interval(secs).............  30


L3SW>
```

表 8-7:インタフェースでの PIM-DM 設定の詳細

8.3.1.1 PIM-DM プロトコル設定パラメータ

本製品では、すべてのユーザが PIM-DM プロトコルに関連した次のパラメータを設定できます。使用するコマンドを次に示します。

- ハローインターバル

PIM-DM ではネイバとハローパケットを交換して、PIM-DM に対応できる隣接スイッチを発見し、またすでに発見済みのノードについてはリンクやノードの障害を検知します。インタフェース 4.1 に関連したプロトコルパラメータは、次のコマンドの実行によって表示できます。

```
L3SW> config router pimdm interface hellointerval <slot.port> <10-3600>
L3SW> config router pimdm interface hellointerval 4.1 60
```

```
L3SW>show router pimdm interface info 4.1

Interface Mode.............................. Enable
Interface Hello Interval (secs).............  60


L3SW>
```

表 8-8：変更後の PIM-DM インタフェースパラメータ

8.3.2 PIM-DM の表示

show コマンドを使うと、マルチキャストルータ状況情報とマルチキャストルートテーブルのエントリを表示できます。これらのコマンドは、マルチキャストルーティング機能に関連した問題の解決に利用できます。この節では、PIM-DM に関連したコマンドを中心に説明します。

次のコマンドを実行すると、PIM-DM ネイバ情報を表示します。

```
L3SW> show router pimdm neighbour <slot.port/all>
L3SW> show router pimdm neighbour all
```

```
L3SW>show router pimdm neighbor all

                    NEIGHBOR TABLE
Neighbor Addr  Interface      Up Time       Expiry Time
                             (hh:mm:ss)    (hh:mm:ss)
------------   ---------     ----------     -----------
20.0.0.2       4.4           00:12:22       00:01:25
40.0.0.2       4.5           00:12:23       00:01:26


L3SW>
```

表 8-9:PIM-DM ネイバの情報

次のコマンドを実行すると、マルチキャストルーティングプロトコルの他に発信元確認済みパケット数などの統計データを表示します。

L3SW> show router mcast info
L3SW> show router mcast info

```
L3SW>show router mcast info

Admin Mode..................................... Enable
Protocol State................................. Operational
Table Max Size................................. 256
Number of Packets For Which Source Not Found 0
Number of Packets For Which Group Not Found. 0
Protocol .....................................  PIMDM
Entry Count.................................... 0
Highest Entry Count............................ 2


L3SW>
```

表 8-10:マルチキャストルータ情報の表示

次のコマンドを実行すると、PIM-DM ネイバの数と PIM-DM インタフェースに対する指名ルータを表示します。

L3SW> show router pimdm interface stats <slot.port/all>
L3SW> show router pimdm interface stats all

8.3.3 PIM-DM の例

図 8-2 は、3 台のマルチキャストルータと 6 台のマルチキャストクライアント、1 台のマルチキャストサーバによるネットワーク構成を表わしています。このネットワークは、DVMRP 設定の説明に使用した例とよく似ています。ルータ#1 はマルチキャストサーバに接続しているため、サーバによって生成されたマルチキャストストリーム用のルータに自動的に指定されます。このネットワークの 3 台のルータ設定に必要なコマンドは、次のとおりです。

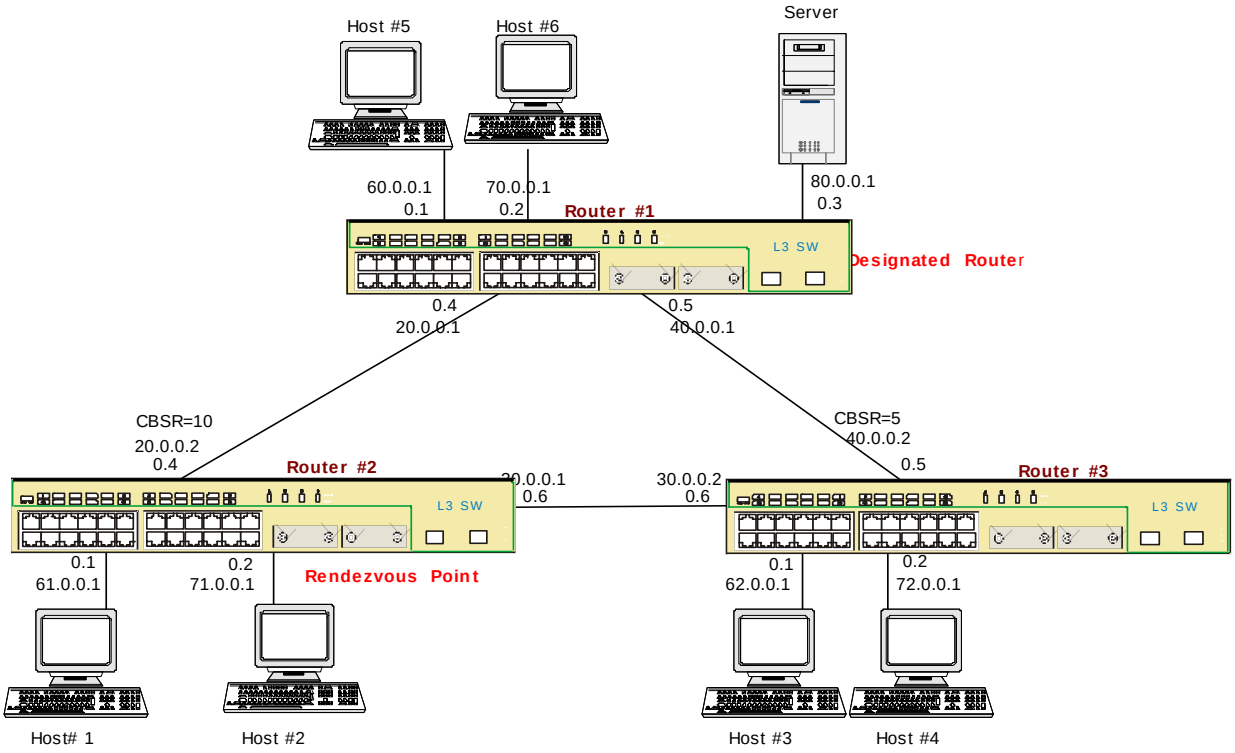

図 8-2：PIM-DM の例

Router #1

- ステップ 1：ルーティングの有効化

```
L3SW-1>config routing enable
```

- ステップ 2：IPインタフェースの設定

```
L3SW-1>config ip port create 0.1 60.0.0.1 255.255.255.0
L3SW-1>config ip port create 0.2 70.0.0.1 255.255.255.0
L3SW-1>config ip port create 0.3 80.0.0.1 255.255.255.0
L3SW-1>config ip port create 0.4 20.0.0.1 255.255.255.0
L3SW-1>config ip port create 0.5 40.0.0.1 255.255.255.0
```

- ステップ 3：ルータIDの設定

```
L3SW-1>config router id 20.0.0.1
```

- ステップ 4：IGMPの設定

```
L3SW-1>config router igmp adminmode enable
L3SW-1>config router igmp interface mode 4.1 enable
L3SW-1>config router igmp interface mode 4.2 enable
L3SW-1>config router igmp interface mode 4.3 enable
L3SW-1>config router igmp interface mode 4.4 enable
L3SW-1>config router igmp interface mode 4.5 enable
```

- ステップ 5：RIPとルート再配分の有効化

```
L3SW-1>config router rip adminmode enable
L3SW-1>config router rip interface mode 4.4 enable
L3SW-1>config router rip interface mode 4.5 enable
```

```
L3SW-1>config router rip redistribution enable static 1
```

- ステップ 6 : マルチキャストルーティングとPIM-DMの有効化

```
L3SW-1>config router mcast adminmode enable
L3SW-1>config router pimdm adminmode enable
L3SW-1>config router pimdm interface mode 4.1 enable
L3SW-1>config router pimdm interface mode 4.2 enable
L3SW-1>config router pimdm interface mode 4.3 enable
L3SW-1>config router pimdm interface mode 4.4 enable
L3SW-1>config router pimdm interface mode 4.5 enable
```

Router #2

```
L3SW-2>config routing enable
L3SW-2>config ip port create 0.1 61.0.0.1 255.255.255.0
L3SW-2>config ip port create 0.2 71.0.0.1 255.255.255.0
L3SW-2>config ip port create 0.4 20.0.0.2 255.255.255.0
L3SW-2>config ip port create 0.6 30.0.0.1 255.255.255.0
L3SW-2>config router id 20.0.0.2
L3SW-2>config router igmp adminmode enable
L3SW-2>config router igmp interface mode 4.1 enable
L3SW-2>config router igmp interface mode 4.2 enable
L3SW-2>config router igmp interface mode 4.3 enable
L3SW-2>config router igmp interface mode 4.4 enable
L3SW-2>config router rip adminmode enable
L3SW-2>config router rip interface mode 4.3 enable
L3SW-2>config router rip interface mode 4.4 enable
L3SW-2>config router rip redistribution enable static 1
L3SW-2>config router mcast adminmode enable
L3SW-2>config router pimdm adminmode enable
L3SW-2>config router pimdm interface mode 4.1 enable
L3SW-2>config router pimdm interface mode 4.2 enable
L3SW-2>config router pimdm interface mode 4.3 enable
L3SW-2>config router pimdm interface mode 4.4 enable
```

Router #3

```
L3SW-3>config routing enable
L3SW-3>config ip port create 0.1 62.0.0.1 255.255.255.0
L3SW-3>config ip port create 0.2 72.0.0.1 255.255.255.0
L3SW-3>config ip port create 0.5 40.0.0.2 255.255.255.0
L3SW-3>config ip port create 0.6 30.0.0.2 255.255.255.0
L3SW-3>config router id 30.0.0.2
L3SW-3>config router igmp adminmode enable
L3SW-3>config router igmp interface mode 4.1 enable
L3SW-3>config router igmp interface mode 4.2 enable
L3SW-3>config router igmp interface mode 4.3 enable
L3SW-3>config router igmp interface mode 4.4 enable
L3SW-3>config router rip adminmode enable
L3SW-3>config router rip interface mode 4.3 enable
L3SW-3>config router rip interface mode 4.4 enable
L3SW-3>config router rip redistribution enable static 1
L3SW-3>config router mcast adminmode enable
L3SW-3>config router pimdm adminmode enable
L3SW-3>config router pimdm interface mode 4.1 enable
L3SW-3>config router pimdm interface mode 4.2 enable
L3SW-3>config router pimdm interface mode 4.3 enable
L3SW-3>config router pimdm interface mode 4.4 enable
```

8.4 PIM-SM

プロトコル非依存型マルチキャスト（PIM）ルーティングでは、RIP や OSPF などのユニキャストルーティングプロトコルによって生成されたルーティングテーブルを使って「リバースパスチェック」を行い、マルチキャストパケットを目的の受信者宛てに転送します。これが、プロトコル非依存型マルチキャストと呼ばれているのは、ユニキャストルーティングプロトコルに依存せずに動作するからです。PIM には、PIM-Dense モード（DM）と Sparse モード（SM）の 2 種類があります。

PIM-DM では、発信元からネットワークのすべての受信者までマルチキャスト配信を使用します。配信ツリーでは発信元から受信者まで最短パスを使用するため、配信ツリーは最短パスツリー（SPT）とも呼ばれます。PIM-SM で使用するツリーには、最短ツリーの他に共有ツリーがあります。共有ツリーは、各グループへのマルチキャスト配信ツリーを、ランデブーポイント（RP）と呼ばれるルートノードからトラフィックのすべての受信者までで構成されます。共有ツリー操作モードでは、発信元に近いマルチキャストルータはトラフィックを RP に送り、RP が送られたトラフィックをマルチキャスト配信ツリーに基づいて目的の受信者まで送ります。DVMRP と異なり、PIM-SM では受信者から RP までのパスに沿ったルータから受け取った JOIN メッセージと PRUNE メッセージを利用して、マルチキャスト配信ツリーを構築維持します。

8.4.1 PIM-SM の設定

本製品での基本的な PIM-SM 動作設定は、次のステップで行います。ここでは、設定可能な他の PIM-SM パラメータにはすべてデフォルト値を割り当てています。

ステップ 1：ルーティングモードを有効にします。

詳しい設定については、「6.1.2 ルーティングモードの設定」（P.101）を参照

ステップ 2：すべての関連ポートに対するIPインタフェースを設定します。

詳しい設定については、「6.2.2.1 物理ポート上の IP インタフェースの設定」（P.106）を参照

ステップ 3：インタフェースでのIGMPの有効化と設定をします。

ホストとルータが接続しているすべての論理インタフェースで IGMP を有効にします。

ステップ 4：ルータIDを設定します。

ステップ 5：ユニキャストルーティングプロトコルを設定します。

RIP や OSPF などのユニキャストプロトコルを使用することもできます。ネットワーク構成によっては、必要なルートをスタティックに設定することもできます。

ステップ 6：マルチキャスト（ルーティング）管理モードを有効にします。

ステップ 7：PIM-SM管理モードを有効にします。

ステップ 8：関連論理インタフェースでのPIM-SMを有効にします。

PIM-SM は、ルータだけでなくマルチキャストクライアントが接続するインタフェースでも有効にします。

ステップ 1～5 については、すでに説明しています。ここでは、PIM－SM プロトコルの設定に必要なその後のステップを中心に説明します。IP インタフェース 4.1 と 4.2 がすでに生成済みで、他の PIM-SM ルータとの接続に利用されているという前提で、PIM-SM の設定について例をあげて説明します。

- **マルチキャスト（ルーティング）管理モードの有効化**

L3SW> config router mcast adminmode <enable/disable>
L3SW> config router mcast adminmode enable

- **PIM－SM 管理モードの有効化**

L3SW> config router pimsm adminmode <enable/disable>
L3SW> config router pimsm adminmode enable

- **関連論理インタフェースでの PIM-SM の有効化**

L3SW> config router pimsm interface mode <slot.port> <enable/disable>
L3SW> config router pimsm interface mode 4.1 enable

PIM-SM は、クライアントとルータが接続しているすべてのインタフェースで有効である必要があります。また、PIM-SM は、ルータだけが接続しているインタフェースで IGMP プロトコルが動作している必要があります。

すべての論理インタフェースに対する PIM-SM 管理状況を表示する場合は、次のコマンドを実行します。次の表は結果を示しています。

L3SW> show router pimsm interface info

```
L3SW>show router pimsm info

PIMSM Admin Mode............................. Enable
RP address................................... 0.0.0.0
Join/Prune Interval (secs)................... 60
Data Threshold Rate (K bits/sec)............. 50
Register Threshold Rate (K bits/sec).......  50

    PIM-SM INTERFACE STATUS
Slot.Port Interface Mode  Protocol State
--------- --------------- ---------------
4.1       Enable          Non-operational
4.2       Enable          Non-operational

L3SW>
```

表 8-11：PIM-SM 設定の詳細

スイッチの特定のインタフェースについて、PIM-SM 設定の詳細を表示する場合は、次のコマンドを実行します。次の表は、このコマンドを実行した結果の一例です。

```
L3SW>show router pimsm interface info 4.1

Slot.Port..................................  4.1
IP address................................. 10.0.0.2
Subnet Mask................................ 255.0.0.0
Interface Mode............................. Enable
Hello Interval............................. 30 seconds
CBSR Preference............................ -1

L3SW>
```

表 8-12:インタフェースでの PIM-SM 構成の詳細

8.4.1.1 PIM-SM RP の設定

RP モードを設定する場合、スイッチが自身の RP 能力をアドバタイズできるように IP アドレスを割り当てる必要があります。ネットワークの他のスイッチはこの IP アドレスを使用して、マルチキャストグループ配信ツリーで配信するパケットを転送します。デフォルトでは、PIM-SM を有効にしただけでは RP モードは動作しません。論理インタフェースで RP モードをサポートするには、インタフェースに対するブートストラップルータ候補(CBSR)優先値を 1 以上に設定します。ここでは、論理インタフェースの IP アドレスと RP の IP アドレスは同じだと仮定します。本製品では、複数の論理インタフェースで RP モードをサポートすることができます。論理インタフェースで CBSR 優先値を設定する場合は(RP モードをサポートする場合)、次のコマンドを実行します。

- インタフェースでの RP モードの有効化

cbsrpreference 値を 1 以上に設定

```
L3SW> config router pimsm interface cbsrpreference <slot.port> <-1 to 255>
L3SW> config router pimsm interface cbsrpreference 4.1 10
```

- インタフェースで RP モードを無効化:cbsrpreference 値に－1 を設定

```
L3SW> config router pimsm interface cbsrpreference <slot.port> <-1 to 255>
L3SW> config router pimsm interface cbsrpreference 4.1 -1
```

次のコマンドを実行すると、どの論理ポート、物理ポートとも接続せずに RP モードを設定できます。

- RP モードを有効化する場合

```
L3SW> config router pimsm rp create <ipaddr>
L3SW> config router pimsm rp create 80.0.0.1
```

- RP モードを無効化する場合

```
L3SW> config router pimsm rp delete
L3SW> config router pimsm rp delete
```

スイッチの RP モードでは、IP アドレスが内部ループバックのインタフェースに割り当てられています。この内部ループバックインタフェースは決してダウンしないので、スイッチでの RP モード有効化を推奨します。

8.4.1.2 PIM-SM プロトコル設定パラメータ

本製品では、PIM-SM プロトコルに関連して次のパラメータを設定することができます。次のコマンドで設定します。

- **JOIN/PRUNE メッセージインターバル**

L3SW> config router pimsm joinpruneintvl <10-3600>
L3SW> config router pimsm joinpruneintval 120

- **データしきい値**

L3SW> config router pimsm datathreshrate <0-2000>
L3SW> config router pimsm datathreshrate 100

- **レジスタしきい値**

L3SW> config router pimsm regthreshrate <0-2000>
L3SW> config router pimsm regthreshrate 200

次の表は、これらのコマンドによる変更後の PIM-SM プロトコルのパラメータを示しています。

```
L3SW>show router pimsm info

PIMSM Admin Mode............................. Enable
RP address................................... 0.0.0.0
Join/Prune Interval (secs)................... 60
Data Threshold Rate (K bits/sec).............50
Register Threshold Rate (K bits/sec).......  50

    PIM-SM INTERFACE STATUS
Slot.Port Interface Mode  Protocol State
--------- --------------- ---------------
4.1       Enable          Non-operational
4.2       Enable          Non-operational


L3SW>
```

- **Hello インターバル**

PIM-SM では隣接するノードと hello パケットを交換して、PIM-SM に対応できるスイッチを発見し、またすでに発見済みのノードについてリンクやノードの障害を探知します。インタフェース 4.1 に関連したプロトコルパラメータは、次のコマンドの実行によって表示できます。

L3SW> config router pimsm interface hellointerval <slot.port> <10-3600>
L3SW> config router pimsm interface hellointerval 4.1 60

```
L3SW>show router pimsm interface info 4.1

Slot.Port.....................................  4.1
IP address.................................... 10.0.0.2
Subnet Mask................................... 255.0.0.0
Interface Mode................................ Enable
Hello Interval................................ 60 seconds
CBSR Preference............................... 0


L3SW>
```

表 8-13:変更後の PIM-SM インタフェースパラメータ

PIM-SM のほかのパラメータと異なり、hellointerval は PIM-SM プロトコルが動作可能な個々の論理インタフェースと関連しています。

8.4.2 PIM-SM の表示

本製品では、さまざまな show コマンドによって、マルチキャストルータ状況情報とマルチキャストルートテーブルエントリを表示することができます。これらのコマンドは、マルチキャストルーティング機能に関連した問題の修正に利用できます。ここでは、PIM-SM に関連したコマンドを中心に説明します。

PIM-SM 隣接情報を表示する場合は、次のコマンドを実行します。

```
L3SW> show router pimsm neighbour <slot.port/all>
L3SW> show router pimsm neighbour all
```

```
L3SW>show router pimsm neighbor all

                    NEIGHBOR TABLE
Slot.Port IP Address       Up Time      Expiry Time
                           (hh:mm:ss)   (hh:mm:ss)
--------- ---------------  ----------   ------------
4.1       10.0.0.1         00:12:22      00:01:25

L3SW>
```

表 8-14:PIM-SM 隣接情報

マルチキャストルーティングプロトコルと、発信元確認済みパケット数(number of packets for which source was found)などの情報に関連した統計データを表示する場合は、次のコマンドを実行します。

```
L3SW> show router mcast info
L3SW> show router mcast info
```

```
L3SW>show router mcast info

Admin Mode..................................... Enable
Protocol State................................. Operational
Table Max Size................................. 256
Number of Packets For Which Source Not Found 0
Number of Packets For Which Group Not Found. 0
Protocol .....................................  PIMSM
Entry Count.................................... 0
Highest Entry Count............................ 2

L3SW>
```

表 8-15:マルチキャストルータ情報の表示

PIM-SM 隣接ノードの数と PIM-SM インタフェースに対する指名ルータを表示する場合は、次のコマンドを実行します。

```
L3SW> show router pimsm interface stats <slot.port/all>
L3SW> show router pimsm interface stats all
```

次も、マルチキャスト関連の問題修正に使用できる便利なコマンドです。このコマンドは、すべてのマルチキャストグループアドレスと、ネットワークにマルチキャストグループへのストリームをブロードキャストするモード（SPT か RPT か）を表示します。下の表は、これによって表示されたマルチキャストルートテーブルです。

```
L3SW> show router mcast mroute detailed <slot.pot/all>
L3SW> show router mcast mroute detailed all
```

```
L3SW>show router mcast mroute detailed all

                  Multicast Route Table
                            Expiry      Up Time
Source IP      Group IP     Time(secs) (secs)   RPF Neighbor  Flags
-------------- ------------ ---------- ------   ------------- -----
      *        224.1.1.1    145          368     0.0.0.0       RPT
20.0.0.10      224.1.1.1    205          289     0.0.0.0       SPT
30.0.0.10      224.1.1.1    25           289     0.0.0.0       RPT

L3SW>
```

表 8-16：マルチキャストルートテーブル

8.4.3 PIM-SM の例

図 8-3：PIM-SM の例は、3 台のマルチキャストルータと 6 台のマルチキャストクライアント、1 台のマルチキャストサーバによるネットワーク構成を表示しています。このネットワークは、DVMRP 設定の説明に使用したネットワークと似ています。マルチキャストサーバはルータ#1 に接続しているため、ルータ#1 はサーバによって生成されたマルチキャストストリームの指名ルータに自動的に指名されます。ルータ#2 とルータ#3 では、それぞれポート 0.4 と 0.5 に RP が設定されています。ルータ#2 のポート 0.4 に割り当てられた高い優先値（CBSR プリファレンス）によって、ルータ#2 はサーバが生成したマルチキャストストリームに関する RP になります。サーバによって生成されたマルチキャストストリームは、ルータ#1（指名ルータ）により適切なヘッダ情報を付けてカプセル化され、ユニキャストパケットとしてルータ#2（RP）に送られます。ルータ#2 は添付されたユニキャストヘッダ情報を除去して、自分自身のローカルインタフェース（ポート 0.1 と 0.2）に接続するクライアント宛てにマルチキャストパケットを送信し、さらにルータ#3 に接続するクライアントへの配信のため、ポート 0.6 からルータ#3 宛てにマルチキャストストリームのコピーを送信します。このネットワークの 3 台のルータ設定に必要なコマンドは、次のとおりです。

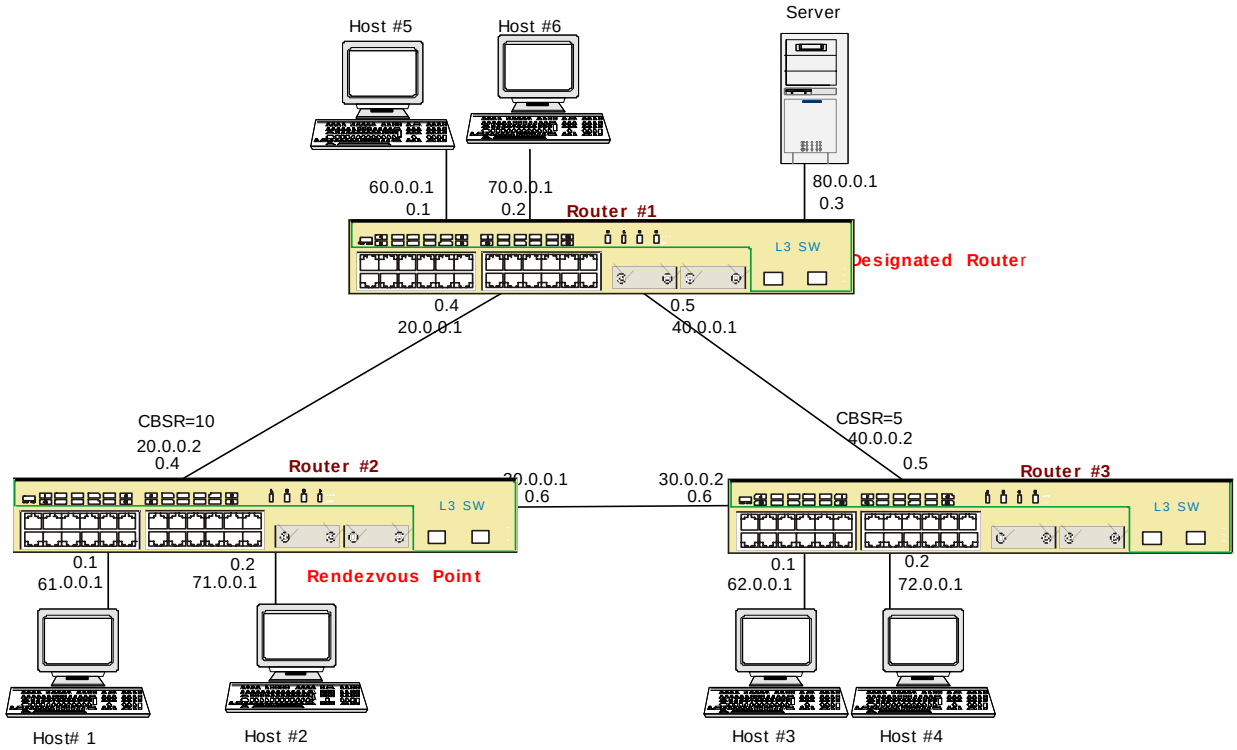

図 8-3：PIM-SM の例

ルータ#1

- ステップ 1：ルーティングを有効にします。

```
L3SW-1>config routing enable
```

- ステップ 2：IPインタフェースを設定にします。

```
L3SW-1>config ip port create 0.1 60.0.0.1 255.255.255.0
L3SW-1>config ip port create 0.2 70.0.0.1 255.255.255.0
L3SW-1>config ip port create 0.3 80.0.0.1 255.255.255.0
L3SW-1>config ip port create 0.4 20.0.0.1 255.255.255.0
L3SW-1>config ip port create 0.5 40.0.0.1 255.255.255.0
```

- ステップ 3：ルータIDを設定します。

```
L3SW-1>config router id 20.0.0.1
```

- ステップ 4：IGMPを設定します。

```
L3SW-1>config router igmp adminmode enable
L3SW-1>config router igmp interface mode 4.1 enable
L3SW-1>config router igmp interface mode 4.2 enable
L3SW-1>config router igmp interface mode 4.3 enable
L3SW-1>config router igmp interface mode 4.4 enable
L3SW-1>config router igmp interface mode 4.5 enable
```

- ステップ 5：RIPとルート再配布を有効にします。

```
L3SW-1>config router rip adminmode enable
```

```
L3SW-1>config router rip interface mode 4.4 enable
L3SW-1>config router rip interface mode 4.5 enable
L3SW-1>config router rip redistribution enable static 1
```

- ステップ 6：マルチキャストルーティングとPIM-SMを有効にします。

```
L3SW-1>config router mcast adminmode enable
L3SW-1>config router pimsm adminmode enable
L3SW-1>config router pimsm interface mode 4.1 enable
L3SW-1>config router pimsm interface mode 4.2 enable
L3SW-1>config router pimsm interface mode 4.3 enable
L3SW-1>config router pimsm interface mode 4.4 enable
L3SW-1>config router pimsm interface mode 4.5 enable
```

ルータ#2

```
L3SW-2>config routing enable
L3SW-2>config ip port create 0.1 61.0.0.1 255.255.255.0
L3SW-2>config ip port create 0.2 71.0.0.1 255.255.255.0
L3SW-2>config ip port create 0.4 20.0.0.2 255.255.255.0
L3SW-2>config ip port create 0.6 30.0.0.1 255.255.255.0
L3SW-2>config router id 20.0.0.2
L3SW-2>config router igmp adminmode enable
L3SW-2>config router igmp interface mode 4.1 enable
L3SW-2>config router igmp interface mode 4.2 enable
L3SW-2>config router igmp interface mode 4.3 enable
L3SW-2>config router igmp interface mode 4.4 enable
L3SW-2>config router rip adminmode enable
L3SW-2>config router rip interface mode 4.3 enable
L3SW-2>config router rip interface mode 4.4 enable
L3SW-2>config router rip redistribution enable static 1
L3SW-2>config router mcast adminmode enable
L3SW-2>config router pimsm adminmode enable
L3SW-2>config router pimsm interface mode 4.1 enable
L3SW-2>config router pimsm interface mode 4.2 enable
L3SW-2>config router pimsm interface mode 4.3 enable
L3SW-2>config router pimsm interface mode 4.4 enable
```

- RP モードの有効化と CBSR 優先値の設定

```
L3SW-2>config router pimsm interface cbsrpreference 4.3 10
```

ルータ#3

```
L3SW-3>config routing enable
L3SW-3>config ip port create 0.1 62.0.0.1 255.255.255.0
L3SW-3>config ip port create 0.2 72.0.0.1 255.255.255.0
L3SW-3>config ip port create 0.5 40.0.0.2 255.255.255.0
L3SW-3>config ip port create 0.6 30.0.0.2 255.255.255.0
L3SW-3>config router id 30.0.0.2
L3SW-3>config router igmp adminmode enable
L3SW-3>config router igmp interface mode 4.1 enable
L3SW-3>config router igmp interface mode 4.2 enable
L3SW-3>config router igmp interface mode 4.3 enable
L3SW-3>config router igmp interface mode 4.4 enable
L3SW-3>config router rip adminmode enable
L3SW-3>config router rip interface mode 4.3 enable
L3SW-3>config router rip interface mode 4.4 enable
L3SW-3>config router rip redistribution enable static 1
L3SW-3>config router mcast adminmode enable
L3SW-3>config router pimsm adminmode enable
L3SW-3>config router pimsm interface mode 4.1 enable
L3SW-3>config router pimsm interface mode 4.2 enable
L3SW-3>config router pimsm interface mode 4.3 enable
```

```
L3SW-3>config router pimsm interface mode 4.4 enable
```

- RP モードの有効化と CBSR 優先値の設定

```
L3SW-3>config router pimsm interface cbsrpreference 4.4 5
```

9. レイヤ 3+の設定

9.1 帯域幅プロビジョニング

9.1.1 帯域幅プロビジョニングの概要

本製品の帯域幅プロビジョニング／割当機能によって、ネットワーク管理者は、同じ物理インタフェースを共有するユーザに異なるレベルの割当帯域幅を提供できます。また、サービスプロバイダは、同じリンクを共有するユーザ、アプリケーション、組織に割り当てた帯域幅を制御できるので、ネットワーク機器を過剰に確保することなく必要なレベルのサービスを提供することが可能になります。この機能はさらに、ネットワークの輻輳を減少させ、少数のアプリケーションやユーザによる帯域幅の独占を防止するという利点もあります。

9.1.2 帯域幅プロビジョニングの関連用語

- トラフィック･クラス：パケットの分類。この分類は、ユーザ定義ルールに基づいてパケットを許可（通過）または拒否（返却、破棄）するトラフィックのフィルタリングで使用されます。本製品では、現在、VLAN のトラフィッククラスだけがサポートされています。将来的には、レイヤ 3／レイヤ 4 情報のトラフィッククラスもサポートされます。
- 帯域幅バケット：指定されたトラフィッククラスの最小・最大帯域幅を作成するときに使用します。本マニュアルでは、帯域幅バケットには帯域幅プロファイルも含まれます。

9.1.3 帯域幅の割り当てとプロビジョニングの設定

トラフィッククラスを設定する場合は、最初に次のようにコマンドを実行して、スイッチ上の帯域幅プロビジョニングを有効にする必要があります。

```
L3SW> config bwprov <disable/enable>
L3SW> config bwprov enable
```

9.1.3.1 トラフィッククラス（TC）の設定

帯域幅の割り当てと管理では、トラフィッククラスの作成、各トラフィッククラスと関連ポート／VLAN との関連付け、各トラフィッククラスの帯域幅制限を行う必要があります。帯域幅プロビジョニングでは、次のようなパラメータを設定します。

- trafficclass：トラフィッククラスを作成します。
- port：スイッチインタフェースをトラフィッククラスに関連付けます。
- vlan：VLAN をトラフィッククラスに関連付けます。
- weight：トラフィッククラスの優先順位です。
- bwprofile：帯域幅割当プロファイルをトラフィッククラスと関連付けます。

本製品でトラフィッククラスを設定する手順と、これらのトラフィッククラスを管理する手順を説明

します。

- **ステップ 1:トラフィッククラスを作成**

```
L3SW> config trafficclass create <type> <name>
L3SW> config trafficclass create vlan tc1
```

トラフィッククラスでサポートされるタイプは VLAN だけです。

トラフィッククラス名は、最大 15 文字の英数字の文字列です。

- **ステップ 2:作成したトラフィッククラスのスイッチポートへの割り当て**

```
L3SW> config trafficclass port <name> <slot.port>
L3SW> config trafficclass port tc1 0.1
```

- **ステップ 3:VLAN ID の作成**

```
L3SW> config vlan create <vlanid>
L3SW> config vlan create 10
```

- **ステップ 4:作成した VLAN へのトラフィッククラスの割り当て**

```
L3SW> config trafficclass vlan <name> <vlanid>
L3SW> config trafficclass vlan tc1 10
```

- **テップ 5:初期設定の VLAN(VLAN ID=1)からポートを取り出し、新しい VLAN に追加**

```
L3SW> config vlan port add <vlanid> <slot.port>
L3SW> config vlan port add 10 0.1
```

- **ステップ 6:帯域幅プロファイルの作成**

帯域幅プロファイルは、トラフィッククラスに割り当てられた最小・最大帯域幅を定義します。

```
L3SW> config bwallocation create <name>
L3SW> config bwallocation create bwprofile1
```

- **ステップ 7:プロファイルの最小帯域幅を定義**

```
L3SW> config bwallocation minbandwidth <name> <0-maxbw supported by the port>
L3SW> config bwallocation minbandwidth bwprofile1 20
```

最小帯域幅は、そのポートでプロファイルに割当可能な最大帯域幅よりも小さい値でなければなりません。デフォルトの最小帯域幅は 64 Kbp です。

最小・最大帯域幅は単位当たりで設定します。1 単位は 64Kbp です。16 単位 = 1Mbp、32 単位 = 2Mbp

- **ステップ 8:プロファイルの最大帯域幅を定義**

```
L3SW> config bwallocation maxbandwidth <name> <0-maxbwsupported by the port>
L3SW> config bwallocation maxbandwidth bwprofile1 80
```

あるポートを通過する全トラフィッククラスに割り当てられた最小帯域幅値の合計＝そのポート

で許容される最大帯域幅値、でなければなりません。

トラフィッククラス当たりの最大許容帯域幅は 100Mbp です。帯域幅の指定は送出トラフィックにのみ適用されます。

- **ステップ 9:トラフィッククラスへの帯域幅プロファイルの割り当て**

L3SW> config trafficclass bwallocation <name> <bwprofile>
L3SW> config trafficclass bwallocation tc1 user1

- **ステップ 10:設定したトラフィッククラスへの優先順位(重み)の割り当て**

トラフィッククラス設定の最後のステップでは、トラフィッククラスに重みを割り当てます。あるポートに関連する全トラフィッククラスの最小帯域幅は、そのトラフィッククラスのあらゆる条件下における保証帯域幅になります。ただしこれは、すべてのトラフィッククラスが割り当てられた最小帯域幅を常に消費することを意味するわけではありません。スイッチのいずれかのポートでトラフィッククラスの競合が発生した場合は、帯域幅が一部未使用になります。このような場合には、スイッチは重み係数を使用して、競合中のトラフィッククラスに未使用の帯域幅を割り当てます。帯域幅は、重み係数の大きいトラフィッククラスに多く割り当てられます。トラフィッククラスに重みを割り当てる場合は、次のようにコマンドを実行します。重みに使用できる値は、1～1024 です。

L3SW> config trafficclass weight <name> <weight>
L3SW> config trafficclass weight tc1 100

9.1.4 帯域幅が割り当てられたトラフィッククラスの表示

トラフィッククラスは、以下の 3 つのレベルで表示できます。

- 割当帯域幅:スイッチのポートに割り当てられた帯域幅を表示します。
- 詳細:選択したトラフィッククラスに関する詳細なトラフィッククラス情報を表示します。
- 要約:設定済みのポートとトラフィッククラスに関するトラフィッククラス情報の要約を表示します。

トラフィッククラスの設定の表示例を次に示します。

L3SW> show trafficclass allocatedbw 0.1

```
                L3SW>show trafficclass allocatedbw 0.1
            Allocated     Allocated
            Minimum       Maximum
Slot.Port   Bandwidth     Bandwidth
---------   ------------  ---------
0.1         20            80

L3SW>
```

表 9-1:選択されたインタフェースの割当帯域幅の表示例

L3SW> show trafficclass detailed tc1

```
L3SW>show trafficclass detailed tcl

Traffic Class Name.............................  tcl
Slot.Port......................................  0.1
VLAN ID........................................  10
Weight.........................................  100
Accept Byte Count..............................  0
Bandwidth Allocation Profile...................  userl
Minimum Bandwidth,.............................  20
Maximum Bandwidth,.............................  80

L3SW>
```

表 9-2:トラフィッククラス詳細の表示例

L3SW> show trafficclass summary

```
L3SW>show trafficclass summary

   Traffic                  VLAN                Bandwidth
  Class Name     Slot.Port   ID    Weight   Allocation Profile
  -------------  ---------  -----  -------  ------------------
  tc1            0.1        10     100      user1
  tc2            0.2        50     50       user2

L3SW>
```

表 9-3:トラフィッククラス要約の表示例

帯域幅割当設定の詳細は、次のフォーマットで確認できます。

- 要約:システム内の全トラフィッククラスに関する帯域幅割当情報を表示します。
- 詳細:指定されたトラフィッククラスに関する帯域幅割当情報を表示します。

割当済みプロファイルには詳細フォーマットを使用し、作成済みのすべてのプロファイルには要約フォーマットを使用して帯域幅割当を表示する場合は、次のようにコマンドを実行します。

L3SW> show bwallocation detailed user1

```
L3SW>show bwallocation detailed user1

Bandwidth Allocation Profile Name..............  user1
Minimum Bandwidth..............................  20
Maximum Bandwidth..............................  80
Weight.........................................  100
Associated Traffic Class(es)...................  tc1

L3SW>
```

表 9-4:帯域幅割当ての表示例

L3SW> show bwallocation summary

```
                L3SW>show bwallocation summary

Bandwidth Allocation     Minimum       Maximum
   Profile Name         Bandwidth     Bandwidth
---------------------  ------------ ---------
Default                 1            100
User1                   20           80
User2                   20           50

L3SW>
```

表 9-5:帯域幅要約の表示例

9.2 Quality Of Service（Qos）/ Type Of Service（TOS）

9.2.1 概要

本製品では、キュープライオリティマッピングを使用した IEEE802.1p と TOS の優先制御がサポートされています。この優先制御では、キュープライオリティマッピングを使用して、発信パケットに対して出力キューイングのプライオリティ(8 段階)を指定します。キュープライオリティが高いほど、数字が大きくなります。発信パケットのキュープライオリティを選択する際の基準となるポリシーには、宛先 MAC アドレス、IEEE802.1p ユーザプライオリティ、IP パケットの TOS プライオリティ、宛先 IP アドレスなどがあります。

パケットには、フィールドごとに異なるポリシーを割り当てることができます。本製品では、マッピングポリシーとして IEEE802.1p と TOS のフィールドが使用されていて、それぞれが異なるキュープライオリティにマップされている場合には、常に IEEE802.1p が優先されます。

IEEE802.1p ユーザプライオリティと、ユーザプライオリティからキュープライオリティへのマッピング(推奨)は、IEEE 802.1p 標準で定義されています。本製品の初期設定のマッピングは、以下のように定義されています(数字が大きいほどキュープライオリティが高くなります)。

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

表 9-6:IEEE802.1p ユーザプライオリティからキュープライオリティへのマッピング

キュープライオリティマッピングに対する TOS 優先制御は、初期設定では次のように定義されています(数字が大きいほどキュープライオリティが高くなります)。

TOS 優先制御ビット	意味	キュープライオリティ
111	ネットワーク制御	7
110	インタネットワーク制御	6
101	CRITIC/ECP	5
100	フラッシュオーバライド	4
011	フラッシュ	3
010	即時	2
001	プライオリティ	1
000	ルーティン	0

表 9-7：TOS 優先制御ビットからキュープライオリへのマッピング

9.2.2 DOT1P（レイヤ 2、IEEE802.1p）の有効化／無効化

DOT1P（レイヤ 2、IEEE802.1p）からキュープライオリティへのマッピングで使用する管理モードを設定します。デフォルトでは、DOT1P からキュープライオリティへのマッピングは無効です。

9.2.2.1 DOT1P（レイヤ 2、IEEE802.1p）パラメータ

- enable：DOT1P－キュープライオリティマッピング機能の管理モード。DOT1P からキュープライオリティへのマッピングは有効です。
- disnable：DOT1P－キュープライオリティマッピング機能の管理モード。DOT1P からキュープライオリティへのマッピングは無効です。

9.2.2.2 DOT1P（レイヤ 2、IEEE802.1p）の有効化／無効化

DOT1P を有効化／無効化する場合は、次のようにコマンドを実行します。

```
L3SW> config switchconfig priority dot1p adminmode <enable | disable>
L3SW> config switchconfig priority dot1p adminmode enable
```

9.2.3 TOS（レイヤ 3、IP）の有効化／無効化

TOS（レイヤ 3、IEEE802.1p）からキュープライオリティへのマッピングで使用する管理モードを設定します。デフォルトでは、TOS からキュープライオリティへのマッピングは無効です。

9.2.3.1 TOS（レイヤ 3、IP）パラメータ

- enable：TOS－キュープライオリティマッピング機能の管理モード。TOS からキュープライオリティへのマッピングは有効です。
- disnable：TOS－キュープライオリティマッピング機能の管理モード。TOS からキュープライオリティへのマッピングは無効です。

9.2.3.2 TOS（レイヤ 3、IP）の有効化／無効化

TOS を有効化／無効化する場合は、次のようにコマンドを実行します。

```
L3SW> config switchconfig priority tos adminmode <enable | disable>
```

```
L3SW> config switchconfig priority tos adminmode enable
```

9.2.4 DOT1P プライオリティマッピング

IEEE802.1p ユーザプライオリティからキュープライオリティへのマッピングのエントリを作成します。

9.2.4.1 DOT1P プライオリティマッピングのパラメータ

- DOT1P_priority：IEEE802.1p ユーザプライオリティ。0～7 の 10 進数で指定します。
- QUEUE_priority：出力キュープライオリティ。0～7 の 10 進数で指定します。

詳細については、表 9-14 を参照してください。

9.2.4.2 CLI を使用した DOT1P プライオリティマッピングの設定

DOT1P プライオリティマッピングを設定する場合は、次のようにコマンドを実行します。

```
L3SW> config switchconfig priority dot1p map <dot1p priority> <queue priority>
L3SW> config switchconfig priority dot1p adminmode enable
L3SW> config switchconfig priority dot1p map 0 7
```

DOT1P サービスを使用する場合は、DOT1P モードを有効にする必要があります。

9.2.5 TOS プライオリティマップの設定

TOS ユーザプライオリティからキュープライオリティへのマッピングのエントリを作成します。

9.2.5.1 TOS プライオリティマッピングのパラメータ

- TOS：TOS 優先制御値。0～7 の 10 進数で指定します。
- Queue_priority：出力キュープライオリティ。0～7 の 10 進数で指定します。

詳細については、表 9-14 を参照してください。

9.2.5.2 CLI を使用した TOS プライオリティマッピングの設定

TOS プライオリティマッピングを設定する場合は、次のようにコマンドを実行します。

```
L3SW> config switchconfig priority tos map <tos priority> <queue priority>
L3SW> config switchconfig priority tos adminmode enable
L3SW> config switchconfig priority tos map 0 7
```

TOS サービスを使用する場合は、TOS モードを有効にする必要があります。

通常は、デフォルトの TOS プライオリティマッピングを使用してください。

DOT1P サービスと TOS サービスは共存できます。この場合は、常に DOT1P が優先されます。

9.2.6 DOT1P プライオリティの表示

IEEE802.1p ユーザプライオリティからキュープライオリティへのマッピングを表示する場合は、次のようにコマンドを実行します。

```
L3SW> show switchconfig priority dot1p
L3SW> show switchconfig priority dot1p

802.1p User Priority:  0  1  2  3  4  5  6  7
   Queue priority:  7  1  2  3  4  5  6  0
```

本製品では、プライオリティキューイングと同時に、WFHBD（Weighted Fair Hash Buffer Distribution）もサポートされています。そのため、ネットワークが過負荷状態の場合は、優先順位の高いトラフィックが少し減少され、その分が優先順位の低いトラフィックに割り当てられます。これは、優先順位の低いトラフィックが利用できる帯域幅がゼロにならないようにするための措置です。この措置が実行された場合は、優先順位の高いトラフィックが送出ポートの最大許容帯域幅を超えていない場合でも、ごく少量のパケット損失が発生します。

9.2.7 TOS プライオリティの表示

TOS ユーザプライオリティからキュープライオリティへのマッピングを表示する場合は、次のようにコマンドを実行します。

```
L3SW> show switchconfig priority tos
L3SW> show switchconfig priority tos

IP Precedence:  0  1  2  3  4  5  6  7
Queue priority: 7  1  2  3  4  5  6  0
```

9.2.8 DOT1P / TOS 要約

DOT1P/TOS 設定情報を表示する場合は、次のようにコマンドを実行します。このコマンドには、表 9-8 に示すような応答が返されます。

```
L3SW> show switchconfig summary
L3SW> show switchconfig summary
```

```
L3SW>show switchconfig summary

Broadcast Storm Recovery Mode.....................  Disable
Broadcast Storm Recovery Maxim Threshold..........  5
802.3x Flow Control Mode..........................  Enable
802.1p Priority Mode..............................  Disable
Tos Priority Mode.................................  Disable

L3SW>
```

表 9-8：スイッチ設定詳細の表示例

9.3 セキュリティ機能

本製品では、次のセキュリティ関連機能がサポートされています。

- アクセス制御リスト（ACL：Access Control List）
- サービス妨害攻撃防止（DAP：Denial of Service Attack Prevention）
- ネットワークアドレス変換（NAT：Network Address Translation）

これらのセキュリティ機能と帯域幅プロビジョニング機能は本製品内の同じ分類リソースをするため、互いに競合することがあります。競合を回避するため、本製品では帯域幅プロビジョニング機能とセキュリティ機能は同時に有効にできないように構成されています。

9.3.1 セキュリティオプションの設定

ACL、DAP、NAT のセキュリティ機能を有効化／無効化する場合は、次のようにコマンドを実行します。

```
L3SW> config security <enable/disable>
L3SW> config security enable
```

セキュリティ機能が無効な場合は、ACL、DAP、NAT に関連するすべてのコマンドが拒否されます。

本製品のセキュリティ機能を有効にする場合は、事前に帯域幅プロビジョニング機能と Static MAC Filtering を無効にする必要があります。

セキュリティに関連する設定は、次のコマンドを実行することにより、個別またはすべてを同時にクリアできます。

```
L3SW> clear security <acl/dap/nat/all>
L3SW> clear security all
```

セキュリティ機能の有効／無効を確認する場合は、次のようにコマンドを実行します。

```
L3SW> show security
L3SW> show security
```

9.4 アクセス制御リスト（ACL）

ACL は、発信元 IP アドレス、宛先 IP アドレス、IP プロトコル、TCP ポート、UDP ポートなど、さまざまな基準に基づいてパケットを選択的に許可または拒否するためのリストです。本製品では、高レベル ACL と低レベル ACL という 2 種類の ACL が使用されています。 高レベル ACL は、ハードウェアがサポートする分類テーブルを取り除き、純粋にアプリケーションの観点から ACL ルールを設定するための一連のコマンドを提供します。本製品は、ユーザ定義の ACL ルールを、ハードウェアが保持する分類テーブルのエントリに変換します。ユーザ定義の ACL ルールを該当する分類テーブルのエントリに変換する作業は非常に複雑なため、高レベル ACL は高レベル ACL ルールの生成に使用されるコマンドの構文とセマンティックスに一定の制限を課します。低レベル ACL ルールは、ハードウェア分類テーブルをそのまま使用するため、ユーザは分類テーブルのエントリを作成することができます。そのため、低レベル ACL ルールは高レベル ACL に比較して制限が少なくなっています。本マニュアルでは、高レベル ACL ルールと

低レベル ACL ルールをそれぞれ「H-ACL」、「L-ACL」と略して示すこともあります。

H-ACL とL-ACL は互いに排他的です。そのため、アプリケーションイメージはブート時にH-ACL またはL-ACL のいずれか一方をサポートするように設定されます。

現在、本製品はすべて、L-ACL をサポートするように設定して出荷されています。H-ACL への切り替えが必要な場合は、販売担当者か技術サポート担当者にお問い合せ下さい。

現在、L-ACL でのNAT はサポートされていません。

本製品では、ハードウェア分類テーブルでサポートされていない処理／分類方式を使用する ACL ルールを設定することも可能です。これらのルールは CPU でサポートされるもので、「ソフトウェア ACL（S-ACL）」と呼ばれます。本製品では、ハードウェア ACL ルールは約 100 個のルールを、ソフトウェア ACL ルールでは 128 個のリストとポリシーを設定できます。

9.5 高レベル ACL

H-ACL は、発信元 IP アドレス、宛先 IP アドレス、IP プロトコル、TCP ポート、UDP ポートなど、さまざまな基準に基づいてパケットを選択的に許可または拒否するためのリストです。

H-ACL の設定は 2 つのステップで行います。最初に、アクセスリストを必要なアクセス制限を盛り込んで定義します。次に、このアクセスリストを特定の物理ポートに適用します。

アクセスリストは、特定の物理ポートに、着信フィルタリングか発信フィルタリングのいずれかとして適用します。H-ACL を着信フィルタリングとして物理ポートに適用した場合は、指定した物理ポートがパケットを受信すると、アクセスルールとマッチするパケットが制御（許可または拒否）されます。H-ACL を発信フィルタリングとして物理ポートに適用した場合は、指定した物理ポートにパケットがスイッチまたはルートされると、アクセスルールとマッチするパケットが制御されます。

各物理ポートは 1 つのアクセスモードに関連付けられます。アクセスモードは、物理ポートで受信した着信パケットを許可すべきかどうかを決定します。アクセスモードはさらに、物理ポートで行われるパケットのフィルタリング方法の初期設定を定義します。本製品では、2 タイプのアクセスモードがサポートされています。

- **loose アクセスモード**
- **strict アクセスモード**

物理ポートが loose モードの場合、初期設定では、出入りするすべてのパケットが許可されます。H-ACL を使用すると、その物理ポートで受信したトラフィックや、その物理ポートにスイッチまたはルートされたトラフィックを選択的に拒否することができます。

物理ポートが strict モードの場合、初期設定では、出入りするすべてのパケットが拒否されます。H-ACL を使用すると、その物理ポートで受信したトラフィックや、その物理ポートにスイッチまたはルートされたトラフィックを選択的に許可することができます。特に明記しない限り、これ以降の部分では H-ACL を単に ACL として示します。

本製品では、2 タイプの ACL がサポートされています。

- 標準 ACL：発信元 IP サブネットアドレスとして指定された発信元 IP アドレスだけに基づいて、パケットを選択的に許可または拒否します。
- 拡張 ACL：発信元 IP アドレスに加えて、宛先 IP アドレス、IP プロトコル、TCP ポート番号、UDP ポート番号の任意の組み合せに基づいて、パケットを選択的に許可または拒否します。

本製品では、着信パケットフィルタリング用の標準 ACL はサポートされていますが、発信パケットフィルタリング用の標準 ACL はサポートされていません。

次の拡張 ACL ルールがサポートされています。

1. 発信元 IP サブネットアドレスに基づく、着信パケットフィルタリング用の ACL。
2. 宛先 IP サブネットアドレスに基づく、発信パケットフィルタリング用の ACL。
3. 発信元または宛先 IP サブネットアドレスと、IP プロトコル、宛先 TCP ポート、宛先 UDP ポートの任意の組み合せとに基づく ACL。
4. 本製品を宛先とするトラフィックに適用される、発信元 IP サブネットアドレスに基づく ACL。telnet 経由 CLI、WBI、SNMP などの本製品の管理機能へのアクセスを制限する場合に使用します。
5. 内部発信元 IP アドレスを持ち、NAT を適用する必要のあるトラフィックを通過させるための、発信元 IP サブネットアドレスに基づく着信パケットフィルタリング用の ACL

アクセスリストは、顧客トラフィックを搬送する通常の物理ポート（ネットワークポート）に適用できます。アクセスリストは、管理アクセス専用の物理ポート（サービスポート）には適用できません。発信元 IP サブネットアドレスで定義されるアクセスリストをスイッチ自体に適用して、本製品を終点とするトラフィックのパケットフィルタリングを行うことも可能です。ただし、スイッチに適用したアクセスリストを同時に物理ポートにも適用することはできません。本製品では、VLAN などの論理インタフェース上の ACL はサポートされていません。

本製品では、発信元 IP サブネットアドレスと宛先 IP サブネットアドレスを同時に定義したアクセスリストはサポートされていません。

内部ネットワークから発信された NAT を要するトラフィックを通過させるように指定するアクセスリストは、IP プロトコル、TCP ポート、UDP ポートの指定のない、許可／着信アクセスリストとしてのみ定義できます。そのため、NAT を要する内部トラフィックを対象に定義できるのは、標準 ACL に限られます。

本製品では、標準 ACL と拡張 ACL を含む最大 36 のアクセスリストを使用できます。また、1 つのアクセスリストに使用できるルール数は 1 つに制限されています。

9.5.1 ACL パラメータ

本製品では、各 ACL エントリは、以下のパラメータを使用して生成されます。

- アクセスリスト番号：アクセスポリシーを識別します。
- 発信元または宛先：発信元または宛先 IP アドレス。
- トラフィックのルール：permit または deny。

- 方向：ACL を適用する方向。インバウンドまたはアウトバウンド。
- 発信元 IP アドレスはインバウンド方向に適用され、宛先 IP アドレスはアウトバウンド方向に適用されます。
- ワイルドカード：ACL ポリシーを適用するサブネットを示すワイルドカード。
- L4 プロトコルタイプ：ACL ポリシーを適用するレイヤ 4 プロトコルタイプ（任意）。
- ポート/ポート範囲：ACL ポリシーを適用する個別 TCP/UDP ポートまたはポート範囲（サイズは 16）（任意）。

ACL をスイッチとスイッチポートに同時に適用することはできません。

ACL は本製品の物理ポート上で機能します。LAG ポート(2.1 など)や仮想ルータポート(4.1 など)には適用できません。

9.5.2 CLI を使用した ACL の設定

9.5.2.1 ACL の生成

次のコマンドで、ACL を生成します。

L3SW> config access list create <access-list-number> <deny | permit> <in | out> <protocol> <source | destination> <wildcard> [<dst-port-start> <dst-port-end>] [log]

以下に、このコマンドの重要なパラメータについて説明します。

- access-list-number：通常の ACL パケットフィルタリング用に 0～47、NAT 用に 100～103 までの 10 進数で指定します。
- protocol：icmp、igmp、ospf など使用可能な値を指定します。
- wildcard：wildcard には“1”または“0”が指定でき、<source | destination>に適用されます。“0”を指定した場合、送信元または宛先パケットの IP アドレスが、<source | destination>で指定された値と完全に一致している必要があります。“1”を指定した場合、IP アドレスの対応は無視されます。
- dst-port-start ：宛先 TCP または宛先 UDP ポート範囲の開始ポートを指定します。宛先 TCP または宛先 UDP ポート範囲のサイズは 2m（2 の m 乗：m は 0～16）以内です。5,68 のような値は無効です。BGP、FTP、TELNET などのプロトコルで使用される標準 TCP ポートや BOOTC/BOOTS、RIP、SNMP などのプロトコルで使用される標準 UDP ポートは、この dst-port-start の値で定義可能です。
- dst-port-end：宛先 TCP または宛先 UDP ポート範囲の終了ポートを指定します。宛先 TCP または宛先 UDP ポート範囲のサイズは 2m（2 の m 乗：m は 0～16）以内です。5,68 のような値は無効です。BGP、FTP、TELNET などのプロトコルで使用される標準 TCP ポートや BOOTC/BOOTS、RIP、SNMP などのプロトコルで使用される標準 UDP ポートは、この dst-port-end の値で定義可能です
- log：このパラメータを指定するとスイッチは、ACL ルールで定義されたフィルタによりドロップされたパケットをカウントします。このパラメータは、拒否ルールに対してのみ有効です。

例えば、サブネット 172.30.30.0 からのすべての IP トラフィックを拒否するための ACL ルールを設定する場合は、次のようにコマンドを実行します。

```
L3SW> config access list create 10 deny in ip 172.30.30.0 0.0.0.255
log
```

9.5.2.2 ACL の削除

次のコマンドで、ACL を削除します。

```
L3SW> config access list delete <acc-list-number>
L3SW> config access list delete 10
```

9.5.2.3 ポートへの ACL の追加と削除

ACL をポートに追加する場合には、ポートのアクセスモードを指定しておく必要があります。デフォルトでは、すべてのポートは loose モードに設定されています。そのため、loose モードのポートに対して ACL を定義する場合は、アクセスモードを設定する必要はありません。ポートを strict モードにする必要がある場合、または strict アクセスモードから loose モードに戻す場合には、次のコマンドを実行します。

```
L3SW> config access mode <slot.port|switch> <loose|strict>
L3SW> config access mode 0.1 loose
```

次のコマンドで、ACL を物理ポートに関連付けます。

```
L3SW> config access group add <slot.port|switch> <acc-list-number>
L3SW> config access group add 0.1 10
```

slot.port 番号には、物理ポート番号を指定します。2.1、2.2、4.1、4.2 のような論理ポート番号は使用できません。複数のポートで同じ ACL を共有する場合は、ポートごとに ACL を追加する必要があります。

ACL グループを削除する場合は、次のコマンドを実行します。

```
L3SW> config access group delete <slot.port|switch> <acc-list-number|all>
L3SW> config access group delete 0.1 10
```

9.5.2.4 ACL の統計と設定の表示

ACL の設定およびドロップしたパケットの統計を表示する場合は、次のコマンドを実行します。

```
L3SW> show access list
```

ポートに設定されているアクセスリストを表示する場合は、次のコマンドを実行します。

```
L3SW> show access group port <slot.port|switch>
L3SW> show access group port 0.1
```

各物理ポートに設定されているアクセスモードを表示する場合は、次のコマンドを実行します。

```
L3SW> show access mode
L3SW> show access mode
```

9.5.3 ACL の設定例

次に説明する一連のコマンドは、本製品に ACL ルールを設定する一例です。

9.5.3.1 Loose アクセスモードの設定例

- **サブネット 172.30.30.0 からのトラフィックをすべて拒否します。**

```
L3SW> config access list create 10 deny in ip 172.30.30.0 0.0.0.255
log
L3SW> config access group add 0.1 10
```

- **172.31.30.0 からの FTP トラフィックをすべて拒否します。**

```
L3SW> config access list create 11 deny in TCP 172.31.30.0 0.0.0.255
ftp ftp log
L3SW> config access group add 0.1 11
```

- **10.1.0.0 への送出トラフィックをすべて拒否します。**

```
L3SW> config access list create 12 deny out ip 10.1.0.0 0.0.255.255
L3SW> config access group add 0.1 12
```

- **サブネット 172.40.2.0 への送出 SMTP トラフィックをすべて拒否します。**

```
L3SW> config access list create 13 deny out TCP 172.40.2.0 0.0.0.255
smtp smtp log
L3SW> config access group add 0.1 13
```

この例で設定された loose モードのアクセスリストルール、アクセスグループ、スイッチポートの表示例を次に示します。

```
L3SW>show access list

Num  Action Dir Prot Source/      Wildcard     Port   Range Log Drop
                       Destination                    Begin  End    NAT
---  ------ --- ---- ------------ ---------- ------ ----- --- ----
10   deny    in   ip   172.30.30.0  0.0.0.255                    Log 0
11   deny    in   ip   172.30.31.0  0.0.0.255     ftp    ftp    Log 0
12   deny    out  ip   10.1.0.0      0.0.0.255                    Log 0
13   deny    out  ip   172.42.2.0   0.0.0.255     smtp   smtp  Log 0

L3SW>
```

表 9-9:アクセスリストルールの表示例

```
L3SW>show access group list

Access List Number (slot, port)
------------------ ------------
10                      0.1
11                      0.1
12                      0.1
13                      0.1
L3SW>
```

表 9-10:アクセスグループの表示例

```
L3SW>show access mod

slot.port Access Mode
---------  -----------
0.1          loose
0.2          loose
0.3          loose
0.4          loose
0.5          loose
0.6          loose
0.7          loose
0.8          loose
0.9          loose
0.10         loose
0.11         loose
0.12         loose
0.13         loose
0.14         loose
0.15         loose
0.16         loose
0.17         loose
0.18         loose
0.19         loose
--More— or (q)uit
```

表 9-11：物理ポートのアクセスモードの表示例

9.5.3.2 strict アクセスモードの設定例

- ポート 0.2 を strict モードに設定します。

```
L3SW> config access mode 0.2 strict
```

- サブネット 172.30.30.0 からのトラフィックをすべて許可します。

```
L3SW> config access list create 20 permit in ip 172.32.30.0 0.0.0.255
L3SW> config access group add 0.2 20
```

- 172.30.30.0 からの FTP トラフィックをすべて許可します。

```
L3SW> config access list create 21 permit in TCP 172.32.31.0 0.0.0.255
FTP
L3SW> config access group add 0.2 21
```

- 10.1.0.0 への送出トラフィックを許可します。

```
L3SW> config access list create 22 permit out ip 12.32.31.0
0.0.255.255
L3SW> config access group add 0.2 22
```

- サブネット 172.40.2.0 への送出 SMTP トラフィックをすべて許可します。

```
L3SW> config access list create 23 deny out TCP 172.40.31.0 0.0.0.255
smtp log
L3SW> config access group add 0.2 23
```

この例で設定された strict モードのアクセスリストルール、スイッチポート 0.2 の表示例を次に示します。

```
 L3SW >show access list

 Num Action Dir Prot Source/       Wildcard       Port   Range Log Drop
                          Destination                    Begin End     NAT
--- ------- --- ---- ------------ ------------ ---- ---- ---- -----
 20  permit in   ip    172.32.30.0  0.0.0.255
 21  permit in   tcp   172.32.31.0  0.0.0.255      ftp   ftp
 22  permit out ip     12.32.31.0   0.0.0.255
 23  deny    out tcp    172.40.31.0  0.0.0.255     smtp  smtp    Log  0

 L3SW>
```

表 9-12:アクセスリストの表示例

```
L3SW>show access mode

slot.port Access Mode
--------- -----------
0.1         loose
0.2         strict
0.3         loose
0.4         loose
0.5         loose
0.6         loose
0.7         loose
0.8         loose
0.9         loose
0.10        loose
0.11        loose
0.12        loose
0.13        loose
0.14        loose
0.15        loose
0.16        loose
0.17        loose
0.13        loose
0.19        loose
—More— or (q)uit
```

表 9-13:アクセスモードの表示例

9.6 ネットワークアドレス変換(NAT)

9.6.1 概要

ネットワークアドレス変換(NAT:Network Address Translation)とポートアドレス変換(PAT:Port

Address Translation）は、多くの場合総称して NAT と呼ばれます。NAT はルータで非常に有用な機能であり、特にルータがイントラネットとインタネットの間に配置されている場合に威力を発揮します。

企業などでは、内部 IP アドレスを内部ホストに割り当てるのが一般的です。これはセキュリティ上の理由による場合もありますが、単にグローバル IP アドレスがないためにこの方法をとらざるを得ないことも少なくありません。インターネットの急速な普及により IP アドレスは不足する傾向にあり、現在では、数百台のコンピュータを備える企業が数個のアドレスしか持てないという状況も発生しています。内部アドレスはイントラネットの中では問題なく使用できますが、インターネットアクセスには使用できません。

NAT は、内部ホスト間でグローバル IP アドレスを共有するための 1 つの方法です。インターネットへのアクセスが実行されると、NAT はグローバル IP アドレスを割り当てて、送出パケットと着信パケットの間で変換を実行します。外部から見ると、これは合法的なグローバルホストからの通信のように見えます。外部ホストと内部ホスト間のセッションが終わると、グローバル IP アドレスは解放され、他の内部ホストによって使用されます。

NAT は、変換のタイプに応じて、静的 NAT と動的 NAT に分類することができます。本製品では、両方の NAT がサポートされています。

9.6.2 NAT 機能の関連用語

9.6.2.1 内部と外部

「内部」と「外部」（または「内側」と「外側」）という用語は、組織内部の（安全な）ネットワークと外部の（安全でない）ネットワーク（インタネットなど）を意味します。NAT は主にイントラネットとインターネット間の変換に使用されます。NAT では、イントラネットは内部（または内側）、インターネットは外部（または外側）と呼ばれます。

9.6.2.2 セッション

アドレス間の変換（内部アドレスと外部アドレスの変換など）は、論理結合から始まります。この論理結合は、「セッション」と呼ばれる期間にわたってアクティブ状態になります。セッションには寿命があります。セッションは変換が必要になると確立され、不要になると終了します。セッションの方向は、セッションを開始したパケットから見た方向です。セッションが確立されると、パケットの送受信が可能になります。標準的な NAT では、セッションのほとんどがアウトバウンド方向（内部ホストによって開始される）です。

本製品の NAT 実装では、最大 1024 の同時セッションがサポートされます。

9.6.2.3 ウトバウンド静的 NAT

内部 IP アドレスから事前定義された外部 IP アドレスへのアドレス変換は、「アウトバウンド静的 NAT」と呼ばれます。静的 NAT を行うためには、各外部アドレスに 1 つの外部アドレスが必要です。

アウトバウンド静的 NAT は、inside source static コマンドを使って設定します。

9.6.2.4 インバウンド静的 NAT

外部 IP アドレス／ポートから事前定義された外部 IP アドレスへのアドレス変換は、「インバウンド静的 NAT」と呼ばれます。この NAT は、イントラネット内のサービスを外部に公開するために使用されます。

アウトバウンド静的 NAT は、inside destination static コマンドを使って設定します。

9.6.2.5 動的 NAT

動的 NAT は、サブネットからの内部 IP アドレスを外部 IP アドレスプールに動的にマッピングするプロセスです。この NAT は、多数の内部ホストが少数の外部 IP アドレスを共有している場合に使用されます。

動的 NAT は、inside source dynamic コマンドを使って設定します。

9.6.2.6 PAT

使用量が膨大な場合には、PAT を使って外部 IP アドレスの可用性を高めることができます。これは、IP アドレスに加えて、ポート番号 10,000～40,000 も変換に使用することで実現されます。この場合は、1 つの外部 IP アドレスで、インターネット上の外部ホストへのアクセスを試みる内部ホストを 30,000 台までサポートできます。

本製品では、config ip nat pool create コマンドにキーワード overload を入力すると、プール内の最後の IP アドレスが PAT 用として予約されます。この場合は、他のすべてのアドレスが使用されていても、システムはこのアドレスを使ってポート変換を実行することができます。

PAT は、性質上、TCP、UDP、ICMP エコー／応答用としてしか使用できません。

9.6.2.7 エージング

エージングは、非アクティブな NAT セッションを除去するための機能です。非アクティブな NAT セッションは除去する必要があります。除去しない場合は、システムリソースがすべて消費され、変換が不可能になります。

タイムアウト値は、パケットタイプによって異なります。この値は、config ip nat translation timeout コマンドを使って設定できます。

9.6.2.8 FTP プロキシ

プロトコルの中には、一般的なアドレス変換やポート変換のほかに、特殊な処理を必要とするものもあります。例えば、FTP では、内容に IP 情報とポート情報が埋め込まれており、これらの情報も変換する必要があります。通常、プロトコルに固有な変換は、アプリケーション層ゲートウェイ（ALG：Application Level Gateways）と呼ばれるアドオンとしてシステムに実装されます。本製品では、NAT 内に「プロキシ」と呼ばれる広く普及したプロトコルをサポートすることにより、高速変換が実現されています。

現在、FTP プロキシだけがサポートされています。

プロキシは自動的にサポートされます。ユーザが明示的にルールを設定する必要はありません。NAT がプロキシを必要とするパケットを検出すると、適切なプロキシが自動的に呼び出され

ます。例えば、パケットの宛先が標準 FTP ポート番号 21 の場合は、FTP プロキシが適用されます。

9.6.3 サポートされる機能

本製品でサポートされる NAT 機能は、次のとおりです。

- **静的 NAT**
- **静的 NAPT(ネットワーク変換、ポート変換)**
- **動的 NAT**
- **PAT**
- **ICMP 変換**
- **FTP プロキシ**

9.6.4 NAT の設定

本製品の NAT 機能は、次のように設定します。

NAT コマンドを実行する前に、セキュリティ機能を有効にしてください。

9.6.4.1 ポート設定

NAT の設定は、物理ポートに関連付けられます。NAT を有効にするポートは、次のコマンドで内部ポートまたは外部ポートに設定しておきます。

```
L3SW> config ip nat interface <slot.port | all> <inside | outside>
L3SW> config ip nat interface 0.10 inside
```

デフォルトでは、すべてのポートは「外部」として設定されています。

9.6.4.2 静的 NAT の設定

9.6.4.2.1 内部発信元 NAT

内部 IP アドレスと外部 IP アドレスを 1 つずつ持つ静的内部発信元 NAT を生成する場合は、次のコマンドを実行します。

```
L3SW> config ip nat inside source static create <internal-ip> <external-ip>
L3SW> config ip nat inside source static create 192.168.10.10 167.254.254.96
```

この変換ルールを適用すると、内部ホスト 192.168.10.10 から送出されるすべてのパケットの IP アドレスが 167.254.254.96 に変換されます。

内部発信元 NAT を削除する場合は、次のコマンドを実行します。

```
L3SW> config ip nat inside source static delete <internal-ip> <external-ip>
L3SW> config ip nat inside source static delete 192.168.10.10 167.254.254.96
```

9.6.4.2.2 内部宛先 NAT

内部宛先 NAT を削除する場合は、次のコマンドを実行します。

```
L3SW> config ip nat inside destination static create <tcp|udp> <internal-ip> <internal-port> <external-ip>
<external-port>
L3SW> config ip nat inside destination static create tcp 192.20.10.2 8084
167.254.250.96 80
```

パケットは、イントラネット上のホストに転送される前に、宛先 IP アドレス 192.20.10.2 とポート番号 8084 に変換されます。

外部ポート番号が FTP などのよく知られたサービスポートの場合は、アプリケーションプロキシが自動的に起動されます。

内部宛先 NAT を削除する場合は、次のコマンドを実行します。

```
L3SW> config ip nat inside destination static delete <tcp|udp> <internal-ip> <internal-port> <external-ip>
<external-port>
L3SW> config ip nat inside destination static delete tcp 192.20.10.2 8084
167.254.250.96 80
```

9.6.4.3 動的 NAT の設定

9.6.4.3.1 PAT を使用しない動的 NAT の設定

PAT を使用しない動的 NAT を設定する場合は、NAT 用の ACL をイントラネット用に設定する必要があります。

```
L3SW> config access list create <access-list-number> permit in ip <source> <wildcard>
L3SW> config access list create 101 permit in ip 192.168.10.1 0.0.0.255
```

NAT に対して最大 4 つの ACL（ACL 番号 100～103）を設定できます。ACL 番号 100～103 は NAT 用として予約されます。

ACL の設定が完了したら、次のコマンドを実行して、overload を含まないグローバル IP アドレスプールを設定します。

```
L3SW> config ip nat pool create <nat-pool-name> <subnet-address> <subnet-mask>
L3SW> config ip nat pool create global1 167.254.254.96 255.255.255.240
```

グローバル IP アドレスプールは、外部 IP アドレスの総数（静的外部 IP アドレスを含む）が 256 以下となる範囲内で、最大 4 つまで設定できます。

さらに、次のコマンドを実行して、動的 NAT を設定します。

```
L3SW> config ip nat inside source dynamic create <access-list-number> <nat-pool-name>
L3SW> config ip nat inside source dynamic create 101 global1
```

1 つの NAT 用 ACL を複数のグローバル IP アドレスプールに関連付けることができます（その逆も同様）。

9.6.4.3.2 PAT を使用する動的 NAT の設定

PAT を使用する動的 NAT を設定する手順は、PAT を使用しない動的 NAT を設定する手順とほぼ同じです。唯一の違いは、次のように、PAT 用プールを作成するときにキーワード

overload を追加することです。

```
L3SW> config ip nat pool create <nat-pool-name> <subnet-address> <subnet-mask> overload
L3SW> config ip nat pool create global1 167.254.254.96 255.255.255.240
overload
```

キーワード overload は、ポートの変換で、プール内の最後の IP アドレス（上記の例では 167.254.254.111）が使用されることを意味します。

1 つの ACL に複数のプールが関連付けられている場合、オーバロードできるのは最後のプールだけです。

9.6.4.4 NAT 表示の設定

静的／動的 NAT の設定とその統計を表示する場合は、次のコマンドを実行します。

```
L3SW)> show ip nat stats <static/dynamic>
L3SW)> show ip nat stats static
L3SW)> show ip nat stats dynamic
```

```
L3SW>show ip nat stats static

Dest                                      UDP  Port Port Count
---- ------------ -------------- --- ---- ---- -----
dst  192.168.1.4   167.251.254.96 tcp 8000 80    0
dst  192.168.1.4   167.254.254.96 tcp 1021 21    0

Total translations.............................    3
Static ....................................... 2
Dynamic ...................................... 1
Hits ......................................... 0
Misses ....................................... 0
Expired translations ......................... 0
Total sessions ............................... 0
Available sessions ........................... 1024

L3SW>
```

表 9-14：静的 NAT のルールと統計の表示例

```
L3SW>show ip nat stats dynamic
Access List          Pool                              PAT Ref
Number:Subnet        Name:Subnet                          Count
-----------------  ----------------------- --- -----
101.192.168.1.0/24  global:167.254 254.96/28      0

Total translations.............................  3
  Static.......................................  2
  Dynamic......................................  1
Hits...........................................  0
Misses.........................................  0
Expired translations...........................  0
Total sessions.................................  0
```

9.7 Available sessions 1024

```
L3SW>
```

表 9-15:動的 NAT のルールと統計の表示例

9.7.1.1 NAT 変換タイムアウトの表示

IP、TCP、UDP のタイムアウト値(単位:秒)を表示する場合は、次のコマンドを実行します。

L3SW)> show ip nat translation timeout
L3SW)> show ip nat translation timeout

9.7.2 L3SW>show ip nat translation timeout

```
IP ..........................................  1800
TCP .........................................  1800
FinRst ......................................  15
UDP .........................................  300

L3SW>
```

表 9-16:NAT 変換タイムアウトの表示例

9.7.3 使用例

次の図は、ポート 0.6 を内部ネットワーク(企業ネットワーク、サブネット 172.30.10.0/24)用に設定し、ポート 0.23 を外部ネットワーク(インタネット)用に設定した構成例です。この例では、内部ネットワークのすべてのユーザがインターネットにアクセスできなければなりません。内部ホスト 172.30.10.2 はウェブサーバで、このサーバのサービスポート 8080 が標準 HTTP ポート 80 からインターネット上に公開されます。

この例では、ISP はこのネットワークのグローバルアドレスとして IP アドレス 144.148.10.16～28

を割り当てるものと想定します。また、このグローバルアドレスプールから、IP アドレス 144.148.10.17 がウェブサーバのグローバル IP アドレスとして割り当てられます。

このネットワーク内で NAT を設定する場合に実行するコマンドセットを次に示します。

- **ステップ 1：内側と外側のインタフェースを設定します。**

```
L3SW> config ip nat interface 0.6 inside
L3SW> config ip nat interface 0.23 outside
```

- **ステップ 2：アクセスリストを生成します。**

```
L3SW)> config access list create 101 permit in ip 172.30.10.0 0.0.0.255
```

- **ステップ 3：NAT プールを生成します。**

```
L3SW)> config ip nat pool create global1 144.148.10.16 255.255.255.240
```

- **ステップ 4：動的 NAT を生成します。**

```
L3SW)> config ip nat inside source dynamic create 101 global1
```

- **ステップ 5：ウェブサービスをインターネットに公開します。**

```
L3SW> config ip nat inside destination static create tcp 172.30.10.2 8080
144.148.10.17 80
```

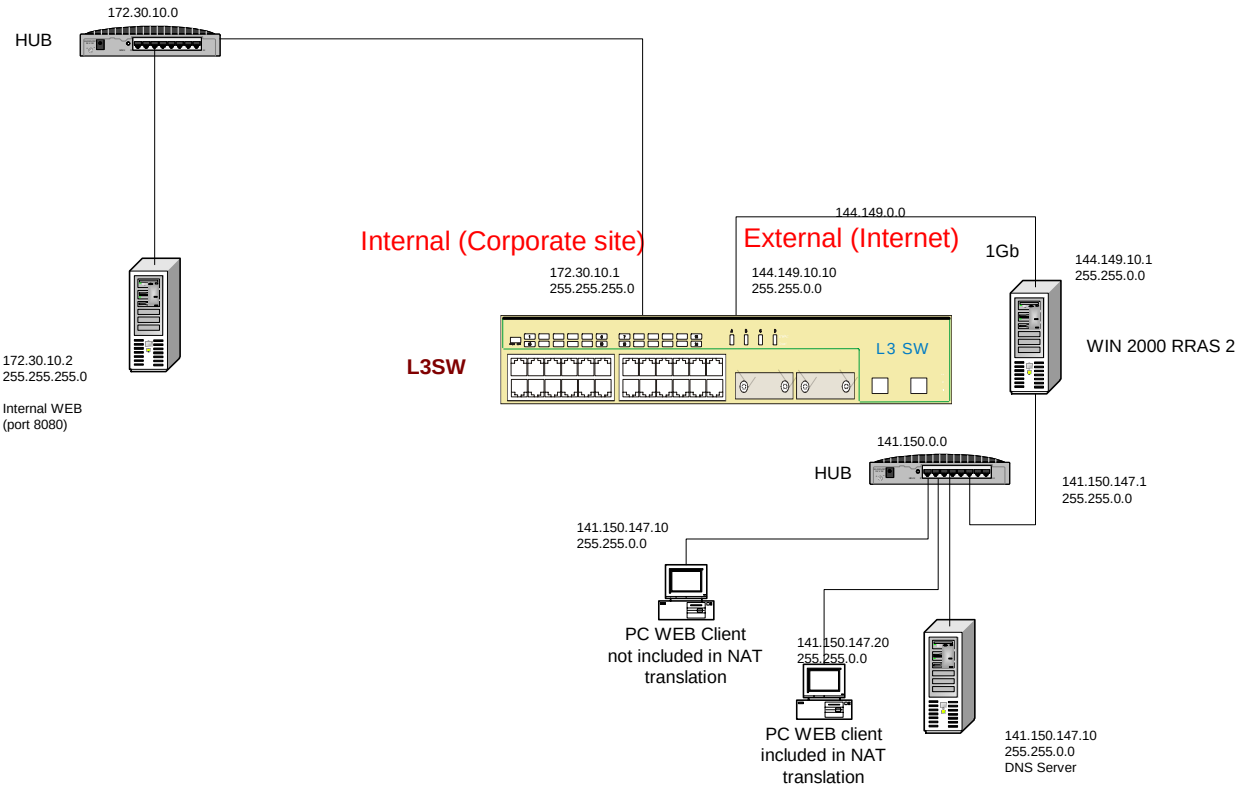

図 9-1：NAT の構成例

9.8 低レベル ACL

L-ACL では、ユーザ自身が一連の CLI コマンドを直接実行して、ハードウェア分類テーブルを設定できます。この機能を使うと、QoS 処理タイプごとに、非常に高度なパケットフィルタリングとフローグループ定義を設定することが可能になります。本製品では、以下の分類テーブルがサポートされています。

- **パケットタイプ分類テーブル**
- **ホストグループ分類テーブル**
- **L4 分類テーブル**
- **メインルールテーブル**

パケットタイプ分類テーブルは、Ethernet タイプ(IP、IPX、ARP など)とパケットタイプ(ユニキャスト、マルチキャスト、ブロードキャスト)に基づいてパケットを分類します。ホストグループ分類テーブルは、L2 MAC アドレスまたは L3 IP アドレスに基づいてパケットを分類します。L4 分類テーブルは、L4 パケットタイプ(TCP、UDP、ICMP など)と L4 プロトコルと関連付けられたポート番号(TCP ポート番号、UDP ポート番号など)などの L4 情報に基づいてパケットを分類します。メインルールテーブルは、他の 3 つの分類テーブルで分類されたパケットに対して実行するアクションまたは QoS 処理を定義します。実行可能なアクションは、drop、permit、copy-to-cpu、no-copy-to-cpu などです。パケットのフィルタリングを行うためには、分類されたパケットに対して実行するアクションタイプ“permit”または“drop”を定義する必要があります。アクションタイプ“copy-to-cpu”は、S-ACL のサポートと、その他の特殊な処理のために使用されます。QoS 処理タイプには、CoS、キュープライオリティ、ToS 値への割り当てなどがあります。

本製品では、分類テーブルとメインルールテーブルでキーワード“any”を指定することによって、“don't care”条件を定義できます。また、エントリの作成時に名前を割り当てると、テーブルのエントリを参照できるようになります。テーブルを構成するエントリのフィールドに“don't care”値を入力できるため、パケットは、テーブル内の複数のエントリで定義された複数のルールとマッチする可能性があります。複数マッチによる競合を解決するため、本製品ではテーブル内の各エントリに優先度値を割り当てられるようになっています。この値を割り当てた場合は、複数マッチが発生すると、ハードウェアは優先度値の最も低いエントリを選択します。以下では、本製品の 3 つの分類テーブルとメインルールテーブルを設定する方法について説明します。

上記のテーブルを生成する前に、“config security enable”コマンドを実行してセキュリティ機能を有効にする必要があります。

低レベル ACL のテーブル数には以下の制限があります。

- ***パケットタイプ分類テーブル:64***
- ***ホストグループ分類テーブル:110***
- ***L4 分類テーブル:110***
- ***メインルールテーブル:360***

9.8.1 パケットタイプ分類テーブルの設定

パケットタイプ分類テーブルでは、Ethernet ヘッダに含まれる ETYPE(Ethernet タイプ)の値とパケットのタイプ(ユニキャスト、ブロードキャスト、またはマルチキャスト)に基づいてパケットを分類できます。

パケットタイプ分類テーブルのエントリを設定する場合は、次のコマンドを実行します。

L3SW>config classifier packet create <name> <preferred priority> <ethernet type> <packet type>

パラメータ

- name：エントリ名。
- preferred priority：パケットタイプ分類テーブルのユーザ設定による優先度レベル。値は 1～62 の範囲です。複数のマッチが発生した場合は、最も低い値のエントリが選択されます。
- ethernet type：オプションは、IP、ARP、または 16 進数形式で表した特定の Ethernet タイプです。
- packet type：オプションは、ユニキャスト、ブロードキャスト、またはマルチキャストです。

パケットタイプ分類テーブルのエントリ 0～63 は予約されます。

```
L3SW>config classifier packet create pkt1 1 ip unicast
L3SW>config classifier packet create pkt2 2 arp any
```

1 番目のエントリ（pkt1）はすべてのユニキャスト IP パケットを識別し、2 番目のエントリ（pkt2）はすべての ARP パケットを識別します。これらのエントリは、それぞれ、ロケーション 1 とロケーション 2 に配置されます。

分類テーブルからエントリを削除する場合は、次のコマンドを実行します。

L3SW>config classifier packet delete <name>

```
L3SW>config classifier packet delete pkt2
```

パケットタイプ分類テーブルのエントリを表示する場合は、次のコマンドを実行します。次は実行例です。

L3SW>show classifier table packet <name|all>

```
KSUlJ   >show classifier table packet all

Packet Type Table entries:

Table                    Ethernet     Packet
Type    Name      Pri    Type         Type
------ -------- ---- ---------  ------
PACKET  RESERVED  0    0x0836       any
PACKET  pktl      1    0x0800       unicast
PACKET  pkt2      2    0x0806       any
PACKET  RESERVED  63   0x0000       unicast

L3SW>
```

表 9-17：パケットタイプ分類テーブルのエントリ例

9.8.2 ホストグループ分類テーブルの設定

ホストグループ分類テーブルは、MAC アドレスまたは IP アドレスに基づいてパケットを分類します。このテーブルでは、さらに、発信元／宛先ポート番号や VLAN ID 値に基づいて分類することもできます。また、IP パケットの場合は、上記に加えて IP ヘッダ内の QoS 値（diffserv）に基づく分類も可能です。

9.8.2.1 IP アドレスホストグループテーブルのエントリの設定

パケットホストグループ分類テーブルのエントリを設定する場合は、次のコマンドを実行します。

L3SW> config classifier host ip create <name> <preferred priority> <src | dst | any> <ip address | any> <ip mask | any> <slot.port | any> <diffserv | any> <vid | any>

パラメータ

- name：エントリ名。
- preferred priority：ホストタイプ分類テーブルのユーザ設定による優先度レベル。値は 5～114 の範囲です。
- src | dst | any：発信元または宛先アドレス、または any。
- ip address | any：IP アドレス、または any。
- ip mask | any：IP アドレスマスク、または any。
- slot.port | any：物理ポート、または any。指定できるのは物理ポートだけです。VLAN ルーティングが定義された論理インタフェースは指定できません。
- diffserv | any：0～63 のサービス識別番号、または any。パケットの IP ヘッダから抽出した QoS（6 ビット）と、このフィールドで指定された値とのマッチングが行われます。
- vid | any：VLAN ID、または any。

ホストグループ分類テーブルのエントリ 1～4 とエントリ 115～127 は、予約されます。

以下に、ホストグループテーブルの IP エントリの例を示します。

```
L3SW>config classifier host ip create hp8 11 any 0.0.0.0 255.0.0.0 0.3 2 3
L3SW>config classifier host ip create hp9 12 src 255.255.255.255 255.0.0.0
0.4 3 4
L3SW>config classifier host ip create hp10 13 dst 224.0.0.1 255.0.0.0 0.5 4
5
```

1 番目のエントリは、ポート 3 経由でスイッチに着信し、diffserv 値が 2 で、かつ Vlan ID が 3 のすべてのパケットを識別します。2 番目のエントリは、ポート 4 経由でスイッチに着信し、diffserv 値が 3 で、かつ Vlan ID が 4 のすべてのサブネットブロードキャストパケットを識別します。3 番目のエントリは、ポート 0.5 を通って着信し、diffserv 値が 4 で、かつ Vlan ID が 0.5 の、224.0.0.1 のアドレスを持つすべての IP マルチキャストパケットを識別します。上記 3 つのエントリはそれぞれ hp8、hp9、hp10 と命名され、ロケーション 11、12、13 に配置されます。

IP アドレスと関連付けられたホスト分類テーブルからエントリを削除する場合は、次のコマンドを実行します。

L3SW>config classifier host ip delete <name>

```
L3SW>config classifier host ip delete hp9
```

ホストグループテーブルエントリの結果を表示するには、次のコマンドを実行します。

次は実行例です。

L3SW>show classifier table host <name|all>
L3SW>show classifier table host all

```
L3SW>show classifier table host all

HostGroup Table entries:

Table              Addr Src/                    Network Mask/           Diff
Type Name      Pri Type Dst Address             Wildcard           Port Serv  VID
---- -------- --- ---- --- ---------------- ---------------  ---- ----  ---
HOST RESERVED 0   IP   src  0.0.0.0          0.0.0.0            any  any  any
HOST RESERVED 1   MAC  any  01:80:C2:00:00:02 00:00:00:00:00   any  ---- any
HOST RESERVED 2   any  src                                          any
HOST RESEHVED 3   any  src                                          any
HOST RESERVED 4   any  src                                          any
HOST hp8      11  IP   any  0.0.0.0             255.0.0.0          0.3  2    3
HOST hp9      12  IP   src 255.255.255.255    255.0.0.0          0.4  3    4
HOST hplO     13  IP   dst 224.0.0.1            255.0.0.0          0.5  4   5
HOST RESERVED 117 any  src                                         any
HOST RESERVED 118 any  src                                         any

L3SW>
```

表 9-18：IP アドレスホストグループテーブルのエントリの表示

9.8.2.2 MAC アドレスホストグループテーブルのエントリの設定

ホストグループテーブルのエントリに基づいて MAC を設定する場合は、次のようなコマンドを実行します。

L3SW> config classifier host mac create <name> <preferred priority> <src | dst | any> <mac address | any> <wildcard> <slot.port | any> <vid | any>

パラメータ

- name：エントリ名。
- preferred priority：ホストタイプ分類テーブルのユーザ設定による優先度レベル。値は 5～114 の範囲です。
- src | dst | any：発信元または宛先アドレス、または any。
- mac address | any：xx:xx:xx:xx:xx:xx 形式の MAC アドレス、または any。
- wildcard：MAC アドレスのビットを対象にマッチングを行うときに使用します。
- slot.port | any：物理ポート、または any。指定できるのは物理ポートだけです。VLAN ルーティングが定義された論理インタフェースは指定できません。
- vid | any：VLAN ID、または any。

MAC アドレスホストグループテーブルのエントリの例を次に示します。

```
L3SW>config classifier host mac create hm2 5 dst 22:22:22:22:22:22 any 0.2 2

L3SW>config classifier host mac create hm3 6 any 33:33:22:22:22:22 any 0.2 2

L3SW>config classifier host mac create hm7 9 src 55:55:55:55:55:55
FF:FF:FF:00:00:00 0.3 5
```

3 番目のコマンドでは、55:55:55:00:00:00～55:55:55:FF:FF:FF の発信元 MAC アドレスを持つすべてのパケットを選択するために、ワイルドカードマスクを使用していることに注意してください。

MAC アドレスと関連付けられたホスト分類テーブルからエントリを削除する場合は、次のコマンドを実行します。

```
L3SW>config classifier host mac delete <name>
L3SW>config classifier host mac delete hm2
```

ホストグループ分類テーブルのすべてのエントリを表示する場合は、次のコマンドを実行します。次は実行例です。

```
L3SW>show classifier table host <name|all>
L3SW>show classifier table host all
```

```
L3SW>show classifier table host all

Host Group Table entries:

Table                Addr Src/                      Network Mask/           Diff
Type Name      Pri Type Dst Address             Wildcard           Port Serv  VID
---- -------- --- ---- --- ---------------- ---------------  ---- ----  ---
HOST RESERVED 0   IP    src  0.0.0.0             0.0.0.0            any  any  any
HOST RESERVED 1   MAC  any  01:80:C2:00:00:02 00:00:00:00:00   any  ---- any
HOST RESERVED 2   any  src                                              any
HOST RESEHVED 3   any  src                                              any
HOST RESERVED 4   any  src                                              any
HOST hm2       5   MAC  dst  22:22:22:22:22:22 FF:FF:FF:FF:FF:FF 0.2 ---- 2
HOST hm3       6   MAC  any  33:33:33:33:33:33 FF:FF:FF:FF:FF:FF 0.3 ---- 3
HOST hm4       7   MAC  src  44:44:44:44:44:44 FF:FF:FF:FF:FF:FF 0.4 ---- 4
HOST RESERVED 117 any  src                                            any
HOST RESERVED 118 any  src                                            any

L3SW>
```

表 9-19：MAC アドレスホストグループテーブルのエントリの表示例

9.8.3 L4 分類テーブルの設定

L4（レイヤ 4）分類テーブルでは、L4 パケットタイプと情報仕様 L4 プロトコルに基づいてパケットを分類できます。本製品の L4 分類テーブルで使用可能なエントリは、以下のとおりです。

- TCP
- UDP
- ICMP
- IGMP

次に、L4 分類テーブルのさまざまなタイプのエントリを設定する方法について説明します。

9.8.3.1 L4 TCP エントリの設定

L4 分類テーブルの TCP エントリを設定する場合は、次のコマンドを実行します。

L3SW> config classifier l4 tcp create <name> <preferred priority> <src | dst | any> <tcp port number | any> <tcpflag | any>

パラメータ

- name：エントリ名。
- preferred priority：レイヤ 4 タイプの分類テーブルのユーザ設定による優先度レベル。3～14、19～30、35～46、53～61、64～126 の範囲で指定します。その他のエントリは予約されます。
- src | dst | any：発信元または宛先アドレス、または any。
- tcp port number | any：0～65535 の TCP ポート番号、または any。
- tcpflag | any：TCP フラッグ。ACK、SYN、PSH または any。

L4 分類テーブルのエントリ 1、2、15～18、31～34、47～52、62～63 は予約されています。

L4 TCP の設定例を次に示します。

```
L3SW> config classifier l4 tcp create tcp3 3 any 2001 syn
L3SW> config classifier l4 tcp create tcp4 4 src 3004 fin
L3SW> config classifier l4 tcp create tcp5 5 dst 4005 rst
L3SW> config classifier l4 tcp create tcp6 6 any 65535 any
```

L4 分類テーブルから TCP エントリを削除する場合は、次のコマンドを実行します。

L3SW> config classifier l4 tcp delete <name>

```
L3SW> config classifier l4 tcp delete tcp3
```

L4 分類テーブルエントリを表示する場合は、次のコマンドを実行します。

L3SW> show classifier table l4 all

```
L3SW>show classifier table l4 all

Layer4 Group Table entries:

Table                  Src/ Protocol Protocol Packet  ICMP IGMP/IP
Type  Name       Pri Dst   Type      Port Num Type      Code Data
---- --------  --- ---- -------- -------- ------  ---- -------
L4    RESEHVED 0    any   TCP       179         any
L4    RESERVED 1    any   TCP       23          any
L4    REEERVED 2    any   TCP       161         any
L4    tcp3     3    any   TCP        2          SYN
L4    tcp4     4    any   TCP        3          FIN
L4    tcp5     5    any   TCP        4          RST
L4    tcp6     6    any   TCP        65535      any
L4    REEERVED 15   any   TCP       any         SYN
L4    REEERVED 16   any   TCP       179         any
L4    REEERVED 17   any   TCP       23          any

L3SW>
```

表 9-20：L4 分類テーブルの TCP エントリの表示例

9.8.3.2 L4 UDP エントリの設定

L4 分類テーブルの UDP エントリを設定する場合は、次のコマンドを実行します。

L3SW> config classifier l4 udp create <name> <preferred priority> <src | dst | any> <udp port number | any>

Parameters:

- name：エントリ名。
- preferred priority：レイヤ 4 タイプの分類テーブルのユーザ設定による優先度レベル。値は 1～120 の範囲です。
- src | dst | any：発信元または宛先アドレス、または any。
- udp port number | any：0～65535 の UDP ポート番号、または any。

L4 UDP の設定例を次に示します。

```
L3SW> config classifier l4 udp create udp1 10 src 1010
L3SW> config classifier l4 udp create udp2 11 dst 2004
L3SW> config classifier l4 udp create udp3 12 any 65535
```

L4 分類テーブルから UDP エントリを削除する場合は、次のコマンドを実行します。

L3SW> config classifier l4 udp delete <name>

```
L3SW> config classifier l4 udp delete udp3
```

L4 分類テーブル内に生成されたエントリを表示する場合は、次のコマンドを実行します。上記のコマンドで生成された L4 分類テーブルのエントリが表示されます。

L3SW> show classifier table l4 all

```
L3SW>show classifier table l4 all

Layer4 Group Table entries:

Table                    Src/ Protocol Protocol Packet  ICMP
IGMP/IP
Type  Name       Pri Dst   Type      Port Num Type      Code Data
----  --------   --- ----  --------  -------- ------  ---- -------
L4    RESEHVED   0   any   TCP       179         any
L4    RESERVED   1   any   TCP       23          any
L4    REEERVED   2   any   TCP       161         any
L4    upd1       10  any   UDP       1010
L4    upd2       11  any   UDP       2004
L4    upd3       12  any   UDP       65535
L4    REEERVED   15  any   TCP       any         SYN
L4    REEERVED   16  any   TCP       179         any
L4    REEERVED   17  any   TCP       23          any
L4    REEERVED   18  any   TCP       161         any


9.8.3.2.1        L3SW>
```

表 9-21：L4 分類テーブルの UDP エントリの表示例

9.8.3.3 L4ICMP エントリの設定

L4 分類テーブルの ICMP エントリを設定する場合は、次のコマンドを実行します。

L3SW> config classifier l4 icmp create <name> <preferred priority> <src | dst | any> [<ICMP packet type | any>] [<code value | any>]

パラメータ

- **name：エントリ名。**
- **preferred priority：レイヤ 4 タイプの分類テーブルのユーザ設定による優先度レベル。値は 1～120 の範囲です。**
- **src | dst | any：発信元または宛先アドレス、または any。**
- **ICMP packet type | any：このフィールドは、前のフィールドで宛先を入力した場合にのみ必要になります。ICMP パケットタイプとコードについては、次の表を参照してください。**
- **code value | any：このフィールドは、前のフィールドで宛先を入力した場合にのみ必要になります。ICMP コードの値は 0～15 の範囲です。**

パケットタイプ	コード	説明
0	0	エコー応答
3	0	ネットワーク到達不能
3	1	ホスト到達不能
3	2	プロトコル到達不能

パケットタイプ	コード	説明
3	3	ポート到達不能
3	4	フラグメント必要だがフラグなし
3	5	送信元指示によるルーティングが失敗
3	6	宛先ネットワーク不明
3	7	宛先ホスト不明
3	8	送信元ホストへのルートなし（廃）
3	9	宛先ネットワークは設定によりアクセス禁止
3	10	宛先ホストは設定によりアクセス禁止
3	11	TOS 種別によりネットワーク到達不能
3	12	TOS 種別によりホスト到達不能
3	13	フィルタリング設定により通信禁止
3	14	ホストの優先度違反
3	15	優先制御によるカットオフ中
4	0	輻輳発生による発信抑制
5	0	指定ネットワークへのリダイレクト要求
5	1	指定ホストへのリダイレクト要求
5	2	TOS とネットワークのリダイレクト要求
5	3	TOS とホストのリダイレクト要求
8	0	エコー要求
9	0	ルータ通知
10	0	ルータ選択要求
11	0	搬送中に TTL が 0 に
11	1	再構成時に TTL が 0 に
12	0	IP ヘッダ異常（あらゆるエラーに共通）
12	1	要求されたオプションは未知
13	0	タイムスタンプ要求（廃）
14	0	タイムスタンプ応答（廃）
15	0	情報要求（廃）
16	0	情報応答（廃）
17	0	ネットマスク通知要求
18	0	ネットマスク通知応答

次に示すのは、L4 ICMP の設定例です。

```
L3SW> config classifier l4 icmp create icmp2 36 dst 0 0
L3SW> config classifier l4 icmp create icmp3 37 dst 3 7
L3SW> config classifier l4 icmp create icmp4 38 dst 8 0
```

最初のコマンドではすべての ICMP エコー応答パケットを、2 番目のコマンドでは“Destination host unknown”の ICMP エコー応答パケットを、そして 3 番目のコマンドではすべての ICMP エコー要求パケットを選択しています。

L4 分類テーブルから ICMP エントリを削除する場合は、次のコマンドを実行します。

```
L3SW> config classifier l4 icmp delete <name>
L3SW> config classifier l4 icmp delete icmp3
```

```
L3SW>show classifier table l4 all

Layer4 Group Table entries:

Table                  Src/ Protocol Protocol Packet  ICMP IGMP/IP
Type  Name      Pri Dst   Type      Port Num Type      Code Data
---- --------  --- ---- -------- -------- ------  ---- -------
L4    RESEHVED 0    any   TCP       179         any
L4    RESERVED 1    any   TCP       23          any
L4    REEERVED 2    any   TCP       161         any
L4    REEERVED 15   any   TCP       any         SYN
L4    REEERVED 16   any   TCP       179         any
L4    REEERVED 17   any   TCP       23          any
L4    REEERVED 18   any   TCP       161         any
L4    REEERVED 31   any   UDP       any         any
L4    REEERVED 32   any   UDP       520         ---
L4    REEERVED 33   any   UDP       67          ---

--More—or (q)uit

Table                  Src/ Protocol Protocol Packet  ICMP IGMP/IP
Type  Name      Pri Dst   Type      Port Num Type      Code Data
---- --------  --- ---- -------- -------- ------  ---- -------
L4    RESEHVED 34   any   UDP       68          ----
L4    icmp1    35   any   ICMP      ----        any    any
L4    icmp2    36   dst   ICMP      ----        0      0
L4    icmp3    37   dst   ICMP      ----        3      7
L4    icmp4    38   dst   ICMP      ----        8      0
L4    REEERVED 47   any   UDP       ---         ---
L4    REEERVED 48   any   ICMP      ----        any    any
L4    REEERVED 49   any   ICMP      ----                    any
L4    REEERVED 50   any   IP        ----                  any
L4    REEERVED 51   any   IP        ----                  any

L3SW>
```

表 9-22:ICMP エントリを含む L4 分類テーブルの表示例

9.8.3.4 L4 IGMP エントリの設定

L4 分類テーブルの IGMP エントリを設定する場合は、次のコマンドを実行します。

```
L3SW> config classifier l4 igmp create <name> <preferred priority> <src | dst | any> [data]
```

パラメータ

- name：エントリ名。
- preferred priority：レイヤ 4 タイプの分類テーブルのユーザ設定による優先度レベル。値は 1～120 の範囲です。
- src | dst | any：発信元または宛先アドレス、または any。
- data：このフィールドには、前のフィールドで宛先を入力した場合に任意で入力します。IP ヘッダに続く 16 ビットのデータがこのフィールドの値とマッチングされます。

IGMP の設定例を次に示します。

```
L3SW> config classifier l4 igmp create igmp2 20 any
L3SW> config classifier l4 icmp create icmp3 21 dst 0
L3SW> config classifier l4 icmp create icmp4 22 dst 65535
```

L4 分類テーブルから IGMP エントリを削除する場合は、次のコマンドを実行します。

```
L3SW> config classifier l4 igmp delete <name>
L3SW> config classifier l4 igmp delete igmp3
```

表 9-23 は、上記 3 つのコマンドを実行すると表示される、IGMP エントリを含む L4 分類テーブルの表示例です。

```
L3SW>show classifier table l4 all

Layer4 Group Table entries:

Table                  Src/ Protocol Protocol Packet  ICMP IGMP/IP
Type  Name       Pri Dst   Type      Port Num Type      Code Data
---- --------  --- ---- -------- -------- ------  ---- -------
L4    RESEHVED 0    any   TCP       179         any
L4    RESERVED 1    any   TCP       23          any
L4    REEERVED 2    any   TCP       161         any
L4    REEERVED 15   dst   TCP       any         SYN
L4    REEERVED 16   any   TCP       179         any
L4    REEERVED 17   any   TCP       23          any
L4    REEERVED 18   any   TCP       161         any
L4    igmp2     20   src   IGMP                              any
L4    igmp3     21   dst   IGMP                                0
L4    igmp4     22   dst   IGMP                            65535

L3SW>
```

表 9-23：IGMP エントリを含む L4 分類テーブルの表示例

9.8.3.5 メインルールテーブルエントリの設定

メインルールテーブルは、他の分類テーブル（パケットタイプ分類テーブル、ホストグループ分類テーブル、L4 分類テーブル）のエントリを組み合わせた複合ルールを生成するために使用されます。メインルールテーブルのエントリは、パケットを、送出前に実行すべきフィルタリングアクションや QoS 処理に基づいて分類するための複合ルールを定義します。

L3SW> config classifier mainrule create <name> <preferred priority> <packet type name | any> <source host type name | any> <destination host type name | any> <source layer 4 type name | any> <destination layer 4 type name | any> <vid | any>

パラメータ

- name：エントリ名。
- preferred priority：ユーザ設定によるメインタイプ ID 番号。18～253 のプライオリティ値を指定できます。
- packet type name | any：パケットタイプ名、または any。
- source host type name | any：発信元ホストタイプ名、または any。
- destination host type name | any：宛先ホストタイプ名、または any。
- source layer 4 type name | any：発信元レイヤ 4 ホストタイプ名、または any。
- destination layer 4 type name | any：宛先レイヤ 4 ホストタイプ名、または any。
- vid | any：VLAN ID、または any。

メインルールテーブルエントリ 1～17、254～374、507～512 は予約されます。

メインルールテーブルの各エントリに、ホストグループテーブルエントリへの参照と L4 分類テーブルへの参照が 2 回ずつ出現していることに注意してください。いずれも、1 回目の参照はホストグループテーブル（L4 分類テーブル）のインバウンド（発信元）パケット用のルールを適用し、2 回目の参照はアウトバウンド（宛先）パケット用のルールを適用しています。例えば、メインルールテーブルに、IP アドレスが 162.1.1.1 のホストからポート 8080 に宛てたすべての TCP パケットを選択するためのエントリを生成する場合は、次のコマンドを実行します。

- **発信元を IP アドレス 162.1.1.1 とするパケットを選択するためのホストグループテーブルエントリを生成します。**

```
L3SW>config classifier host ip create hp9 12 src 162.1.1.1 255.0.0.0 any
any any
```

- **ポート 8080 を宛先とするすべての TCP パケットを選択するための L4 TCP エントリを生成します。**

```
L3SW> config classifier l4 tcp create tcp5 5 dst 8080 any
```

- **インルールテーブルのエントリを生成します。**

  メインルールテーブルのエントリで、IP アドレスが 162.1.1.1 のホストからポート 8080 に宛てたすべての TCP パケットを選択するために、ホストグループテーブルのエントリと L4 分類テーブルのエントリを結合します。

```
L3SW> config classifier mainrule create mr10 20 any hp9 any any tcp5 any
```

上記のメインルールにより、ロケーション 20 に mr10 という名のエントリが作成されます。

これにより、ホスト 162.1.1.1（ホストグループテーブルのエントリ hp9 で定義）を発信元とし、ポート 8080（L4 TCP 分類テーブルのエントリ tcp5 で定義）を宛先とする、すべての（TCP）パケットが選択されます。

メインテーブルのエントリを削除する場合は、次のコマンドを実行します。

```
L3SW> config classifier mainrule delete <name>
L3SW> config classifier mainrule delete mr10
```

9.8.3.6 メインルールのアクションタイプの設定

メインルールテーブルの各エントリに関連付けて、permit、drop、copy-to-cpu などのパケットフィルタリングアクションを定義することができます。メインルールテーブルの各エントリに対してアクションタイプを定義する場合は、次のコマンドを実行します。

```
L3SW> config classifier mainrule action <name> <action type> <enable|disable>
```

パラメータ

- name：エントリ名。
- action type：オプションは、drop、copy-to-cpu、permit など。
- <enable|disable>：ヒットカウンタの有効／無効を指定します。

メインルールテーブルの各エントリへのヒットカウンタの割り当てを、有効化または無効化することができます。メインルールテーブルのヒットカウンタを有効化すると、メインルールテーブルの関連するエントリで定義された分類ルールとマッチしたパケット数が示されます。その後の処理のために CPU に転送されるパケットフローは、copy-to-cpu アクションによって制御できます。このタイプのアクションはさらに、SACL によって、ソフトウェアの ACL 機能を実行するパケットフローを CPU に送るためにも使用されます。例えば、メインルールテーブルエントリ mr10 によって選択されたすべてのパケットを破棄する場合は、次のコマンドを実行します。

```
L3SW> config classifier mainrule action mr10 drop disable
```

メインルールテーブルエントリ mr10 は、ホスト 162.1.1.1 を発信元、ポート 8080 を宛先とする TCP パケットを選択することに注意してください。「9.8.3.5 メインルールテーブルエントリの設定」（P.226）に示す例を参照してください。

メインルールテーブルのエントリに対して定義されたアクションタイプは、そのエントリが削除されると無効になります。

表 9-24：ヒットカウンタが無効化されたメインルールテーブルエントリの表示例は、ヒットカウンタが無効化されたメインルールテーブルエントリの表示例です。

```
L3SW>show classifier table mainrule mrl0

Main Rule Table entries:

Table              Pkt Name/  Src/Dst    Src/Dst                 Qos    Qos
Type  Name Pri  CounterID  Host Name L4 Name VID Action Type   Value
MAIN  mr10 20    any          hp9          any      any drop    que     3
                 ----         any         tcp5

L3SW>
```

表 9-24:ヒットカウンタが無効化されたメインルールテーブルエントリの表示例

9.8.3.7 メインルールの QoSValue タイプの設定

メインルールテーブルの各エントリに関連付けて、そのエントリによって選択されたパケットに対して実行する QoS 処理を定義することができます。QoS 処理は、次の 3 タイプがサポートされています。

- サービスクラス(COS:Class of Service)
- キュープライオリティ
- サービスタイプ(TOS:Type of Service)

メインルールテーブルのエントリの QoS 値として COS を選択することによって、そのエントリによって選択されたパケットを全 4 クラスのうち 1 つのクラスに割り当てることができます。これにより、ハードウェアは選択されたパケットに対し、そのクラスの COS 定義に従って QoS 処理(帯域幅制限、または RED(Random Early Discard))を実行できるようになります。メインルールテーブルエントリの QoS 値としてキュープライオリティを選択した場合、そのエントリによって選択されたパケットは送出ポート上の該当するプライオリティキューに置かれます(どのプライオリティキューかは、コマンドで指定されたキュープライオリティ値によって決まります)。メインルールテーブルエントリの QoS 値として TOS を選択した場合は、そのエントリによって選択されたパケットに、このコマンドの指定に従って更新された TOS 値が付加されます。

メインルールテーブルの各エントリに対して QoS 値タイプを定義する場合は、次のコマンドを実行します。

L3SW> config classifier mainrule qosvalue <name> <cos|queue|tos> <qosvalue>

パラメータ

- name:エントリ名。
- cos|queue|tos:qos 値タイプ。cos、queue、tos のいずれかです。
- <qosvalue>:qos 値。選択された qos 処理のタイプによって異なります。COS には 0～3、queue には 0～7 か 0～255、tos には none を指定します。

例えば、メインルールテーブルのエントリ mr10 によって選択されたパケットをプライオリティ値 #3 のキューに割り当てる場合は、次のコマンドを実行します。

L3SW> config classifier mainrule qosvalue mr10 queue 3

表 9-25:キュープライオリティが 3 に設定されたメインルールテーブルエントリの表示例は、qos 値が 3、ヒットカウンタが有効に設定されたメインルールエントリ mr10 の表示例です。

```
L3SW>show classifier table mainrule mrl0

Main Rule Table entries:

Table             Pkt Name/  Src/Dst   Src/Dst                Qos    Qos
Type  Name Pri  CounterID  Host Name L4 Name VID Action Type   Value
MAIN  mr10 20    any         hp9          any      any drop    que     3
                 ----        any         tcp5

Main rule name.................    mr10
Hit counter ID ................    0
Hit counter value..............    0

L3SW>
```

表 9-25:キュープライオリティが 3 に設定されたメインルールテーブルエントリの表示例

メインルールテーブルのエントリに TOS 値を設定する場合は、次のコマンドを実行します。

```
L3SW> config classifier mainrule qosvalue mr10 tos 224
```

メインルールテーブルのエントリ mr10 によって選択されたパケットを、COS 値として 2 が設定された CoS に割り当てる場合は、次のコマンドを実行します。CoS は、通常、パケットクラスに対して帯域幅制限と RED プロファイルを定義するために使用されます。CoS については、DiffServ の項で詳細に説明します。

```
L3SW> config classifier mainrule qosvalue mr10 cos 2
```

QoS 機能(TOS、COS、キュー)を正常に動作させるため、フロー制御を無効に設定することをお勧めします。

9.8.4 DiffServ の設定

本製品では、DiffServ の設定時に、帯域幅制限または RED プロファイルを定義することができます。現在、本製品では 4 つのサービスクラスがサポートされています。分類テーブルを使用し、メインルールテーブルで qos 値タイプを“cos”に指定することによって、パケットをいずれかのクラスに分類することができます。Diffserv 機能を設定する場合は、次のコマンドを実行して有効にする必要があります。

```
L3SW> config classifier cos adminmode <enable|disable>
L3SW> config classifier cos adminmode enable
```

9.8.4.1 帯域幅制限の設定

メインルールテーブルのエントリで定義されたトラフィッククラスの帯域幅を制限する場合は、次のコマンドを実行します。

```
L3SW> config classifier cos bandwidth <slot.port|all> <cosvalue> <<minbw> <maxbw> <weight>
```

パラメータ

- slot.port| all：物理ポート slot.port の ID、または all ports。
- cosvalue：0～3 の Cos 値。
- minbw：最小帯域幅制限（または保証帯域幅）。0～15200 の値を、64Kbs 単位で指定します。0 は最小帯域幅制限がないことを示します。
- maxbw：最大帯域幅制限。0～15200 の値を、64Kbs 単位で指定します。0 は最小帯域幅制限がないことを示します。
- weight：ポートの帯域幅を巡って複数クラスのトラフィック間で競合が発生した場合は、“weight”パラメータに指定された値に基づいて、各クラスに割り当てる帯域幅の量が決定されます。1～8 の値を指定できます。値が小さいほど、帯域幅を多く割り当てられます。

最小帯域幅 64Kbps、最大帯域幅 640 Kbps を、COS 値 2 のトラフィッククラスに割り当てる場合は、次のコマンドを実行します。

```
L3SW> config classifier cos bandwidth all 2 1 10 3
```

特定のクラスに設定された帯域幅を表示する場合は、次のコマンドを実行します。

```
L3SW>show classifier cos 2

Table-based DiffServ feature   Enable

Slot.Port  MinBanduidth  Max Banduidth  Weight  RED Profile ID
0.1         1                10          3        None
0.2         1                10          3        None
0.3         1                10          3        None
0.4         1                10          3        None
0.5         1                10          3        None
0.6         1                10          3        None
0.7         1                10          3        None
0.8         1                10          3        None
0.9         1                10          3        None
0.10        1                10          3        None
0.11        1                10          3        None
0.12        1                10          3        None
0.13        1                10          3        None
0.14        1                10          3        None
0.15        1                10          3        None
0.16        1                10          3        None
0.17        1                10          3        None

—More— or <q>uit
0.18        1                10          3        None
0.19        1                10          3        None
0.20        1                10          3        None
0.21        1                10          3        None
0.22        1                10          3        None
0.23        1                10          3        None
0.24        1                10          3        None

L3SW>
```

表 9-26:サービスクラスに設定された帯域幅制限の表示例

9.8.4.2 RED(Random Early Discard)の設定

パケットクラスに RED を設定する場合は、RED プロファイルを生成し、そのプロファイルにトラフィッククラスを割り当てる必要があります。RED プロファイルには、start queue length、stop queue length、drop probability などのパラメータがあります。RED プロファイルを生成する場合は、次のコマンドを実行します。

L3SW> config classifier redprofile create <redprofileid> <startqlen> <stopqlen> <drop-probability>

パラメータ

- redprofileid:1～63 の整数。
- startqlen:RED アルゴリズムが起動した時点のキューのサイズ。0～16383 の値を、16Kbps 単位で指定します。
- stopqlen:RED アルゴリズムが終了し、すべてのパケットを破棄した時点のキューのサイズ。0～16383 の値を、16Kbps 単位で指定します。

- drop-probability：0～100%の値。

たとえば、startqlen に 16Kbps、drop-probability に 30%を指定して RED プロファイルを生成する場合は、次のコマンドを実行します。

L3SW> config classifier redprofile create 10 1 8 30

RED プロファイルを削除する場合は、次のコマンドを実行します。

L3SW> config classifier redprofile delete 10
L3SW> config classifier redprofile delete 10

RED プロファイルを表示する場合は、次のコマンドを実行します。

```
L3SW>show classifier redprofile

RED Profile ID Start Queue Length Stop Queue Length Drop Probability
-------------- ------------------ ----------------- ----------------
10             4                  8                 10

L3SW>
```

表 9-27：RED プロファイル

COS の RED 設定の最後には、次のコマンドを実行して、RED プロファイルをそのクラスに割り当てます。

L3SW> config classifier cos red <slot.port|all> <cosvalue> <redprofileid|none>

パラメータ

- slot.port|all：物理ポート番号。
- cosvalue：0～-3 の Cos 値。
- redprofileid|none：RED プロファイル ID（1～63）、または“none”。RED プロファイルのクラスへの関連付けを解除する場合は、“none”を指定します。

例えば、生成した RED プロファイル 10 を、COS 値 2 に割り当てる場合は、次のコマンドを実行します。

表 9-28：RED 割り当て後の COS の表示例は、RED プロファイル 10 を COS 値 2 に割り当てた結果の表示例です。

```
L3SW>show classifier cos 2

Table-based DiffSeru Feature ..............Enable
Slot.Port Min Bandwidth Max Bandwidth  Weight  RED Profile ID
--------- ------------- -------------  ------  --------------
0.1           1                    10                 3          10
0.2           1                    10                 3          10
0.3           1                    10                 3          10
0.4           1                    10                 3          10
0.5           1                    10                 3          10
0.6           1                    10                 3          10
0.7           1                    10                 3          10
0.8           1                    10                 3          10
0.9           1                    10                 3          10
0.10          1                    10                 3          10
0.11          1                    10                 3          10
0.12          1                    10                 3          10
0.13          1                    10                 3          10
0.14          1                    10                 3          10
0.15          1                    10                 3          10
0.16          1                    10                 3          10
0.17          1                    10                 3          10

--More-or (q)uit
```

表 9-28：RED 割り当て後の COS の表示例

9.9 ソフトウェア ACL

ソフトウェア ACL は、L-ACL と共に使用するもので、ユーザはこれらを使用して、スイッチ上でパケットフィルタリングを実行するための複雑な ACL ルールを設定することができます。SACL は、アクションタイプ copy-to-cpu が設定されたメインルールテーブルエントリによって転送されてきたパケットに対し、SACL ルールで定義されたフィルタリング機能を実行します。そのため、ユーザは最初に、SACL による追加の処理を必要とするパケットを捕捉するための L-ACL ルールを、分類テーブルとメインルールテーブルに適切なエントリを作成することによって設定する必要があります。SACL を設定する場合は、次の手順を実行します。

ステップ 1. 分類テーブルを設定する。

メインルールテーブルエントリのアクションタイプ“copy-to-cpu”を使って、「9.8 低レベル ACL」（P.215）で説明する分類テーブル設定を行います。

ステップ 2. SACLを有効化します。

ステップ 3. アクセスリストを生成します。

ステップ 4. アクセスリストポリシーを生成します。

ACL ルールを論理インタフェースと関連付けます。

ステップ 5：ACLルールをアクセスリストに追加します。

9.9.1 SACL の設定

SACL は、アクセスリストを使って、CPU 内で行われるパケットフィルタリングのアクションを定義します。SACL を有効にする場合は、次のコマンドを実行します。

```
L3SW> config ip access-list adminmode <enable/disable>
L3SW> config ip access-list adminmode enable
```

各アクセスリストセットは、1000～1127 の一意の番号で識別されます。新規のアクセスリストを生成する場合は、次のコマンドを実行します。

```
L3SW> config ip access-list list create <access-list-number>
L3SW> config ip access-list list create 1001
```

新規のアクセスリストを削除する場合は、次のコマンドを実行します。

```
L3SW> config ip access-list list delete <access-list-number>
L3SW> config ip access-list list delete 1001
```

アクセスリストを生成したら、SACL 設定の次のステップ、論理ポートと生成済みアクセスリストの関連付けを行います。この関連付けは、次のコマンドを実行することによって行うことができます。

```
L3SW> config ip access-list policy add <policy-name> <in/out> <slot.port> <access-list-number>
L3SW> config ip access-list policy add pl1 out 4.3 1001
L3SW> config ip access-list policy add pl2 in 4.2 1002
```

既存のアクセスリストを削除する場合は、次のコマンドを実行します。

```
L3SW> config ip access-list policy delete <policy-name>
L3SW> config ip access-list policy delete pl2
```

設定したアクセスリストを一覧表示する場合は、次のコマンドを実行します。

表 9-29：SACL（アクセスリスト）要約は、アクセスリスト設定の要約の表示例です。

```
L3SW> show ip access-list summary
L3SW> show ip access-list summary
```

```
L3SW>show ip access-list summary

Admin Mode ............................... Enable
Maxinun Number of Policies ............... 128
Maximum Number of Access Lists ........... 128
Configured Number of Access Lists ....... 2
Configured Access Lists:
ACL Nun   ACL Num   ACL Num   ACL Num   ACL Num   ACL Num
-------   -------   -------   -------   -------   -------
1001       1002

L3SW>
```

表 9-29：SACL（アクセスリスト）要約

アクセスリストポリシーを一覧表示する場合は、次のコマンドを実行します。

表 9-30:ACL ポリシーは、設定済み ACL ポリシーの表示例です。

```
(ESS r2.5> >sbou ip access-list policy

Name       Interface Dir Access List Number
-------- --------- --- ------------------
p11        4.3         out 1001
p12        4.2         in  1002

L3SW>
```

表 9-30:ACL ポリシー

SACL 設定の最後のステップでは、アクセスリストと関連付けた ACL ルールのリストを設定します。アクセスリストに追加する SACL ルールを生成する場合は、次のコマンドを実行します。

L3SW> config ip access-list rule add <access-list-number> [rule-number] <deny | permit> <protocol> <source> <source-wildcard> [<operator> <source-tcp/udp-port>] <destination> <destination-wildcard> [<icmp-type>] [<operator> <destination-tcp/udp-port>] [log]

パラメータ

- access-list-number:1001～1127 のアクセスリスト番号。
- rule-number:1～127 の整数。
- deny|permit:パケットフィルターアクション。permit(転送)または deny(破棄)のいずれかです。
- protocol:プロトコルタイプ。指定できるプロトコルは、TCP、UDP、ICMP、IGMP、OSPF、PIM、VRRP です。
- source:発信元 IP アドレス。
- source wild-card:発信元 IP アドレスのワイルドカード。この値は、パケット分類時にビット単位のマスクとして使用されます。ビット位置にゼロ値が設定されている場合は、完全一致が要求されることを示します。
- operator:TCP/UDP ポート比較用の演算子を指定します。指定できる演算子は、eq、neq、gt、lt、range です。
- source-tcp/udp-port:発信元 TCP/UDP ポート。
- destination:宛先 TCP/UDP ポート。
- estination wildcard:宛先 IP アドレスのワイルドカードマスク。
- icmp-type:ICMP 要求のタイプ。エコー、エコー応答など。0～18 の値を指定できます。
- operator:宛先 TCP/UDP ポート用の演算子を指定します。
- destination-tcp/udp-port:宛先 TCP/UDP ポート。
- log:ロギングを有効化するためのフィールド(任意)。

例えば、30.1.1.1 からのすべての TCP パケットを破棄する場合は、次のコマンドを実行します。

L3SW> config ip access-list rule add 1001 1 deny tcp 30.1.1.1 0.0.0.0

アクセスリストに対して設定されたルールを一覧表示する場合は、次のコマンドを実行します。

表 9-31:アクセスリストに関連付けられた ACL ルールの表示例は、アクセスリストに関連付けられたアクセスルールの表示例です。

L3SW> show ip access-list list <access-list number>
L3SW> show ip access-list list 1001

```
L3SW>show ip access-list list 1001

Num Action Prot Source          Wildcard   Operator port port Icmp-type
--- ------ --- ------------ ----------- ------- ---- ---- ---------
                Destination Wildcard    Operator port port Log
                ------------ ----------- -------- ---- ---- ----
                Packet                        Bytes
                ----------------------   ------------------------
1    permit tcp  Any             Any                0    0
                 30.1.1.1       0.255.255.255      0     0
                 0                        0
2     deny  tcp  Any              Any                0     0
                 30.1.1.1       0.255.255.255      0     0
                 0                        0
L3SW>
```

表 9-31:アクセスリストに関連付けられた ACL ルールの表示例

9.10 サービス妨害(DoS)攻撃からの保護

9.10.1 概要

サービス妨害(DoS:Denial of Service)は、ネットワーク／企業リソースの合法的なユーザに対するサービスを妨害する攻撃手法です。最も一般的な DoS 攻撃は、コンピュータ接続または帯域幅を標的として、大量のトラフィックや接続要求を発生させる方法です。どちらを標的とする場合も、合法的なユーザの要求は到達不能になり、サーバに保持されるネットワークリソースやオペレーティングシステムリソースがすべて消費されてしまいます。また、さまざまなソフトウェアツールを使って、多数のコンピュータから 1 つまたは複数の標的に対して一斉に DoS 攻撃を仕掛けることもあります。

この攻撃手法は、通常、「分散サービス妨害」(DDoS:Distributed Denial of Service)と呼ばれます。現在のところ、DDoS 攻撃を容易に、かつ完全に撃退できるセキュリティソリューションはありません。ただし、こうした攻撃を完全に封じ込める方法はないにしても、適切な手順をとれば、コンピュータが侵入者によって攻撃プラットフォームとして利用されないようにしたり、攻撃の影響を最低限に抑えたりすることはできます。

9.10.2 DoS 攻撃のタイプ

本製品には、以下のタイプの DoS 攻撃に対する保護が組み込まれています。

9.10.2.1 ICMP 攻撃

攻撃者は、大量の ICMP エコー要求パケットを送りつけます。その結果、要求パケットの量が膨大となって標的サーバが迅速に応答できなくなり、要求と応答の迅速な処理が困難になります。この攻撃は、パフォーマンス低下やシステム停止を引き起こします。

9.10.2.2 IP スウィープ攻撃

ICMP エコー要求を複数の宛先アドレスに送信する攻撃手法です。標的ホストが応答すると、その IP アドレスが攻撃者に知られてしまいます。

9.10.2.3 スマーフィング攻撃

偽造した ICMP エコーパケット（標的 IP アドレスを発信元 IP アドレスとして使用）を脆弱なネットワークのアドレスにブロードキャストする攻撃手法です。ネットワーク上のすべてのシステムが標的に ICMP エコー応答を送信します。短時間で帯域幅を消費しつくすため、合法的なユーザがサービスを受けられなくなります。

9.10.2.4 UDP 攻撃

UDP フラッディング攻撃は、UDP パケットを大量に送り、システムの速度を低下させてタイムアウトにより接続を切断させる攻撃手法です。

UDP はコネクションレスプロトコルなので、接続セットアップ手順を実行しなくてもデータの転送が可能です。UDP フラッディング攻撃では、攻撃者が標的システム上のランダムポートに UDP パケットを送付します。標的システムは、UDP パケットを受信すると、宛先ポート上の待機中のアプリケーションを探します。ポート上に待機中のアプリケーションがない場合は、偽造された発信元アドレスに対して、不達通知を含む ICMP パケットを発行します。標的システム上のポートに大量の UDP パケットが送信されると、システムは停止します。

9.10.3 DoS 攻撃からの保護（DAP）

本製品は、フラッドゲートメカニズムを利用して攻撃トラフィックからの保護を行います。着信する攻撃トラフィックをカウントし、しきい値に達すると事前に定義された期間にわたってフローを停止します。DAP はさらに、ICMP、TCP SYN、UDP フラッディング攻撃からのシステム保護も行います。DAP では、トラフィックがしきい値を超えたために破棄された ICMP、TCP SYN、UDP パケットの統計が生成されます。

9.10.4 DAP の関連用語

DAP 機能を設定する前に、次の 3 つの用語を理解しておく必要があります。

- ノーマルバースト – 指定されたスイッチポートまたはホストに 1 秒当たりに送信可能な ICMP/TCP SYN/UDP パケット数のしきい値。この値を超えると、スイッチは一定期間（ロック期間）にわたって ICMP/TCP SYN/UDP パケットの受信を拒否します。しきい値の範囲は、1～1000,000 です。

- 最大バースト：指定されたスイッチポートまたはホストに 1 秒当たりに送信可能な、ノーマルバーストにより破棄されるパケットを含む ICMP/TCP SYN/UDP パケット数のしきい値。この値を超えると、スイッチはロックアウト期間にわたって ICMP/TCP SYN/UDP パケットの受信を拒否します。しきい値の範囲は、1～1000,000 です。
- ロックアウト期間：1 秒当たりの ICMP/TCP SYN/UDP パケット数が最大バースト時間（単位：秒）を超えた場合に、スイッチがインタフェース上での ICMP/TCP SYN/UDP パケット受信を拒否する時間の長さ（単位：秒）。

9.10.5 DAP ポリシーの設定

DAP は次の 2 レベルで設定できます。

- **IP サブネットレベル**
- **スイッチレベル**

DAP コマンドを実行する前に、セキュリティ機能を有効にしてください。

9.10.5.1 IP サブネットレベル

指定された IP サブネットに対して DAP を設定する場合は、次のコマンドを実行します。

- **DAP ポリシーを有効または生成します。**

L3SW> config dap ip create <ipaddr> <netmask> <icmp/syn/udp> <normalburst> <maxburst> <lockoutperiod>

```
L3SW> config dap ip create 172.30.30.0 255.255.255.0 icmp 10 100 30
L3SW> config dap ip create 172.30.30.0 255.255.255.0 udp 20 200 30
```

- **ノーマルバーストしきい値の設定を変更します。**

L3SW> config dap ip normalburst <ipaddr> <netmask> <icmp/syn/udp> <threshold>

```
L3SW> config dap ip normalburst 172.30.30.0 255.255.255.0 icmp 5
```

- **最大バーストしきい値の設定を変更します。**

L3SW> config dap ip maxburst <ipaddr> <netmask> <icmp/syn/udp> <threshold>

```
L3SW> config dap ip maxburst 172.30.30.0 255.255.255.0 icmp 50
```

- **ロックアウト期間を変更します。**

L3SW> config dap ip lockout <ipadd> <netmask> <icmp/syn/udp> <time>

```
L3SW> config dap ip lockout 172.30.30.0 255.255.255.0 icmp 45
```

- **DAP ポリシーを有効化または削除します。**

L3SW> config dap ip delete <ipaddr> <netmask> <icmp/syn/udp>

```
L3SW> config dap ip delete 172.30.30.0 255.255.255.0 icmp
```

9.10.5.2 スイッチレベル DAP

スイッチの DAP（サーバポートに適用される DAP ルール）を設定する場合は、次のコマンドセットを実行します。

- **DAP ポリシーを有効または生成します。**

L3SW> config dap switch create <icmp/syn/udp> <normalburst> < maxburst> <lockoutperiod>
L3SW> config dap switch create icmp 20 50 60

- **ノーマルバーストしきい値の設定を変更します。**

L3SW> config dap switch normalburst <icmp/syn/udp> <threshold>
L3SW> config dap switch normalburst icmp 25

- **最大バーストしきい値の設定を変更します。**

L3SW> config dap switch maxburst <icmp/syn/udp> <threshold>
L3SW> config dap switch maxburst icmp 60

- **ロックアウト期間を変更します。**

L3SW> config dap switch lockout <icmp/syn/udp> <time>
L3SW> config dap switch lockout icmp 120

- **DAP ポリシーを有効化または削除します。**

L3SW> config dap switch delete <icmp/syn/udp>
L3SW> config dap switch delete icmp

DoS 攻撃保護ポリシー（サブネット／ホストの保護方法）は、スイッチに接続されたサブネットやホストに対しては定義できますが、スイッチ上のポートに割り当てられたレイヤ 3 インタフェース IP アドレスに対しては定義できません。

9.10.6 DAP ポリシーの表示

IP またはスイッチ上で設定されたポリシーを表示する場合は、次のコマンドを実行します。

設定済みホストに対する DAP 設定を表示する場合は、次のコマンドを実行します（表示は IP アドレス順）。

L3SW> show dap conf ip

```
L3SW>show  dap conf ip

IpAddr          NetMask         Flood   NormalBurst MaxBurst  Lockout
------------    -------------   -----   ----------- --------- -------
192.168.10.0    255.255.255.0   icmp    2000        100000     2
192.168.20.0    255.255.255.0   icmp    3000        150000     2
192.168.20.0    255.255.255.0   upd     2000        110000     2
192.168.30.0    255.255.255.0   icmp    2000        250000     3
192.168.30.0    255.255.255.0   syn     4000        210000     2

L3SW>
```

表 9-32：IP の DAP 設定の表示例

L3SW> show dap conf switch

```
L3SW>show  dap stats ip

 Flood  NormalBurst   MaxBurst   Lockout
------  ------------  --------  --------
Icmp     2000          150000     1
Syn      3000          130000     2
Upd      5000          100000     1

L3SW>
```

表 9-33:スイッチの DAP 設定の表示例

9.10.7 DAP 統計の表示

ネットワーク管理者は、DAP 統計を IP レベルまたはスイッチレベルのどちらで表示するかを選択できます。統計を表示する場合は、次のコマンドを実行します。

L3SW> show dap stats <ip/switch>
L3SW> show dap stats ip

統計情報をクリアする場合は、次のコマンドを実行します。

L3SW> clear dap stats
L3SW> clear dap stats

コマンドの表示結果の例を次に示します。

```
L3SW>show  dap stats ip

 IP Addr     MetMask       Flood  PktDropcnt  HrmlBrstCrsCnt MaxBrst CrsCnt
------------ ------------- -----  ---------- --------------- ------- ------
192.168.10.0 255.255.255.0 ICMP   0           0                0      0
192.168.20.0 255.255.255.0 ICMP   0           0                0      0
192.168.20.0 255.255.255.0 UPD    0           0                0      0
192.168.30.0 255.255.255.0 ICMP   0           0                0      0
192.168.30.0 255.255.255.0 SYN    0           0                0      0

 L3SW>
```

表 9-34:DAP 統計の表示例

9.11 DAP の例

次図は、DoS 攻撃を受けているメインサーバと本製品の例です。サーバ IP とスイッチの DAP を有効にする場合は、次のようにコマンドを実行して、ICMP、TCP SYN、UDP パケットを対象と

するポリシーを生成します。

```
L3SW> config security enable
L3SW> config dap ip create 192.30.16.0 255.255.255.0 icmp 200 1000 60
L3SW> config dap ip create 192.30.16.0 255.255.255.0 udp 200 1000 30
L3SW> config dap ip create 192.30.16.0 255.255.255.0 syn 500 1000 5

L3SW> config dap switch create icmp 30 100 120
L3SW> config dap switch create udp 50 100 30
L3SW> config dap switch create syn 100 200 10
```

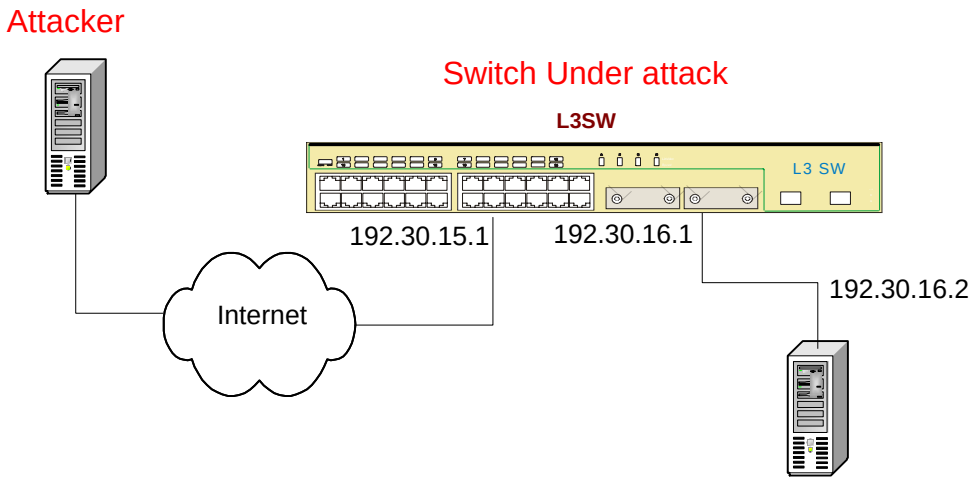

図 9-2：IP またはスイッチレベルの DAP

9.12 BOOTP とDHCP

9.12.1 概要

本製品では、BOOTP/DHCP のクライアントサービスとリレーサービスの両方が用意されています。任意のポート（サービスポートを含みます）を、BOOTP/DHCP クライアントとして設定し、BOOTP/DHCP サーバから IP アドレスを取得できます。あるポートをリレーポートとして設定すると、そのポートと同じサブネット上のクライアントから送信されてきた BOOTP/DHCP メッセージが、異なるサブネット上のサーバに転送されます。次にスイッチ内の BOOTP/DHCP クライアント／リレーサービスを設定するためのコマンドについて説明します。

9.12.2 BOOTP/DHCP クライアントの設定

BOOTP/DHCP クライアントサービスは、サービスポート上のみ、またはすべてのネットワークポート上において、アクティブ化することができます。サービスポート上で BOOTP/DHCP サービスをアクティブ化する場合は、次のコマンドを実行します。

```
L3SW> config serviceport protocol <none/bootp/dhcp>
L3SW> config serviceport protocol bootp
```

デフォルトでは、DHCP サービスはサービスポート上でアクティブ化されます。サービスポート上の

DHCP サービスは、コマンド config serviceport protocol none を実行して無効にすることができます。

DHCP/BOOTP プロトコルをすべてのネットワークポート上で有効にする場合は、次のコマンドを実行します。

```
L3SW> config network protocol <none/bootp/dhcp>
L3SW> config network protocol bootp
```

BOOTP/DHCP クライアントサービスは、ポートごとに個別にアクティブ化することはできません。

プロトコルモードを変更すると、ネットワークポートに対して設定されたすべての IP アドレスがリセットされます。

ポートに割り当てられた IP アドレスが意図せず変更されないようにするための措置として、次の確認メッセージが表示されます。

```
Are you sure you want to continue? (y/n)
```

「y」を入力すると、指定されたプロトコルをすべてのポート上で有効化するための設定変更が実行されます。「n」を入力すると、変更は行われません。

9.12.3 9.12.3 BOOTP/DHCP リレーの設定

ユーザが設定できる BOOTP/DHCP リレーサービス関連のパラメータには、次のものがあります。

- adminmode：管理モードを有効化／無効化します。
- cidoptmode：回路 ID オプションモードを有効化／無効化します。
- maxhopcount：最大ホップカウントを指定します。
- minwaittime：最小待機時間を指定します。
- serverip：BOOTP/DHCP サーバの IP アドレスを指定します。

DHCP/BOOTP リレーを設定する場合は、次のコマンドセットを実行します。

- **ステップ 1：BOOTP/DHCP リレーの管理モードを有効化します（必須）。**

```
L3SW> config router bootpdhcprelay adminmode <enable/disable>
L3SW> config router bootpdhcprelay adminmode enable
```

- **ステップ 2：BOOTP/DHCP リレーサーバの IP アドレスを設定します（必須）。**

```
L3SW> config router bootpdhcprelay serverip <ipaddr>
L3SW> config router bootpdhcprelay serverip 172.30.40.100
```

- **ステップ 3：BOOTP 要求の最小待機時間を設定します（任意）。**

最小待機時間は、同じクライアントから次の BOOTPREQUEST メッセージが送られてくるまでの最小予想時間です。スイッチは、最小待機時間が経過するまでに受信したメッセージを破棄し

ます。最小待機時間のデフォルト値は 0 です。この初期設定値を変更する場合は、次のコマンドを実行します。

```
L3SW> config router bootpdhcprelay minwaittime <0-100>
L3SW> config router bootpdhcprelay minwaittime 5
```

- **ステップ 4:最大ホップカウントを設定します(任意)。**

最大ホップカウントは、ネットワーク内で BOOTP/DHCP リレーメッセージが無限ループに陥るのを防止するために、BOOTP/DHCP メッセージを破棄する機能です。デフォルトの最大ホップカウントは 4 です。このデフォルト値を変更する場合は、次のコマンドを実行します。

```
L3SW> config router bootpdhcprelay maxhopcount <1-16>
L3SW> config router bootpdhcprelay maxhopcount 16
```

- **ステップ 5:回路 ID オプションを有効化します(任意)。**

```
L3SW> config router bootpdhcprelay cidoptmode <enable/disable>
L3SW> config router bootpdhcprelay cidoptmode enable
```

DOT1P/TOS リレー設定情報を表示する場合は、次のコマンドを実行します。

```
L3SW> show router bootpdhcprelay
L3SW> show router bootpdhcprelay
```

```
L3SW>show router bootpdhcprelay

Maximum Hop Count..........................  16
Minimum Wait Time (Seconds)...............  5
Admin Mode.................................  Enable
Server IP Address..........................  192.168.10.1
Circuit Id Option Mode.....................  Enable
Requests Received..........................  0
Requests Relayed...........................  0
Packets Discarded..........................  0

L3SW>
```

表 9-35:BOOTP/DHCP リレーの表示例

9.12.4 DHCP サーバ

DHCP サーバに関連する機能を設定する手順を次に示します。

ステップ 1:IPルーティングを有効化します。

ステップ 2:目的の物理ポート上のIPアドレスを設定します。

ステップ 3:DHCP管理状態を有効化します。

ステップ 4:関連の仮想ルータポート上でDHCPサービスを有効化します。

ステップ 5:DHCPサーバのIPアドレスプールを 1 つ以上生成します。

ステップ 6：各プールの使用可能なIPアドレスの範囲を指定します。

ステップ 7：各プールに対して、初期設定のルータIPアドレスを設定します。

ステップ 8：各プールに対して、DNSサーバのIPアドレスを設定します。

ステップ 9：各プールに対して、通常および最大許容リース期間を設定します。

ステップ 10：“applyconfig”コマンドを実行して、設定変更を有効にします。

ステップ 1 とステップ 2 については前述しているので、ここでは省略します。ここでは、DHCP サーバの残りの設定手順について説明します。

9.12.4.1 DHCP 管理状態の有効化

DHCP 管理状態を有効化する場合は、次のコマンドを実行します。

```
L3SW> config router dhcp adminmode <enable/disable>
L3SW> config router dhcp adminmode enable
```

9.12.4.2 論理ポート上の DHCP サービスの有効化

論理ポート上の DHCP サービスを有効化する場合は、次のコマンドを実行します。論理インタフェース 4.1 および 4.2 上で DHCP サービスを有効化した例を次に示します。

```
L3SW> config router dhcp interface set <logical port numbers separated by space>
L3SW> config router dhcp itnerface set 4.1 4.2
```

複数の論理ポート上の DHCP サービスを無効化する場合は、次のコマンドを実行します。

```
L3SW> config router dhcp interface clear <logical port numbers separated by space>
L3SW> config router dhcp itnerface clear 4.1 4.2
```

DHCP が有効化されたインタフェースとその状態を一覧表示する場合は、次のコマンドを実行します。

表 9-36：DHCP インタフェースの設定の表示例は、DHCP インタフェースの設定と状態の表示例です。

```
L3SW> show router dhcp interface
```

```
L3SW>show router dhcp interface


Interface  Status
---------  ------------
4.1         Active
4.2         Active
4.3

L3SW>
```

表 9-36：DHCP インタフェースの設定の表示例

9.12.4.3 IP アドレスプールの設定

DHCP サーバ用の新規 IP アドレスプールを生成する場合は、次のコマンドを実行します。

```
L3SW> config router dhcp pool create <name> <ip address> <netmask>
L3SW> config router dhcp pool create p1 10.0.0.0 255.0.0.0
L3SW> config router dhcp pool create p2 20.0.0.0 255.0.0.0
```

IP アドレスプールを生成したら、そのプール内で許容される IP アドレスの範囲を定義します。IP アドレスプール内で許容される IP アドレスの範囲を定義する場合は、次のコマンドを実行します。

```
L3SW> config router dhcp pool range add <name> <low IP address> <high IP address>
L3SW> config router dhcp pool range add p1 10.0.0.100 10.0.0.200
L3SW> config router dhcp pool range add p2 20.0.0.21 20.0.0.30
```

IP アドレスプールを一覧表示する場合は、次のコマンドを実行します。

```
L3SW> show router dhcp pool summary
L3SW> show router dhcp pool summary
```

```
L3SW>show router dhcp pool summary

Name      IP/Mask        Range<Lo to Hi)                    Avail
------- -----------  ------------------------------ ------
p1        10.0.0.0       10.0.0.100   to 10.0.0.200       0
p3       30.0.0.0       30.0.0.31       to 30.0.0.40       0
p4        40.0.0.0       40.0.0.41       to 40.0.0.50       0
p2        20.0.0.0       20.0.0.21       to 20.0.0.30       0

L3SW>
```

表 9-37:IP アドレスプール要約の表示例

プール全体、またはプールの一定範囲のアドレスを削除する場合は、次のコマンドを実行します。

```
L3SW> show router dhcp pool summary
L3SW> show router dhcp pool summary
```

```
L3SW>show router dhcp pool detailed p2

DHCP admin. node            Enable
DHCP ping node              Enable
Pool                        p2
Lease                       600 seconds
Max Lease                   7200 seconds
Domain Name Servers         80.0.0.2; 60.0.0.2;
Routers                     20.0.0.1; 20.0.0.10;
Domain                      direct2
Subnet & Mask               20.0.0.0 255.0.0.0
Valid Address Range         20.0.0.21       to 20.0.0.30
```

表 9-38:IP アドレスプール詳細

プール全体、またはプールの一定範囲のアドレスを削除する場合は、次のコマンドを実行します。

L3SW> config router dhcp pool delete <name>
L3SW> config router dhcp pool delete p1

L3SW> config router dhcp pool range remove <name> <low IP address> <high IP address>
L3SW> config router dhcp pool range remove p1 10.0.0.150 10.0.0.200

9.12.4.4 デフォルト設定ルータと DNS サーバの設定

プールから IP アドレスを割り当てられたクライアントは、DHCP サーバから、デフォルト設定ルータの IP アドレスと DNS サーバの IP アドレスも割り当てられます。各プールについて、デフォルト設定ルータの IP アドレスと DNS サーバの IP アドレスを最大 8 個ずつ設定できます。一定範囲のプールに対して初期設定ルータの IP アドレスを設定する場合は、次のコマンドを実行します。

L3SW> config router dhcp defaultrouter <pool-name> <ip address-list>
L3SW> config router dhcp defaultrouter p1 10.0.0.100 10.0.0.101 10.0.0.102
L3SW> config router dhcp pool create p2 20.0.0.1 20.0.0.10

プールに関連付けられた DNS サーバの IP アドレスを設定する場合は、次のコマンドを実行します。

L3SW> config router dhcp dnsserver <pool-name> <IP address-list>
L3SW> config router dhcp dnsserver p1 60.0.0.1 60.0.0.2
L3SW> config router dhcp dnsserver p2 80.0.0.1 80.0.0.10

9.12.4.5 リース期間の設定

プールから IP アドレスを割り当てられたクライアントには、その IP アドレス割当の有効期間が設定されます。この期間は、「リース」期間と呼ばれます。プールから割り当てられた IP アドレスに関連するリース期間を設定変更する場合は、次のコマンドを実行します。

L3SW> config router dhcp lease <pool-name> <value in seconds>
L3SW> config router dhcp lease p1 600
L3SW> config router dhcp lease p2 1000

最大リース期間値を設定することもできます。この値は、IP アドレス割当元のプールに設定さ

れたリース期間よりも長い期間をクライアントが要求した場合に、DHCP サーバがクライアントに許可する最大値です。

L3SW> config router dhcp maxlease <pool-name> <value in seconds>
L3SW> config router dhcp maxlease p1 800
L3SW> config router dhcp maxlease p2 1500

現在アクティブなリース期間を表示する場合は、次のコマンドを実行します。

表 9-39:アクティブリース期間の表示例は、このコマンドの実行後に表示されるアクティブリース期間の表示例です。

L3SW> show rotuer dhcp leasetable
L3SW> show router dhcp leasetable

```
L3SW>show router dhcp leasetable

                                  Start       Start       End         End
Ip Address      MAC address      Date        Time        Date        Time        Status
--------------- ---------------- ---------- ----------- ----------- --------- ------
L0.0.0.200      00:01:02:39:8i:cd  2002/08/04 14:07:17  2002/08/04 14:23:57  active
10.0.0.199      00:00:00:01:02:05  2002/08/04 14:09:19  2002/08/04 14:25:59  active
10.0.0.194      00:00:00:01:02:0a  2002/08/04 14:09:20  2002/08/04 14:26:00  active
10.0.0.195      00:00:00:01:02:09  2002/08/04 14:09:20  2002/08/04 14:26:00  active
10.0.0.196      00:00:00:01:02:08  2002/08/04 14:09:20  2002/08/04 14:26:00  active
10.0.0.197      00:00:00:01:02:07  2002/08/04 14:09:20  2002/08/04 14:26:00  active
10.0.0.198      00:00:00:01:02:06  2002/08/04 14:09:20  2002/08/04 14:26:00  active
10.0.0.189      00:00:00:01:02:0f  2002/08/04 14:09:21  2002/08/04 14:26:01  active
10.0.0.190      00:00:00:01:02:06  2002/08/04 14:09:21  2002/08/04 14:26:01  active
10.0.0.191      00:00:00:01:02:0d  2002/08/04 14:09:21  2002/08/04 14:26:01  active
10.0.0.192      00:00:00:01:02:0c  2002/08/04 14:09:21  2002/08/04 14:26:01  active
10.0.0.193      00:00:00:01:02:0b  2002/08/04 14:09:21  2002/08/04 14:26:01  active
10.0.0.187      00:00:00:02:02:07  2002/08/04 14:09:22  2002/08/04 14:26:02  active
10.0.0.188      00:00:00:02:02:06  2002/08/04 14:09:22  2002/08/04 14:26:02  active
10.0.0.182      00:00:00:02:02:0c  2002/08/04 14:09:23  2002/08/04 14:26:03  active
10.0.0.183      00:00:00:02:02:0b  2002/08/04 14:09:23  2002/08/04 14:26:03  active
```

表 9-39:アクティブリース期間の表示例

9.12.4.6 Applyconfig コマンドと IP アドレスの予約

本製品では、DHCP サーバを停止しなくても、DHCP サーバに関連するパラメータを変更できます。これらの変更は、次のコマンドを実行しなければ有効になりません。

L3SW> config router dhcp applyconfig
L3SW> config router dhcp applyconfig

本製品では、ネットワーク内の特定のデバイスに IP アドレスを事前に割り当てておくことができます。DHCP サーバは、ユーザからこれらの予約 IP アドレスへの要求を受信すると、それを該当するデバイスに割り当てます。デバイスの識別には、Ethernet MAC アドレスが使用されます。IP アドレスを予約する場合は、次のコマンドを実行します。

L3SW> config router dhcp reservation add <IP address> <Mac-address> <name>
L3SW> config router dhcp reservation add 10.0.0.21 00:00:00:01:01:01 client1
L3SW> config router dhcp reservation add 20.0.0.32 00:00:00:01:01:02 client2
L3SW> config router dhcp reservation add 30.0.0.43 00:00:00:01:01:03 client3
L3SW> config router dhcp reservation add 40.0.0.54 00:00:00:01:01:04 client4

予約した IP アドレスを削除する場合は、次のコマンドを実行します。

L3SW> config router dhcp reservation remove <IP address>
L3SW> config router dhcp reservation remove 10.0.0.21

予約する IP アドレスは、IP アドレスプールに関連付けられている IP アドレス範囲以外のアドレスでなければなりません。

予約 IP アドレスを一覧表示する場合は、次のコマンドを実行します。

表 9-40:予約済み IP アドレスの表示例は、予約済み IP アドレスの表示例です。

```
L3SW>show router dhcp reservation

MAC ADDRESS         IP Address        Host Name
------------------  ----------------- ---------
00:00:00:01:01:01    10.0.3.21        clientl
00:00:00:01:01:02    20.0.3.32        client2
00:00:00:01:01:03    30.0.3.43        client3
00:00:00:01:01:04    40.0.3.54        client4

L3SW>
```

表 9-40:予約済み IP アドレスの表示例

9.12.4.7 PING 検査モード

DHCP サーバが、クライアントに割り当てようとする IP アドレスがすでに使用されているかどうか確認するように設定できます。DHCP サーバは、PING コマンドを使ってこの確認を行います。この機能を有効化／無効化は、次のコマンドを実行します。

L3SW> config router dhcp ping <enable/disable>
L3SW> config router dhcp ping enable

10. ソフトウェアと設定情報の管理

ソフトウェアや設定情報を本製品にダウンロードすることができます。また、本製品から設定情報をアップロードすることもできます。アップロード/ダウンロードは、XMODEM または TFTP プロトコルで行います。

10.1 XMODEM モード

XMODEM モードでは、本製品の RS-232C シリアルポートを、管理用のステーションにローカル接続(図 10-1 参照)またはリモート接続(図 10-2 参照)します。 管理用ステーションでは、ソフトウェアや設定ファイルを保存しておき、アップロードやダウンロードを行います。

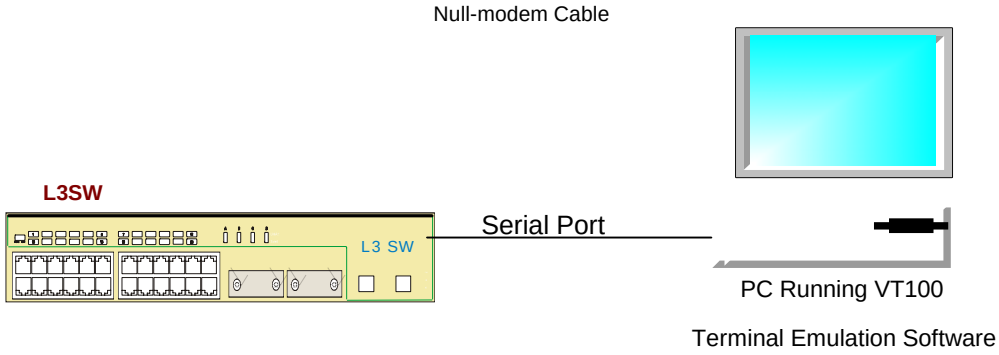

図 10-1:XMODEM モードーローカル接続端末

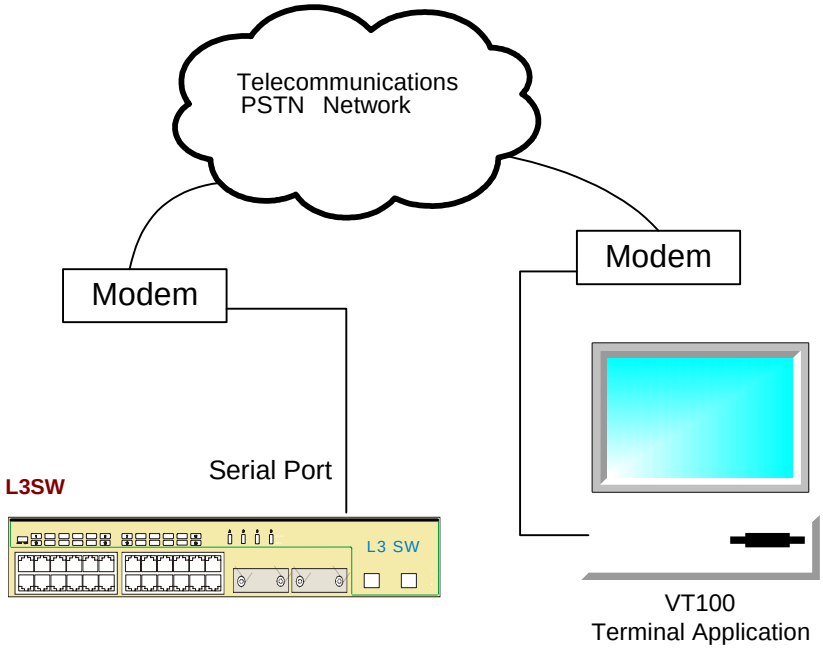

図 10-2:XMODEM モードーリモート接続端末

10.1.1 TFTP モード

TFTP モードでは、帯域外サービスポート（図 10-3 参照）または帯域内ネットワークポート（図 10-4 参照）を、管理用ステーションに接続します。 管理用ステーションでは、ソフトウェアや設定ファイルを保存しておき、アップロードやダウンロードを行います。

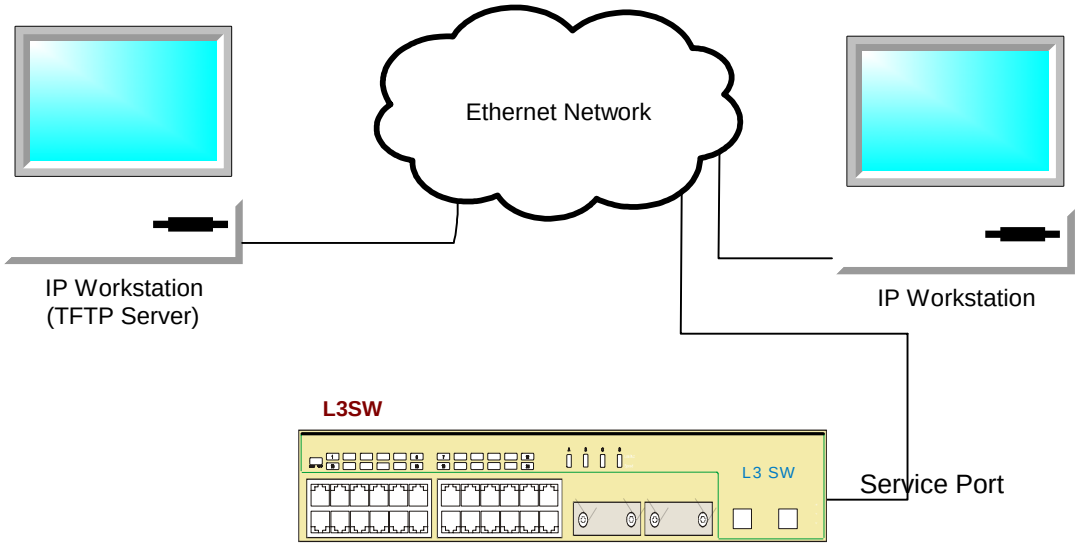

図 10-3：TFTP モード－アウトオブバンドサービスポート接続

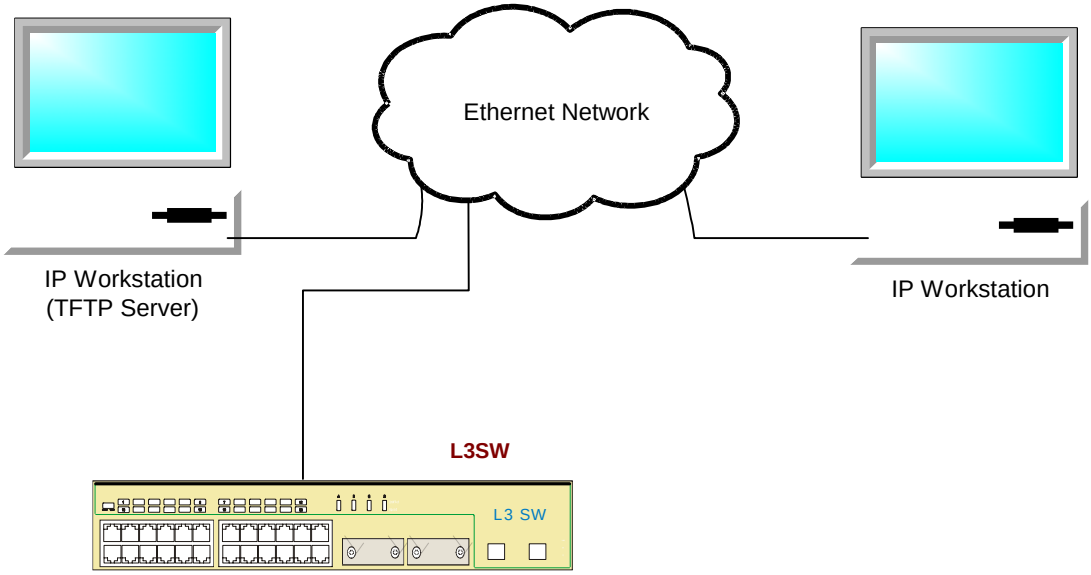

図 10-4：TFTP モード－帯域内ネットワークポート接続

10.2 ダウンロードとアップロード

本製品にダウンロードできるファイルには、次のものがあります。

- **実行コードイメージファイル（Operational code image file）**
- **設定ファイル**

本製品からアップロードできるファイルには、次のものがあります。

- **設定ファイル**
- **エラーログファイル**
- **システムトレースファイル**
- **トラップログファイル**

次に示すダウンロード／アップロード手順は変更される場合があります。そのため、ソフトウェアリリースノートをダウンロードし、手順を確認されることをお薦めします。

10.2.1 ブートメニューからの XMODEM モードのダウンロード

ステップ 1：イメージファイルをローカルディレクトリにコピーします。

実行コードイメージファイルを、本製品付属の CD から管理用システムのローカルディレクトリ（例：d:¥image¥ESSAr22v6b1.tgz）にコピーします。

ステップ 2：PCの端末設定をします。

端末エミュレーションソフトウェア（PC 上の HyperTerminal など）を開きます。[Baud Rate]を[9600bps]、[Data bits]を[8]、[Parity]を[none]、[Stop bits]を[1]、[Flow control]を[none]に、それぞれ設定します。端末エミュレーションソフトウェアの[Connect]をクリックします。

ステップ 3：電源をオン／オフするか、CLIコマンドreset systemを実行して、本製品をリセットします。

ステップ 4：スタートアップメニューが表示されたら、「2」を入力してブートメニューに進みます。

1 - *Start Operational Code*

2 - Start Boot Menu

Select (1, 2): 2

ステップ 5：ブートメニューが表示されたら、「5」を入力してブートメニューに進みます。

1 - Start ESSential Operational Code

2 - Load Operational Code Image using XMODEM/YMODEM/ZMODEM

3 - Load Operational Code Image using TFTP

4 - Display Vital Product Data

5 - Change Baud Rate

6 - Retrieve Error Log using TFTP

7 - Retrieve Error Log using XMODEM/YMODEM/ZMODEM

8 - Erase current Configuration

9 - Erase Crash Information files

10 - Format Compact Flash

0 - Quit from ESSential Startup Code Menu

Select option (0-10):10

ステップ 6:ボーレートメニューが表示されたら、「7」を入力してボーレートを[115200]に設定します。

ステップ 7:端末エミュレーションソフトウェアの[Disconnect]をクリックします。

ステップ 8:端末エミュレーションソフトウェアで[Baud rate]を[115200]に設定して、[Connect]をクリックしてから＜Enter＞キーを押します。本製品へのソフトウェアのダウンロードが、指定したボーレートで開始されます。

ステップ 9:設定情報メニューが表示されたら、「2」を入力して[Load Operational Code Image using XMODEM/YMODEM/ZMODEM]を選択します。

ステップ 10:端末エミュレーションソフトウェアで[send file]を選択して、ファイル送信ウィンドウを表示します。

ステップ 11:ファイル送信ウィンドウが表示されたら、ローカルディレクトリに保存されている本製品ソフトウェアイメージのパスを含んだファイル名（例：d:\image\ESSAr22v6b1.tgz）を入力するか、[Browse]ウィンドウから選択します。プロトコルとして[XMODEM]を選択して、[Send]ボタンをクリックします。

ステップ 12:ファイルの転送が開始されます。転送を中止する場合は、＜Control＋X＞キーを数回押してください。

ステップ 13:ファイルの転送が完了したら、本製品の電源を切って、再度入れます。新しいソフトウェアイメージで自動的にブートします。

ステップ 14:端末エミュレーションソフトウェアで[Disconnect]をクリックして、[Baud rate]を 9600 に戻します。[Connect]をクリックして＜Enter＞キーを押し、本製品からのメッセージが 9600 のボーレートになっていることを確認します。

10.2.2 CLI プロンプトからの XMODEM モードのダウンロード

ステップ 1:実行コードイメージファイルを、本製品付属の CD から管理用システムのローカルディレクトリ（例：d:\image\ESSAr22v6b1.tgz）にコピーします。また、スイッチ設定ファイルもローカルディレクトリ（例：d:\image\ESSConfig）にコピーしておきます。

ステップ 2:端末エミュレーションソフトウェア（PC 上の HyperTerminal など）を開きます。[Baud Rate]を[9600bps]、[Data bits]を[8]、[Parity]を[none]、[Stop bits]を[1]、[Flow control]を[none]に、それぞれ設定します。端末エミュレーションソフトウェアの[Connect]をクリックします。

ステップ 3:ユーザ ID とパスワードを入力して本製品にログインします。CLI コマンド config serial

baudrate 115200 を実行して、シリアルポートのボーレートを 115200 に設定します。

ステップ 4:端末エミュレーションソフトウェアの[Disconnect]をクリックします。

ステップ 5:端末エミュレーションソフトウェアで[Baud rate]を[115200]に設定して、[Connect]をクリックしてから＜Enter＞キーを押します。本製品へのソフトウェアのダウンロードが、指定したボーレートで開始されます。

ステップ 6:ソフトウェアのダウンロードの場合は CLI コマンド transfer download datatype code を、設定情報のダウンロードの場合はコマンド transfer download datatype config を実行します。CLI コマンドの transfer download mode xmodem と transfer download start で転送パラメータを表示します。転送プロンプトが表示されたら＜y＞キーを押し、XMODEM モードでの転送を開始します。

ステップ 7:端末エミュレーションソフトウェアで[send file]を選択して、ファイル送信ウィンドウを表示します。

ステップ 8:ファイル送信ウィンドウが表示されたら、ローカルディレクトリに保存されている本製品ソフトウェアイメージのパスを含んだファイル名（例：d:\image\ESSAr22v6b1.tgz）、または設定ファイル（例：d:\image\ESSConfig）のファイル名を入力します。プロトコルとして[XMODEM]を選択して、[Send]ボタンをクリックします。

ステップ 9:ファイルの転送が開始されます。転送を中止する場合は、＜Control＋X＞キーを数回押してください。

ステップ 10:設定ファイルをダウンロードした場合は、転送終了後、自動的に再起動します。

ソフトウェアイメージファイルをダウンロードした場合は、新しいソフトウェアイメージをフラッシュメモリに保存するかどうかを確認するメッセージが表示されます。＜y＞キーを押すとフラッシュメモリに保存されます。イメージの CRC 検証が終わると確認メッセージが表示されるので、もう一度＜y＞キーを押して保存します。ソフトウェアイメージのダウンロードが完了したら、通常の操作を行うことができます。新しいソフトウェアイメージは次回ブート時（次回の電源投入時、または CLI コマンド reset system 実行時）に自動的に起動します。

ステップ 11:端末エミュレーションソフトウェアで[Disconnect]をクリックして、[Baud rate]を 9600 に戻します。[Connect]をクリックして＜Enter＞キーを押し、本製品からのメッセージが 9600 のボーレートになっていることを確認します。

10.2.3 CLI プロンプトからの XMODEM モードのアップロード

ステップ 1:端末エミュレーションソフトウェア（PC 上の HyperTerminal など）を開きます。[Baud Rate]を[9600bps]、[Data bits]を[8]、[Parity]を[none]、[Stop bits]を[1]、[Flow control]を[none]に、それぞれ設定します。端末エミュレーションソフトウェアの[Connect]をクリックします。
ステップ 2:設定ファイルをダウンロードする場合は CLI コマンド transfer download datatype config を、エラーログのダウンロードの場合はコマンド transfer download datatype errorlog を、システムトレースのダウンロードの場合はコマンド transfer download datatype systemtrace を、トラップログのダウンロードの場合はコマンド transfer download datatype traplog を、それぞれ実行します。CLI コマンドの transfer download mode xmodem と transfer download start で転送パラメータを表示します。転送プロンプトが表示されたら＜y＞キーを押し、XMODEM モードでの転送を開始します。
ステップ 3:端末エミュレーションソフトウェアで[receive file]を選択して、ファイル受信ウィンドウを表示します。

ステップ 4:ファイル受信ウィンドウが表示されたら、転送データを保存するローカルディレクトリのパスを含んだファイル名（例：d:\image\ESSTrapLog）を入力するか、[Browse]ウィンドウからファイルを選択します。プロトコルとして[XMODEM]を選択して、[Receive]ボタンをクリックします。
ステップ 5:ファイルの転送が開始されます。転送を中止する場合は、＜Control＋X＞キーを数回押してください。
ステップ 6:ファイル転送が終わると、ファイルがローカルディレクトリに保存されます。

10.2.4 CLI プロンプトからの TFTP モードのダウンロード

ステップ 1:管理用ステーションで TFTP サーバを設定します。

管理用ステーションでの TFTP サーバ・Exceed バージョン 5.3.1 のセットアップについて説明します。他の TFTP サーバでも同じように設定できます。コントロールパネルで[HCL Inetd]をダブルクリックします。[Inetd Configuration]ウィンドウで、[Inetd Service]の[Tftpd]をクリックしてから、[configure]ボタンをクリックします。図 10-5 を例に[Daemon Configuration]ウィンドウを設定します（任意指定のパラメータ-r c:¥image¥read と-w c:¥image¥write は、TFTP サーバ内でのデフォルトのダウンロード／アップロードパスを指定します）。

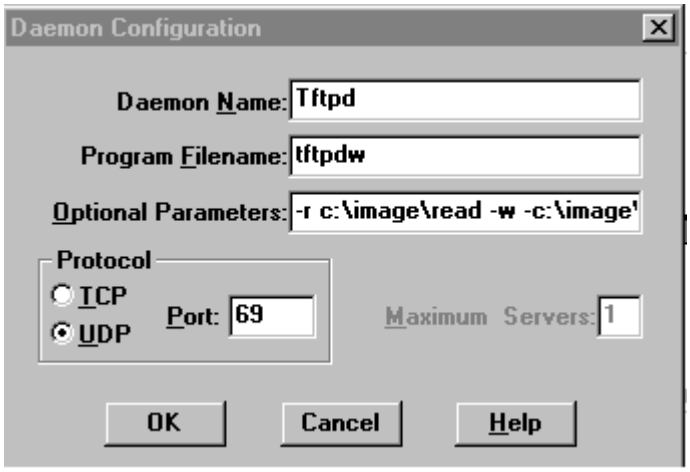

図 10-5：[Daemon Configuration]ウィンドウ

ステップ 2:ソフトウェアのダウンロードの場合は CLI コマンド transfer download datatype code を、設定情報のダウンロードの場合はコマンド transfer download datatype config を実行します。本製品のイメージが TFTP サーバ内に ESSAr22v6b1.tgz のファイル名で保存されている場合は、CLI コマンドの transfer download filename ESSAr22v6b1.tgz を実行します。また、設定イメージが TFTP サーバ内に ESSConfig として保存されている場合は、CLI コマンドの transfer download filename ESSConfig を実行します。TFTP サーバの IP アドレスが 172.30.40.100 の場合は、CLI コマンドの transfer download mode tftp, transfer download serverip 172.30.40.100 を実行します。転送プロンプトが表示されたら＜y＞キーを押し、TFTP モードでの転送を開始します。

ステップ 3:設定ファイルをダウンロードした場合は、転送終了後、自動的に再起動します。

TFTP パスを再定義する場合は、config transfer download path を使用しないでください。ダウンロードファイルが tftpboot ディレクトリにあるとシステムが認識してしまいます。

ソフトウェアイメージファイルをダウンロードした場合は、新しいソフトウェアイメージをフラッシュメモリに保存するかどうかを確認するメッセージが表示されます。＜y＞キーを押すとフラッシュ

メモリに保存されます。イメージの CRC 検証が終わると確認メッセージが表示されるので、もう一度＜y＞キーを押して保存します。ソフトウェアイメージのダウンロードが完了したら、通常の操作を行うことができます。新しいソフトウェアイメージは次回ブート時（次回の電源投入時、または CLI コマンド reset system 実行時）に自動的に起動します。

10.2.5 ブートメニューからの TFTP モードのダウンロード

ステップ 1：実行コードイメージファイルを、本製品付属の CD から管理用システムのローカルディレクトリ（例：d:\image\ESSAr22v6b1.tgz）にコピーします。

ステップ 2：10.2.4 項のステップ 1 に従って TFTP サーバを設定します。

ステップ 3：電源をオン／オフするか、CLI コマンド reset system を実行して、本製品をリセットします。

ステップ 4：スタートアップメニューが表示されたら、「2」を入力してブートメニューに進みます。

1 - Start Operational Code

2 - Start Boot Menu

Select (1, 2): 2

ステップ 5：ブートメニューが表示されたら、「3」を入力して TFTP メニューに進みます。

1 - Start ESSential Operational Code

2 - Load Operational Code Image using XMODEM/YMODEM/ZMODEM

3 - Load Operational Code Image using TFTP

4 - Display Vital Product Data

5 - Change Baud Rate

6 - Retrieve Error Log using TFTP

7 - Retrieve Error Log using XMODEM/YMODEM/ZMODEM

8 - Erase current Configuration

9 - Erase Crash Information files

10 - Format Compact Flash

0 - Quit from ESSential Startup Code Menu

Select option (0-10):3

ステップ 6：TFTP メニューが表示されたら、TFTP サーバの IP アドレス（例：172.30.40.200）、本製品の

IP アドレス（例：172.30.40.201）、ゲートウェイ IP アドレス（任意）（例：172.30.40.2）、そしてソフトウェアイメージのファイル名（例：ESSAr22v6b1.tgz）を入力します。確認メッセージが表示されたら＜y＞キーを押して転送を開始します。

Enter Server IP : 172.30.40.200

Enter Host IP : 172.30.40.201

Enter Gateway IP (optional): 172.30.40.2

Enter File Name : ESSAr22v6b1.tgz

Do you want to continue? Press (Y/N): y

ステップ 7：ファイルの転送が完了したら、本製品の電源を切って、再度入れます。新しいソフトウェアイメージで自動的にブートします。

10.2.6 CLI プロンプトからの TFTP モードの設定データベースアップロード

ステップ 1：10.2.4 項のステップ 1 に従って TFTP サーバを設定します。

ステップ 2：設定情報のアップロードは、次のように CLI コマンドを実行します。

- **データタイプのアップロードを設定する場合は、次のコマンドを実行します。**

```
L3SW>transfer upload datatype <config/traplog>
L3SW> transfer upload datatype config
```

- **設定情報のアップロードに使用するファイル名を設定する場合は、次のコマンドを実行します。**

```
L3SW>transfer upload filename <name>
L3SW>transfer upload filename ess100config
```

- **ファイル転送モードを設定する場合は、次のコマンドを実行します。**

```
L3SW>transfer upload mode <xmodem/ymodem/zmodem/tftp>
L3SW>transfer upload mode tftp
```

- **FTP サーバ上へのファイルのアップロードパスを設定する場合は、次のコマンドを実行します。**

```
L3SW>transfer upload path <path>
L3SW>transfer upload path  /tftpboot
```

DHCP サービスでデフォルト設定のパスを使用している場合はアップロードやダウンロード用のパスを設定する必要はありません。デフォルト設定のパスは、TFTP サーバ上で設定された TFTP サービス用のパスです。

- **TFTP サーバの IP アドレスを設定する場合は、次のコマンドを実行します。**

```
L3SW>transfer upload serverip <ipaddr>
L3SW>transfer upload serverip 172.30.10.8
```

```
L3SW>transfer upload start
   Y
```

```
L3SW>transfer upload start

Mode ..................................  TFTP
TFTP Server IP ........................  172.30.10.8
TFTP Path. ............................
TFTP Filename .........................  l3config

Data Type .............................  Config File

Are you sure you want to start? (y/n) y TFTP Confix transfer
  starting. File transfer operation completed successfully.

L3SW>
```

表 10-1：CLI による TFTP アップロード

TFTP ディレクトリパスを空白に戻す場合は、バックシーケンス' 'を使用してください。

付録 A: 略語一覧

ABR	Area Border Router
AC	Alternating Current
ACL	Access Control List
ALG	Application Level Gateway
AN	Auto Negotiation
ARP	Address Resolution Protocol
ASBR	Autonomous System Border Router
BDR	Backup Designated Router
BGP	Border Gateway Protocol
BOOTP	Bootstrap protocol
BPDU	Bridge PDU
BSR	Broadcast Storm Recovery
CAM	Content Addressable Memory
CIDR	Classless Inter Domain Routing
CLI	Command Line Interface
CRC	Cyclic Redundancy Check
DAP	DOS Attack Protection
DC	Direct Current
DDOS	Distributed DOS
DHCP	Dynamic Host Configuration/Control Protocol
DIAG	Diagnostics (refers to both Manufacturing and POST diagnostics)
DIMM	Dual In-line Memory Module
DOS	Denial Of Service
DR	Designated Router
DVMRP	Distance Vector Multicast Routing Protocol
ESS	Ethernet Smart Switch
FE	Fast Ethernet
FEC	Fast Ethernet Controller
FTP	File Transfer Protocol
GE	Gigabit Ethernet

GMRP	GARP Multicast Registration Protocol
GVRP	Generic VLAN Registration Protocol
HTML	Hyper Text Markup Language
HTTP	Hyper Text Transfer Protocol
Hz	Hertz
ICMP	Internet Control Message Protocol
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IGP	Interior Gateway Protocol
IP	Internet Protocol
IPL	Initial Program Loader
IRDM	ICMP Router Discovery Message
IRDP	ICMP Router Discovery Protocol
kbps	kilobits per second
L2	OSI Layer 2
L3	OSI Layer 3
LACP	Link Access Control Protocol
LAG	Link Aggregation
LAN	Local Area Network
LED	Light Emitting Diode
MAC	Media Access Controller
Max	Maximum
Min	Minimum
MIB	Management Information Base
Mbps	Megabits per second
MBONE	Multicast backbone of the internet
Min	Minimum
NAPT	Network And Port Translation
NAT	Network Address Translation
NE	Network Element
NIC	Network Interface Card
NLRI	Network Link Reachability Information
NTS	Network Time Server
NVM	Non Volatile Memory

OID	Object Identifier
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
PAT	Port Address Translation
PDU	Protocol Data Unit
PING	Packet Internet Groper
PIM-DM	Protocol Independent Multicast – Dense Mode
PIM-SM	Protocol Independent Multicast – Sparse Mode
POST	Power On Self Test
PVID	Port VLAN ID
QOS	Quality Of Service
RAM	Random Access Memory
RARP	Reverse Address Resolution Protocol
RD	Route Discovery
RFC	Request For Comment (TCP/IP Standard-Document)
RIMM	RAMBUS In-Line Memory Module
RIP	Routing Information Protocol
RMC	Rambus Memory Controller
RMON	Remote Monitoring
RO	Read Only
RP	Rendezvous Point
RPM	Revolutions Per Minute
RW	Read Write
RX	Receive
SDRAM	Synchronous Dynamic RAM
SEEPROM	Serial Electronically Erasable Programmable Read Only Memory
SNMP	Simple Network Management Protocol
STP	Spanning Tree Protocol
TCP	Transmission Control Protocol
TFTP	Trivial File transfer Protocol (TCP/IP)
TOS	Type Of Service

TX	Transmit
UDP	User Datagram Protocol
VAC	Voltage Alternate Current
VLAN	Virtual LAN
VRRP	Virtual Router Redundancy Protocol
WAN	Wide Area Network
WBI	Web Based Interface
kHz	kilohertz
ms	millisecond
ps	picosecond
u s	microsecond

FXC7024 マネージメントガイド

2005 年 1 月 1.0 版

・本説明書に記載された内容は、改良のため予告なく変更することがあります。

・本説明書に記載されている社名、製品名はそれぞれの会社の商標、または登録商標です。

(FXC05-DC-200002-R1.0)