NEC

GVT-228149-001-00 1.5

QX-S700G シリーズ

Ethernet PoE スイッチ オペレーションマニュアル

改版履歴

版数	日付	改版内容
1.0	2023/9/14	・初版
1.1	2023/12/11	・1-はじめに 2 章 装置へのログイン 2.2 Telnet を介した設定環境のセットアップ ユーザ認証とローカル認証用パスワードの設定コマンドを追加 ・1-はじめに 3 章 コマンドラインインタフェース 3.2 view とコマンドライン SNMP-server host view を削除 ・2-システム管理 2 章 ユーザラインの設定 2.2 ユーザラインの設定 2.2.2 ユーザの設定 authentication-mode コマンドと set authentication-mode password コマンドを使用した説明に変更 ・2-システム管理　3 章ソフトウェア管理 3.1 ソフトウェア管理設定 3.1.3 PoE ソフトウェアのアップグレード 注意を追加 表 3-3 PoE ソフトウェアのアップグレード 「ポートを有効のまま PoE ソフトウェアをアップグレードする」、no-port-shutdown オプションの説明を追加 ・2-システム管理 4 章ハードウェア情報 4.1.1 ハードウェア情報の表示を追加、display device コマンドを追加 ・2-システム管理 8 章ログ情報 8.3 SYSLOG の表示 表 8-2 SYSLOG の表示 「SYSLOG の情報の表示」と display info-center コマンドを追加 「ログバッファに記録された情報の表示」コマンドを変更 変更前：display info-center [id | informational | notice | warning | error]

		変更後：display logbuffer [*id* | informational | notice | warning | error] 「フラッシュ情報の表示」コマンドを変更 変更前：display info-center flash-info 変更後：display logbuffer flash-info ・2-システム管理　9 章ユーザ 9.2 ユーザの設定 9.2.1 ローカルユーザの設定 デフォルトを変更 変更前：qx_admin 変更後：設定なし ・2-システム管理 14 章 SNMP 14.2.3 コミュニティ名の設定 snmp-agent community コマンドを修正 14.2.8 SNMP グループの設定/削除 snmp-agent security-to-group model コマンドの修正 14.2.9　トラップ送信のための SNMP エージェントの有効/無効の設定 snmp-agent target-host コマンドの修正 shutdown コマンドを削除 target-host コマンドを削除 snmp-agent trap コマンドを修正 14.2.11 SNMP バージョンの設定を削除 14.4 SNMP 通知の設定例 Ⅱ設定手順を修正 ・2-システム管理 17 章 Telnet サーバ 17.4 Telnet サーバの設定例　Ⅲ接続手順を修正 ・2-システム管理 18 章 TFTP を追加 ・3-ポート 1 章 Ethernet ポート 1.3　Ethernet ポートの表示 表 1-10 Ethernet ポートの状態表示 「SFP の情報を表示する」を追加

		display transceiver-information コマンド追加 ・3-ポート 5 章リンクアグリゲーション 5.1 リンクアグリゲーションの概要 最大グループ数の変更 変更前： QX-S708GT-2W-PW：最大 10 グループ(最大 8 ポート/1 グループ） QX-S716GT-4W-PW：最大 20 グループ(最大 8 ポート/1 グループ） 変更後： QX-S708GT-2W-PW：最大 5 グループ(最大 8 ポート/1 グループ） QX-S716GT-4W-PW：最大 10 グループ(最大 8 ポート/1 グループ） ・7-リモート給電 1 章リモート給電 「Underload の検出電流の設定」を削除
1.2	2023/12/13	・表紙　文書番号の位置を修正 ・1-はじめに 1 章 製品の概要 1.2 機能の説明 表 1-1 ロードとアップグレードの修正 ・1-はじめに 2 章 装置へのログイン 2.1 コンソールポートを介した設定環境のセットアップ ステップ 4 に初期パスワードについて文章を追加 ・2-システム管理 3 章 ソフトウェア管理 3.4 ファームウェアアップグレードの実施例 display version コマンドの表示例を修正 ・2-システム管理 6 章 日時情報 6.2 タイムゾーンの設定 表 6-2 clock timezone コマンドを修正、メモを修正 ・2-システム管理 8 章 ログ情報 8.1 SYSLOG ログ情報の表示例を修正 ・2-システム管理 14 章 SNMP 14.3 SNMP 設定の表示

		トラップ情報を表示する コマンドを修正 ・3-ポート 2 章ポートミラーリング 2.2 ポートミラーリングの設定 ポートミラーリング機能と PTP 機能を併用する場合について注意を追加 ・4-VLAN 1 章 VLAN 1.2.3 指定 VLAN への Ethernet ポート追加 表 1-3 port hybrid vlan コマンドを修正 ・8-PTP 1 章 PTP 1.2 PTP の設定 ポートミラーリング機能と PTP 機能を併用する場合について注意を追加
1.3	2023/12/20	・2-システム管理 14 章 SNMP 14.2.1 SNMP エージェントの有効/無効の設定 説明文を修正
1.4	2023/12/27	・2-システム管理 2 章 ユーザラインの設定 2.2.2 ユーザの管理 III. ユーザの設定 参照の表現を修正 ・2-システム管理 6 章 日時情報 参照の表現を修正 ・2-システム管理 17 章 Telnet サーバ 17.2.1 ユーザラインの設定 参照の表現を修正 17.2.2 ユーザの作成 参照の表現を修正 ・9-セキュリティ 1 章 AAA、RADIUS および TACACS+プロトコルの設定 1.3 RADIUS プロトコルの設定 参照の表現を修正
1.5	2024/3/28	・7-リモート給電 1 章 リモート給電 1.2 サポートするリモート給電機能 説明文に IEEE802.3bt を追加 ガードバンド値 Class7、8 を削除

© NEC Corporation 2023-2024

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

商標

本マニュアルに記載されているその他の商標は、各社が保有します。

注意

本マニュアルの内容は、予告なく変更されることがあります。本マニュアルの作成にあたっては、その内容の正確さを期していますが、本マニュアルのすべての記述、情報、および推奨事項は、明示的か暗黙的かにかかわらず、いかなる種類の保証の対象になりません。

本マニュアルは以下に示す 9 個のセクションで構成されています。

01-はじめに

02-システム管理

03-ポート

04-VLAN

05-QoS

06-MAC アドレス

07-リモート給電

08-PTP

09-セキュリティ

本マニュアルについて

バージョン

本マニュアルに対応する製品バージョンは Version1.1.5 以降です。

関連マニュアル

次のマニュアルには、QX-S700G シリーズ Ethernet PoE スイッチに関する詳細な説明があります。

マニュアル	内容
QX-S700G シリーズ Ethernet PoE スイッチインスタレーションマニュアル	システムのインストールに関して説明しています。
QX-S700G **シリーズ** Ethernet PoE **スイッチオペレーションマニュアル**	**（本マニュアル）** **データ設定や代表的なアプリケーションについて記述しています。**
QX-S700G シリーズ Ethernet PoE スイッチコマンドマニュアル	ユーザがさまざまなコマンドを使用するときの参考になります。

マニュアルの構成

QX-S700G シリーズEthernet PoE スイッチ オペレーションマニュアルは、以下の章で構成されます。

- **はじめに**

  Ethernet PoE スイッチへのアクセス方法について説明します。

- **システム管理**

  Ethernet PoE スイッチのシステム管理に使用するコマンドについて説明します。

- **ポート**

  Ethernet ポートの設定に使用するコマンドについて説明します。

- **VLAN**

  VLAN の設定に使用するコマンドについて説明します。

- **QoS**

  QoS の設定に使用するコマンドについて説明します。

- **MAC アドレス**

  MAC アドレスの設定に使用するコマンドについて説明します。

- **リモート給電**

  リモート給電の設定に使用するコマンドについて説明します。

- **PTP**

  PTP の設定に使用するコマンドについて説明します。

- **セキュリティ**

  セキュリティの設定に使用するコマンドについて説明します。

表記規則

本マニュアルでは、次の表記規則を使用しています。

I. コマンドの表記規則

表記規則	説明
太字体	コマンド行のキーワードには**太字体**を使用します。
イタリック体	コマンドの引数には*イタリック体*を使用します。
[]	大カッコに囲まれた項目 (キーワードまたは引数) はオプションです。
{x|y|...}	選択する項目は中カッコに入れて、縦線で区切ってあります。1 つを選択します。
[x|y|...]	オプションの選択項目は大カッコに入れて、縦線で区切ってあります。1 つまたは複数を選択します。
{x|y|...}*	選択する項目は中カッコに入れて、縦線で区切ってあります。少なくとも 1 つ、多い場合はすべてを選択できます。
[x|y|...]*	オプションの選択項目は大カッコに入れて、縦線で区切ってあります。複数選択することも、何も選択しないこともできます。
#	#で始まる行はコメントです。

II. GUI の表記規則

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

III. キーボード操作

書式	説明
<キー>	三角カッコ内の名前のキーを押します。たとえば、<Enter>、<Tab>、<Backspace>、<A>となります。
<キー1 + キー2>	複数のキーを同時に押します。たとえば、<Ctrl+Alt+A>は 3 つのキーを同時に押すことを表します。
<キー1、キー2>	複数のキーを順番に押します。たとえば、 <Alt、A>は 2 つのキーを順に押すことを表します。

IV. マウス操作

動作	説明
クリック	左ボタンまたは右ボタンを素早く押します (特に記述がない場合は左ボタン)。
ダブルクリック	左ボタンを素早く 2 回続けて押します。
ドラッグ	左ボタンを押したまま、別の位置まで移動します。

V. コマンドの表記規則

本マニュアルでは、以下のような記号も使用して、操作中に特に注意すべき点を強調しています。意味は次のとおりです。

⚠ **注意、警告、危険**：操作中に特に注意すべきことを表します。

🕮 **メモ、コメント、ヒント、ノウハウ、アイディア**：補助的な説明を表します。

VI. 設定例

本マニュアルの設定例の記述は、各機能の設定例です。インタフェース番号、システム名の表記、display コマンドでの情報表示がご使用の装置と異なることがあります。

VII. セキュリティ強化

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

QX-S700G シリーズ Ethernet PoE スイッチ

オペレーションマニュアル

1.はじめに

本マニュアルは以下に示す章で構成されています。

01-製品の概要

02-装置へのログイン

03-コマンドラインインタフェース

目次

このセクションのページは **1-x-x** です。

1 章 製品の概要 1-1

1.1 製品の概要 1-1

1.2 機能の説明 1-1

1章 製品の概要

1.1 製品の概要

QX-S700G シリーズ Ethernet PoE スイッチは、ワイヤスピードの L2 スイッチング機能を提供します。

このシリーズには、以下の主要なタイプのスイッチがあります。

- QX-S708GT-2X-PW
- QX-S716GT-4X-PW

QX-S708GT-2X-PW には､8 の固定 10BASE-T/100BASE-TX/1000BASE-T 自動検出、給電ポート、2 つの固定 1000BASE-X/10GBASE-R の SFP ポート、1 つのコンソールポートがあります。

QX-S716GT-4X-PW には､16 の固定 10BASE-T/100BASE-TX/1000BASE-T 自動検出、給電ポート、4 つの固定 1000BASE-X/10GBASE-R の SFP ポート、1 つのコンソールポートがあります。

1.2 機能の説明

表1-1 機能の説明

機能	実装
VLAN	● IEEE 802.1Q規格に準拠したVLANをサポートしています。 ● ポートベースのVLANをサポートしています。
フロー制御	● IEEE 802.3xフロー制御(全二重)をサポートしています。 ● バックプレッシャーベースのフロー制御(半二重)をサポートしています。
ブロードキャスト抑止	● ブロードキャスト抑止をサポートしています。
リンクアグリケーション	● リンクアグリケーションをサポートしています。
ミラーリング	● ポートベースのミラーリングをサポートしています。
ポートアイソレート	● ポートアイソレートをサポートしています。
QoS	● 帯域幅制御をサポートしています。 ● 802.1pおよびDSCPの優先順位をサポートしています。 ● ポートで異なる優先順位のキューをサポートしています。

	● キュースケジューリング：重み付けラウンドロビン(WRR)、Strict-priority(SP)
セキュリティ機能	● MACアドレスによるポートセキュリティ機能 ● マルチレベルユーザ管理とパスワード保護をサポートしています。
管理と保守	● コマンドラインインタフェース設定をサポートしています。 ● コンソールポートを介した設定をサポートしています。 ● Telnetを介したリモート設定をサポートしています。 ● システムログをサポートしています。 ● デバッグ情報の出力をサポートしています。 ● PINGをサポートしています。 ● ループバック検出機能をサポートしています。 ● 装置内の温度監視機能をサポートしています。
ロードとアップグレード	● XModemプロトコルを使用したソフトウェアのロードとアップグレードをサポートしています。 ● TFTP(Trivial File Transfer Protocol)を使用したソフトウェアのロードとアップグレードをサポートしています。

目次

このセクションのページは **1-x-x** です。

2 章 装置へのログイン 2-1

2.1 コンソールポートを介した設定環境のセットアップ 2-1

2.2 Telnet を介した設定環境のセットアップ 2-2

2章 装置へのログイン

2.1 コンソールポートを介した設定環境のセットアップ

ステップ 1：図 2-1 に示すように、ローカル設定環境をセットアップするには、コンソールケーブルでコンソール端末のシリアルポートを装置のコンソールポートに接続します。

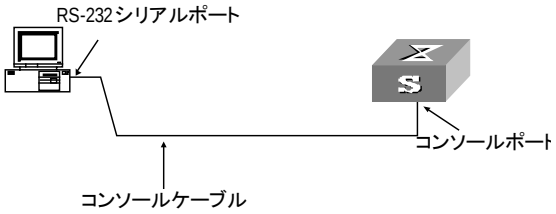


図2-1 コンソールポートを介したローカル設定環境のセットアップ

ステップ 2：コンソール端末で端末エミュレータ(ここでは TeraTerm ver4.92 を使用)を実行します。新しい接続から「シリアル」を選択し、COM ポート番号を選択します。

図2-2 新しい接続

ステップ 3：「設定」「シリアルポート」からパラメータを設定します。ボーレートを 9600、データを 8bit、パリティを none、ストップを 1bit、フロー制御を none を選択します。

図2-3 パラメータ設定

ステップ 4 : 装置の電源を入れます。装置のセルフテスト情報が表示され、Enter キーを押すことを要求します。<QX-S708GT-2X-PW>などのコマンドラインプロンプトが表示されます。パスワード入力を要求されたら、パスワードを入力してください。初期パスワードは「qx_admin」です。

ステップ 5 : コマンドを入力して、装置を設定するか、動作状態を表示します。“?”を入力すると、コマンドのヘルプが表示されます。

2.2 Telnetを介した設定環境のセットアップ

装置のリモート管理を行うため、Telnet サーバを使用することができます。

Telnet を使用する場合、以下の作業を行ってください。

- 装置 IP アドレスを設定します。
- Telnet を有効にします。
- ユーザー認証とローカル認証用パスワードの設定を行います。
- ネットワーク環境をセットアップします。
- PC 端末から Telnet ログインします。
- パスワードを入力します。

ステップ 1：コンソールポートを通じて装置 IP アドレスを設定し、Telnet を有効にします。

```
<QX-S716GT-4X-PW>system-view
[QX-S716GT-4X-PW]telnet server enable
[QX-S716GT-4X-PW]interface vlan 1
[QX-S716GT-4X-PW-Vlan-interface1]ip address 192.168.1.100 255.255.240.0
```

ステップ 2：ユーザー認証の設定とローカル認証用のパスワードを設定します。ここでは例として 1234 というパスワードを設定します。

```
<QX-S716GT-4X-PW>system-view
[QX-S716GT-4X-PW]line vty 0
[QX-S716GT-4X-PW-line-vty0]authentication-mode password
[QX-S716GT-4X-PW-line-vty0]set authentication password simple 1234
```

ステップ 3：ネットワーク環境をセットアップし、PC 端末の Ethernet ポートを装置のポートに接続します。

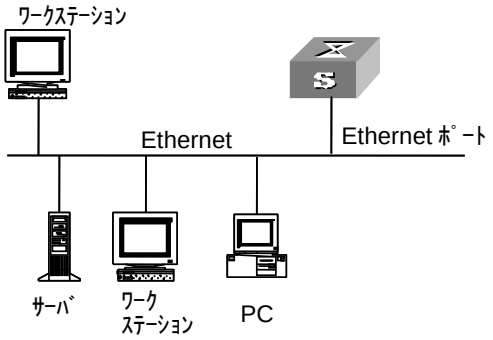


図2-4 Telnet を介した設定環境のセットアップ

ステップ 4：PC 端末で装置 IP アドレスを指定し、Telnet を実行します。

ステップ 5：PC 端末で、パスワードを正しく入力します。

メモ：

パスワードを入力する時、入力画面に表示されません。

目次

このセクションのページは **1-x-x** です。

3 章 コマンドラインインタフェース 3-1

3.1 コマンドラインインタフェース 3-1

3.2 view とコマンドライン 3-1

3.3 コマンドラインの特徴と機能 3-3

3.3.1 コマンドラインのオンラインヘルプ 3-3

3.3.2 コマンドラインの表示特性 3-5

3.3.3 コマンドラインのヒストリコマンド 3-5

3.3.4 コマンドライン共通のエラーメッセージ 3-6

3.3.5 コマンドラインの編集特性 3-6

3章 コマンドラインインタフェース

3.1 コマンドラインインタフェース

QX-S700G シリーズ Ethernet PoE スイッチには、装置を設定および管理するために一連の設定コマンドとコマンドラインのインタフェースが用意されています。コマンドラインインタフェースには以下の特徴があります。

- コンソールポートからのローカル設定
- Telnet 経由によるローカルまたはリモート設定
- 権限を持たないユーザのアクセスを防止するためのコマンドレベルによる保護
- “?”入力によるオンラインヘルプ
- ネットワークトラブルシューティングのための、Ping などのネットワークテストコマンド
- ネットワークトラブルシューティングのための、さまざまな詳細デバッグ情報
- ヒストリコマンド実行のための、Doskey と同様の機能
- キーワードと完全に一致しなくても検索可能なコマンドラインインタープリタ(キーワードの解釈が多岐にわたらない限り、キーワードの全体または一部を入力して検索可能)

3.2 viewとコマンドライン

QX-S700G シリーズ Ethernet PoE スイッチでは、それぞれの view は、それぞれの必要性に基づいて実装されており、互いに関連付けられています。 たとえば、装置にログインした後で、User view では、実行状態と統計情報の表示などの基本機能しか使用できません。User view で system-view を入力して System view に入ると、さまざまな設定コマンドを入力して、対応する view に入ることができます。

コマンドラインには以下の view があります。

User view
System view
Ethernet port view
VLAN view
Vlan-interface view
Local-user view

User Line view

図 3-1 に各 view の関係図を示します。

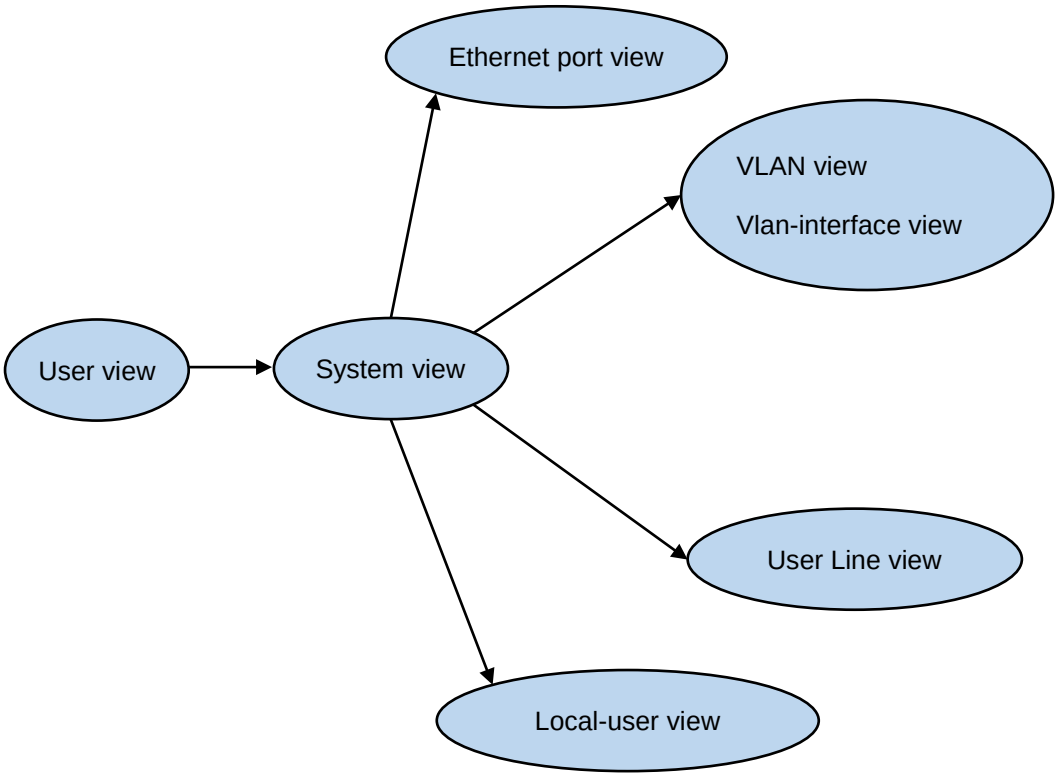


図3-1 各 view の関係図

表 3-1 では、view の機能とその表示または終了方法について説明します。

表3-1 view の機能

コマンド view	機能	プロンプト	表示するためのコマンド	終了するためのコマンド
User view	動作と統計に関する基本情報を表示します。	<QX-S716GT-4X-PW>	スイッチに接続した直後に表示されます。	quitでスイッチとの接続が切断されます。
System view	システムパラメータを設定します。	[QX-S716GT-4X-PW]	User viewでsystem-viewと入力します。	quitまたはreturnでUser viewに戻ります。
Ethernet port view	Ethernetポートパラメータを設定します。	[QX-S716GT-4X-PW-Ethernet0/1]	System viewでinterface gigabitEthernet 1/1または、interface ten-gigabitEthernet 1/17と入力します。	quitでSystem viewに戻ります。
VLAN view	VLANパラメータを設定します。	[QX-S716GT-4X-PW-Vlan1]	System viewでvlan 1と入力します。	
VLAN interface view	VLANまたはVLAN集約のために、IPインタフェースパラメータを設定します。	[QX-S716GT-4X-PW-Vlan-interface1]	System viewでinterface vlan 1と入力します。	
Local-user view	ローカルユーザパラメータを設定します。	[QX-S716GT-4X-PW-luser-user1]	System viewでlocal-user user1と入力します。	
User Line view	ユーザラインパラメータを設定します。	[QX-S716GT-4X-PW-line-vty0]	System viewでline vty 0と入力します。	

3.3 コマンドラインの特徴と機能

3.3.1 コマンドラインのオンラインヘルプ

コマンドラインインタフェースには、以下のオンラインヘルプモードがあります。

詳細ヘルプ

部分ヘルプ

以下に説明するオンラインヘルプコマンドを使用して、ヘルプ情報を取得できます。

1) 任意の view で“?”と入力すると、その view のすべてのコマンドと、対応する説明が表示されます。

```
<QX-S716GT-4X-PW>?
User view commands:
  boot         Set boot option
  copy         Copy from source to destination
  delete       Delete one file in flash: file system
```

2) コマンドの後にスペースを入れて、“?”を入力してください。“?”の位置がキーワード用ならば、関連するすべてのキーワードとその簡潔な説明が一覧表示されます。

```
<QX-S716GT-4X-PW>boot ?
  bootrom    Update bootrom
```

3) コマンドの後にスペースを入れて、“?”を入力してください。“?”の位置がパラメータ用ならば、関連するすべてのパラメータとその簡潔な説明が一覧表示されます。

```
[QX-S716GT-4X-PW]vlan ?
  <vlan_list>    ISL VLAN IDs
[QX-S716GT-4X-PW]vlan 1 ?
  <cr>
```

<cr>は、この位置にパラメータがないことを示しています。以下のコマンドラインではコマンドが繰り返されます。<Enter>を押してそのコマンドを直接実行できます。

4) 文字列と“?”を入力すると、その文字列で始まるすべてのコマンドが一覧表示されます。

```
<QX-S716GT-4X-PW>p?
  ping
```

5) コマンドの後に文字列と“?”を入力すると、コマンドのその文字列で始まるすべてのキーワードが一覧表示されます。

```
<QX-S716GT-4X-PW>display ver?
  version
```

6) キーワードの最初の文字を入力し、<Tab>を押します。この文字で始まるキーワードが自動的に表示されます。

```
<QX-S716GT-4X-PW>d

delete   dir      display  dot1x
```

3.3.2 コマンドラインの表示特性

コマンドラインインタフェースには、以下の表示特性があります。

複数の画面にわたって表示される情報では、一時停止機能が用意されています。

この場合、表 3-2 に示すように 3 つの選択肢があります。

表3-2 表示機能

キーまたはコマンド	機能
表示が一時停止したときに、<Ctrl+C>を押す	表示とコマンドの実行を停止します。
表示が一時停止したときに、スペースキーを押す	次の画面の情報を引き続き表示します。
表示が一時停止したときに、<Enter>を押す	次の行の情報を引き続き表示します。

3.3.3 コマンドラインのヒストリコマンド

コマンドラインインタフェースには、DosKey に似た機能があります。ユーザが入力したコマンドは、コマンドラインインタフェースによって自動的に保存され、後でいつでもそのコマンドを呼び出して実行できます。ヒストリコマンドバッファのデフォルトは 10 です。つまり、コマンドラインインタフェースは、ユーザごとに 10 のヒストリコマンドを保存できます。表 3-3 に操作方法を示します。

表3-3 ヒストリコマンドの取得

操作	キー	結果
前のヒストリコマンドを表示する	上矢印キーまたは <Ctrl+P>	存在する場合には、前のヒストリコマンドが取得されます。
次のヒストリコマンドを表示する	下矢印キーまたは <Ctrl+N>	存在する場合には、次のヒストリコマンドが取得されます。

3.3.4 コマンドライン共通のエラーメッセージ

文法チェックにパスすれば、ユーザによるすべての入力コマンドは正しく実行できます。パスしなかった場合は、エラーメッセージが表示されます。表 3-4 に共通エラーメッセージを一覧表示します。

表3-4 コマンドライン共通のエラーメッセージ

エラーメッセージ	原因
Unrecognized command	コマンドを見つけることができません。
	キーワードを見つけることができません。
	パラメータの型が間違っています。
	パラメータの値が範囲外です。
Incomplete command	入力したコマンドが不完全です。
Too many parameters	入力したパラメータが多すぎます。
Ambiguous command	入力したパラメータを特定できません。

3.3.5 コマンドラインの編集特性

コマンドラインインタフェースには基本的なコマンド編集機能があり、複数行の編集をサポートしています。コマンドは 256 文字以下で編集します。下表を参照してください。

表3-5 編集機能

キー	機能
一般的なキー	カーソル位置から入力され、編集バッファにまだ空き領域がある場合は、カーソルが右に移動します。
Backspace	カーソルの後ろの文字を削除し、カーソルは後ろに移動します。
左矢印キーまたは <Ctrl+B>	カーソルを1文字後ろに移動します。
右矢印キーまたは <Ctrl+F>	カーソルを1文字前に移動します。
<Ctrl+D>	カーソル上の文字を1文字削除
上矢印キーまたは <Ctrl+P>	ヒストリコマンド（履歴を一つ前に遡る）を取得します。

キー	機能
下矢印キーまたは <Ctrl+N>	ヒストリコマンド（履歴を逆順に遡る）を取得します。
<Tab>	キーワードの一部を入力してから<Tab>を押すと、部分ヘルプが実行されます。入力した文字列と一致するキーワードが一意の場合は、入力した文字列は完全なキーワードに置き換えられて、新しい行に表示されます。一致するキーワードがないか、一致するキーワードが一意ではない場合、変更は加えられず、入力した元の文字列が新しい行に表示されます。

QX-S700G シリーズ Ethernet PoE スイッチ

オペレーションマニュアル

2.システム管理

本マニュアルは以下に示す章で構成されています。

01-ホスト名

02-ユーザライン

03-ソフトウェア管理

04-ハードウェア情報

05-設定情報

06-日時情報

07-システム情報

08-ログ情報

09-ユーザ

10-装置の再起動

11-温度センサ

12-ファイルシステム

13-NTP

14-SNMP

15-ネットワーク管理

16-SSH

17-Telnet サーバ

18-TFTP

目次

このセクションのページは **2-x-x** です。

1 章 ホスト名の設定 1-1

1.1 ホスト名の設定 1-1

1章 ホスト名の設定

1.1 ホスト名の設定

スイッチのホスト名を設定するには、System view で以下のコマンドを実行します。

表1-1 ホスト名の設定

操作	コマンド
スイッチのホスト名を設定する	**sysname** *sysname*
スイッチのホスト名をデフォルトに戻す	**undo sysname**

目次

このセクションのページは **2-x-x** です。

2 章 ユーザラインの設定 2-1

2.1 ユーザラインの概要 2-1

2.2 ユーザラインの設定 2-1

2.2.1 User Line view への移行 2-1

2.2.2 ユーザの管理 2-2

2.2.3 ヘッダの設定 2-3

2.2.4 コマンド履歴件数の設定 2-4

2.2.5 アイドルタイムアウトの設定 2-4

2.2.6 ロケーション名の設定 2-4

2.2.7 画面表示行数の設定 2-5

2.2.8 画面表示文字数の設定 2-5

2.3 ユーザラインの表示 2-6

2.3.1 コマンド履歴の表示 2-6

2.3.2 Line インターフェース情報の表示 2-6

2.3.3 ユーザライン情報の表示 2-6

2章 ユーザラインの設定

2.1 ユーザラインの概要

装置では、ユーザラインの設定によっても、ポートデータを設定および管理できます。

以下の設定方法をサポートしています。

コンソールポートを介したローカル設定

Ethernet ポート上の Telnet を介したリモート設定

上記の設定方法用に、以下の 2 種類のユーザラインがあります。

AUX ユーザライン

AUX ユーザラインは、コンソールポートを通じて装置にログインするために使用します。装置は、1 つの AUX ポートを実装します。

VTY ユーザライン

VTY ユーザラインは、装置に Telnet 接続するために使用します。装置は、4 つの VTY ポートを実装します。

メモ:

装置では、AUX ポートとコンソールポートは同一です。

2.2 ユーザラインの設定

ユーザラインでは、以下の項目を設定します。

- User Line view への移行
- ユーザの管理
- ヘッダの設定
- コマンド履歴保存件数の設定
- アイドルタイムアウトの設定
- 画面表示行数の設定
- 画面表示文字数の設定

2.2.1 User Line viewへの移行

以下のコマンドは、User Line view に入るために使用します。

System view で、以下のコマンドを実行します。

表2-1 User Line view への移行

操作	コマンド
User Line viewに移行する。	**line** { **aux 0** | **vty** *num* }

2.2.2 ユーザの管理

I. 認証方法の設定

以下のコマンドは、ユーザログイン認証方法を設定して、権限のないユーザのアクセスを拒否するために使用します。

User Line view で、以下のコマンドを実行します。

表2-2 認証方法の設定

操作	コマンド
認証方法を設定する	**authentication-mode** { **password** | **scheme** }
認証をデフォルトに設定する	**undo authentication-mode**

デフォルト:ユーザライン AUX（コンソールポート）を介してログインするとき、ユーザ認証は実行されません。ユーザライン VTY（Telnet ユーザ）がログインする場合には、認証のためにパスワードが要求されます。

II. パスワードの設定

set authentication-mode password コマンドを使用して、パスワードのローカル認証を実行できます。つまり、正常にログインするためには、以下のコマンドを使用してログインパスワードを設定する必要があります。

User Line view で、以下のコマンドを実行します。

表2-3 パスワードの設定

操作	コマンド
ローカル認証パスワードを設定する	**set authentication password** { **hash** | **simple** } *password*
ローカル認証パスワードを削除する	**undo set authentication password**

ユーザが VTY 0 ユーザラインを通じてログインした場合のパスワード認証を設定し、パスワードを passabcde に設定する

```
[QX-S708GT-2X-PW]line vty 0
[QX-S708GT-2X-PW-line-vty0]authentication-mode password
[QX-S708GT-2X-PW-line-vty0]set authentication password simple passabcde
```

III.　ユーザの設定

authentication-mode scheme コマンドを使用して、ユーザ名とパスワードによるローカル認証を実行できます。詳細については、セクション 2 システム管理 “ユーザ” を参照してください。

```
[QX-S708GT-2X-PW-line-vty0]authentication-mode scheme
[QX-S708GT-2X-PW-line-vty0]quit
[QX-S708GT-2X-PW]local-user user1 password simple passabcde
```

メモ:

- デフォルトでは、Telnet ユーザがログインする場合には、認証のためにパスワードが要求されます。
- 設定したパスワードはコンフィグレーションファイルに暗号化テキストで保存されます。

2.2.3 ヘッダの設定

ユーザログイン時にヘッダを表示するかどうかを設定します。System view にて実行します。

表2-4 ヘッダの設定

操作	コマンド
ユーザログイン時に表示するヘッダを設定する	**header shell** *text*
ユーザログイン時に表示するヘッダをデフォルトにする。	**undo header shell**

デフォルト：以下のメッセージを表示

Please change the password from the default settings.

2.2.4 コマンド履歴件数の設定

ログインした aux/vtx ユーザラインにコマンド履歴件数を設定します。User Line view にて実行します。

表2-5 コマンド履歴件数の設定

操作	コマンド
コマンド履歴件数を設定する	**history-command max-size** *his_num*
コマンド履歴件数をデフォルトに戻す	**undo history-command max-size**

デフォルト:32

2.2.5 アイドルタイムアウトの設定

ログインした aux/vtx ユーザラインにアイドルタイムアウトを設定します。User Line view にて実行します。

表2-6 アイドルタイムアウトの設定

操作	コマンド
アイドルタイムアウトを設定する	**idle-timeout** *minutes* [*seconds*]
アイドルタイムアウトをデフォルトに戻す	**undo idle-timeout**

デフォルト:有効。すべてのユーザラインで 10 分に設定（つまり、何も操作を行わなければ、ユーザラインは 10 分後に自動的に切断される）

idle-timeout 0 に設定すると、アイドルタイムアウトが無効になります。

2.2.6 ロケーション名の設定

ログインした aux/vtx ユーザラインにロケーション名を設定します。User Line view にて実行します。

表2-7 ロケーション名の設定

操作	コマンド
ロケーション名を設定する	**location** *location*
ロケーション名ををデフォルトに戻す	**undo location**

デフォルト:設定なし

2.2.7 画面表示行数の設定

ログインした aux/vty ユーザラインに、画面に表示できる行数を設定します。User Line view で、以下のコマンドを実行します。

表2-8 画面表示行数の設定

操作	コマンド
画面に表示できる最大行数を設定する	screen-length *screen-length*
画面に表示できる最大行数をデフォルトにする	undo screen-length

デフォルト：最大 24 行

最大数を 0 とすると画面の表示は停止しません。

2.2.8 画面表示文字数の設定

ログインした aux/vty ユーザラインに、画面上で表示される 1 行あたりの表示文字数を設定します。User Line view で、以下のコマンドを実行します。

表2-9 画面上で表示される 1 行あたりの表示文字数の設定

操作	コマンド
画面に表示できる1行あたりの表示文字数を設定する	screen-width *screen-width*
画面に表示できる1行あたりの表示文字数をデフォルトに戻す	undo screen-width

デフォルト：80

最大数を 0 とすると制限なしになります。

2.3 ユーザラインの表示

2.3.1 コマンド履歴の表示

実行したコマンド履歴を表示します。

表2-10 コマンド履歴の表示

操作	コマンド
コマンド履歴を表示する	**display history-command**

2.3.2 Lineインターフェース情報の表示

ユーザライン設定の実行結果を表示し、設定を確認します。

表2-11 Line インターフェース情報の表示

操作	コマンド
Lineインターフェース情報を表示する	**display line**

2.3.3 ユーザライン情報の表示

ユーザライン情報を表示します。

表2-12 ユーザライン情報の表示

操作	コマンド
ユーザライン情報を表示する	**display terminal**

目次

このセクションのページは **2-x-x** です。

3 章 ソフトウェア管理 3-1

3.1 ソフトウェア管理設定 3-1

3.1.1 ブート ROM のアップグレード 3-1

3.1.2 ファームウェアのアップグレード 3-1

3.1.3 PoE ソフトウェアのアップグレード 3-2

3.2 システムバージョンの表示 3-3

3.3 ファイル内容の表示 3-3

3.4 ファームウェアアップグレードの実施例 3-3

3章 ソフトウェア管理

3.1 ソフトウェア管理設定

ソフトウェア管理設定では、以下の設定を行います。

- ブート ROM のアップグレード
- ファームウェアのアップグレード
- PoE ソフトウェアのアップグレード

3.1.1 ブートROMのアップグレード

ブート ROM をアップグレードするには、User view で以下のコマンドを実行します。

リモート側から TFTP を使用してスイッチにブート ROM プログラムファイルをダウンロードし、ブート ROM をアップグレードします。

表3-1 ブート ROM のアップグレード

操作	コマンド
ブートROMをアップグレードする	**boot bootrom** *//A.A.A.A/*xxx.yyy */*

例：TFTP サーバ(10.10.10.1)の指定のディレクトリからファイル 700g_boot.bin をダウンロードする場合、tftp://10.10.10.1/700g_boot.bin と指定します。

3.1.2 ファームウェアのアップグレード

ファームウェアをアップグレードするには、User view で以下のコマンドを実行します。

リモート側から TFTP を使用してスイッチにファームウェアをダウンロードし、ファームウェアをアップグレードします。

表3-2 ファームウェアのアップグレード

操作	コマンド
ファームウェアをアップグレードする	**boot boot-loader** *//A.A.A.A/*xxx.yyy

例:TFTP サーバ(10.10.10.1)の指定のディレクトリからファイル 700g.bin をダウンロードする場合、tftp://10.10.10.1/700g.bin と指定します。

3.1.3 PoEソフトウェアのアップグレード

PoE ソフトウェアをアップグレードするには、System view で以下のコマンドを実行します。

リモート側から TFTP を使用してスイッチにファームウェアをダウンロードし、ファームウェアをアップグレードします。

表3-3 PoE ソフトウェアのアップグレード

操作	コマンド
PoEソフトウェアをアップグレードする	**poe-chip update** *//A.A.A.A/*xxx.yyy
ポートを有効のままPoEソフトウェアをアップグレードする	**poe_chip update** //A.A.A.A/xxx.yyy **no-port-shutdown**

例：TFTP サーバ(10.10.10.1)の指定のディレクトリからファイル 700g_poe.s19 をダウンロードする場合、tftp://10.10.10.1/700g_poe.s19 と指定します。

⚠ **注意：**

- poe-chip update コマンドは、コマンドラインインタープリタ(コマンドの省略入力)が使用できません。コマンドを正確に入力して実行してください。
- poe-chip update コマンドで PoE ソフトウェアのアップグレードを実施した後、装置は自動的に再起動します。
- poe-chip update コマンドで PoE ソフトウェアのアップグレード中は、装置の給電機能を無効にします。
- poe-chip update コマンドで PoE ソフトウェアのアップグレード中は、すべてのポートをシャットダウン(無効)します。ポートを有効のまま PoE ソフトウェアのアップグレードをする場合は、no-port-shutdown オプションを指定してコマンドを実行してください。

- PoE ソフトウェアのアップグレードに失敗した場合は、装置の交換が必要になります。お買い上げの販売店へご連絡をお願いいたします。

3.2 システムバージョンの表示

display コマンドを実行してシステムのバージョンを表示できます。

表3-4 システムバージョンの表示

操作	コマンド
システムバージョンを表示する	**display version**

3.3 ファイル内容の表示

more コマンドを実行してファイルの内容を表示できます。

表3-5 ファイルの内容の表示

操作	コマンド
ファイルの内容を表示する	**more** *filename*

3.4 ファームウェアアップグレードの実施例

tftp サーバ(10.10.10.1)からファイル 700g.bin をダウンロードし、ファームウェアをアップグレードします。

```
<QX-S708GT-2X-PW>boot boot-loader tftp://10.10.10.1/700g.bin
Downloading...
Got 11005933 bytes
Starting flash update - do not power off device!
Checking old image linux.bk... needs update
Erasing 'linux.bk'... done!
Programming 'linux.bk'... done!
```

```
Swapping  images...done

Restarting,  please  wait...


Service  "switch_[   883.125633]  reboot:  Restarting  system

app"  of  type  =  "

Starting  ...
```

リブート後、display version コマンドでバージョンを確認します。

```
<QX-S708GT-2X-PW>display version

QX Software, Version 1.1.x    2023-11-24T08:19:45+08:00

Copyright (c) 2023 HIRAKAWA HEWTECH CORP. All rights reserved.

QX-S708GT-2X-PW uptime is 02:12:16


QX-S708GT-2X-PW with 416M MIPS32-24KEc Processor

256MB bytes SDRAM

32M bytes Flash Memory

Config Register points to FLASH


Hardware Version is RB0

Serial Number is 23700014

Bootrom Version is 1.1.4    11:13:41, Nov    7 2023


PSE HARD VERSION                                :0

PSE SOFT VERSION                                :355


System Contact                                  :NEC Corporation

System Name                                     :QX-S708GT-2X-PW

System Location                                 :
```

目次

このセクションのページは **2-x-x** です。

4 章 ハードウェア情報 4-1

4.1 ハードウェア情報の概要 4-1

4.1.1 ハードウェア情報の表示 4-1

4.1.2 CPU 使用率の表示 4-1

4.1.3 メモリ情報の表示 4-1

4.1.4 FAN の状態表示 4-2

4章 ハードウェア情報

4.1 ハードウェア情報の概要

ハードウェアに関する以下の情報を表示できます。

- ハードウェア情報の表示
- CPU 使用率の表示
- メモリ情報の表示
- ファン情報の表示

4.1.1 ハードウェア情報の表示

display コマンドを実行してハードウェア情報を表示できます。

表4-1 ハードウェア情報の表示

操作	コマンド
ハードウェア情報を表示する	**display device**

4.1.2 CPU使用率の表示

装置の CPU 使用率を表示できます。

表4-2 CPU 使用率の表示

操作	コマンド
CPU使用率を表示する。	**display cpu**

4.1.3 メモリ情報の表示

装置のメモリ情報を表示できます。

表4-3 メモリ情報の表示

操作	コマンド
メモリ情報を表示する。	**display memory**

4.1.4 FANの状態表示

ファンの状態を確認できます。

このコマンドはファン搭載製品でのみ使用可能です。

表4-4 FAN の状態表示

操作	コマンド
FANの状態を表示する	**display fan**

目次

このセクションのページは **2-x-x** です。

5 章 設定情報 5-1

5.1 設定情報の概要 5-1

5.1.1 Ethernet スイッチのコンフィグレーション表示 5-1

5.1.2 現在のコンフィグレーションの保存 5-2

5.1.3 コンフィグレーションのリセット 5-2

5章 設定情報

5.1 設定情報の概要

設定情報では、ユーザフレンドリーなマン・マシンインタフェースを提供しています。装置は、スイッチのコンフィグレーションをコマンドラインのテキスト形式で保存し、設定プロセス全般にわたり記録します。

このため、設定情報の表示が容易です。

コンフィグレーションファイルの形式は、以下のとおりです。

- コンフィグレーションをコマンド形式で保存します。

デフォルト以外の定数のみ保存されます。コンフィグレーションファイルの管理では、以下の操作および設定を行います。

- Ethernet スイッチのコンフィグレーション表示
- 現在のコンフィグレーションの保存
- コンフィグレーションのリセット

5.1.1 Ethernetスイッチのコンフィグレーション表示

電源を投入すると、システムはフラッシュメモリからコンフィグレーションファイルを読み出して、装置の起動を行います（ここで読み出すコンフィグレーションファイルを「保存したコンフィグレーション」と呼ぶ）。フラッシュメモリ内にコンフィグレーションファイルが存在しない場合は、デフォルトのパラメータで初期化を開始します。システムの稼動状態で有効になっている設定を、「保存したコンフィグレーション」に対して「運用中のコンフィグレーション」と呼びます。

装置の現在のコンフィグレーションおよび保存されたコンフィグレーションを表示するには、以下のコマンドを実行します。これらのコマンドは、すべての view で実行可能です。

表5-1 Ethernet スイッチのコンフィグレーション表示

操作	コマンド
運用中のコンフィグレーションを表示する。	**display current-configuration** [**configuration** **user-interface** | **interface** { *interface-type interface-num* | **vlan** *vlan_id* }]

保存したコンフィグレーションを表示する。	**display saved-configuration**

5.1.2 現在のコンフィグレーションの保存

save コマンドを使用して運用中のコンフィグレーションをフラッシュメモリに保存すると、その設定は「保存したコンフィグレーション」として、次回のシステム電源投入時に使用されます。

User view で以下のコマンドを実行します。

表5-2 現在のコンフィグレーションの保存

操作	コマンド
運用中のコンフィグレーションを保存する。	**save**

5.1.3 コンフィグレーションのリセット

reset saved-configuration コマンドは、Ethernet スイッチのフラッシュメモリのコンフィグレーションファイルをリセットします。

User view で以下のコマンドを実行します。

表5-3 コンフィグレーションのリセット

操作	コマンド
フラッシュメモリのコンフィグレーションファイルをリセットする。	**reset saved-configuration**

目次

このセクションのページは **2-x-x** です。

6 章 日時情報 6-1

6.1 システムクロックの設定 6-1

6.2 タイムゾーンの設定 6-2

6.3 システムクロックの表示 6-2

6章 日時情報

システムクロックは、NTP (Network Time Protocol) クロック、または、ローカルシステムクロックのどちらかを選択して設定することができます。

NTP クロックを選択する場合は、自動時刻同期を行いますので、コマンドを用いて手動で設定する必要はありません。NTP の設定については、セクション 2 システム管理 “NTP”を参照してください。

NTP 時刻同期が使用できない状況では、コマンドを用いて手動でシステムクロックを設定する必要があります。（ローカルシステムクロック）

6.1 システムクロックの設定

システムクロックソースがローカルなシステム時間である場合、システム時間は UTC (Universal Time Coordinated) 時間、タイムゾーン、およびサマータイムによって決定されます。

ローカルシステムクロックを設定するには、User view で以下のコマンドを実行します。

表6-1 システムクロックの設定

操作	コマンド
システムクロックを設定する。	**clock datetime** *HH:MM:SS YYYY/MM/DD*

メモ：

本スイッチは、時刻情報を装置内にバックアップすることができませんので、電源をオフした場合には時刻情報は初期値の 2021/1/1　00:00:00 (UTC 時間) に戻ります。スイッチをリブートした場合には、時刻情報は保持されます。

6.2 タイムゾーンの設定

ローカルタイムゾーン名、ローカルタイムと UTC 時間との時間差を設定するには、System view で以下のコマンドを実行します。

表6-2 タイムゾーンの設定

操作		コマンド
1	System viewに移行する。	**system-view**
2	ローカルタイムゾーンを設定する。	**clock timezone** *zone_name HH MM num*
	UTCタイムゾーン（デフォルト）に戻す。	**undo clock timezone**

デフォルト：UTC タイムゾーンを適用

メモ：

日本の標準時（JST）は「UTC」よりも 9 時間進んでいるため「UTC+09:00」と表現されます。ローカルタイムゾーンに日本の標準時(JST)タイムゾーンを適用する場合は、clock timezone JST 9 と設定します。

6.3 システムクロックの表示

システムクロック(システムの現在時刻、日付)、タイムゾーン、サマータイムを確認するために、すべての view で display clock コマンドを使うことができます。

表6-3 システムクロックの表示

操作	コマンド
システムクロック(システムの現在時刻、日付)、タイムゾーン、サマータイムを表示する。	**display clock**

目次

このセクションのページは **2-x-x** です。

7 章 システム情報 7-1

7.1 システム情報の表示 7-1

7章 システム情報

7.1 システム情報の表示

装置の動作状態が良好でない場合は、スイッチについてのあらゆる情報を収集して、障害の原因を特定します。ただし、各モジュールが、それぞれの表示コマンドを有している場合は、必要な情報をすべて収集することは困難です。このような場合は、**display diagnostic-information** コマンドを使用します。

コマンド実行後、表示内容がフラッシュ内に diagnostic-information.txt として保存されます。

以下の操作は、どの view からでも実行できます。

表7-1 システム情報の表示

操作	コマンド
システム情報を表示する	**display diagnostic-information**

目次

このセクションのページは **2-x-x** です。

8 章 ログ情報 8-1

8.1 SYSLOG 8-1

8.2 SYSLOG の設定 8-1

8.3 SYSLOG の表示 8-1

8.4 SYSLOG の設定例 8-1

8章 ログ情報

8.1 SYSLOG

SYSLOG は、スイッチに不可欠な要素であり、このロギングシステムで、ほとんどの情報出力を処理するほか、細かな分類を行って、情報を効率的にフィルタリングします。

SYSLOG は、デバッグプログラムと組み合わせて使用します。ネットワーク管理者や開発担当者がネットワークの動作状態を監視したり、ネットワーク障害を診断する際に役立ちます。

端末やログバッファに出力されるログ情報には以下の項目が含まれます。

%タイムスタンプ システム名 モジュール モジュール名/ダイジェスト: 内容

例:

```
%2014-02-08T02:12:36+09:00 QX-S716GT-4X-PW [Notice] LINK-UPDOWN:
 Interface GigabitEthernet 1/1, changed state to down.
```

8.2 SYSLOGの設定

SYSLOG の有効/無効の設定と、ログの送信先を設定します。

ログの送信先は最大 4 つまで設定できます。

system view から以下の設定を行います。

表8-1 SYSLOG の設定

操作	コマンド
SYSLOGを有効にする。	**info-center on**
SYSLOGを無効にする。	**undo info-center on**
SYSLOGの検出レベルを設定する。	**info-center level {** error **|** informational **|** notice **|** warning **}**
SYSLOGの検出レベルをデフォルトに戻す。	**undo info-center level**
ログの送信先の設定	**info-center host** *ip_addr*
ログの送信先の削除	**undo info-center host** *ip_addr*

8.3 SYSLOGの表示

display コマンドで、ログバッファ情報の表示をします。

reset コマンドでログバッファ情報をクリアーにします。

表8-2 SYSLOG の表示

操作	コマンド
SYSLOGの情報の表示	**display info-center**
ログバッファに記録された情報の表示	**display logbuffer [** *id* **| informational | notice | warning | error]**
フラッシュ情報の表示	**display logbuffer flash-info**
ログバッファ内の情報のリセット	**reset logbuffer**

8.4 SYSLOGの設定例

I. ネットワーク要件

ネットワーク要件は、次のとおりです。

- スイッチのログ情報を loghost に送信する
- loghost の IP アドレスは、10.10.10.1

II. ネットワークダイアグラム

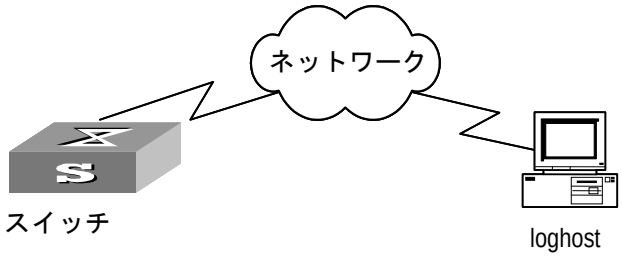


図8-1 ネットワークダイアグラム

III. 設定手順

#info-center を有効にする

```
[switch]info-center on
 Information center is enable
[switch]
```

#ログ送信先を設定する。

```
[switch]info-center host 10.10.10.1
[switch]
```

目次

このセクションのページは **2-x-x** です。

9 章 ユーザ 9-1

9.1 ユーザの概要 9-1

9.2 ユーザの設定 9-1

9.2.1 ローカルユーザの作成・削除 9-1

9.3 ユーザの表示 9-2

9.4 ユーザの設定例 9-2

9章 ユーザ

9.1 ユーザの概要

ユーザに関する以下の設定ができます。

- ローカルユーザの作成・削除

9.2 ユーザの設定

9.2.1 ローカルユーザの作成・削除

ローカルユーザを作成するには、system view から以下のコマンドを実行します。

表9-1 ローカルユーザの作成・削除

操作	コマンド
ローカルユーザを追加する。	**local-user** *user-name* **password** { { **simple** | **hash** *password* } | **none** }
ローカルユーザを削除する。	**undo local-user** *user-name*

user-name はローカルユーザ名（32 文字以内）で指定できます。使用可能な文字は、“0-9”、“a-z”、“A-Z”、“_”で、大文字と小文字が区別されます。

ローカルユーザの設定最大数は、20 となります。

デフォルト:設定なし

⚠ **注意：**

ご使用のパスワードは定期的に変更してください。またパスワードは推測されにくくするため、アルファベット、記号、数字の混在など、安全なパスワードにしてください。

9.3 ユーザの表示

ローカルユーザの情報を表示するには、以下のコマンドを実行します。

表9-2 ローカルユーザの情報を表示

操作	コマンド
ローカルユーザの情報を表示します。	**display local-user**

9.4 ユーザの設定例

#ユーザ名「user1」パスワード「abcd」を作成します。

```
[switch]local-user user1 password simple abcd
```

目次

このセクションのページは **2-x-x** です。

10 章 装置の再起動 10-1

10.1 装置の再起動 10-1

10章 装置の再起動

10.1 装置の再起動

ソフトウェアのアップグレードや、コンフィグレーションファイルの指定を行った場合など、装置の再起動を行う場合、User view から以下のコマンドを実行します。

reboot コマンド実行時、設定情報の保存を行う可否の質問があります。

表10-1 装置の再起動

操作	コマンド
装置を再起動します。	**reboot**

目次

このセクションのページは **2-x-x** です。

11 章 温度センサ 11-1

11.1 温度センサの設定..... 11-1

11章 温度センサ

11.1 温度センサの設定

装置内部の温度が設定された温度範囲を超えた場合、スイッチは温度異常を示す SYSLOG メッセージを表示します。温度範囲（下限値と上限値）を設定するには、System view で、以下のコマンドを実行します。

表11-1 温度センサの設定

操作	コマンド
装置内温度の制限値を設定する。	**temperature-limit slot** *slot-number* **hotspot** *sensor-number lowlimit warninglimit [alarmlimit]*
上記設定をデフォルトに戻す。	**undo temperature-limit slot** *slot-number* **hotspot** *sensor-number*
装置内温度および温度条件設定値を表示する。	**display environment**

目次

このセクションのページは **2-x-x** です。

12 章 ファイルシステム 12-1

12.1 ファイルシステムの概要 12-1

12.2 ファイルシステムの操作 12-1

12章 ファイルシステム

12.1 ファイルシステムの概要

装置では、ユーザがフラッシュメモリなどの記憶デバイスを使って効果的に管理できるようなファイルシステムモジュールを提供しています。本ファイルシステムでは、ファイル一覧の表示、削除、コピーが可能です。

⚠ **注意:**

ソフトウェアファイルのダウンロード中や、フラッシュメモリへのアクセスが行われている期間は、電源を落とさないように注意してください。
ソフトウェアの再ダウンロードやコンフィグの再作成が必要となる可能性があります。

12.2 ファイルシステムの操作

ファイルシステムの操作を実行するには、User view で以下のコマンドを実行します。

表12-1 ファイルシステムの操作

操作	コマンド
フラッシュ内のディレクトリ内容を表示する	**dir**
ファイルを削除する	**delete** *file-name*
ファイルをコピーする	**copy** *source-file-name destination-file-name*

目次

このセクションのページは **2-x-x** です。

13 章 NTP 13-1

13.1 NTP の概要 13-1

13.1.1 NTP の機能 13-1

13.1.2 NTP アーキテクチャ 13-1

13.1.3 NTP の同期モード 13-2

13.1.4 NTP セキュリティ 13-3

13.2 NTP の設定 13-3

13.2.1 NTP サーバの設定 13-3

13.2.2 NTP の表示 13-4

13.3 NTP の設定例 13-4

13章 NTP

13.1 NTPの概要

13.1.1 NTPの機能

NTP（Network Time Protocol）は、ネットワークを介して機器が持つシステムクロック（時計）を正しい時刻へ同期するためのプロトコルです。NTP により時刻同期を行うことで指定時間に正しくサービスを動作させたり、出力ログを正しく管理できたり、証明書を利用した認証なども正しく行うことができます。

NTP クライアントが NTP サーバにアクセスする際、宛先ポート番号として UDP ポート番号 123 を使用します。また、NTP クライアントが NTP サーバにアクセスする際の送信元ポート番号も、ポート番号 123 を使用します。

13.1.2 NTPアーキテクチャ

NTP は stratum（層）と呼ばれる「図 13-1　NTP 階層構造」に示すような階層構造を持っており、最上位の NTP サーバが原子時計や GPS の正確な時刻源から正しい時刻情報を得て、下位の NTP サーバはそれを参照して時刻同期を行っていきます。

stratum の値が小さいほど高い精度を持ちます。最上位の NTP サーバは「stratum 1」であり、階層を降りるごとに stratum の値が増えていきます。最大で stratum 15 まで NTP サーバを構築できます。stratum のレベル 16 のクロックは同期されていないことを示します。

一般的に stratum レベル 1 の NTP サーバは、原子時計のような基準となるソースから時間を取得し、NTP サーバとして他の装置に時間を提供します。各サーバの精度は、最上位レベル(プライマリサーバ)に割り当てられた stratum のレベルは 1 で、階層化された下のレベル(セカンダリサーバ)に割り当てられた stratum のレベルは 2、そして下の階層に下がるにつれて stratum のレベルの値が大きくなります。

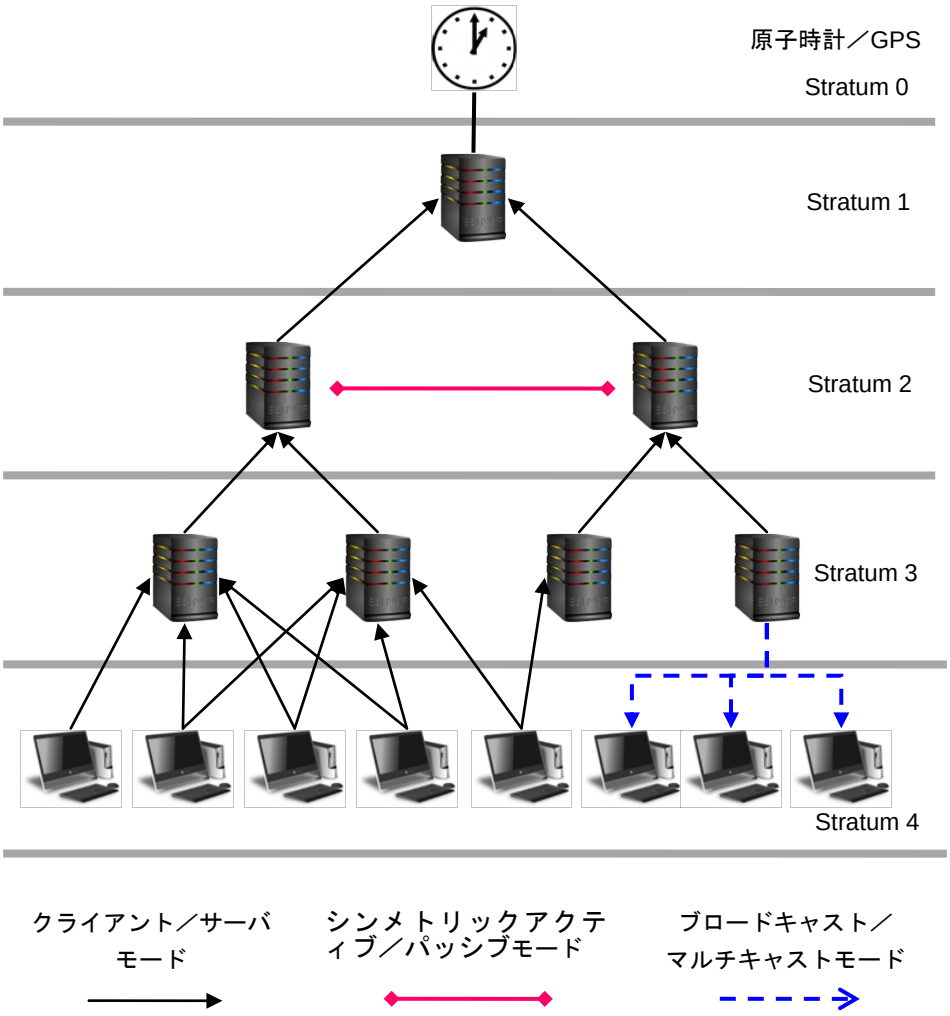


図 13-1　NTP 階層構造

13.1.3 NTPの同期モード

本装置では、以下の NTP 同期モードのうちクライアント／サーバモードのみをサポートし、クライアントとしてのみ動作します。

- クライアント／サーバモード
- シンメトリックアクティブ／パッシブモード
- ブロードキャストモード
- マルチキャストモード

クライアント／サーバモードでは、以下のように動作します。

① クライアントは NTP サーバの IP アドレスを指定して、クロック同期メッセージを NTP サーバに送信します。

② メッセージを受信したサーバは自動的にサーバのモードで動作し、応答を返します。

③ クライアントは複数のサーバに同期した場合、サーバからの応答を受信した後に最適なクロックを選択して、ローカルクロックを最適な参照ソースと同期させます。

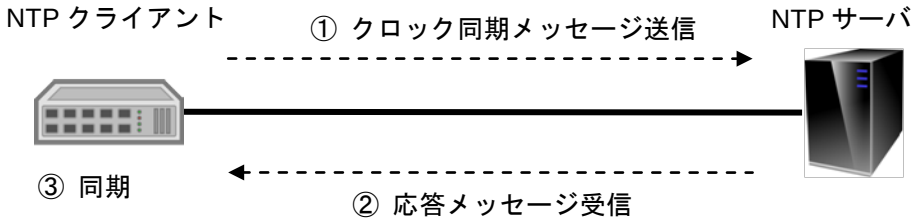


図 16-2　クライアント／サーバモード

13.1.4 NTPセキュリティ

本装置では、NTP サービスアクセス制御権と NTP 認証機能はサポートされません。

13.2 NTPの設定

13.2.1 NTPサーバの設定

ローカル装置は、クライアントモードで動作します。このモードでは、ローカルデバイスは、リモートサーバに同期することはができますが、リモートサーバを同期させることはできません。

表13-1 NTP サーバの設定

操作	コマンド
system viewに移行する	**system-view**
NTP機能を有効にする	**ntp-service**
装置のNTPサーバを指定する	**ntp-service unicast-serve** *index_number* **{** *server_name* **|** *ip_addr* **}**

server_name または ip-addr パラメータのリモートサーバをタイムサーバとして設定します。

13.2.2 NTPの表示

上記の設定終了後、display コマンドを実行して、NTP の実行状態と設定を確認します。

表13-2 NTP の表示

操作	コマンド
NTPサービスによるセッションの状態を表示する	**display ntp-service sessions**

13.3 NTPの設定例

本装置は、NTP クライアントとしてのみ動作するため、NTP サーバの設定を行う必要があります。

- サーバは他の装置によって同期させる必要があります。あるいは NTP クライアントを同期する前に参照ソースとしてローカルクロックを使用する必要があります。そうでなければクライアントは NTP サーバに同期することができません。
- サーバの stratum レベルがクライアントと等しいあるいは高いレベルである場合クライアントはサーバに同期しません。
- ntp-service unicast-serve コマンドを繰り返して設定することで複数のサーバを設定することができます。

I. ネットワーク要件

NTP サーバ(A), NTP サーバ(B)をタイムサーバとして設定します。

II. ネットワークダイアグラム

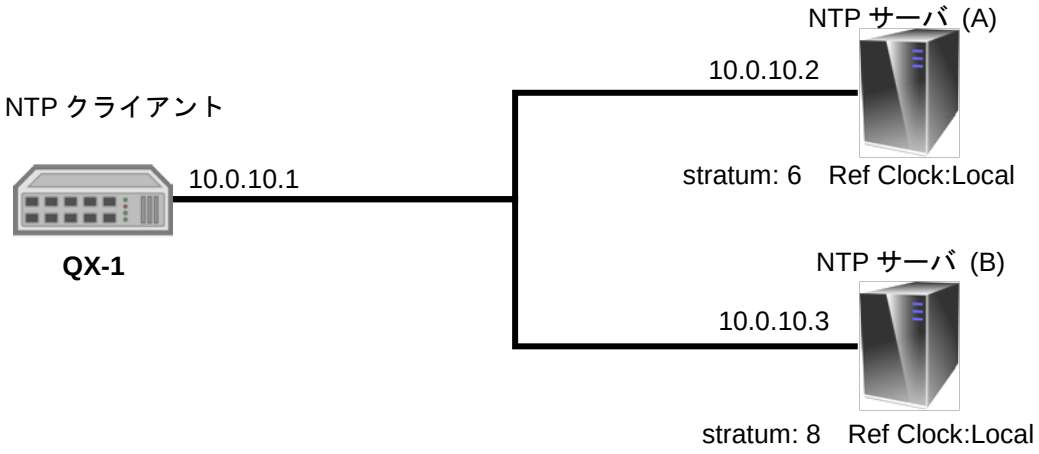


図 16-3 ネットワーク構成

III. 設定手順

#スイッチの IP アドレスを設定する。

```
<Switch>system-view
[Switch]interface vlan 1
[Switch-Vlan-interface1]ip address 10.0.10.1 255.0.0.0
[Switch-Vlan-interface1]quit
[Switch]
```

NTP 機能を有効に設定する

```
[Switch] ntp-service
```

#NTP サーバ(A)をタイムサーバ(Index Number:1)として設定する。

```
[Switch] ntp-service unicast-serve 1 10.0.10.2
```

#NTP サーバ(B)をタイムサーバ(Index Number:2)として設定する。

```
[Switch] ntp-service unicast-serve 2 10.0.10.3
```

目次

このセクションのページは **2-x-x** です。

14 章 SNMP 14-1
14.1 SNMP の概要 14-1
14.2 SNMP の設定 14-1
14.2.1 SNMP エージェントの有効/無効の設定 14-1
14.2.2 ユーザアクセス方法の登録 14-1
14.2.3 コミュニティ名の設定 14-2
14.2.4 管理者の識別と連絡のための手段の設定 14-2
14.2.5 ローカルまたはリモートデバイスのエンジン ID の設定 14-3
14.2.6 sysLocation の設定 14-3
14.2.7 View 情報の作成/更新または View の削除 14-3
14.2.8 SNMP グループの設定/削除 14-4
14.2.9 トラップ送信のための SNMP エージェントの有効/無効の設定 14-4
14.2.10 SNMP ユーザの作成 14-5
14.3 SNMP 設定の表示 14-5
14.4 SNMP 通知の設定例 14-6
14.5 SNMP の設定例 14-6

14章 SNMP

14.1 SNMPの概要

SNMP（Simple Network Management Protocol）はネットワークで装置にアクセスし、操作させるための管理システムとして、ベンダ、物理的な特徴、相互接続技術に関係なく、広く使われているインターネット標準プロトコルです。

14.2 SNMPの設定

14.2.1 SNMPエージェントの有効/無効の設定

SNMP エージェントを有効にするには、System view で、以下のコマンドを実行します。

表14-1 SNMP エージェントの有効/無効の設定

操作	コマンド	補足
SNMPエージェントを有効にする。	snmp-agent	デフォルト：無効
SNMPエージェントを無効にする。	undo snmp-agent	―

14.2.2 ユーザアクセス方法の登録

ユーザのアクセス方法を登録するには、System-view で以下のコマンドを登録します。

表14-2 コミュニティ名の設定

操作	コマンド	補足
ユーザのアクセス方法を登録する。	snmp-agent access *accessname* model { any | v1 | v2c | v3 } level { auth | noauth | priv] [read *readuser* | write *writeuser*]	デフォルト：無効
SNMPエージェントを無効にする。	undo snmp-agent access *accessname* model { any | v1 | v2c | v3 } level { auth | noauth | priv]	―

14.2.3 コミュニティ名の設定

SNMP V1 および SNMPV2C では、コミュニティ名認証スキーマが使用されます。受け入れられるコミュニティ名に適合しない SNMP メッセージは廃棄されます。SNMP コミュニティには文字列で名称が付けられますが、この文字列をコミュニティ名と呼びます。コミュニティごとに、読み出し専用モードに設定したり、読み出し書き込みモードに設定できます。読み出し専用権限のあるコミュニティでは、デバイス情報の問い合わせしかできませんが、読み出し書き込み権限のあるコミュニティでは、デバイスの設定もできます。

コミュニティ名を設定するには、System view で、以下のコマンドを実行します。

表14-3 コミュニティ名の設定

操作	コマンド	補足
コミュニティ名およびアクセス権限を設定する	snmp-agent community { read | write } *community-name*	デフォルト：なし
コミュニティ名およびアクセス権限を削除する	undo snmp-agent community *community-name*	―

14.2.4 管理者の識別と連絡のための手段の設定

sysContact は、MIB II のシステムグループの管理変数で、管理対象デバイスの担当者を識別し、連絡を取るための手段を示します。

管理者を識別し、連絡を取るための手段を設定するには、System view で以下のコマンドを実行します。

表14-4 管理者の識別と連絡のための手段の設定

操作	コマンド	補足
管理者を識別し､連絡を取るための手段を設定する	snmp-agent contact *contact*	デフォルト：なし
管理者を識別し､連絡を取るための手段をデフォルトに戻す	undo snmp-agent contact	―

14.2.5 ローカルまたはリモートデバイスのエンジンIDの設定

ローカルデバイスまたはリモートデバイスのエンジン ID を設定するには、System view で以下のコマンドを実行します。

表14-5 ローカルまたはリモートデバイスのエンジン ID の設定

操作	コマンド	補足
デバイスのエンジンIDを設定する	snmp-agent engine-id local *engine_id*	デフォルト：なし
デバイスのエンジンIDをデフォルトに戻す	undo snmp-agent engine-id local	―

デフォルト：エンジン ID は、企業番号+デバイス情報で表される。デバイス情報は、IP アドレス、MAC アドレス、ユーザ定義のテキストのいずれか

14.2.6 sysLocationの設定

sysLocation は、MIB システムグループの管理変数で、管理対象デバイスの場所を指定する場合に使用します。

sysLocation を設定するには、System view で、以下のコマンドを実行します。

表14-6 sysLocation の設定

操作	コマンド	補足
sysLocationを設定する	snmp-agent location *location*	デフォルト：なし
装置の場所をデフォルトに戻す	undo snmp-agent location	―

14.2.7 View情報の作成/更新またはViewの削除

View 情報の作成/更新または View の削除をするには、System view で以下のコマンドを実行します。

表14-7 View 情報の作成/更新または View の削除

操作	コマンド	補足
View情報を作成/更新する	snmp-agent mib-view { exclude | include } *view OID*	デフォルト：なし
View情報を削除する	undo snmp-agent mib-view *view OID*	―

14.2.8 SNMPグループの設定/削除

SNMP グループを設定または削除するには、System view で以下のコマンドを実行します。

表14-8 SNMP グループの設定/削除

操作	コマンド	補足
SNMPグループを設定する	snmp-agent security-to-group model v3 name *username* group *groupname*	デフォルト：なし
SNMPグループを削除する	undo snmp-agent security-to-group model v3 name *username*	―

14.2.9 トラップ送信のためのSNMPエージェントの有効/無効の設定

重要かつ緊急のイベント(再起動など)をレポートするために、管理対象デバイスから NMS に送信要求がなくてもトラップが送信されます。

管理対象デバイスからのトラップメッセージ送信を有効あるいは無効にするには、以下の手順でコマンドを実行します。

表14-9 トラップ送信のため SNMP エージェントの有効/無効の設定

操作 view	操作内容	コマンド
System-view	トラップの送信先、ポート番号、トラップバージョンを設定する	snmp-agent target-host trap address udp-domain *host-addr* udp-port *port* params [v1 | v2c]

System View	**トラップメッセージの種類を設定し、有効にする**	snmp-agent trap enable [standard [authenticationFailure | coldStart | warmStart | fanStatus |linkDown | linkUp]]

coldstart トラップは電源 OFF/ON による装置再開時に送出されます。warmstart トラップは reboot コマンドまたはシステム障害による装置再開時に送出されます。

無効の方法は以下になります。

操作 view	操作内容	コマンド
System-view	**トラップ設定を削除する**	undo snmp-agent target-host *host-addr*
System View	**トラップメッセージを無効にする**	undo snmp-agent trap enable [standard [authenticationFailure | coldStart | warmStart | fanStatus |linkDown | linkUp]]

14.2.10 SNMPユーザの作成

SNMP ユーザを作成するには、System view で下記のコマンドを実行します。

表14-10 SNMP ユーザの作成

操作	コマンド	補足
SNMPユーザを作成する	snmp-agent user *username* engine-id *engine_id* [{ md5 | sha } { encrypted *encrypted_password* | *password* } [priv { aes | des } { encrypted *encrypted_password* | *password* }]]	デフォルト：なし
トラップの宛先アドレスを削除する	undo snmp-agent user *username* engine-id *engine_id*	ー

14.3 SNMP設定の表示

上記設定終了後、SNMP 設定を確認します。

表14-11 SNMP 設定の表示

操作	コマンド	補足
SNMP設定を表示する	display snmp-agent	—
現在のコミュニティ名を表示する	display snmp-agent community	
グループ情報を表示する	display snmp-agent group	
MIB-View情報を表示する	display snmp-agent mib-view	
security-to-group情報を表示する	display snmp-agent security-to-group	
target-host情報を表示する	display snmp-agent target-host	
トラップ情報を表示する	display snmp-agent trap-list	
ユーザ情報を表示する	display snmp-agent user	

14.4 SNMP通知の設定例

I. ネットワーク要件

Switch から同一ネットワーク上の server 10.1.1.1 へ SNMP 通知を送信します。

Switch の IP アドレスは 10.1.1.2 とします。

II. 設定手順

以下は Switch の設定です。

```
<Switch>system-view
[Switch] interface vlan 1
[Switch-Vlan-interface1] ip address 10.1.1.2 255.255.255.0
[Switch-Vlan-interface1] quit
[Switch] snmp-agent
[Switch] snmp-agent trap enable standard coldStart
[Switch] snmp-agent target-host trap address udp-domain 10.1.1.1 udp-port 162 params v1
```

14.5 SNMPの設定例

I. ネットワーキング要件

ネットワーク管理システム(NMS: Network Management System)と装置は、Ethernet で接続されています。NMS の IP アドレスは 129.102.149.23、スイッチの VLAN インタフェースの IP アドレスは 129.102.0.1 です。ここでは、スイッチ上で、コミュニテ

ィ名、アクセス権限、管理者 ID、連絡先、およびスイッチの場所を設定し、スイッチからのトラップパケット送信を有効にします。

II. ネットワークダイアグラム

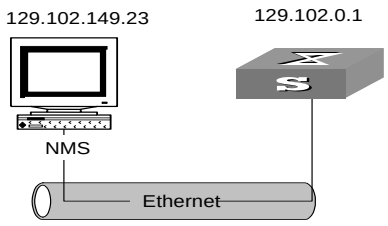


図14-1 SNMP の設定例

III. 設定手順

System view に移行する

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

SNMP エージェントを有効にする

```
[Switch] snmp-agent
```

コミュニティ名とパスワードを設定する

```
[Switch] snmp-agent community read public
```

管理者 ID、連絡先、装置の物理的な場所を設定する

```
[Switch] snmp-agent contact Administrator1-Tel:03-3456-7890
[Switch] snmp-agent location telephone-closet,3rd-floor
```

trap の種類を設定する

```
[Switch] snmp-agent trap enable standard coldStart
```

trap 送信先、ポート番号、trap バージョンを設定する

```
[Switch] snmp-agent target-host trap address udp-domain 129.102.149.23 udp-port 162 params v2c
```

目次

このセクションのページは **2-x-x** です。

15 章 ネットワーク管理 15-1

15.1 ARP について 15-1

15.2 ARP 設定の表示 15-2

15章 ネットワーク管理

15.1 ARPについて

I. ARP の必要性

ARP（Address Resolution Protocol）はネットワークレイヤアドレス（IP アドレス）と物理アドレス（MAC アドレス）のマッピング解決に使用されます。

LAN 上で、ネットワーク装置が別の装置へデータを送信する時、送信元の装置は宛先装置のネットワークレイヤアドレスだけでなく、物理アドレスも知っている必要があります。ARP はネットワークレイヤアドレスと物理アドレスのマッピングを解決するプロトコルです。

II. ARP の実行手順

Ethernet 上の 2 つのホストが通信する場合、お互いの MAC アドレスが必要になります。どのホストも、ARP マッピングテーブルという、IP アドレスと MAC アドレス間の変換テーブルを持ちます。ARP マッピングテーブルには、ローカルホストとの通信に最近使用された、他のホストの IP アドレスと MAC アドレスのマッピングが保存されています。一定時間使用されない ARP マッピングエントリは、メモリ空間を節約するため、およびスイッチが ARP マッピングテーブルを検索する間隔を短縮するために、ARP マッピングテーブルから削除されます。

Ethernet 上に、ホスト A とホスト B の 2 つのホストがあるとします。ホスト A の IP アドレスは IP_A で、ホスト B の IP アドレスは IP_B です。ホスト A はホスト B にメッセージを送信します。ホスト A はまず自分の ARP マッピングテーブルで、IP_B に対応する ARP エントリがテーブル内にあるかどうかを確認します。対応する MAC アドレスを検出すると、ホスト A は ARP マッピングテーブル内のその MAC アドレスを使用して IP パケットをフレームにカプセル化し、ホスト B に送信します。関連する MAC アドレスが検出されない場合、ホスト A は送信待ちのキューに IP パケットを保存し、Ethernet を通してそれをブロードキャストします。この ARP 要求パケットにはホスト B の IP アドレスとホスト A の MAC アドレスが入っています。ARP 要求パケットはブロードキャストされるため、Ethernet 上のすべてのホストがこの要求を受信できます。ただし、要求を処理しなければならないのは要求されたホスト(ホスト B)だけです。ホスト B はまず、ARP 要求パケット内にある要求の送信者(ホスト A)の IP アドレスと MAC アドレスを自分の ARP マッピングテーブルに保存します。次に、ホスト B は、ホスト B の MAC アドレスを追加した ARP 応答パケットを生成し、それをホスト A に送信します。応答パケットは、ブロードキャストされるのではなく、

ホスト A に直接送信されます。応答パケットを受信すると、ホスト A はホスト B の IP アドレスとそれに対応する MAC アドレスを抽出し、自分の ARP マッピングテーブルに追加します。そうしてから、ホスト A はキュー待ちのすべてのパケットをホスト B に送信します。

通常、IP アドレスから Ethernet MAC アドレスへの変換は、管理者を通さずにダイナミック ARP によって実行され、自動的に検索されます。

15.2 ARP設定の表示

上記の設定終了後、**display** コマンドを実行すると、現行の ARP の情報を確認することができます。ARP エントリを初期化するには、user view で **reset** コマンドを実行します。

表15-1 ARP の表示

操作	コマンド
ARP情報を表示する	display arp
ARPエントリを初期化する	reset arp

目次

このセクションのページは **2-x-x** です。

16 章 SSH 16-1

16.1 SSH の概要 16-1

16.2 SSH の操作 16-3

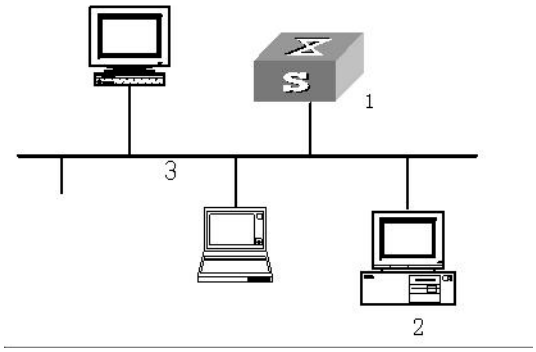
16.3 SSH の状態表示 16-3

16章 SSH

16.1 SSHの概要

SSH（Secure Shell）は、強力な暗号化と認証によって、安全性が確保されていない経路上でも、ユーザがリモートからスイッチにアクセスする際、IP スプーフィング（偽造）や平文パスワードの傍受を防止します。スイッチには複数の SSH クライアントを接続できます。SSH クライアントは、SSH サーバをサポートする GigabitEthernet スイッチや UNIX ホストとユーザ間の SSH 接続を可能にします。SSH チャネルはローカル接続ごとに設定できます。LAN 上で SSH チャネルを設定した例を図 16-1 に示します。

SSH V1, 2 両方に対応しています。また、最大 5 クライアントまで接続可能です。



1: SSH サーバを実行するスイッチ　2: SSH クライアントを実行する PC　3: Ethernet LAN

図 16-1 LAN 上の SSH チャネル構成

メモ

この例では、GigabitEthernet ポートの VLAN を VLAN インタフェースと IP アドレスで設定する必要があります。

サーバとクライアントの通信プロセスは、バージョンネゴシエーションステージ、鍵ネゴシエーションステージ、認証ステージ、セッション要求ステージ、対話型セッションステージの 5 段階で実行されます。

- **バージョンネゴシエーションステージ:** クライアントは TCP 接続要求をサーバに送信します。TCP 接続が確立すると、サーバとクライアントは、SSH のバージョンのネゴシエーションを行います。両方のバージョンが一致すると、鍵ア

ルゴリズムのネゴシエーションに移行します。バージョンが一致しない場合、サーバは TCP 接続を切断します。

- **鍵ネゴシエーションステージ:** サーバとクライアントは、鍵アルゴリズムのネゴシエーションを行い、共通鍵を計算します。サーバは RSA 鍵をランダムに生成し、公開鍵をクライアントに送ります。クライアントは、サーバから受け取った公開鍵と自身が生成した乱数を使用して共通鍵を計算します。クライアントは、サーバから受け取った公開鍵で乱数を暗号化し、その結果をサーバに送り返します。サーバは受け取ったデータを自身の秘密鍵で複合化し、クライアントの乱数を取得します。次に、サーバは、同じアルゴリズムを使い、自身の公開鍵と受信した乱数を使用して共通鍵を計算します。こうしてサーバとクライアントは、ネットワーク上でデータを転送せずに、同じ鍵を取得します。サーバとクライアントは、この鍵を暗号化と複合化に使用します。
- **認証ステージ:** サーバは、共通鍵を取得した後、クライアント側のユーザを認証します。クライアントはユーザ名をサーバに送信します。すでに作成されたユーザ名に「認証なし」が設定されている場合、このユーザの認証ステージはスキップされます。それ以外の場合は、認証プロセスが続行されます。SSH は認証方式としてパスワード認証と RSA 認証をサポートしています。パスワード認証の場合、サーバは、クライアントから受け取ったユーザ名とパスワードをローカルで設定されたユーザ名とパスワードと比較します。ユーザ名とパスワードが正確に一致すると、ユーザはスイッチへのログオンを許可されます。RSA 認証は、次のように行われます。クライアントユーザの RSA 公開鍵をローカルサーバ側で設定します。クライアントは最初に RSA 公開鍵のメンバモジュールをサーバに送信します。サーバはその妥当性を確認します。メンバモジュールが有効であれば、サーバは乱数を生成し、RSA 公開鍵で暗号化した後、クライアントに送信します。サーバとクライアントは、乱数とセッション ID を使用して認証データを計算します。クライアントは、計算した認証データをサーバに送り返します。サーバは受け取ったデータとローカルで取得したアテンションデータを比較します。両者が正確に一致すると、ユーザはスイッチへのアクセスを許可されます。両者が一致しない場合、認証プロセスは失敗します。
- **セッション要求ステージ:** クライアントはセッション要求メッセージをサーバに送信します。サーバは受信した要求を処理します。
- **対話型セッションステージ:** サーバとクライアントは、セッションが終了するまでデータを交換します。

セッションパケットは送信時に暗号化され、共通鍵がランダムに生成されます。共通鍵は暗号化して交換されます。RSA 認証では、このように、ネットワーク上で鍵を交換することなく、必要な鍵を取得できます。SSH はサーバとクライアントが交換

するデータを最大限に確保します。ユーザ名がサーバ側で設定されていなくても、認証プロセスは開始されるため、不法な侵入者は、自分が入力したユーザ名が存在するかどうか判断できません。その結果、ユーザ名も保護されます。

16.2 SSHの操作

SSH の有効/無効を設定するには、System view で以下のコマンドを実行します。

表16-1 SSH の有効/無効の設定

操作	コマンド
SSHを有効にする	**ssh server enable**
SSHを無効にする	**undo ssh server enable**

デフォルト：無効

16.3 SSHの状態表示

display コマンドを使用して、SSH の状態を表示します。

表16-2 SSH の状態表示

操作	コマンド
SSHの状態を表示する	**display ssh server**

目次

このセクションのページは **2-x-x** です。

17 章 Telnet サーバ 17-1

17.1 Telnet サーバの概要 17-1

17.2 Telnet サーバの設定 17-1

17.2.1 ユーザラインの設定 17-1

17.2.2 ユーザの作成 17-1

17.2.3 Telnet サーバの有効/無効 17-2

17.3 Telnet サーバの表示 17-2

17.4 Telnet サーバの設定例 17-2

17章 Telnet サーバ

17.1 Telnetサーバの概要

装置のリモート管理を行うため、Telnet サーバを使用することができます。Telnet を利用するには以下の設定を行います。

- ユーザラインの設定
- ユーザの作成
- Telnet サーバの有効/無効

17.2 Telnetサーバの設定

17.2.1 ユーザラインの設定

ユーザラインの設定を行います。Telnet では VTY を使用します。詳細はセクション 1 はじめに “Telnet を介した設定環境のセットアップ”を参照ください。

表17-1 ユーザラインの設定

操作	コマンド
User Line viewに移行する。	**line vty 0**

17.2.2 ユーザの作成

ローカルユーザによる認証を行う場合、ユーザを作成します。詳細はセクション 2 システム管理 “ユーザの設定”を参照ください。

表17-2 ユーザの作成

操作	コマンド
ローカルユーザを追加する。	**local-user** *user-name* **password { { simple | hash** *password* **} | none }**
ローカルユーザを削除する。	**undo local-user** *user-name*

17.2.3 Telnetサーバの有効/無効

Telnet サーバの有効/無効の設定を行います。System view から以下の設定を行います。

表17-3 Telnet サーバの有効/無効

操作	コマンド
Telnetサーバを有効に設定する	**telnet server enable**
Telnetサーバを無効に設定する	**undo telnet server enable**

デフォルト：無効

17.3 Telnetサーバの表示

display コマンドで、Telnet サーバの情報を表示します。

表17-4 Telnet サーバの表示

操作	コマンド
Telnetサーバの情報を表示する	**display telnet server**

17.4 Telnetサーバの設定例

I.　ネットワーク要件

ネットワーク要件は、次のとおりです。

- スイッチの Telnet サーバ機能を設定する
- PC の IP アドレスは、10.10.10.1

II.　ネットワークダイアグラム

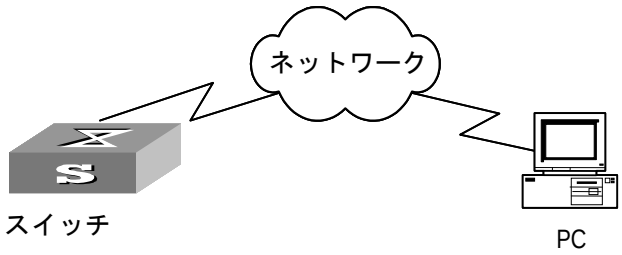


図17-1 ネットワークダイアグラム

III.　設定手順

#スイッチの IP アドレスを設定する。

```
<Switch>system-view
[Switch]interface Vlan 1
[Switch-Vlan-interface1]ip address 10.10.10.2 255.0.0.0
[Switch-Vlan-interface1]quit
[Switch]
```

#Telnet でログインするためのユーザ「user1」を作成する。パスワードは「1234」

```
[Switch] local-user user1 password simple 1234
[Switch]
```

#Telnet サーバを有効に設定する。

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

#User line view に入り、ログインユーザ用の認証方法を「scheme」に設定する。

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

目次

このセクションのページは **2-x-x** です。

18 章 TFTP 18-1

18.1 TFTP の概要 18-1

18.2 TFTP の設定 18-1

18.2.1 TFTP によるファイルのダウンロード 18-1

18.2.2 TFTP によるファイルのアップロード 18-2

18章 TFTP

18.1 TFTPの概要

簡易ファイル転送プロトコル（TFTP: Trivial File Transfer Protocol）は、ファイル転送のための簡易プロトコルです。FTP などのファイル転送プロトコルとは異なり、複雑な対話式アクセスインタフェースを持たないため、クライアントとサーバ間の複雑な要求・応答なしで使用できます。TFTP は、UDP に実装します。

TFTP 送信は、クライアント側から開始されます。ファイルをダウンロードする場合は、クライアントから TFTP サーバに要求を送信したのち、データを受信し、応答を TFTP サーバに送信します。ファイルをアップロードする場合は、クライアントから TFTP サーバに要求を送信したのち、データを送信し、応答を TFTP サーバから受信します。

TFTP の設定は、以下のとおりです。

- TFTP によるファイルのダウンロード
- TFTP によるファイルのアップロード

18.2 TFTPの設定

18.2.1 TFTPによるファイルのダウンロード

ファイルをダウンロードする場合は、クライアントから TFTP サーバに要求を送信したのち、データを受信し、ACK を TFTP サーバに送信します。

TFTP でファイルをダウンロードするには、System view で、以下のコマンドを実行します。

表18-1 TFTP によるファイルのダウンロード

操作	コマンド
TFTPでファイルをダウンロードする	**tftp** *A.A.A.A* **get** *xxx.yyy mmm.nnn*

18.2.2 TFTPによるファイルのアップロード

ファイルをアップロードする場合は、クライアントから TFTP サーバに要求を送信したのち、データを送信し、応答を TFTP サーバから受信します。

ファイルをアップロードするには、System view で以下のコマンドを実行します。

表18-2 TFTP によるファイルのアップロード

操作	コマンド
TFTPでファイルをアップロードする	**tftp** *A.A.A.A* **put** *mmm.nnn xxx.yyy*

QX-S700G シリーズ Ethernet PoE スイッチ

オペレーションマニュアル

3.ポート

本マニュアルは以下に示す章で構成されています。

01-Ethernet ポート

02-ポートミラーリング

03-PVLAN

04-ループ検出

05-リンクアグリゲーション

06-EEE

07-スパニングツリー

08-IGMP スヌーピング

目次

このセクションのページは **3-x-x** です。

1 章 Ethernet ポート 1-1

1.1 Ethernet ポートの概要 1-1

1.2 Ethernet ポートの設定 1-1

1.2.1 Ethernet port view への移行 1-1

1.2.2 Ethernet ポートの有効/無効の設定 1-2

1.2.3 Ethernet ポートの Duplex の設定 1-2

1.2.4 Ethernet ポートの速度の設定 1-4

1.2.5 Ethernet ポートのフロー制御の有効/無効の設定 1-5

1.2.6 Ethernet ポートの通信フレームの MTU の設定 1-5

1.2.7 フレーム透過の設定 1-6

1.2.8 インターフェースの説明の設定 1-6

1.2.9 frame-length-check の設定 1-6

1.3 Ethernet ポートの表示 1-7

1章 Ethernet ポート

1.1 Ethernetポートの概要

QX-S700G シリーズ Ethernet PoE スイッチには、
10BASE-T/100BASE-TX/1000BASE-T インターフェースと
1000BASE-X/10GBASE-R の SFP インターフェースがあります。

Ethernet ポートは、ケーブルタイプ MDI/MDI-X 自動検出をサポートし、半/全二重および自動ネゴシエーションモードで動作します。また、隣接機器との伝送速度を自動ネゴシエートおよび自動選択して、システム設定および管理を容易にします。

以下のセクションで説明します。

1.2 Ethernetポートの設定

Ethernet ポートの設定は、次のとおりです。

1. Ethernet port view への移行
2. Ethernet ポートの有効/無効の設定
3. Ethernet ポートの Duplex の設定
4. Ethernet ポートの速度の設定
5. Ethernet ポートのフロー制御の有効/無効の設定
6. Ethernet ポートの通信フレームの MTU の設定
7. フレーム透過の設定
8. インターフェースの説明の設定
9. frame-length-check の設定

1.2.1 Ethernet port viewへの移行

Ethernet ポートを設定する前に、Ethernet port view に入ります。

QX-S708GT-2X-PW のポート 1～8、QX-S716GT-4X-PW のポート 1～16 は

interface GigabitEthernet

QX-S708GT-2X-PW のポート 9、10、QX-S716GT-4X-PW のポート 17、18 は

interfece ten-GigabitEthernet

System view で、以下のコマンドを実行します。

表1-1 Ethernet port view への移行

操作	コマンド
Ethernet port viewへ移行する	**interface** *interface-type interface-number*

1.2.2 Ethernetポートの有効/無効の設定

以下のコマンドを使用して、ポートを有効または無効に設定します。ポートに関連するパラメータを設定した後、ポートを有効にします。ポートにデータを転送させたくない場合は、そのポートを無効にします。

Ethernet port view で、以下のコマンドを実行します。

表1-2 Ethernet ポートの有効/無効の設定

操作	コマンド
Ethernetポートを無効にする	**shutdown**
Ethernetポートを有効にする	**undo shutdown**

デフォルト：有効

1.2.3 EthernetポートのDuplexの設定

データパケットを同時に送受信するようにポートを設定するには、ポートを全二重に設定します。一度にデータパケットの送信または受信のいずれかを行うようにポートを設定するには、ポートを半二重に設定します。ポートを自動ネゴシエーションモードに設定した場合、ローカルポートと隣接ポートは Duplex モードを自動的にネゴシエートします。

Ethernet port view で、以下のコマンドを実行します。

表1-3 Ethernet ポートの Duplex の設定

操作	コマンド
Ethernetポートのduplex属性を設定する	**duplex** { **auto** | **full** | **half** }
Ethernetポートのduplex属性をデフォルトに戻す	**undo duplex**

デフォルト：auto

10BASE-T/100BASE-TX/1000BASE-T Ethernet ポートは、全二重、半二重、および自動ネゴシエーションをサポートしています。

10BASE-T/100BASE-TX/1000BASE-TEthernet ポートは、10Mbps/100Mbps 設定時は、全二重、半二重の設定をサポートしています。自動ネゴシエーション設定はサポートしていません。1000Mbps 設定時は、全二重をサポートしています。半二重や自動ネゴシエーションの設定はサポートしていません。

速度自動ネゴシエーション設定時は、全二重や半二重の設定はサポートしていません。

ten-GigabitEthernet ポートは、設定ができません。

⚠ **注意：**

・duplex auto コマンドは speed auto コマンドに対応しています。duplex auto コマンドを実行すると、自動的に speed auto が設定されます。
・duplex auto コマンドは speed 1000 コマンド、speed 100、speed 10 コマンドとの併用はできません。
・duplex full コマンドを実行すると、speed 1000 や speed 100 を設定したい場合は、duplex full コマンドを実行後、speed 1000 や speed 100 コマンドを実行してください。
・duplex full コマンドは speed 1000 コマンド、speed 100 コマンド、speed 10 と併用可能です。speed auto コマンドとの併用はできません。
・duplex half コマンドは speed 1000 コマンド、speed auto コマンドとの併用はできません。

Speed/Duplex	10	100	1000	auto
auto	×	×	×	○
full	○	○	○	×
half	○	○	×	×

○：併用可能です。　×：併用不可です。

・speed 1000 コマンドと duplex full を併用して設定した状態で、duplex half コマンドを実行した場合、エラーが表示されます。エラーの内容は以下の通りです。

エラー内容「GigabitEthernet 1/1 does only support half duplex in 10 and 100 Mbit mode, duplex changed to full duplex」

1.2.4 Ethernetポートの速度の設定

以下のコマンドを使用して、Ethernet ポートの速度を設定できます。ポート速度を自動ネゴシエーションモードに設定した場合、ローカルポートと隣接ポートはポート速度を自動的にネゴシエートします。

Ethernet port view で、以下のコマンドを実行します。

表1-4 Ethernet ポートの速度の設定

操作	コマンド
Ethernetポートの速度を設定する	**speed** { **10** | **100 | 1000** | **auto** }
Ethernetポートの速度をデフォルトに戻す	**undo speed**

デフォルト：auto

ten-GigabitEthernet ポートは、自動ネゴシエーションのみサポートしています。

⚠ **注意：**

Speed/Duplex 設定は以下の組み合わせをサポートしています。

・auto/auto
・1000/full
・100/full
・100/half
・10/full
・10/half

上記設定の組み合わせに一致しないポート速度を設定した場合、設定仕様に合うように自動的に speed と duplex の設定が変更されます。

・speed10、speed 100 コマンドは duplex full に対応しています。
・speed 10、speed 100 コマンドは duplex full コマンドと duplex half コマンドと併用可能です。duplex auto コマンドとの併用はできません。
・speed 1000 コマンドは duplex full に対応しています。Speed 1000 コマンドを実行すると、自動的に duplex full が設定されます。
・speed 1000 コマンドは duplex half コマンド、duplex auto コマンドとの併用はできません。
・speed auto コマンドは duplex auto コマンドに対応しています。speed auto コマンドを実行すると、自動的に duplex auto が設定されます。

・speed auto コマンドは duplex full コマンド、duplex half コマンドとの併用はできません。

Speed/Duplex	10	100	1000	auto
auto	×	×	×	○
full	○	○	○	×
half	○	○	×	×

○：併用可能です。　×：併用不可です。

1.2.5 Ethernetポートのフロー制御の有効/無効の設定

ローカルスイッチと隣接スイッチの両方でフロー制御を有効にした後、ローカルスイッチで輻輳が発生すると、そのスイッチは隣接スイッチにその旨通知して、パケットの送信を一時停止させます。隣接スイッチはこのメッセージを受信すると、パケットの送信を一時停止します。ローカルスイッチがこのメッセージを受信した場合も同様です。この方法により、パケット損失を効果的に減少させることができます。Ethernet ポートのフロー制御機能を有効/無効にするには、Ethernet port view で、以下のコマンドを実行します。

表1-5 Ethernet ポートのフロー制御の有効/無効の設定

操作	コマンド
Ethernetポートでフロー制御を有効にする	**flowcontrol**
Ethernetポートでフロー制御を無効にする	**undo flowcontrol**

デフォルト：無効

1.2.6 Ethernetポートの通信フレームのMTUの設定

GigabitEthernet ポートが受信できる最大フレームサイズを設定します。設定するには、Ethernet View で以下のコマンドを実行します。

表1-6 GigabitEthernet ポートの MTU の設定

操作	コマンド
通信フレームのMTUを設定する	**mtu** *size*

通信フレームのMTUをデフォルトに戻す	**undo mtu**

デフォルト：10240 バイト

1.2.7 フレーム透過の設定

特定フレーム透過の許可/拒否を設定するには、Ethernet port view で以下のコマンドを実行します。

表1-7 特定フレーム透過の許可./拒否の設定

操作	コマンド
特定フレームの透過を許可する	**forwarding { bpdu | eapol | lldpdu }**
特定フレームの透過を拒否する	**undo forwarding { bpdu | eapol | lldpdu }**

1.2.8 インターフェースの説明の設定

インターフェースの説明を設定するには、Ethernet port view で、以下のコマンドを実行します。

表1-8 インターフェースの説明の設定

操作	コマンド
インターフェースの説明を設定する	**description** *string*
インターフェースの説明をデフォルトに戻す	**undo description**

デフォルト:Interface ID

1.2.9 frame-length-checkの設定

EtherType/Length フィールドと実際のペイロードサイズが一致しない場合に、フレームをドロップする frame-length-check を設定できます。この設定をするには、Ethernet port view で以下のコマンドを実行します

表1-9 frame-length-check の設定

操作	コマンド
frame-length-checkを有効にする	**frame-length-check**
frame-length-checkを無効にする	**undo frame-length-check**

1.3 Ethernetポートの表示

上記の設定終了後、display コマンドを実行し、Ethernet ポートの実行状態を確認します。

User view で reset コマンドを実行し、ポートの統計情報をリセットします。

表1-10 Ethernet ポートの状態表示

操作	コマンド
ポートのすべての情報を表示する	**display interface** *interface-type interface-number* **port** [**access | trunk | hybrid**]
指定されたポートあるいはポートの概要情報を表示する	**display interface** *interface-type* [*interface-number* **{ capabilities | description | forwarding | statistics | status }**]
ポートの統計情報をリセットする	**reset counters** [**interface** [*interface-type interface-number*]]
SFPの情報を表示する	**display transceiver-information interface** *interface-type interface-number*

目次

このセクションのページは **3-x-x** です。

2 章 ポートミラーリング 2-1

2.1 ポートミラーリングの概要 2-1

2.2 ポートミラーリングの設定 2-1

2.2.1 ローカルミラーリンググループの作成 2-1

2.2.2 モニタポート（監視ポート）の設定 2-2

2.2.3 ミラーリングポートの設定 2-2

2.3 ポートミラーリング設定の表示 2-3

2.4 ポートミラーリングの設定例 2-3

2章 ポートミラーリング

2.1 ポートミラーリングの概要

QX-S700G シリーズ Ethernet PoE スイッチは、調査および監視のためのポートベースのミラーリング機能を有しており、複数のミラーリングポート（指定ポート）の入力パケットをモニタポート（監視ポート）でモニタすることができます。

スイッチは、1 つのポートミラーリンググループだけをサポートします。この機能は、監視ポートおよびミラーリングポートの両方の設定によって決まります。

たとえば、ミラーリングポートではインバウンドパケットだけを監視するように設定されていれば、監視ポートではミラーリングポートで受信されたパケットだけを監視します。

2.2 ポートミラーリングの設定

ポートミラーリングを設定するには、以下の作業を行います。

- ローカルミラーリンググループの作成
- モニタポート（監視ポート）の設定
- ミラーリングポートの設定

⚠ **注意：**

ミラーリング機能と PTP 機能を併用するとき、ミラーリング機能で PTP パケットはキャプチャされません。

2.2.1 ローカルミラーリンググループの作成

ポートミラーリングを行うためのグループを作成します。System view で以下のコマンドを実行します。

表2-1 ローカルミラーリンググループの作成

操作	コマンド
ローカルミラーリンググループを作成する	**mirroring-group 1 local**
ローカルミラーリンググループを削除する	**undo mirroring-group 1 local**

デフォルト：設定無し

2.2.2 モニタポート（監視ポート）の設定

モニタポート（監視ポート）を設定するには、System view で以下のコマンドを実行します。すべてのパケットを監視します。

表2-2 モニタポート（監視ポート）の設定

操作	コマンド
監視ポートを設定する	**mirroring-group 1 monitor-port** *interface-type interface-number*
監視ポートの設定を解除する	**undo mirroring-group 1 monitor-port**

⚠ **注意**：

- 監視ポート設定は Port isolate 機能、リンクアグリゲーション機能と同時に使用することができません。Port isolate 機能が有効な場合は、排他状態にある監視ポートは無効状態となるため、コンフィグに表示されません。
- 監視ポートの装置あたりサポート数は 1 つです。複数設定することはできません。複数設定操作をした場合、最後に設定したポートが監視ポートとなります。

2.2.3 ミラーリングポートの設定

ミラーリングポートを設定するには、System view で以下のコマンドを実行します。

表2-3 ミラーリングポートの設定

操作	コマンド
1つまたは複数のミラーリングポートを設定する	**mirroring-group 1 mirroring-port** *interface-type interface-number* { **both** | **inbound** | **outbound** }
1つまたは複数のミラーリングポートの設定を解除する	**undo mirroring-group 1 mirroring-port** *interface-type interface-number*

⚠ **注意：**

ミラーリング対象ポートを増やすことにより、モニタポートの回線帯域を超え、必要なパケットをモニタポートから出力できなくなる可能性があります。モニタポートの帯域や実トラフィック量を考慮してミラーリングポートを設定してください。

2.3 ポートミラーリング設定の表示

display コマンドを実行して設定状態を確認できます。

表2-4 ポートミラーリング設定の表示

操作	コマンド
ポートミラーリングのパラメータ設定を表示する	**display mirroring-group**

2.4 ポートミラーリングの設定例

I. ネットワーク要件

1 つのサーバを使用して、ポート GigabitEthernet 1/1 および GigabitEthernet 1/2 で受信されたパケットを監視します。

サーバはスイッチのポート GigabitEthernet1/8 に接続されています。

II. ネットワークダイアグラム

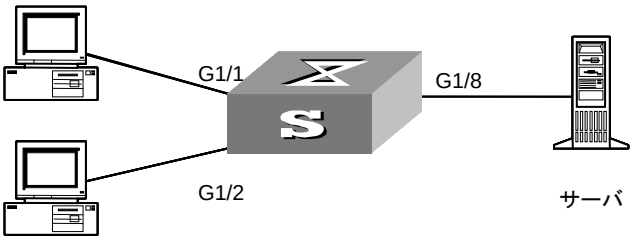


図2-1 ポートミラーリングの設定例

III. 設定手順

#ローカルミラーリンググループを作成する。

```
[switch]mirroring-group 1 local
```

#Ethernet1/8 を監視ポートに設定する。

```
[switch]mirroring-group 1 monitor-port GigabitEthernet 1/8
```

#Ethernet1/1 および Ethernet1/2 をミラーリングポートに設定する

```
[switch]mirroring-group 1 mirroring-port GigabitEthernet 1/1 GigabitEthernet 1/2
inbound
```

目次

このセクションのページは **3-x-x** です。

3 章 PVLAN 3-1

3.1 PVLAN の概要 3-1

3.2 PVLAN の設定 3-1

3.2.1 ポートへの PVLAN id の設定/削除 3-1

3.2.2 ポートの PVLAN isolate の有効/無効の設定 3-1

3.3 PVLAN 状態の表示 3-2

3章 PVLAN

3.1 PVLANの概要

pvlan isolation は、isolation 設定でポート間の通信を停止します。isolation 設定したポート同士は通信できないようにします。ポートの isolation 設定は有効か無効の一つの設定のみになります。

pvlan は、pvlan id でポート間の通信を決めています。同一 pvlan id 内のポート同士は通信できます。異なる pvlan id のポート同士は通信できません。pvlan id 設定数は装置のポート数分まで設定できます。ポートの pvlan id 設定は複数 id 設定が可能です。

3.2 PVLANの設定

3.2.1 ポートへのPVLAN idの設定/削除

ポートに PVLAN id を設定/削除するには、Ethernet port view から以下のコマンドを実行します。

表3-1 ポートに PVLAN id の設定

操作	コマンド
ポートにPVLANを設定する	**pvlan** *pvlan_id*
ポートをPVLANから外す	**undo pvlan** *pvlan_id*

デフォルト：PVLAN 1

3.2.2 ポートのPVLAN isolateの有効/無効の設定

ポートの PVLAN Isolation を有効/無効を設定するには、Ethernet port view から以下のコマンドを実行します。

表3-2 ポートの PVLAN isolate の有効/無効の設定

操作	コマンド
ポートのPVLAN isolateを有効にする	**pvlan isolation**
ポートのPVLAN isolateを無効にする	**undo pvlan isolation**

デフォルト：無効

3.3 PVLAN状態の表示

display コマンドを実行して設定状態を確認できます。

表3-3 PVLAN の状態の表示

操作	コマンド
PVLANの設定を表示する	**display pvlan [** *pvlan_id* **]**
isolation状態を表示する	**display pvlan isolation [interface** *interface-type interface-number* **]**

目次

このセクションのページは **3-x-x** です。

4 章 ループ検出 4-1

4.1 ループ検出の概要 4-1

4.2 ループ検出の設定 4-1

4.2.1 ループ検出機能の有効/無効の設定 4-1

4.2.2 ループ検出間隔の設定 4-2

4.3 ループ検出の状態の表示 4-2

4章 ループ検出

4.1 ループ検出の概要

誤ったケーブル結線をして、ネットワークループが構築されると、ブロードキャストストームを引き起こす可能性があります。ループ検出機能により、ループの検知及びポートをブロックすることで、ブロードキャストストームの回避が可能です。

Ethernet インタフェースでループ検出機能が有効になっていると、装置はポートのループを定期的にチェックします。ループを検出すると、ループを検出したポートをブロックし、通信を遮断します。

4.2 ループ検出の設定

ループ検出を設定するには、System view と Ethernet port view の両方に設定する必要があります。

4.2.1 ループ検出機能の有効/無効の設定

装置全体ループ検出機能を設定するには、System view に設定する必要があります。個別ポートのループ検出を設定するには、Ethernet port view に設定する必要があります。装置全体ループ検出機能の設定は優先されます。

表4-1 ループ検出機能の有効/無効の設定

操作	コマンド
ループ検出を有効にする	**loopback-detection enable**
ループ検出を無効にする	**undo loopback-detection enable**

デフォルト：有効

メモ：

ループバック検出の保護アクションが block である場合、ポートがループバック検出間隔の 3 倍の時間ループを検出しない時、ブロック状態を自動的に解除します。ただし、ポートのリンクダウンによってループ状態が解除された場合、そのループに関連したポートは即時解除されます。

4.2.2 ループ検出間隔の設定

ループ検出が有効であるとき、装置は、指定された間隔でループ検出フレームを送信します。

表4-2 ループ検出間隔の設定

操作	コマンド
ループ検出間隔を設定する	**loopback-detection interval-time** *interval-time*
ループ検出間隔をデフォルトに戻す	**undo loopback-detection interval-time**

検出間隔は 5～30 秒（デフォルト 5 秒）

メモ：

ループ検出間隔の設定値によって、ループ検出時間とループ解除時間が決定します。ループの解除時間はループ検出間隔の設定値の 3 倍となる。

例：ループ検出間隔が 5 秒の場合

　　ループ検知時間：5 秒

　　ループ解除時間：15 秒

4.3 ループ検出の状態の表示

display コマンドを実行してループ検出の状態を確認できます。

表4-3 ループ検出の状態の表示

操作	コマンド
ループ検出の状態表示	**display loopback-detection**

目次

このセクションのページは **3-x-x** です。

5 章 リンクアグリゲーション 5-1

5.1 リンクアグリゲーションの概要 5-1

5.2 リンクアグリゲーションの設定 5-1

5.3 リンクアグリゲーションの設定例 5-2

5.4 リンクアグリゲーションのロードバランスの設定 5-2

5.5 LACP の設定 5-3

5.5.1 LACP の有効/無効の設定 5-3

5.5.2 LACP のタイムアウトの設定 5-3

5.5.3 LACP のポートの優先度の設定 5-3

5.5.4 LACP の装置の優先度の設定 5-4

5.5.5 LACP の状態の表示 5-4

5.5.6 LACP の統計情報の削除 5-4

5章 リンクアグリゲーション

5.1 リンクアグリゲーションの概要

リンクアグリゲーションとは、複数の物理リンクを束ねて 1 つの論理リンクとして扱うことのできる機能です。リンクアグリゲーションは、通信時に複数の物理リンクを同時に使用できることから、2 つのポートを使ってリンクアグリゲーションを設定した場合、2 倍の帯域幅で通信することが可能になります。

QX-S700G シリーズでは、アグリゲーショングループは、集約された Ethernet インタフェースのグループです。

- リンクアグリゲーショングループは、単一の論理的なリンクのように見えます。
- アグリゲートインタフェースを通じてデータトラフィックが送信されるように見えます。

QX-S708GT-2W-PW：最大 5 グループ(最大 8 ポート/1 グループ)

QX-S716GT-4W-PW：最大 10 グループ(最大 8 ポート/1 グループ)

1 つのリンクアグリゲーショングループでは、メンバポートの以下の設定を同じにする必要があります。

・vlan の設定

・link-type の設定

・speed の設定

・duplex の設定

・qos の設定

・flow control の設定

・loop-detection の設定

・unicast/multicast/broadcast suppression rates の設定

5.2 リンクアグリゲーションの設定

アグリゲーショングループへのメンバポートを設定する場合は、Ethernet port view でコマンドを実行します。

表5-1 リンクアグリゲーションの設定

操作	コマンド
リンクアグリゲーショングループに追加する	**link-aggregation group** *group_num*
リンクアグリゲーショングループから削除する	**undo link-aggregation group**

注意：

- リンクアグリゲーション機能は、スタティック MAC アドレス設定、セキュリティ MAC アドレス設定、監視ポート設定、Port isolate 機能と同時に使用することができません。Port isolate 機能が有効な場合は、排他状態にあるリンクアグリゲーション機能は無効状態となるため、コンフィグに表示されません。ただしアップリンクポートは Port isolate 機能が有効な場合でもリンクアグリゲーションを有効にすることができます。

5.3 リンクアグリゲーションの設定例

設定例では Ethernet ポート 2 と 4 をリンクアグリゲーショングループ 2 に追加するとして設定手順を説明します。

```
[Switch]interface GigabitEthernet 1/2
[Switch-GigabitEthernet1/2]link-aggregation group 2
[Switch-GigabitEthernet1/2]interface GigabitEthernet 1/4
[Switch-GigabitEthernet1/4]link-aggregation group 2
[Switch-GigabitEthernet1/4]quit
[Switch]
```

5.4 リンクアグリゲーションのロードバランスの設定

ロードバランスを設定するには、System-view で以下のコマンドを実行します。

表5-2 リンクアグリゲーションのロードバランスの設定

操作	コマンド
リンクアグリゲーションのロードバランスを設定する	**link-aggregation mode { dmac | smac | ip | port }**
リンクアグリゲーションのロードバ	**undo link-aggregation mode**

ランスをデフォルトに戻す	

デフォルト：SMAC,ip,port

5.5 LACPの設定

5.5.1 LACPの有効/無効の設定

LACP を有効にするには、Ethernet port view で以下のコマンドを実行します。

表5-3 LACP の有効/無効の設定

操作	コマンド
LACPを有効にする	**lacp**
LACPを無効にする	**undo lacp**

デフォルト：無効

5.5.2 LACPのタイムアウトの設定

LACP のタイムアウトの設定をするには、Ethernet port view で以下のコマンドを実行します。

表5-4 LACP のタイムアウトの設定

操作	コマンド
LACPのタイムアウトを設定する	**lacp timeout { fast | slow }**
LACPのタイムアウトをデフォルトに戻す	**undo lacp timeout { fast | slow }**

デフォルト：fast

5.5.3 LACPのポートの優先度の設定

LACP のポートの優先度を設定するには、Ethernet port view で以下のコマンドを実行します。

表5-5 LACP のポートの優先度の設定

操作	コマンド
LACPのポートの優先度を設定する	**lacp port-priority** *priority*

LACPのポートの優先度をデフォルトに戻す	**undo lacp port-priority** *priority*

デフォルト：32768

5.5.4 LACPの装置の優先度の設定

LACP の装置の優先度を設定するには、System view から以下のコマンドを実行します。

表5-6 LACP の装置の優先度の設定

操作	コマンド
LACPの装置の優先度を設定する	**lacp system-priority** *priority*
LACPの装置の優先度をデフォルトに戻す	**undo lacp system-priority** *priority*

デフォルト：32768

5.5.5 LACPの状態の表示

display コマンドを使用して、LACP の状態を確認します。

表5-7 LACP の各状態の表示

操作	コマンド
LACPの各情報を表示する	**display lacp { internal | neighbor | statistics | system-id }**

5.5.6 LACPの統計情報の削除

LACP の統計情報を削除するには、User view から以下のコマンドを実行します。

表5-8 LACP の統計情報の削除

操作	コマンド
LACPの統計情報を削除する	**reset lacp statistics**

目次

このセクションのページは **3-x-x** です。

6 章 EEE 6-1

6.1 EEE の概要 6-1

6.2 EEE の設定 6-1

6.3 EEE の状態の表示 6-1

6章 EEE

6.1 EEEの概要

EEE(Energy Efficient Ethernet）省電力機能を有効にすることで、ポートで一定期間、パケットを受信しない場合、アップリンクポートを低電力状態に遷移します。この期間はチップの仕様に依存し、設定を変更することができません。パケットが到着した後、ポートは通常の状態に遷移します。

6.2 EEEの設定

EEE を設定する場合は、Ethernet port view でコマンドを実行します。

表6-1 EEE の設定

操作	コマンド
EEEを有効にする	**green-ethernet eee**
EEEを無効にする	**undo green-ethernet eee**

ten-GigabitEthernet ポートは、設定ができません。

6.3 EEEの状態の表示

display コマンドを実行して EEE の状態を確認できます。

表6-2 EEE の状態の表示

操作	コマンド
EEEの状態を表示する	**display green-ethernet eee**

目次

このセクションのページは **3-x-x** です。

7 章 スパニングツリー 7-1
7.1 スパニングツリーの概要 7-1
7.2 STP の実装 7-1
7.3 スパニングツリーの設定 7-7
7.3.1 ポートでのスパニングツリーの有効/無効の設定 7-7
7.3.2 STP の動作モードの設定 7-8
7.3.3 指定したスイッチのブリッジ優先順位の設定 7-8
7.3.4 指定したスイッチの転送遅延の設定 7-9
7.3.5 指定したスイッチの max age の設定 7-9
7.3.6 STP/RSTP の Hello-time の設定 7-10
7.3.7 STP/RSTP の Transmit hold-count の設定 7-10
7.4 スパニングツリーの状態表示 7-11

7章 スパニングツリー

7.1 スパニングツリーの概要

スパニングツリープロトコルは、ループネットワーク内で適用されるプロトコルです。特定のアルゴリズムによって望ましくない冗長パスをブロックし、ネットワークをループのないツリー構造にします。これによって、ループネットワーク内でパケットが増殖して無限に循環するという問題を回避できます。

7.2 STPの実装

STP の原理は、スイッチ同士が特殊なプロトコルパケット(IEEE 802.1D では BPDU(Bridge Protocol Data Units)と呼ばれる)を交換してネットワークのトポロジを決定するというものです。BPDU には、スイッチによるスパニングツリーの計算に必要な情報が含まれます。

BPDU には主に以下の情報が含まれます。

- ルートの優先順位と MAC アドレスで構成されるルート ID
- ルートへの最短パスのコスト
- 指定スイッチの優先順位と MAC アドレスで構成される指定スイッチ ID
- ポートの優先順位とポート番号で構成される指定ポート ID
- 世代：MessageAge
- 最大世代：MaxAge
- 送信間隔：HelloTime
- ポートの転送遅延：ForwardDelay

指定スイッチ、指定ポートについて、以下に説明します。

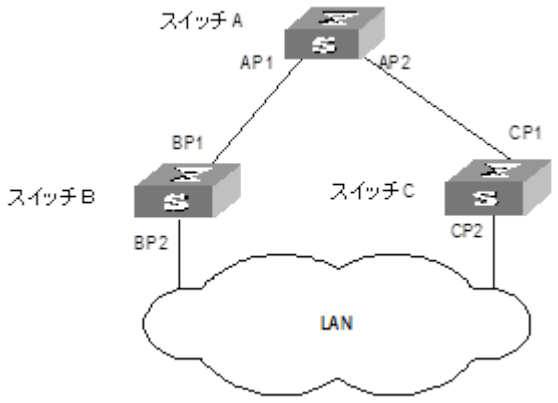


図7-1 指定スイッチと指定ポート

スイッチの場合の指定スイッチとは、指定ポートと呼ばれるポートを経由してローカルスイッチにパケットを転送するスイッチのことです。LAN の場合の指定スイッチとは、指定ポートと呼ばれるポートを経由してネットワークセグメントにパケットを転送するスイッチのことです。図 7-1 では、スイッチ A がポート AP1 を経由してスイッチ B にデータを転送します。したがって、スイッチ B から見て指定スイッチはスイッチ A、指定ポートはスイッチ A の AP1 です。スイッチ B とスイッチ C は LAN に接続されていて、スイッチ B が LAN にパケットを転送します。したがって、LAN から見て指定スイッチはスイッチ B、指定ポートはスイッチ B の BP2 です。

メモ：

AP1、AP2、BP1、BP2、CP1、CP2 は、それぞれスイッチ A、スイッチ B、スイッチ C のポートを示しています。

次に STP の計算プロセスの例を示します。

図 7-2 にネットワークを示します。

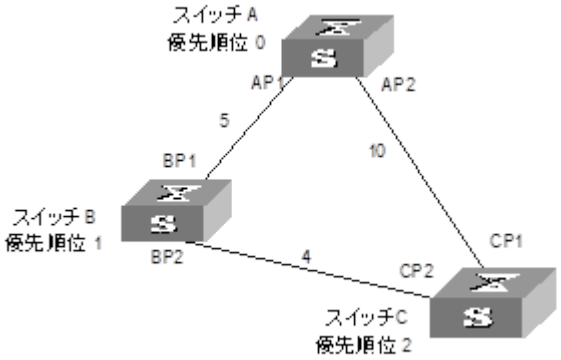


図7-2 Ethernet スイッチネットワーク

分かりやすくするために、この例では BPDU に含まれる最初の 4 つの情報だけを説明します。4 つの情報とは、ルート ID(装置の優先順位)、ルートへのパスコスト、指定スイッチ ID(装置の優先順位)、指定ポート ID(ポート番号)です。図 1-2 に示すように、スイッチ A、B、C の優先順位はそれぞれ 0、1、2、リンクのパスコストはそれぞれ 5、10、4 です。

1) 初期状態

初期化時、スイッチの各ポートは、ポート自身をルートパスコスト 0 のルート、指定スイッチ ID を自身のスイッチ ID、指定ポートを自身のポートとする BPDU を生成します。

スイッチ A：

AP1 の BPDU：{0, 0, 0, AP1}

AP2 の BPDU：{0, 0, 0, AP2}

スイッチ B：

BP1 の BPDU：{1, 0, 1, BP1}

BP2 の BPDU：{1, 0, 1, BP2}

スイッチ C：

CP1 の BPDU：{2, 0, 2, CP1}

CP2 の BPDU：{2, 0, 2, CP2}

2) 最適 BPDU の選択

すべてのスイッチが、自身の BPDU を他のスイッチに送信します。ポートが自身より低い優先順位の BPDU を受信すると、そのメッセージを廃棄します。このときローカル BPDU は変わりません。ポートが自身より高い優先順位の BPDU を受信すると、ローカル BPDU が更新されます。このようにしてすべてのポートの BPDU が比較され、最適 BPDU が選択されます。

比較ルール：

□ ルート ID が小さい BPDU ほど優先順位が高い。

□ ルート ID が同じ場合は、ルートパスコストが比較される。ルートパスコストの比較は、次のように行われる。BPDU に含まれるルートへのパスコストにローカルポートの対応パスコストを加算したコストを S とすると、S が小さい BPDU ほど優先順位が高い。

□ ルートパスコストも同じ場合は、指定スイッチ ID、指定ポート ID、BPDU を受信したポートの ID の順に比較される。

つまり、上の例ではルート ID の比較によって最適 BPDU が選択されます。

3) ルートポートの指定、冗長リンクのブロック、指定ポートの BPDU の更新最適 BPDU を受信したポートが、ルートポートに指定されます。ルートポートの BPDU は変わりません。「最適 BPDU の選択」手順で BPDU が更新された他のポートはブロックされ、データを転送できなくなります。引き続き BPDU の受信はしますが、送信はできなくなるのでそのポートの BPDU は変わりません。「最適 BPDU の選択」手順で BPDU が、更新されなかったポートが指定ポートになります。

指定ポートの BPDU は、次のように変更されます。ルート ID がルートポートの BPDU 内のルート ID で置き換えられ、ルートへのパスコストがルートパスコストにルートポートに対応するパスコストを加算した値で置き換えられ、指定スイッチ ID がローカルスイッチ ID で置き換えられ、指定ポート ID がローカルポート ID で置き換えられます。

各スイッチの比較プロセスは、以下のとおりです。

スイッチ A：

AP1 がスイッチ B から BPDU を受信し、比較の結果、ローカル BPDU の優先順位が受信した BPDU より高いことが分かり、受信した BPDU を廃棄します。AP2 でも同様に BPDU が処理されます。スイッチ A が各ポートの BPDU を比較して、自身がルートの指定スイッチであると判断し、自身をルートと見なし、各ポートの BPDU を保持し、それ以降、BPDU を他のポートに定期的に送信します。現時点の 2 つのポートの BPDU は、以下のとおりです。

AP1 の BPDU：{0, 0, 0, AP1}

AP2 の BPDU：{0, 0, 0, AP2}

スイッチ B：

BP1 がスイッチ A から BPDU を受信し、受信した BPDU の優先順位がローカル BPDU より高いと判断し、BPDU を更新します。

BP2 がスイッチ C から BPDU を受信し、ローカル BPDU の優先順位が受信した BPDU より高いと判断し、受信した BPDU を廃棄します。

現時点の各ポートの BPDU は、以下のとおりです。

BP1 の BPDU：{0, 0, 0, AP1}

BP2 の BPDU：{1, 0, 1, BP2}

スイッチ B が各ポートの BPDU を比較し、BP1 の BPDU を最適設定として選択します。つまり、BP1 がルートポートとして選択され、スイッチ B のポートの BPDU が次のように更新されます。

ルートポート BP1 の BPDU は、{0, 0, 0, BP1}のままです。BP2 のルート ID が最適 BPDU 内のルート ID に更新され、パスコストルートが 5 に更新され、指定スイッチがローカルスイッチ ID に設定され、指定ポート ID がローカルポート ID に設定されます。つまり、BPDU は{0, 5, 1, BP2}になります。

スイッチ B のすべての指定ポートが、BPDU を定期的に送信します。

スイッチ C：

CP2 がスイッチ B の BP2 から、更新前の BPDU {1, 0, 1, BP2}を受信し、更新プロセスを開始します。

CP1 がスイッチ A から BPDU {0, 0, 0, AP2}を受信し、スイッチ C が更新を開始します。BPDU が{0, 0, 0, AP2}に更新されます。

比較の結果、CP1 の BPDU が最適設定として選択されます。CP1 がルートポートに指定されます。このポートの BPDU は変わりません。CP2 はブロックされます。この BPDU は変わりませんが、新しいイベントが発生してスパニングツリー計算が開始されるまでは、スイッチ B から転送されるデータ(STP パケットを除く)を受信しなくなります。たとえば、スイッチ B からスイッチ C へのリンクが停止したり、ポートが優先順位の高い BPDU を受信しなくなります。

CP2 がスイッチ B から更新後の BPDU {0, 5, 1, BP2}を受信します。この BPDU は更新前より優先順位が高いため、更新前の BPDU が{0, 5, 1, BP2}に更新されます。

CP1 がスイッチ A から BPDU を受信しますが、この BPDU は更新されず、{0, 0, 0, AP2}のままです。

比較の結果、CP2 の BPDU が最適設定として選択され、CP2 がルートポートとして選択されます。このポートの BPDU は変わりません。CP1 はブロックされ、BPDU は変わりませんが、何らかの変化が起こってスパニングツリー計算が開始されるまでは、スイッチ A から転送されるデータを受信しなくなります。たとえば、スイッチ B からスイッチ C へのリンクが停止します。

こうしてスパニングツリーが安定状態になります。スイッチ A をルートとするツリーを図 7-3 に示します。

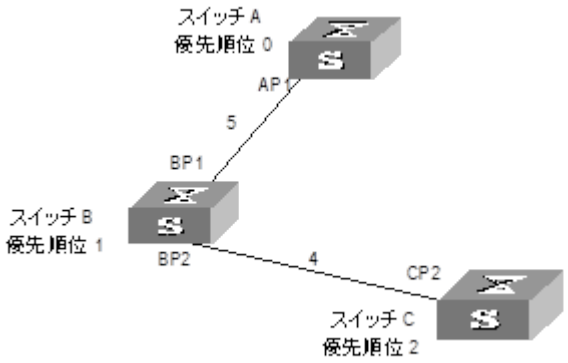


図7-3 最終安定スパニングツリー

分かりやすくするために、説明を簡略化します。たとえば、実際の計算ではルート ID と指定スイッチ ID は、スイッチ優先順位とスイッチ MAC アドレスの両方で構成されます。指定ポート ID は、ポート優先順位とポート MAC アドレスで構成されます。BPDU の更新プロセスでは、BPDU に含まれる最初の 4 つ以外の情報も特定のルールに従って変更されます。計算の基本プロセスを、以下に示します。

□ STP の BPDU 転送メカニズム：

ネットワークの初期状態では、すべてのスイッチが自身をルートと見なします。指定ポートがローカルポートの BPDU を定間隔(HelloTime)で送信します。BPDU を受信したポートがルートポートの場合、スイッチが BPDU のタイミングをとるタイマを有効にして、BPDU 内の MessageAge を特定のルールに従って増やします。パスに障害が発生すると、このパスのルートポートは BPDU を受信しなくなり、古い BPDU はタイムアウトによって廃棄されます。そこでスパニングツリーの再計算が開始され、新しいパスが生成され、障害のあるパスが新しいパスで置き換えられ、ネットワークの接続性が復旧します。

ただし、再計算によって生成された新しい BPDU はすぐにはネットワークに送信されないため、トポロジの変化を検出していない再計算前のルートポートと指定ポートは古いパスを使用してデータの転送を続けます。新しいルートポートと指定ポートが選択されてすぐにデータの転送を開始すると、偶発的なループが発生する可能性があります。このような問題を防ぐため、RSTP には過渡状態メカニズムが使用されていて、新しい BPDU がネットワークに送信されてからルートポートと指定ポートがデータの送信を再開するようになっています。つまり、ルートポートと指定ポートは転送遅延期間の過渡状態を経てから転送状態になります。

7.3 スパニングツリーの設定

スパニングツリーの設定では、以下の設定を行います。

- ポートでのスパニングツリーの有効/無効の設定
- スパニングツリーの動作モードの設定
- 指定したスイッチのブリッジ優先順位の設定
- 指定したスイッチの転送遅延の設定
- 指定したスイッチの Hello 時間の設定
- 指定したスイッチの max age の設定
- 指定したポートの優先順位の設定

これらの設定のうち必須設定は、ポートでの STP の有効設定だけです。その他の設定は、特に設定しなければデフォルト設定が使用されます。

スパニングツリーを有効にする前に、Ethernet ポートまたはデバイスの関連パラメータを設定できます。スパニングツリーを無効にすると、これらの設定パラメータが保存され、その後スパニングツリーを再び有効にしたときに有効になります。

7.3.1 ポートでのスパニングツリーの有効/無効の設定

指定ポートでスパニングツリーを有効あるいは無効に設定するには、Ethernet port view で、以下のコマンドを実行します。

表7-1 ポートでのスパニングツリーの有効/無効の設定

操作	コマンド
指定ポートでスパニングツリーを有効にする	**stp enable**
指定ポートでスパニングツリーを無効にする	**undo stp enable**

デフォルト：無効

Ethernet ポートでスパニングツリーを無効にすると冗長ルートが生成されることがあるので注意してください。

7.3.2 STPの動作モードの設定

スパニングツリーは RSTP か STP で実行できます。

スパニングツリーの動作モードを設定するには、System view で、以下のコマンドを実行します。

表7-2 スパニングツリーの動作モードの設定

操作	コマンド
スパニングツリーの動作モードを STP /RSTPに設定する	**stp mode { rstp | stp }**

デフォルト：RSTP

7.3.3 指定したスイッチのブリッジ優先順位の設定

スイッチがスパニングツリーの「ルート」として選択されるかどうかは、スイッチのブリッジ優先順位によって決まります。スイッチに低いブリッジ優先順位を割り当てることで、人為的にスイッチをスパニングツリーのルートに指定できます。

指定したスイッチのブリッジ優先順位を設定するには、System view で、以下のコマンドを実行します。

表7-3 指定したスイッチの優先順位の設定

操作	コマンド
指定したスイッチの優先順位を設定する	**stp priority** *priority*
指定したスイッチの優先順位をデフォルトに戻す	**undo stp priority**

デフォルト：32768

スイッチングネットワーク内のすべてのスイッチのブリッジ優先順位が同じ場合は、MAC アドレスが最小のスイッチが「ルート」として選択されることに注意してください。スパニングツリーが有効になっている場合、スイッチにブリッジ優先順位を割り当てるとスパニングツリーが再計算されます。

7.3.4 指定したスイッチの転送遅延の設定

リンクに障害が発生すると、スパニングツリーの再計算が行われ、ツリーの構造が変わります。ただし、再計算によって新しく生成された BPDU はすぐにはネットワークに送信できません。新しく選択されたルートポートと指定ポートがすぐにデータフレームの転送を開始すると、偶発的なループが発生する可能性があります。このため、このプロトコルには過渡状態メカニズムが使用されていて、ルートポートと指定ポートは転送遅延期間の過渡状態を経てから転送状態になりデータフレームの転送を再開するようになっています。この転送遅延は、確実に新しい BPDU がネットワーク全体に送信されてからデータフレームの転送を再開するための手段です。

指定したスイッチの転送遅延を設定するには、System view で、以下のコマンドを実行します。

表7-4 指定したスイッチの転送遅延の設定

操作	コマンド
STP及びRSTPのforward-timeを設定する	**stp forward-time** *time*
STP及びRSTPのforward-timeをデフォルトに戻す	**undo stp forward-time**

デフォルト：15 秒

スイッチの転送遅延はスイッチングネットワークの規模に関係します。通常、ネットワークの規模が大きいほど、転送遅延が長くなります。転送遅延が短すぎると、偶発的に冗長パスが発生することがあります。逆に、転送遅延が長すぎると、ネットワーク接続の復旧に時間がかかることがあります。デフォルト設定の使用が推奨されます。

7.3.5 指定したスイッチのmax ageの設定

max age は、BPDU の「タイムアウト」を判断するパラメータです。ネットワークの状態に合わせてユーザがこのパラメータを設定できます。

指定したブリッジの max age を設定するには、System view で、以下のコマンドを実行します。

表7-5 指定したブリッジの max age の設定

操作	コマンド
指定したスイッチのmax ageを設定する	**stp max-age** *time*
指定したスイッチのmax ageをデフォルトに戻す	**undo stp max-age**

デフォルト：20 秒

max age が短すぎると、スパニングツリーの計算頻度が増えたり、ネットワークの輻輳がリンク障害と誤認されます。逆に、max age が長すぎると、スイッチが適時にリンク障害を発見できないことがあり、ネットワークの自動検出能力が低下します。デフォルト設定の使用が推奨されます。

7.3.6 STP/RSTPのHello-timeの設定

STP/RSTP の Hello Time を設定するには、System view から以下のコマンドを実行します。

表7-6 STP/RSTP の hello-time の設定

操作	コマンド
STP及びRSTPのhello-timeを設定する	**stp hello-time** *time*
STP及びRSTPのhello-timeをデフォルトに戻す	**undo stp hello-time**

デフォルト：2

7.3.7 STP/RSTPのTransmit hold-countの設定

STP/RSTP の Transmit Hold-count を設定するには、System view から以下のコマンドを実行します。

表7-7 STP/RSTP の Transmit hold-count の設定

操作	コマンド
STP及びRSTPのTransmit	**stp transmit hold-count** *hold-count*

hold-countを設定する	
STP及びRSTPのTransmit hold-countをデフォルトに戻す	**undo stp transmit hold-count**

デフォルト：6

7.4 スパニングツリーの状態表示

前述の設定終了後、display コマンドを実行して、スパニングツリーの設定の動作状態を表示し、設定を確認します。

表7-8 スパニングツリーの状態表示

操作	コマンド
ローカルスイッチと指定したポートのスパニングツリー設定情報を表示する	**display stp [active | detailed | interface** *interface-type interface-number* **| summary]**
スパニングツリー統計情報を消去する	**reset stp [interface** *interface-type interface-number* **]**

目次

このセクションのページは **3-x-x** です。

8 章 IGMP スヌーピング 8-1

8.1 IGMP スヌーピングの概要 8-1

8.2 IGMP スヌーピングの設定 8-1

8.2.1 IGMP スヌーピングの有効/無効の設定 8-1

8.2.2 IGMP スヌーピングのサポートバージョンの設定 8-2

8.2.3 IGMP スヌーピングのクエリー送信間隔の設定 8-2

8.2.4 IGMP スヌーピングの離脱間隔の設定 8-3

8.2.5 IGMP グループからの即時脱退の有効/無効の設定 8-3

8.2.6 ポートが加入可能なグループ最大値の設定 8-3

8.2.7 Ethernet ポートのルータポート設定 8-4

8.2.8 IGMP メッセージの優先度の設定 8-4

8.2.9 IGMP スヌーピングのクエリー送信機能の有効/無効 8-4

8.2.10 IGMP スヌーピングの最大応答時間の設定 8-5

8.2.11 IGMP スヌーピングのロバストネス変数の設定 8-5

8.2.12 Unknown マルチキャストの透過許可/拒否の設定 8-6

8.2.13 IGMP スヌーピングの最初のレポートの繰り返し送信間隔の設定 8-6

8.3 IGMP スヌーピングの状態の表示 8-7

8章 IGMP スヌーピング

8.1 IGMPスヌーピングの概要

IGMP スヌーピング (Internet Group Management Protocol Snooping) は、レイヤ 2 Ethernet スイッチで実行されるマルチキャスト制御メカニズムで、マルチキャストグループの管理と制御に使用されます。

IGMP スヌーピングはリンクレイヤで実行されます。ホストとルータ間で伝送される IGMP メッセージを受信すると、レイヤ 2 Ethernet スイッチは IGMP スヌーピングを使用して、IGMP メッセージで伝達される情報を分析します。スイッチが、IGMP ホストからの IGMP ホストレポートメッセージを認識すると、そのホストを対応するマルチキャストテーブルに追加します。スイッチが、IGMP ホストからの IGMP 離脱メッセージを認識すると、そのホストを対応するマルチキャストテーブルから削除します。スイッチは常に IGMP メッセージを監視し、レイヤ 2 の MAC マルチキャストアドレステーブルを作成および維持します。また、上流ルータから伝送されたマルチキャストパケットを、この MAC マルチキャストアドレステーブルに従って転送します。

8.2 IGMPスヌーピングの設定

8.2.1 IGMPスヌーピングの有効/無効の設定

IGMP スヌーピングは、System view と Vlan-interface view の両方を有効に設定することで、はじめて IGMP スヌーピングが有効になります。

表8-1 IGMP スヌーピングの有効/無効の設定

操作	コマンド	
1. System viewに移行する	**system-view**	
2. IGMPスヌーピングをシステムで有効にする	**igmp-snooping enable**	デフォルト：システムで有効
3. Vlan-interface viewに移行する	**interace vlan** *vlan_id*	
4. IGMPスヌーピングをVlan-interface viewで有効にする	**igmp snooping**	デフォルト：VLANインターフェースで無効

8.2.2 IGMPスヌーピングのサポートバージョンの設定

IGMP スヌーピングのサポートバージョンを設定します。System view から以下のコマンドを実行します。

表8-2 IGMP スヌーピングのサポートバージョンの設定

操作	コマンド
IGMPスヌーピングのサポートバージョンを設定する	**igmp-snooping compatibility { auto | v1 | v2 |v3 }**
IGMPスヌーピングのサポートバージョンをデフォルトに戻す	**undo igmp-snooping compatibility**

デフォルト：v2

⚠ **注意：**

- **igmp-snooping compatibility** を **v3** および **auto** に設定した場合は、**igmp-snooping querier election** を有効にすることが出来ません。
- **igmp-snooping querier election** を有効に設定した場合は、**igmp-snooping compatibility** を **v3** および **auto** に設定することが出来ません。

8.2.3 IGMPスヌーピングのクエリー送信間隔の設定

クエリーパケットの送信間隔を設定するには、Vlan-interface view から以下のコマンドを実行します。

表8-3 IGMP スヌーピングのクエリー送信間隔の設定

操作	コマンド
IGMPスヌーピングのクエリー送信間隔を設定する	**igmp-snooping query-interval** *time*
IGMPスヌーピングのクエリー送信間隔をデフォルトに戻す	**undo igmp-snooping query-interval**

デフォルト：125 秒

8.2.4 IGMPスヌーピングの離脱間隔の設定

IGMP スヌーピングの離脱間隔を設定するには、Vlan-interface view から以下のコマンドを実行します。

表8-4 IGMP スヌーピングの離脱間隔の設定

操作	コマンド
IGMPスヌーピングの離脱間隔を設定する	**igmp-snooping last-member-query-interval** *time*
IGMPスヌーピングの離脱間隔をデフォルトに戻す	**undo igmp-snooping last-member-query-interval**

デフォルト：10 秒

8.2.5 IGMPグループからの即時脱退の有効/無効の設定

IGMP グループからの即時脱退の有効/無効を設定するには、Ethernet port view から以下のコマンドを実行します。

表8-5 IGMP グループからの即時脱退有効/無効の設定

操作	コマンド
IGMPグループからの即時脱退を有効にする	**igmp-snooping fast-leave**
IGMPグループからの即時脱退を無効にする	**undo igmp-snooping fast-leave**

デフォルト：無効

8.2.6 ポートが加入可能なグループ最大値の設定

ポートが加入できるグループの最大数を設定するには、Ethernet port view で以下のコマンドを実行します。

表8-6 ポートが加入可能なグループ最大値の設定

操作	コマンド
ポートが加入できるグループの最大	**igmp-snooping group-limit** *throtling*

値を設定する	
ポートが加入できるグループの最大値をデフォルトに戻す	**undo igmp-snooping group-limit**

デフォルト：設定なし

8.2.7 Ethernetポートのルータポート設定

ルータポートを設定するには、Ethernet view から以下のコマンドを実行します。

表8-7 Ethernet ポートのルータポート設定

操作	コマンド
Ethernetポートをルータポートに設定する	**igmp-snooping mrouter**
Ethernetポートのルータポートを解除する	**undo igmp-snooping mrouter**

デフォルト：無効

8.2.8 IGMPメッセージの優先度の設定

IGMP メッセージの優先度を設定するには、Vlan-interace view から以下のコマンドを実行します。

表8-8 IGMP メッセージの優先度の設定

操作	コマンド
IGMPメッセージの優先度を設定する	**igmp-snooping priority** *cos_priority*
IGMPメッセージの優先度をデフォルトに戻す	**undo igmp-snooping priority**

デフォルト：設定なし

8.2.9 IGMPスヌーピングのクエリー送信機能の有効/無効

IGMP スヌーピングのクエリー送信機能の有効/無効を設定するには、Vlan-interface view から以下のコマンドを実行します。

表8-9 IGMP メッセージのクエリー送信機能有効/無効の設定

操作	コマンド
IGMPスヌーピングのクエリー送信機能を有効にし、有効時のクエリー送信先アドレスを設定する	**igmp-snooping querier { address** *ip_addr* **| election }**
IGMPスヌーピングのクエリー送信機能を無効に設定する	**undo igmp-snooping querier { address | election }**

デフォルト：無効

⚠ **注意：**

- **igmp-snooping compatibility** を **v3** および **auto** に設定した場合は、**igmp-snooping querier election** を有効にすることが出来ません。
- **igmp-snooping querier election** を有効に設定した場合は、**igmp-snooping compatibility** を **v3** および **auto** に設定することが出来ません。

8.2.10 IGMPスヌーピングの最大応答時間の設定

IGMP スヌーピングの最大応答時間を設定するには、Vlan-interface view から以下のコマンドを実行します。

表8-10 IGMP メッセージのクエリー送信機能有効/無効の設定

操作	コマンド
IGMPスヌーピングの最大応答時間を設定する	**igmp-snooping query-max-response-time** *time*
IGMPスヌーピングの最大応答時間をデフォルトに設定する	**undo igmp-snooping query-max-response-time**

デフォルト： 100

8.2.11 IGMPスヌーピングのロバストネス変数の設定

IGMP スヌーピングのロバストネス変数を設定するには、Vlan-interface view から以下のコマンドを実行します。

表8-11 IGMP メッセージのロバストネス変数の設定

操作	コマンド
IGMPスヌーピングのロバストネス変数を設定する	**igmp-snooping robustness-variable** *value*
IGMPスヌーピングのロバストネス変数をデフォルトに設定する	**undo igmp-snooping robustness-variable**

デフォルト： 2

8.2.12 Unknownマルチキャストの透過許可/拒否の設定

Unknown マルチキャストの透過許可/拒否を設定するには、System view から以下のコマンドを実行します。

表8-12 Unknown マルチキャストの透過許可/拒否の設定

操作	コマンド
Unknownマルチキャストの透過を許可する	**igmp-snooping unknown-flooding**
Unknownマルチキャストの透過を拒否する	**undo igmp-snooping unknown-flooding**

デフォルト： 透過を許可

8.2.13 IGMPスヌーピングの最初のレポートの繰り返し送信間隔の設定

グループのメンバーシップに関する最初のレポートを繰り返し送信する間隔を設定するには、Vlan-interface view から以下のコマンドを実行します。

表8-13 メンバーシップに関する最初のレポートを繰り返し送信する間隔の設定

操作	コマンド
非請求間隔の設定をする	**igmp-snooping unsolicited-report-interval** *time*
非請求間隔の設定をデフォルトに戻す	**undo igmp-snooping unsolicited-report-interval**

デフォルト： 100 秒

8.3 IGMPスヌーピングの状態の表示

display コマンドを使用し、IGMP スヌーピングの状態を表示します。

表8-14 IGMP スヌーピングの各種情報の表示

操作	コマンド
IGMPスヌーピングの各種情報を表示する	**display igmp-snooping [group vlan** *vlan_id* **] [group-database [interface** *interface-type interface-number* **]] [sfm-information]] [detail]**
IGMPスヌーピングのルータ情報を表示する	**display igmp-snooping mrouter [detail]**
IGMPスヌーピングの統計情報をクリアする	**reset igmp-snooping statistics [vlan** *vlan_id* **]**

QX-S700G シリーズ Ethernet PoE スイッチ

オペレーションマニュアル

4.VLAN

本マニュアルは以下に示す章で構成されています。

01-VLAN

02-管理 VLAN インタフェース

目次

このセクションのページは **4-x-x** です。

1 章 VLAN 1-1

1.1 VLAN の概要 1-1

1.2 VLAN の設定 1-1

1.2.1 VLAN の作成と削除 1-1

1.2.2 Ethernet ポートのリンクタイプの設定 1-2

1.2.3 指定 VLAN への Ethernet ポート追加 1-2

1.2.4 Ethernet ポートのデフォルト VLAN ID の設定 1-3

1.2.5 VLAN の name の設定と削除 1-4

1.2.6 受信可能なフレームタイプの指定 1-4

1.2.7 フレーム出力時の tag 付加の有無の設定 1-5

1.2.8 ポートのイングレスフィルタリングの有効/無効の設定 1-5

1.2.9 デフォルト VLAN に属するフレームの出力時の tag 設定 1-5

1.3 VLAN の表示 1-6

1.4 VLAN の設定例 1-6

1章 VLAN

1.1 VLANの概要

バーチャルローカルエリアネットワーク(VLAN)は、LAN のデバイスを論理的にグループ化し、仮想ワークグループを実現します。IEEE では 1999 年に、VLAN の実装ソリューションの標準化を目的とした IEEE 802.1Q を発行しています。

VLAN 技術により、ネットワーク管理者は物理 LAN を異なるブロードキャストドメインに論理的に分けることができます。

VLAN 内のブロードキャストおよびユニキャストのトラフィックは他の VLAN に転送されることはありません。VLAN 技術は、ネットワークトラフィックの制御、デバイス投資の節約、ネットワーク管理の簡素化、およびセキュリティの強化に役立ちます。

1.2 VLANの設定

まず、必要条件に合わせて VLAN を作成します。

VLAN の設定では、以下の設定を行います。

- VLAN の作成と削除
- Ethernet ポートのリンクタイプの設定
- 指定 VLAN への Ethernet ポート追加
- Ethernet ポートのデフォルト VLAN ID の設定
- VLAN の name の設定と削除
- 受信可能なフレームタイプの指定
- フレーム出力時の tag 付加の有無の設定
- ポートのイングレスフィルタリングの有効/無効の設定
- デフォルト VLAN に属するフレームを出力時の tag の設定

1.2.1 VLANの作成と削除

VLAN ID を作成/削除するには、System view で以下のコマンドを実行します。

表1-1 VLAN の作成と削除

操作	コマンド
VLANを作成して、VLAN viewを表示する	**vlan** *vlan_id*

指定したVLANを削除する	**undo vlan** { *vlan_id* | **all** }

注意:

- 本コマンドにおいて、装置に設定可能な VLAN 登録数は最大 64 となります。
- VLAN 機能は、Port isolate 機能と同時に使用することはできません。Port isolate 機能が有効な場合は、VLAN 機能の設定が排他状態となるため、コンフィグに表示されません。

1.2.2 Ethernetポートのリンクタイプの設定

Ethernet ポートは、アクセス、ハイブリッド、およびトランクの 3 種類のリンクタイプで動作します。アクセスポートは、1 つの VLAN のみに属します。トランクポートは、スイッチ間の接続に使用する複数の VLAN に属し、複数の VLAN でパケットを送受信できます。ハイブリッドポートも、スイッチとユーザのコンピュータの両方の接続に使用する複数の VLAN に接続し、複数の VLAN でパケットを送受信できます。

Ethernet ポートのリンクタイプを設定するには Ethernet port view で以下のコマンドを実行します。

表1-2 Ethernet ポートのリンクタイプの設定

操作	コマンド
リンクタイプを設定する	**port link-type** { **access** | **hybrid** | **trunk** }
リンクタイプをデフォルト（access）に戻す	**undo port link-type**

1.2.3 指定VLANへのEthernetポート追加

指定した VLAN に Ethernet ポートを追加します。アクセスポートは 1 つの VLAN のみに追加できます。ハイブリッドポートとトランクポートは、複数の VLAN に追加できます。

Ethernet port view で、以下のコマンドを実行します。

表1-3 VLAN への GigabitEthernet ポートの追加

操作	コマンド
指定したVLANに現在のポートをアクセスポートとして追加する	**port access vlan** *vlan_id*
指定したVLANから現在のアクセスポートを削除する	**undo port access vlan**
指定したVLANに現在のポートをハイブリッドポートとして追加する	**port hybrid vlan** *vlan_id_list*
指定したVLANから現在のハイブリッドポートを削除する	**undo port hybrid vlan** *vlan_id_list*
指定したVLANに現在のポートをトランクポートとして追加する	**port trunk permit vlan** *vlan_id_list*
指定したVLANから現在のトランクポートを削除する	**undo port trunk permit vlan** *vlan_id_list*

1.2.4 EthernetポートのデフォルトVLAN IDの設定

アクセスポートは１つのVLANのみに属することができるため､そのデフォルトVLANはそのポートが属する VLAN となります。ハイブリッドポートとトランクポートは複数の VLAN に属することができるため、デフォルトの VLAN ID を設定する必要があります。デフォルト VLAN ID を設定すると、VLAN タグのないパケットは、デフォルト VLAN に属するポートに転送されます。

Ethernet port view で、以下のコマンドを実行します。

表1-4 Ethernet ポートのデフォルト VLAN ID の設定

操作	コマンド
ハイブリッドポートのデフォルトVLANIDを設定する	**port hybrid pvid vlan** *vlan_id*
ハイブリッドポートのデフォルトVLANIDをデフォルト（VLANID：1）に戻す	**undo port hybrid pvid**
トランクポートのデフォルトVLAN IDを設定する	**port trunk pvid vlan** *vlan_id*
トランクポートのデフォルトVLANIDをデフォルト（VLANID：1）に戻す	**undo port trunk pvid**

⚠ **注意:**

適切なパケットの送信を保証するために、ローカルのハイブリッドポートまたはトランクポートのデフォルト VLAN ID は、隣接スイッチのハイブリッドポートまたはトランクポートのデフォルト VLAN ID と同じにします。

1.2.5 VLANのnameの設定と削除

VLAN の name を設定あるいは削除するには、VLAN view で、以下のコマンドを実行します。

name はワークグループ名や部署名などで、異なる VLAN を識別するために使用します。

表1-5 VLAN の name の設定と削除

操作	コマンド
指定したVLANのnameを設定する	**name** *vlan_name*
指定したVLANのnameを削除する	**undo name**

デフォルト：VLAN＊＊＊＊

1.2.6 受信可能なフレームタイプの指定

受信可能なフレームタイプを指定するには、Ethernet port view で以下のコマンドを実行します。

表1-6 受信可能なフレームタイプの指定

操作	コマンド
受信可能なフレームタイプを指定する	**port hybrid acceptable-frame-type { all | tagged | untagged }**
受信可能なフレームタイプをデフォルトに戻す	**undo port hybrid acceptable-frame-type**

デフォルト：all

1.2.7 フレーム出力時のtag付加の有無の設定

フレーム出力時の tag の付加の有無を設定するには、Ethernet port view で以下のコマンドを実行します。

表1-7 フレーム出力時の tag 付加の有無の設定

操作	コマンド
フレーム出力時にtagの付加の有無を設定する	**port hybrid egress-tag { all [except-native] | none }**
フレーム出力時にtagの付加の有無をデフォルトに戻す	**undo port hybrid egress-tag**

デフォルト：all expect-native

1.2.8 ポートのイングレスフィルタリングの有効/無効の設定

ポートのイングレスフィルタリングの有効/無効を設定するには、Ethernet port view で以下のコマンドを実行します。

入力フィルタリングが有効な場合、ポートがメンバーではない VLAN に分類されたフレームは破棄されます。

入力フィルタリングが無効になっている場合、ポートがメンバーではない VLAN に分類されたフレームは受け入れられ、スイッチ エンジンに転送されます。

表1-8 ポートのイングレスフィルタリングの有効/無効の設定

操作	コマンド
ポートのイングレスフィルタリングを有効に設定する	**port hybrid ingress-filtering**
ポートのイングレスフィルタリングを無効に設定する	**undo port hybrid ingress-filtering**

デフォルト：無効

1.2.9 デフォルトVLAN に属するフレームの出力時のtag設定

デフォルト VLAN に属するフレームを出力時の tag を設定するには、Ethernet port view で以下のコマンドを実行します。

表1-9 デフォルト VLAN に属するフレームを出力時の tag の設定

操作	コマンド
tagを有りに設定する	**port trunk vlan tag pvid**
tagを無しに設定する	**undo port trunk vlan tag pvid**

デフォルト：tag 無し

1.3 VLANの表示

display コマンドを実行すると、VLAN の現行の設定を表示し、設定を確認することができます。

表1-10 VLAN の表示

操作	コマンド
VLANの関連情報を表示する	**display vlan** [*vlan_id* | **all**]

1.4 VLANの設定例

I. ネットワーク要件

VLAN2 と VLAN3 を作成します。VLAN2 に GigabitEthernet ポート 1/1 と GigabitEthernet ポート 1/2 を、VLAN3 に GigabitEthernet 1/3 と GigabitEthernet 1/4 を追加します。

II.　ネットワークダイアグラム

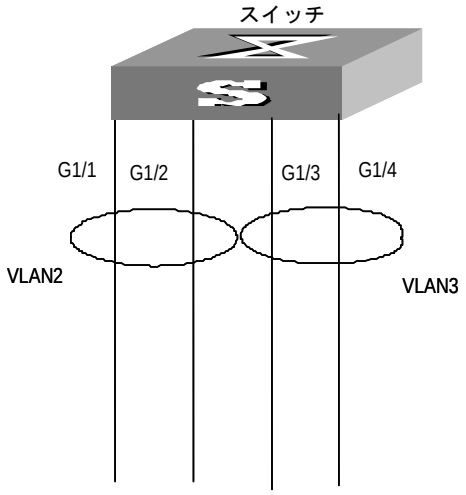


図1-1 VLAN の設定例

III.　設定手順

#VLAN2 を作成し、VLAN view に入る

```
[switch]vlan 2
[switch-vlan2]
```

#VLAN2 に GigabitEthernet 1/1 と GigabitEthernet 1/2 を追加する

```
[switch-vlan2]port GigabitEthernet 1/1 GigabitEthernet 1/2
```

#VLAN 3 を作成し、VLAN view に入る

```
[switch]vlan 3
[switch-vlan3]
```

#VLAN3 に GigabitEthernet 1/3 と GigabitEthernet 1/4 を追加する

```
[switch-vlan3]port GigabitEthernet 1/3 GigabitEthernet 1/4
```

目次

このセクションのページは **4-x-x** です。

2 章 管理 VLAN インタフェース 2-1

2.1 管理 VLAN インタフェースの概要 2-1

2.2 管理 VLAN インタフェースの設定 2-1

2.2.1 管理 VLAN インタフェースの作成/削除 2-1

2.2.2 IP アドレスの設定 2-2

2.2.3 デフォルトルートの設定 2-2

2.2.4 DNS サーバーの設定 2-2

2.3 管理 VLAN インタフェースの表示 2-3

2.4 管理 VLAN インタフェースの設定例 2-3

2.5 ネットワーク接続のテストツール 2-4

2.5.1 ping 2-4

2章 管理 VLAN インタフェース

2.1 管理VLANインタフェースの概要

Telnet のリモート管理を実行する場合は、あらかじめ装置の IP アドレスを設定しておく必要があります。

QX-S700G シリーズ Ethernet PoE スイッチでは、1 つの VLAN インタフェースにのみ IP アドレスを設定できます。そのインタフェースに対応する VLAN は、管理 VLAN となります。

2.2 管理VLANインタフェースの設定

管理 VLAN インタフェースでは以下の設定を行います。

- 管理 VLAN インタフェースの作成/削除
- IP アドレスの設定
- デフォルトルートの設定
- DNS サーバの設定

2.2.1 管理VLANインタフェースの作成/削除

管理 VLAN インタフェースを作成するには、System view で、以下のコマンドを実行します。

表2-1 管理 VLAN インタフェースの作成/削除

操作	コマンド
管理VLANインタフェースを作成し、その viewを表示する	**interface vlan** *vlan-id*
管理VLANインタフェースを削除する	**undo interface vlan** *vlan-id*

この設定作業を実行する場合は、vlan-id パラメータを指定して VLAN をあらかじめ作成しておく必要があります。ただし、VLAN1 はデフォルトの VLAN であるため、作成の必要はありません。

2.2.2 IPアドレスの設定

管理 VLAN インタフェースは他のホストと通信するため、IP アドレスが必要です。手動でインタフェースに IP アドレスを割り当てるか、DHCP によって IP アドレスを取得することができます。IP アドレスを取得する方法を変更した場合、新しい IP アドレスは古い IP アドレスに上書きします。

Vlan- interface view で、以下のコマンドを実行します。

表2-2 IP アドレスの設定

操作	コマンド
管理VLANインタフェースのIPアドレスを手動で割り当てる	**ip address** *ip-address net-mask*
管理VLANインタフェースのIPアドレスをDHCPより取得する	**ip address** *dhcp-alloc*
管理VLANインタフェースのIPアドレスを削除する	**undo ip address** [*ip-address net-mask* **|** *dhcp-alloc*]

デフォルト:管理 VLAN インタフェースに IP アドレスは割り当てられていない

2.2.3 デフォルトルートの設定

ネットワーク経由でスイッチにログインするためのデフォルトルートを設定するには、System view で、以下のコマンドを実行します。

表2-3 デフォルトルートの設定

操作	コマンド
デフォルトルートを追加する	**ip route-static 0.0.0.0 0.0.0.0** *gateway-address*
デフォルトルートを削除する	**undo ip route-static**

2.2.4 DNSサーバーの設定

DNS サーバーを設定するには DNS サーバーの IP アドレスを用いて、System view で、以下のコマンドを実行します。

表2-4 DNS サーバーの設定

操作	コマンド
DNSサーバーを設定する	**ip name-server** *number ipv4_address*
設定したDNSサーバーを解除する	**undo ip name-server** *number*

2.3 管理VLANインタフェースの表示

display コマンドを実行し、システム IP 設定状態を確認することができます。

表2-5 管理 VLAN インタフェースの表示

操作	コマンド
管理VLANインタフェースの情報を表示する	**display interface vlan** [*vlan_id*]
ルーティングテーブルサマリーを表示する	**display ip routing-table**
ipインターフェースの情報を表示する	**display ip interface [brief]**
設定したDNS設定情報を表示する	**display ip name-server**
VLANインターフェースの統計情報をクリアする	**reset ip statistics**

2.4 管理VLANインタフェースの設定例

#管理 VLAN インタフェース 1 を作成し、Vlan-interface view に入る。

```
[switch] interface vlan 1
[switch-Vlan-interface1]
```

#IP アドレスを 10.10.10.2 に設定する

```
[switch-Vlan-interface1]ip address 10.10.10.2 255.255.0.0
```

2.5 ネットワーク接続のテストツール

2.5.1 ping

ping コマンドを使用すると、ネットワーク接続の状況と、ホストに到達可能かどうかを確認できます。

ping コマンドは、すべての view で実行できます。

表2-6 ping コマンド

操作	コマンド
pingの実行	**ping ip** [**-c** *count*] *host*

このコマンドの出力には、以下の内容が表示されます。

- 各 ping メッセージに対する応答。タイムアウトまでに応答パケットが受信されない場合は、”Request time out”情報が表示されます。受信された場合は、データバイト数、パケットシーケンス番号、TTL、および応答パケットの往復時間が表示されます。
- スイッチが送受信したパケット数、パケット損失率、往復時間の最短/平均/最長値などの最終統計情報。

⚠ **注意**：

ping 実行中は中断ができません。-c オプションで多量の値を設定する際はご注意ください。

QX-S700G シリーズ Ethernet PoE スイッチ

オペレーションマニュアル

5.QoS

本マニュアルは以下に示す章で構成されています。

01-QoS

02-ポート送受信帯域制限

目次

このセクションのページは **5-x-x** です。

1 章 QoS 1-1

1.1 QoS の概要 1-1

1.1.1 トラフィック 1-1

1.1.2 トラフィッククラシファイ 1-1

1.1.3 トラフィックポリシング 1-2

1.1.4 トラフィックプライオリティ 1-2

1.1.5 キュースケジューリング 1-2

1.2 QoS の設定 1-3

1.2.1 QoS モードの設定 1-4

1.2.2 QoS マップの設定 1-4

1.2.3 ポートプライオリティの設定 1-4

1.2.4 キュースケジューリングの設定 1-5

1.3 QoS の設定状態の表示 1-5

1.4 QoS の設定例 1-6

1章 QoS

1.1 QoSの概要

従来の IP ネットワークでは､すべてのパケットを優先順位に関わりなく同等に処理します。各スイッチ/ルータは、先入れ先出し（FIFO）方式にパケットを処理します。つまり、パケットをベストエフォートで宛先に送信し、送信の信頼性や遅延その他の性能要件に関して何らかの保証を行うことはありません。

今日では、コンピュータネットワークの急速な発展により、帯域幅や遅延やジッタに敏感なデータ、すなわち音声、イメージ、重要データなどがリアルタイムで大量に配信されるようになりました。ネットワーク資源が豊かになる一方で、ネットワーク輻輳の発生も増加しており、ネットワーク通信により高いサービス品質（QoS）を求める声が高まっています。

Ethernet は今日最も広範に使用されているネットワーク技術です。Ethernet は、ローカルエリアネットワーク（LAN）で最も有力な技術であり､Ethernet で構築された LAN の多くがインターネットを形成しています。発展を続ける Ethernet 技術は、将来一般のユーザがインターネットにアクセスするための主要な方式になることでしょう。したがってネットワーク全体でエンドツーエンドの QoS ソリューションを実現するには、Ethernet で QoS サービスを保証できる必要があります。つまり Ethernet スイッチングデバイスに QoS テクノロジを適用し、異なるタイプのサービス（特に短い遅延時間と低ジッタを要求するサービス）に対して複数レベルの QoS 保証を提供できなくてはなりません。

1.1.1 トラフィック

本マニュアルでは､「トラフィック」とは、スイッチを通過する全パケットを指します。

1.1.2 トラフィッククラシファイ

トラフィッククラシファイとは、管理者が要件に基づいて設定したクラシファイルールと呼ぶマッチングルールを使用して、特定の特性を持つパケットを識別することを意味します。ルールは極めて簡単にすることができます。たとえば、プライオリティが異なるトラフィックは､IP パケットヘッダの ToS フィールドにしたがって識別できます。一方でたとえば MAC アドレス、IP プロトコル、送信元 IP アドレス、宛先 IP アドレス、アプリケーションのポート番号など、リンクレイヤ（レイヤ 2)、ネットワークレイヤ（レイヤ 3)、トランスポートレイヤ（レイヤ 4）に関わる情報を利用する

複雑なルールをトラフィッククラシファイに適用することもできます。一般に、トラフィッククラシファイの基準となるこれらの情報はパケットヘッダ中に存在し、パケットの内容がクラシファイに使用されることはほとんどありません。

1.1.3 トラフィックポリシング

限られたネットワーク資源でより良いサービスを提供する QoS では、割り当てられたリソースを最大限に活用するため、ネットワークの入口で特定のユーザのトラフィックを監視します。

1.1.4 トラフィックプライオリティ

Ethernet スイッチは、一部の特殊なパケットに対するプライオリティタグサービスを提供します。タグには ToS、DSCP、802.1p などがあり、各種の QoS モジュールで使用および定義することが可能です。

1.1.5 キュースケジューリング

輻輳が発生すると、複数のパケットがリソースを求めて競合します。この問題を克服するため、Ethernet スイッチはストリクトプライオリティキュー（SP）、重み付けラウンドロビン（WRR）の 2 種類のキュースケジューリングアルゴリズムを採用しています。

- SP

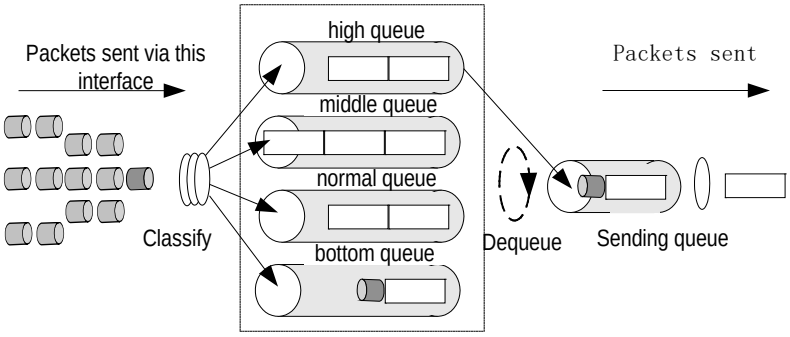


図 1-1 SP

SP は特に重要なサービスアプリケーション向けに開発された技術です。重要なサービスには、輻輳が発生したときに生じる遅延を減少させるサービス・プライオリティを必要とするものがあります。図 1-1 は、ポートごとに 4 つの出力キューを設定した例です。SP ではポートのキューを ハイプライオリティ（高優先順位）、ミディアムプライオリティ（中優先順位）、ノーマルプライオリティ（通常優先順位）、ロープラ

イオリティ（低優先順位）の 4 種類のキュー（順にキュー4、3、2、1 と表示）に分けます。

SP のキューイング処理では、プライオリティに厳密にしたがってパケットに優先権を与え、ハイプライオリティキューのパケットをまず送信します。ハイプライオリティキューが空の場合は、ロープライオリティグループのパケットを優先順位にしたがって送信します。たとえば優先度が高いサービスのパケットをハイプライオリティキューに入れ、電子メールなどの低優先サービスのパケットをロープライオリティキューに入れることにより、優先度が高いサービスパケットをまず送信し、優先度が低いパケットを、高優先パケットがないときに送信するよう設定することが可能です。

ただし SP には短所もあります。たとえば輻輳発生時に多くのパケットがハイプライオリティキューにキューイングしている場合、高サービス優先順位パケットを送信するのに長時間を要するため、ロープライオリティキューのパケットは放置されてしまいます。

- WRR

WRR では、各キューにスイッチポートのサービスタイムを割り当てることを保証します。図 1-1 の例と同様、ポートごとに 4 つの出力キューがあるとします。WRR では、各キューにリソース取得用の重み（それぞれ w3、w2、w1、w0）を与えます。たとえば、100M ポートの WRR アルゴリズムの重みが各キューに対して 8、4、2、1 となり、ロープライオリティキューは最小帯域幅 10Mbps を与えられ、SP スケジューリングで長時間サービスを受けられないという状況を確実に避けることができます。WRR キューには、複数キューのラウンドスケジューリングでも、各キューにサービス時間を割り当てられるという利点もあります。あるキューが空の場合直ちに次のキューに切り替えることによって、帯域幅リソースを適切に利用できます。

1.2 QoSの設定

QoS 設定には以下のものがあります。

- QoS モードの設定
- QoS マップの設定
- ポートプライオリティの設定
- キュースケジューリングの設定

1.2.1 QoSモードの設定

QoS モードの設定には、Ethernet port view で以下のコマンドを実行します。

表1-1 QoS モードの設定

操作	コマンド
QoSモードを設定する	**qos trust** [**dscp** | **cos**]
QoSモードをデフォルト設定に戻す	**undo qos trust [dscp | cos]**

デフォルト：無効

1.2.2 QoSマップの設定

QoS マップの設定には、System view から以下のコマンドを実行します。

表1-2 QoS マップの設定

操作	コマンド
CoSマップを設定します。	**qos map cos-priority cos** *cos* **priority** *priority*
CoSマップをデフォルトに戻します。	undo **qos map cos-priority** cos *cos*
DSCPマップを設定します。	**qos map dscp-priority** *priority* **queue-id** *queue*
DSCPマップをデフォルトに戻します。	**undo qos map dscp priority** *priority*

1.2.3 ポートプライオリティの設定

ポートプライオリティを設定するには、Ethernet port view で以下のコマンドを実行します。スイッチは、VLAN タグを持たないパケットに、そのパケットを受信したポートが属する VLAN のタグを付けます。一方、システムは、パケットへのタグ付け時にポートプライオリティをパケットの 802.1p プライオリティとして使用します。VLAN タグを持つパケットには、タグ付けは行いません。

表1-3 ポートプライオリティの設定

操作	コマンド
ポートプライオリティを設定する	qos priority *priority*
ポートプライオリティをデフォルトに戻す	undo qos priority

Ethernet スイッチのポートは、8 プライオリティレベル（0～7）をサポートしています。必要に応じてプライオリティレベルを設定してください。スイッチはパケットのプライオリティをポートプライオリティに置き換えます。

デフォルト：0

1.2.4 キュースケジューリングの設定

一般にキュースケジューリングは、ネットワーク輻輳の発生時に複数のメッセージがリソースを求めて競合する問題を解決するために適用されます。キュースケジューリングでは、パケットの 802.1p プライオリティにしたがって、パケットをポートの出力キューに分配します。802.1p プライオリティとポートの出力キューのマッピングについて以下に示します。

キュースケジューラの設定には、Ethernet port view で以下のコマンドを実行します。

表1-4 ポートプライオリティの設定キュースケジューリングの設定

操作	コマンド
キュースケジューリングアルゴリズムを設定する	**qos queue-scheduler** { **strict-priority | wrr** *w0 w1* [*w2* [*w3* [*w4* [*w5* [*w6* [*w7*]]]]]] }
キュースケジューリングアルゴリズムの設定をデフォルトに戻す	**undo qos queue-scheduler**

デフォルト：strict-priority

1.3 QoSの設定状態の表示

display コマンドを実行して、QoS 設定を確認できます。

表1-5 QoS の設定状態の表示

操作	コマンド
QoSの情報を表示する	display qos-interface [*interface-type interface-number*]
DSCPのプライオリティマップを表示する	display qos dscp-priority-map

1.4 QoSの設定例

#Ethernet port view に入る

```
[switch]interface GigabitEthernet 1/1
```

#QoS の優先制御を CoS に設定する

```
[switch-GigabitEthernet1/1]qos trust cos
```

#CoS マップを設定する

```
[switch-GigabitEthernet1/1] qos map cos-priority cos 0 priority 0
[switch-GigabitEthernet1/1] qos map cos-priority cos 1 priority 1
[switch-GigabitEthernet1/1] qos map cos-priority cos 2 priority 2
[switch-GigabitEthernet1/1] qos map cos-priority cos 3 priority 3
[switch-GigabitEthernet1/1] qos map cos-priority cos 4 priority 4
[switch-GigabitEthernet1/1] qos map cos-priority cos 5 priority 5
[switch-GigabitEthernet1/1] qos map cos-priority cos 6 priority 6
[switch-GigabitEthernet1/1] qos map cos-priority cos 7 priority 7
```

#キュースケジューリングを strict-priority に設定する

```
[switch-GigabitEthernet1/1] qos queue-scheduler strict-priority
```

目次

このセクションのページは **5-x-x** です。

2 章 ポート送受信帯域制限 2-1

2.1 ポート送受信帯域制限の概要 2-1

2.2 ポート送受信帯域制限の設定 2-1

2.2.1 ブロードキャスト/マルチキャスト/ユニキャストパケット抑制の設定 2-1

2.2.2 帯域制限の設定 2-2

2.3 ポート送受信帯域制限の設定の表示 2-2

2.3.1 帯域制限の情報の表示 2-2

2章 ポート送受信帯域制限

2.1 ポート送受信帯域制限の概要

入力ポートにおいて受信を許容するパケットの最大帯域、及び入力ポートにおいて出力するパケットの最大帯域を制御することが出来ます。

2.2 ポート送受信帯域制限の設定

ポート送受信帯域制限の設定には以下のものがあります。

- ブロードキャスト/マルチキャスト/ユニキャストパケット抑制
- 帯域制限の設定

2.2.1 ブロードキャスト/マルチキャスト/ユニキャストパケット抑制の設定

ブロードキャスト/マルチキャスト/ユニキャスト/Unknown フレームのトラフィックを抑制します。System view と Ethernet port view から以下のコマンドを実行します。なお、マルチキャストフレームは System view、Unknown フレームは Ethernet port view のみで抑制の設定を行うことができます。

表2-1 ブロードキャスト/マルチキャスト/ユニキャストパケット抑制の設定

操作	コマンド
許容できるブロードキャストフレームの最大値を設定する	**qos storm broadcast** *rate* { **fps** | **kfps** | **kbps** | **mbps** }
許容できるマルチキャストフレームの最大値を設定する	**qos storm multicast** *rate* { **fps** | **kfps** | **kbps** | **mbps** }
許容できるユニキャストフレームの最大値を設定する	**qos storm unicast** *rate* { **fps** | **kfps** | **kbps** | **mbps** }
許容できるUnknownフレームの最大値を設定する	**qos storm unknown** *rate* { **fps** | **kfps** | **kbps** | **mbps** }
全てのブロードキャストが透過できるように設定する（デフォルト）	**undo qos storm broadcast**
全てのマルチキャストが透過できるように設定する（デフォルト）	**undo qos storm multicast**
全てのユニキャストが透過できるように設定する（デフォルト）	**undo qos storm unicast**

すべてのUnknownフレームが透過できるように設定する（デフォルト）	**undo qos storm unknown**

設定可能帯域は、10～13128147[kbps] となります。

2.2.2 帯域制限の設定

ポート毎に 受信，送信 の最大帯域を、policer, shaper コマンドで設定出来ます。Ethernet port view より以下のコマンドを実行します。

表2-2 最大帯域制限の設定

操作	コマンド
受信の帯域を制限する	**qos policer** *rate* **[fps | kfps | kbps | mbps]**
受信の帯域制限を無効にする	**undo qos policer**
送信の帯域を制限する	**qos shaper** *rate* **[kbps | mbps]**
送信の帯域制限を無効にする	**undo qos shaper**

デフォルト：制限なし

送信の帯域制限 : 100～13107100[kbps]、受信の帯域制限 : 10～13128147[kbps]です。

2.3 ポート送受信帯域制限の設定の表示

2.3.1 帯域制限の情報の表示

display コマンドを実行して帯域制限の情報を確認できます。

表2-3 帯域制限の情報の表示

操作	コマンド
帯域制限の情報の表示	**display qos storm**

QX-S700G シリーズ Ethernet PoE スイッチ

オペレーションマニュアル

6.MAC アドレス

本マニュアルは以下に示す章で構成されています。

01-MAC アドレス

02-ポートセキュリティ

目次

このセクションのページは **6-x-x** です。

1 章 MAC アドレス 1-1

1.1 MAC アドレスの概要 1-1

1.2 MAC アドレスの設定 1-2

1.2.1 MAC アドレスエントリの設定 1-2

1.2.2 MAC アドレスエージングタイムの設定 1-3

1.2.3 MAC 学習の設定 1-4

1.2.4 MAC アドレステーブルのクリア 1-4

1.3 MAC アドレステーブルの表示 1-4

1章 MAC アドレス

1.1 MACアドレスの概要

Ethernet スイッチには、パケットの高速フォワーディングのための MAC アドレステーブルが保管されています。 テーブルエントリには、デバイスの MAC アドレスや、そのデバイスに Ethernet スイッチを接続するためのポート ID などがあり、Ethernet スイッチは、ダイナミックエントリ（手動では設定されません）を学習します。本装置の MAC アドレステーブルは最大 32768 エントリです。

Ethernet スイッチが、MAC アドレスを学習する仕組みは、以下のとおりです。ポート（ポート A とします）からデータフレームを受信したスイッチは、その送信元 MAC アドレス（MAC_SOURCE とします）を分析し、MAC_SOURCE 宛のパケットが、ポート A 経由で転送可能なものかどうかを判断します。MAC_SOURCE が MAC アドレステーブルに含まれていれば、スイッチは対応するエントリを更新し、含まれていなければ、その新しい MAC アドレス（および対応する転送ポート）を新しいエントリとしてテーブルに追加します。

MAC アドレステーブルに宛先アドレスがあるパケットはハードウェアから直接転送され、同テーブルに宛先アドレスがないパケットはブロードキャストされます。ブロードキャストパケットを受信したネットワークデバイスは、自身の MAC アドレス付きで応答しますが、この MAC アドレスをスイッチが学習し、保持している MAC アドレステーブルに追加します。その結果、以後の同一アドレス宛のパケットは、直接転送されることになります。ブロードキャスト後も MAC アドレスが見つからないパケットはドロップされ、宛先に到達不可能であることが送信側に通知されます。

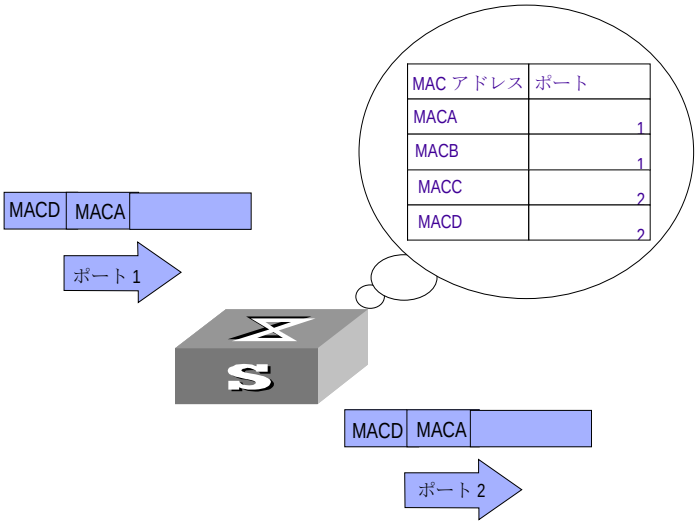


図1-1 MAC アドレステーブルを使用した、Ethernet スイッチによるパケットの転送

Ethernet スイッチには、MAC アドレスエージングの機能もあり、一定の時間、パケットが受信されないと、関連するエントリが MAC アドレステーブルから削除されます。ただし、この機能は、スタティック MAC アドレスには適用されません。

MAC アドレスエントリは、実際のネットワーキング環境に応じて、手動で設定（追加または変更）できます。スタティックエントリもダイナミックエントリも、その対象となります。

1.2 MACアドレスの設定

MAC アドレスの設定は以下のとおりです。

- MAC アドレスエントリの設定
- MAC アドレスエージングタイムの設定
- MAC アドレス学習の設定

1.2.1 MACアドレスエントリの設定

管理者は、必要に応じて、MAC アドレステーブルのエントリを、手動で追加、変更、削除できます。 また、指定のポートに関連付けられたすべての（ユニキャスト）MAC アドレステーブルエントリを削除したり、ダイナミックエントリやスタティックエントリなど指定のタイプのエントリを削除することもできます。

MAC アドレステーブルのエントリを、手動で追加、変更または削除するには、System view で以下のコマンドを実行します。

表1-1 MAC アドレスエントリの設定

操作	コマンド
アドレスエントリを追加/変更する	**mac-address static** *mac-addr* **vlan** *vlan-id* [**interface** *interface-type interface-number*]
アドレスエントリを削除する	**undo mac-address static** *mac-addr* **vlan** *vlan-id* [**interface** *interface-type interface-number*]

⚠ **注意**：

- スタティック MAC アドレス設定は、Port isolate 機能、セキュリティ MAC アドレス設定、リンクアグリゲーション機能と同時に使用することはできません。上

記機能が有効な場合は、スタティック MAC アドレス設定が排他状態となるため、コンフィグに表示されません。

1.2.2 MACアドレスエージングタイムの設定

適切なエージング時間を設定すると、MAC アドレスエージングの機能を効果的に実現できます。加入者がエージング時間を長く設定し過ぎたり、逆に短く設定し過ぎると、Ethernet スイッチから MAC アドレスなしの多量のデータパケットがブロードキャストされることになり、スイッチの動作パフォーマンスに影響を与えます。

エージング時間を長く設定し過ぎると、Ethernet スイッチに、データなしの MAC アドレステーブルが多量に格納されます。こうなると、MAC アドレステーブルのリソースが消費され、スイッチはネットワークの変化に応じた MAC アドレスの更新ができなくなります。

エージング時間を短く設定し過ぎると、Ethernet スイッチから有効なアドレステーブルが削除される場合があります。

システムの MAC アドレスエージング時間を設定するには、System view で以下のコマンドを実行します。

表1-2 MAC アドレスエージングタイムの設定

操作	コマンド
ダイナミックMACアドレスエージング時間を設定する	**mac-address time** { **aging** *age* | **no-aging** }
ダイナミックMACアドレスエージング時間をデフォルトに戻す	**undo mac-address time aging**

このコマンドは、すべてのポートを実行対象としますが、 アドレスエージングは、ダイナミックアドレス（学習済みエントリ）のみが対象となります。

デフォルト値：aging-time は、5 分です。no-aging パラメータを指定すると、アドレスエントリに対して MAC エージングが実行されなくなります。

1.2.3 MAC学習の設定

MAC 学習の有効/無効を設定するには、Ethernet port view から以下のコマンドを実行します。

表1-3 MAC 学習の設定

操作	コマンド
MAC学習を有効に設定する	**mac address learning {** *<cr>* **| secure}**
MAC学習を無効に設定する	**undo mac address learning**

1.2.4 MACアドレステーブルのクリア

装置の MAC アドレステーブルをクリアします、User view から以下のコマンドを実行します。

操作	コマンド
装置のMACアドレステーブルをクリアする	**reset mac-address**

1.3 MACアドレステーブルの表示

すべての view で **display** コマンドを実行すると、MAC アドレステーブル設定の実行状況を表示し、設定を確認できます。

表1-4 MAC アドレステーブルの表示

操作	コマンド
アドレステーブルの情報を表示する	**display mac-address** [*mac-addr* | **static** | **dynamic** | [**interface** *interface-type interface-number*] | [**vlan** *vlan-id*] | **count**]

目次

このセクションのページは **6-x-x** です。

2 章 ポートセキュリティ 2-1

2.1 ポートセキュリティの概要 2-1

2.2 ポートセキュリティの設定 2-1

2.2.1 インターフェースでポートセキュリティを有効にする 2-1

2.2.2 インターフェースでセキュア MAC アドレスを設定する 2-2

2.2.3 ポートセキュリティエージングの設定 2-2

2.2.4 エージングタイムの設定 2-3

2.2.5 ホールドタイムの設定 2-3

2.2.6 セキュア MAC アドレスの最大値の設定 2-3

2.2.7 違反 MAC アドレス数の最大値の設定 2-4

2.2.8 セキュリティ違反モード違反した場合のアクションの設定 2-4

2.2.9 セキュア MAC アドレスの削除 2-4

2.3 ポートセキュリティの状態の表示 2-5

2.4 ポートセキュリティの設定例 2-5

2章 ポートセキュリティ

2.1 ポートセキュリティの概要

ポートセキュリティ機能はインターフェースに接続し通信することのできる端末機器の MAC アドレスを予めセキュリティ MAC アドレスとして登録しておき、セキュリティ MAC アドレス以外の MAC アドレスを持つ端末機器が接続された場合、その端末機器による通信を遮断します。すなわち、許可された端末のみネットワークへの接続が許可されるため、容易にセキュリティ性を高めることが可能となります。

本機能により接続許可されていない端末機器が接続されてもその端末からの通信はサイレントに廃棄します。（違反通信についてのログや TRAP 通知はサポートしていません）

2.2 ポートセキュリティの設定

ポートセキュリティ機能を設定するには以下の順番で設定を行う必要があります。順番通りに設定しなかった場合、以降のコマンド設定がエラーとなります。

- インターフェースでポートセキュリティを有効にする
- ポートセキュリティエージングの設定
- エージングタイムの設定
- ホールドタイムの設定
- セキュア MAC アドレスの最大値の設定
- 違反 MAC アドレス数の最大値の設定
- セキュリティ違反モードを違反した場合のアクション
- セキュア MAC アドレスの削除

2.2.1 インターフェースでポートセキュリティを有効にする

該当インターフェースでポートセキュリティ機能を有効にします。

Ethernet port view で、以下のコマンドを実行します。

表2-1 インターフェースでポートセキュリティを有効/無効にする

操作	コマンド
ポートセキュリティを該当インターフェースで有効にする	**port-security**
上記を無効にする	**undo port-security**

デフォルト：無効

2.2.2 インターフェースでセキュアMACアドレスを設定する

インターフェースでセキュア MAC アドレスを指定するには、Ethernet port view から以下のコマンドを実行します。

セキュリティ MAC アドレスはインターフェース当たり最大 1023 個まで設定することができます。装置当たりでは最大 1024 個まで設定することができます。

表2-2 セキュリティ MAC アドレスを設定する

操作	コマンド
セキュアMACアドレスを指定する	**port-security mac-address** { [**sticky**] [*mac* [**vlan** *vlan_id*]] }
セキュアMACアドレスを無効にする	**undo port-security mac-address { [sticky] [** *mac* **[vlan** *vlan_id* **]] }**

2.2.3 ポートセキュリティエージングの設定

ポートセキュリティエージングの有効/無効を設定するには、System view から以下のコマンドを実行します。

表2-3 ポートセキュリティエージングを設定する

操作	コマンド
ポートセキュリティエージングを有効にする	**port-security aging**
ポートセキュリティエージングを無効にする	**undo port-security aging**

2.2.4 エージングタイムの設定

エージングタイムを設定するには、System view から以下のコマンドを実行します。

表2-4 システムでエージングタイムを設定する

操作	コマンド
エージングタイムを設定する	**port-security aging time** *aging_time*
エージングタイムをデフォルトに戻す	**undo port-security aging time**

デフォルト：3600

2.2.5 ホールドタイムの設定

ホールドタイムを設定するには、System view から以下のコマンドを設定します。

表2-5 ホールドタイムの設定

操作	コマンド
ホールドタイムを設定する	**port-security hold time** *hold_time*
ホールドタイムをデフォルトに戻す	**undo port-security hold time**

デフォルト：300

2.2.6 セキュアMACアドレスの最大値の設定

セキュア MAC アドレスを設定するには、Ethernet port view から以下のコマンドを実行します。

表2-6 セキュア MAC アドレスの最大値を設定する

操作	コマンド
セキュアMACアドレスの最大値を設定する	**port-security maximum** *limit*
セキュアMACアドレスの最大値をデフォルトに戻す	**undo port-security maximum**

デフォルト：4

2.2.7 違反MACアドレス数の最大値の設定

違反 MAC アドレス数の最大値を設定するには、Ethernet port view　から以下のコマンドを実行します。

表2-7 違反 MAC アドレスの最大値を設定する

操作	コマンド
違反MACアドレスの最大値を設定する	**port-security maximum-violation** *violate_limit*
違反MACアドレスの最大値をデフォルトに戻す	**undo port-security maximum-violation**

デフォルト：4

2.2.8 セキュリティ違反モード違反した場合のアクションの設定

セキュリティ違反モードを違反した場合のアクションを設定するには、Ethernet port view　から以下のコマンドを実行します。

表2-8 セキュリティ違反モード違反時に実行するアクションを設定する

操作	コマンド
セキュリティ違反モード違反した場合に実行するアクションの設定	**port-security violation { protect | restrict | shutdown }**
実行するアクションをデフォルトに戻す	**undo port-security violation**

デフォルト：protect

2.2.9 セキュアMACアドレスの削除

セキュア MAC アドレスを削除します。User view から以下のコマンドを実行します。

表2-9 セキュア MAC アドレスの削除

操作	コマンド
セキュアMACアドレスを削除する	**reset port-security**

2.3 ポートセキュリティの状態の表示

display コマンドを実行して、ポートセキュリティの設定状態および、装置で登録されているセキュリティ MAC アドレスを確認することができます。

表2-10 ポートセキュリティの状態を表示する

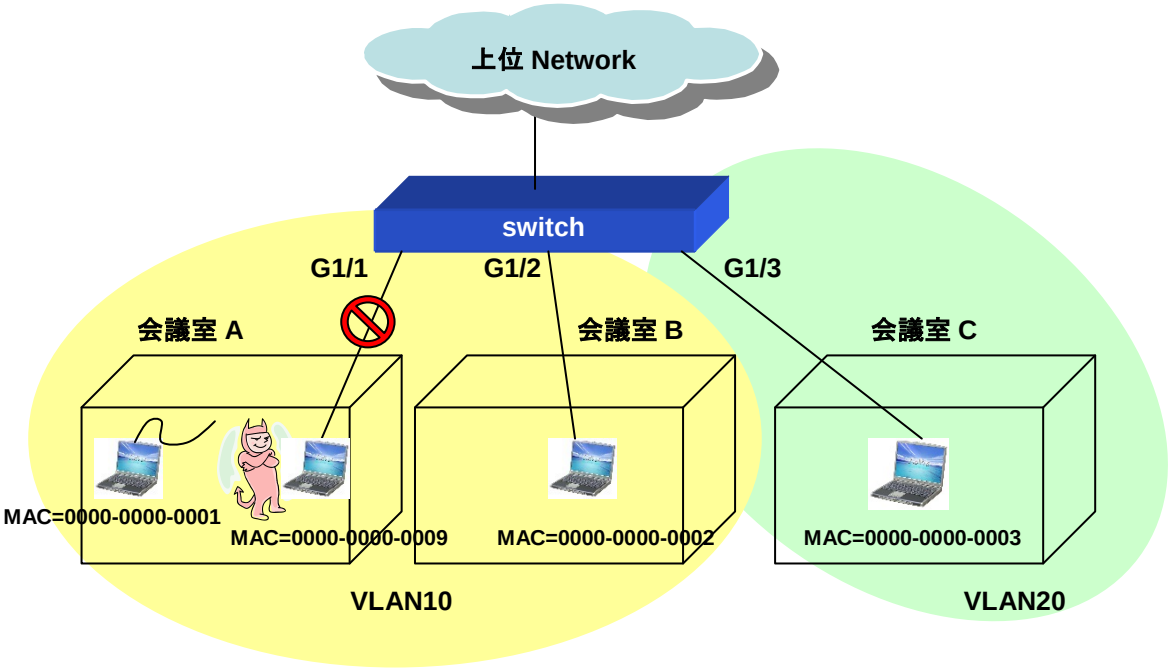
操作	コマンド
ポートセキュリティの設定情報を表示する	**display port-security**
セキュリティMACアドレスを表示する	**display port-security address [interface *interface-num*]**

2.4 ポートセキュリティの設定例

I. ネットワーキング要件

会議室 A、会議室 B は VLAN10、会議室 C は VLAN20 に属しています。会議室 A で接続可能な機器は MAC アドレス=0000-0000-0001 を持つ機器のみ許可しそれ以外の機器が接続された場合は装置へのアクセスを禁止します。同様に会議室 B では MAC アドレス=0000-0000-0002 の機器のみ、会議室 C では MAC アドレス=0000-0000-0003 を持つ機器のみ許可します。

II.　ネットワークダイアグラム



III.　設定手順

VLAN10、 20 を登録します

```
[switch]vlan 10
[switch-vlan10]vlan 20
[switch-vlan20]quit
```

G1/1、G1/2 ポートを VLAN10 に、G1/3 を VLAN20 に所属させます

```
[switch]interface GigabitEthernet 1/1
[switch-GigabitEthernet1/1]port access vlan 10
[switch-GigabitEthernet1/1]quit
[switch]interface GigabitEthernet 1/2
[switch-GigabitEthernet1/2]port access vlan 10
[switch-GigabitEthernet1/2]quit
[switch]interface GigabitEthernet 1/3
[switch- GigabitEthernet 1/3] port access vlan 20
[switch- GigabitEthernet 1/3] quit
```

各ポートでポートセキュリティを有効にし、接続許可する MAC アドレス(セキュリティ MAC アドレス)を設定します。

(GigabitEthernet 1/1 ポートで接続許可する MAC アドレスを 00-00-00-00-00-01、GigabitEthernet 1/2 ポートで接続許可する MAC アドレスを 00-00-00-00-00-02、GigabitEthernet 1/3 ポートで接続許可する MAC アドレスを 00-00-00-00-00-03)

```
[switch]interface GigabitEthernet 1/1
[switch-GigabitEthernet 1/1]port-security
[switch-GigabitEthernet 1/1]port-security mac-address 00-00-00-00-00-01 vlan 10
[switch-GigabitEthernet 1/1]quit
[switch]interface GigabitEthernet 1/2
[switch-GigabitEthernet 1/2]port-security
[switch-GigabitEthernet 1/2]port-security mac-address 00-00-00-00-00-02 vlan 10
[switch-GigabitEthernet 1/2]quit
[switch]interface GigabitEthernet 1/3
[switch-GigabitEthernet 1/3]port-security
[switch-GigabitEthernet 1/3]port-security mac-address 00-00-00-00-00-03 vlan 20
[switch-GigabitEthernet 1/3]quit
```

QX-S700G シリーズ Ethernet PoE スイッチ

オペレーションマニュアル

7.リモート給電

本マニュアルは以下に示す章で構成されています。

01-リモート給電

目次

このセクションのページは **7-x-x** です。

1 章 リモート給電 1-1

1.1 リモート給電の概要 1-1

1.2 サポートするリモート給電機能 1-1

1.3 リモート給電の設定 1-2

1.3.1 リモート給電の有効/無効 1-2

1.3.2 装置最大給電電力の設定 1-3

1.3.3 電源管理モードの設定 1-3

1.3.4 ポートの給電プライオリティの設定 1-4

1.3.5 レガシーPoE 装置への給電許可設定 1-4

1.3.6 Underload の検出時間の延長設定 1-5

1.3.7 再起動中の PoE 給電状態の設定 1-5

1.4 リモート給電状態の表示 1-6

1.5 リモート給電の設定例 1-6

1章 リモート給電

1.1 リモート給電の概要

PoE（Power over Ethernet）機能は、IP 電話端末、WLAN AP、ネットワークカメラなどの PD（Powered Device）に、LAN ケーブルを介して-48VDC 電源を供給します。

1.2 サポートするリモート給電機能

QX-S700G シリーズでサポートするリモート給電機能は、以下の機能を提供します。

- IEEE802.3af、IEEE802.3at、IEEE802.3bt 準拠の PSE（Power Sourcing Equipment）としての機能を提供します。
- ツイストペアケーブルの信号線 1,2,3,6 を利用して端末に電源供給します。
- アップリンクポート（QX-S708GT-2X-PW はポート 9,10、QX-S716GT-4X-PW はポート 17,18）を除いた Ethernet ポートより給電可能です。
- 各 Ethernet ポートからは、最大 60W の電力を供給することができます。許容ケーブル長は、最大 100m です。
- 装置全体として、以下の給電を行うことができます。新規でリモート PD を検出した際に、その PD に対する給電を開始するかは、供給可能な電力を算出して決めています。

製品名	最大給電電力
QX-S708GT-2X-PW	180[W]
QX-S716GT-4X-PW	360[W]

- 各 Ethernet ポート単位もしくは装置全体の PoE 給電に関する設定を行うことが可能です。設定内容は display コマンドにより確認することができます。
- 供給電力値がフルロード状態（実際の供給電力が装置の最大供給電力に達した状態）になった際、auto と manual のいずれかの方法で給電状態を制御することが可能です。
- 供給電力値により、装置内部温度が異常上昇して不測の事態が発生するのを防止する為の保護機能を持っています。装置内部温度が、QX-S708GT-2X-PW では閾値温度 68℃、QX-S716GT-4X-PW では閾値温度 63℃を超えた場合、

全ての Ethernet ポートの給電を停止します。装置内部温度が閾値温度より5℃以下にまで下がった場合、Ethernet ポートの給電を再開します。

- 保証余力電力値は装置・クラスとは無関係に"給電要求電力+2W"です。
- PoE 給電のガードバンド値は PD のクラスにより異なり、クラス別のガードバンド値は下記となります。

Class	ガードバンド値
0	15.4[W]
1	4.0[W]
2	7.0[W]
3	15.4[W]
4	30.0[W]
5	45.0[W]
6	60.0[W]

1.3 リモート給電の設定

リモート給電の設定は以下のとおりです。

- リモート給電の有効/無効
- 装置最大給電電力の設定
- 電源管理モードの設定
- ポートの給電プライオリティの設定
- レガシーPoE 装置への給電許可設定
- Underload の検出時間の延長設定
- Underload の検出時間の設定
- 再起動中の PoE 給電状態の設定

1.3.1 リモート給電の有効/無効

装置全体または、ポート単位でリモート給電の有効/無効を設定するには、System view または、Ethernet port view で以下のコマンドを実行します。

表1-1 リモート給電の有効/無効

操作	コマンド
リモート給電を有効にする	**poe enable**
リモート給電を無効にする	**undo poe enable**

デフォルト:有効

1.3.2 装置最大給電電力の設定

装置最大電力の設定には、system view で以下のコマンドを実行します。

表1-2 装置最大給電電力の設定

操作	コマンド
最大電力の設定する	**poe max-power *max-power***
最大電力をデフォルトに戻す	**undo poe max-power**

max-power の設定値:QX-S708GT-2X-PW は 5000～180000mW、QX-S716GT-4X-PW は 5000～360000mW

デフォルト:QX-S708GT-2X-PW は 180000mW、QX-S716GT-4X-PW は 360000mW

1.3.3 電源管理モードの設定

QX-S700G シリーズでは､QX-S708GT-2X-PW の場合 180W､QX-S716GT-4X-PW の場合 360W のリモート給電を行うことができます。

デフォルトでは、PD が新しく接続されても最大電力以上は供給しません。

本コマンドは、スイッチのポートの poe プライオリティと共に使用します。給電がフルロード（全負荷）になると有効になります。

auto: 給電がフルロードになると、スイッチは、"low"プライオリティのポートに接続された PD より先に、" high" プライオリティのポートに接続された PD に電源を供給します。例えば、給電がフルロードのときに" high " プライオリティのポート A に新しい PD が接続されたとします。この場合、"low"プライオリティのポートに接続されている PD への給電を自動的に停止し、ポート A の新しい PD に給電を開始します。

manual: 給電がフルロードになると、スイッチに新しい PD が接続されると新しい PD には給電されません。給電中にフルロードを超えると、給電されている老番ポートの PD への給電が停止します。例えば、ポート 1 とポート 8 に PD が接続されています。給電がフルロードを超えたときに、老番ポート 8 の PD への給電が停止します。

電源管理モードを設定するには、system view で以下のコマンドを実行します。

表1-3 電源管理モードの設定

操作	コマンド
電源管理モードをautoに設定する	**poe power-management [auto | manual]**
電源管理モードをデフォルトに戻す	**undo poe power-management**

デフォルト:auto

1.3.4 ポートの給電プライオリティの設定

ポートの給電プライオリティを設定するには、Ethernet port view で以下のコマンドを実行します。

表1-4 ポートの給電プライオリティの設定

操作	コマンド
ポートの給電プライオリティを設定する	**poe priority { high | low }**
ポートの給電プライオリティをデフォルトに戻す	**undo poe priority**

デフォルト:low

1.3.5 レガシーPoE装置への給電許可設定

レガシーPoE 装置に対して、給電を許可する設定は、System view で以下のコマンドを実行します。

表1-5 レガシーPoE 装置への給電許可設定

操作	コマンド
レガシーPoE装置へ給電を許可する。	**poe legacy**
レガシーPoE装置へ給電を許可しない。	**undo poe legacy**

デフォルト: レガシーPoE 装置へ給電を許可しない。

1.3.6 Underloadの検出時間の延長設定

Underload による検出時間を IEEE802.3at 規格内の 400ms から 508ms に延長するには、System view で以下のコマンドを実行します。

表1-6 Underload の検出時間の延長の設定

操作	コマンド
Underloadの検出時間を延長する。	**poe underload dropout-time extend enable**
Underloadの検出時間を戻す。	**undo poe underload dropout-time extend enable**

デフォルト: IEEE802.3at 規格内の 400ms

1.3.7 再起動中のPoE給電状態の設定

ソフトウェアリブート時に PoE の給電状態を維持する設定ができます。

system-view より以下のコマンドを実行します。

表1-7 再起動中の PoE 給電状態の設定

操作	コマンド
再起動中もPoE給電状態を維持する。	**poe non-stop enable**
再起動中はPoE給電しない	**undo poe non-stop enable**

デフォルト：再起動中も PoE 給電状態を維持する。

メモ：

装置再起動中は、給電状態の LED 表示を行いませんが、給電状態は維持されます。

1.4 リモート給電状態の表示

display コマンドを実行すると、リモート給電設定の実行状況を表示し、設定を確認できます。

表1-8 リモート給電状態の表示

操作	コマンド
指定ポートまたは全ポートのリモート給電状態を表示する	**display poe interface** [*interface-type interface-number*]
指定ポートまたは全ポートの電源を表示する	**display poe interface power** [*interface-type interface-number*]
PSEのPoEパラメータを表示する	**display poe pse**

1.5 リモート給電の設定例

I. ネットワーク要件

Ethernet1/1 はスイッチ A に、Ethernet1/2 は AP（Access Point）に接続しています。そして Ethernet1/8 は重要な AP が接続しているとします。

接続している装置に対して電源を供給します。QX-S716GT-4X-PW の電源供給がフル（全負荷）になっても、Ethernet1/8 に接続された PD は優先的に給電されるようにします。

II.　ネットワークダイアグラム

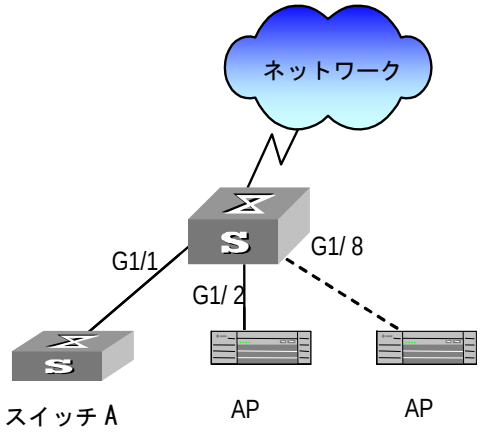


図1-1 リモート給電の設定例

III.　設定手順

GigabitEthernet1/8 の給電プライオリティを high に設定し、その PD への給電を優先します。

```
[switch-GigabitEthernet1/8]poe priority high
```

#電源管理モードを auto に設定します。

```
[switch]poe power-management auto
```

QX-S700G シリーズ Ethernet PoE スイッチ

オペレーションマニュアル

8.PTP

本マニュアルは以下に示す章で構成されています。

01-PTP

目次

このセクションのページは **8-x-x** です。

1 章 PTP 1-1

1.1 PTP の概要 1-1

1.1.1 伝送遅延の計測方法 1-2

1.1.2 送信時刻の通知方法 1-2

1.1.3 サポート機能 1-2

1.1.4 E2E-TC の動作 1-3

1.1.5 P2P-TC の動作 1-4

1.2 PTP の設定 1-5

1.2.1 クロックタイプの設定 1-5

1.2.2 PTP 機能の有効/無効の設定 1-6

1.2.3 遅延の非対称性の設定 1-6

1.2.4 Pdelay-Req フレームの送信間隔の設定 1-6

1.3 PTP の表示 1-7

1.4 PTP の設定例 1-7

1章 PTP

1.1 PTPの概要

PTP(Precision Time Protocol)機能は、IEEE 1588 で規格されている、ネットワークのクロック同期機能です。イーサネットでの利用に特化し，NTP（最大数ミリ秒）よりも高精度（最大数百ナノ秒）で同期させることを目的としています。当スイッチは IEEE1588v2 TC モードに対応します。

PTP では，マスタ装置とスレーブ装置の間でパケットが中継される時間（以降，伝送遅延時間）を測定し，送信されたマスタ装置の時刻情報と伝送遅延時間によって，時刻を同期します。PTP での各装置の役割について次の表に示します。

表1-1 PTP での各装置の役割

PTP 装置の種別	説明
マスタ装置	基準時刻を配信する装置
スレーブ装置	マスタ装置から受信した基準時刻に同期する装置
Transparent Clock（TC）	伝送遅延時間を計算するための PTP メッセージを中継する装置
Management Node（MN）	リモート制御装置

本装置は TC として動作します。

PTP 装置は，PTP 専用 VLAN によって時刻を同期します。PTP の適用例を次の図に示します。

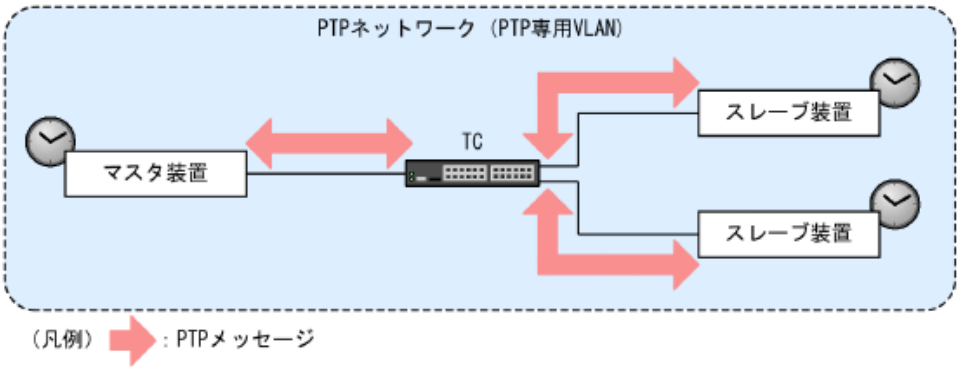


図1-1 PTP の適用例

1.1.1 伝送遅延の計測方法

PTP の伝送遅延時間の計測方法には，E2E（end-to-end）と P2P（peer-to-peer）があります。E2E と P2P の特長を次の表に示します。

表1-2 E2E と P2P の特長

項目	E2E	P2P
伝送遅延時間計測単位	マスタ装置とスレーブ装置間で伝送遅延時間を計測	マスタ装置・スレーブ装置・TC の各装置で隣接装置との伝送遅延時間を計測
PTP 未サポート装置との接続可否	接続できる	接続できない
中継段数による同期精度の劣化	劣化が大きい	劣化が小さい
スレーブ装置数によるマスタ装置への処理負荷	影響が大きい	影響が小さい

1.1.2 送信時刻の通知方法

PTP では，伝送遅延時間を計測するために，PTP メッセージを送信した時刻（送信時刻）を使用します。

送信時刻の通知方法には，One-step clock，Two-step clock の 2 種類があります。

表1-3 送信時刻の通知方法

送信時刻の通知方法	概要
One-step clock	一つのメッセージによって送信時刻を通知する方法です。
Two-step clock	二つのメッセージによって送信時刻を通知する方法です。

1.1.3 サポート機能

本装置がサポートする PTP 機能を下表に示します。

表1-4 サポート機能

項目			内容
PTP サポートバージョン			IEEE 1588v2
PTP 装置種別	マスタ装置		×
	スレーブ装置		×
	TC	E2E-TC	○
		P2P-TC	○
送信時刻通知方法	E2E	One-step clock	○
		Two-step clock	○

1.1.4 E2E-TC の動作

E2E-TC 機能は下記の処理を行います。

・すべての PTP バージョン 2 メッセージは、MAC/IP アドレスに従って転送します。

・Sync メッセージを転送するとき、ResidenceTime を Sync メッセージの CorrectField に追加します。

・Delay_Request メッセージを転送するとき、ResidenceTime を Delay_Request メッセージの CorrectField に追加します。

・Slave クロックに対して Offset の値は、<Offset>＝[(t2 - t1)－(t4 - t3)]/2 として計算されます。

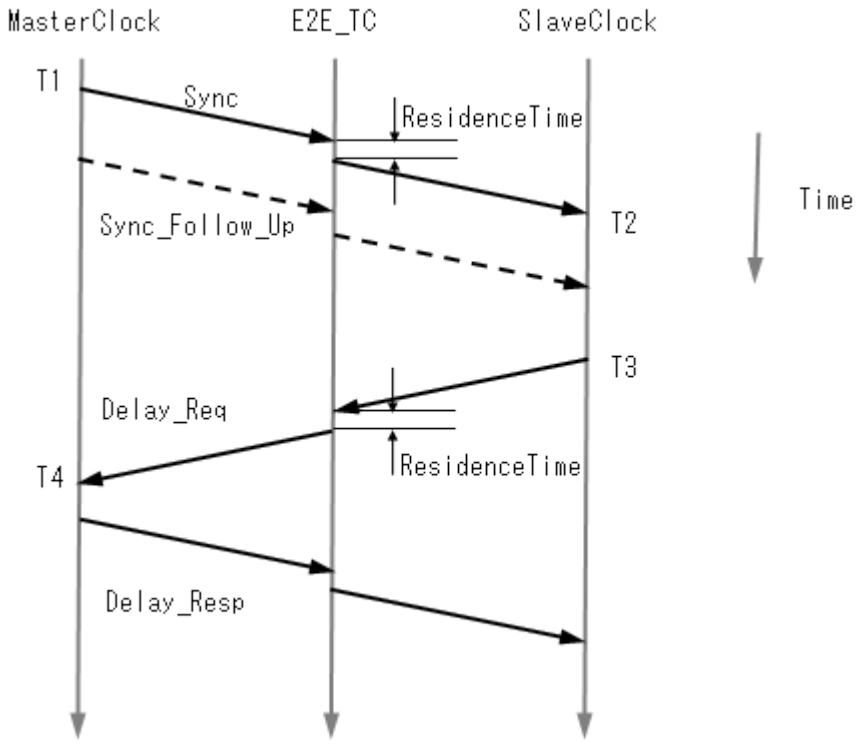


図1-2 E2E-TC の動作

1.1.5 P2P-TC の動作

P2P-TC 機能は下記の処理を行います。

・PTP バージョン 2 の Announce、Sync、Follow_Up、Management および Signaling メッセージは、MAC/IP アドレスに従って転送します。

・PTP バージョン 2 の Delay_Req および Delay_Resp メッセージは破棄します。

・MeanPathDelay の値は、<meanPathDelay> = [(t2 - t1) + (t4 - t3)]/2 として計算されます。

・Sync メッセージを転送するとき、MeanPathDelay と ResidenceTim を Sync メッセージの CorrectField に追加します。

・Pdelay_Req メッセージは PTP_TC の全ポートに定期的に送信します。

・Pdelay_Req メッセージを受信するとき、該当ポートに Pdelay_Resp メッセージを返信します。

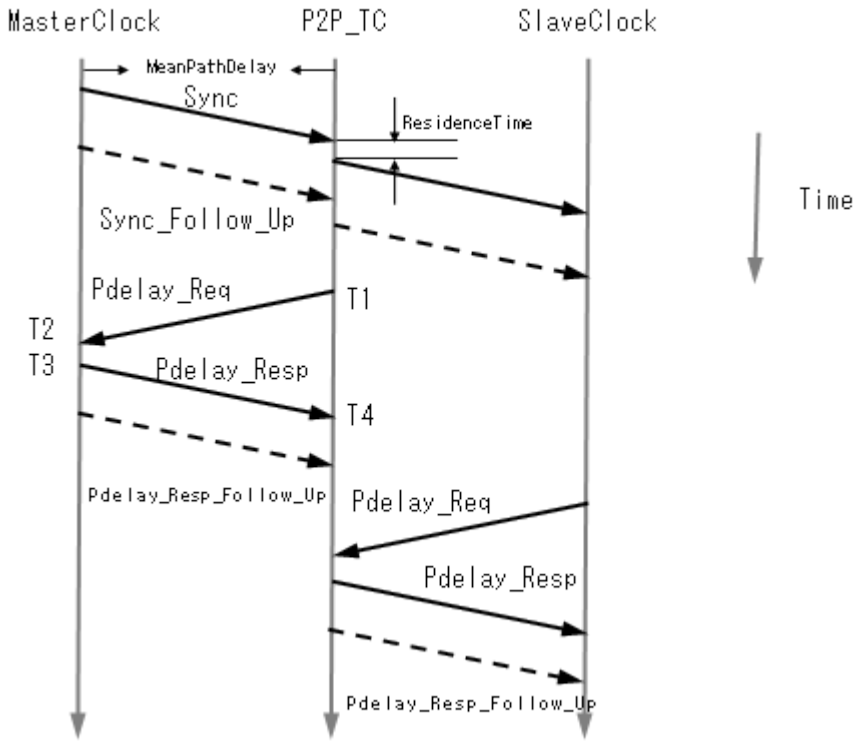


図1-3 P2P-TC の動作

1.2 PTPの設定

⚠ **注意：**

ミラーリング機能と PTP 機能を併用するとき、ミラーリング機能で PTP パケットはキャプチャされません。

1.2.1 クロックタイプの設定

クロックタイプの設定をするには、System view で以下のコマンドを実行します。

表1-5 PTP 動作の詳細設定

操作	コマンド
クロックタイプの設定をする	**ptp mode { e2etransparent { onestep | twostep } { ethernet | ipv4 } | p2ptransparent { onestep | twostep }**

操作	コマンド
	{ ethernet | ipv4 } domain *number* }
クロックタイプをデフォルトに戻す	**undo ptp mode**

デフォルト：設定なし

1.2.2 PTP 機能の有効/無効の設定

指定したポートで PTP 機能を有効にするには、Ethernet port view で以下のコマンドを設定します。

表1-6 PTP 機能の有効/無効設定

操作	コマンド
PTP機能を有効にする。	**ptp enable**
PTP機能を無効にする。	**undo ptp enable**

デフォルト：無効

1.2.3 遅延の非対称性の設定

PTP 機能を有効にしたポートで、遅延の非対称性を補正するには、Ethernet port view で以下のコマンドを設定します。

表1-7 遅延の非対称性補修の設定

操作	コマンド
遅延の非対称性補正を設定する	**ptp delay-asymmetry** *value*
遅延の非対称性補正をデフォルトに戻す	**undo ptp delay-asymmetry**

デフォルト：0

1.2.4 Pdelay-Req フレームの送信間隔の設定

Pdelay-Req フレームの送信間隔を設定するには、Ethernet port view で以下のコマンドを実行します。

表1-8 Pdelay-Req フレームの送信間隔の設定

操作	コマンド
Pdelay-Reqフレームの送信間隔を設定する。	**ptp pdelay-req interval** *value*
Pdelay-Reqの送信間隔をデフォルトに戻す。	**undo ptp pdelay-req interval**

デフォルト：0

1.3 PTPの表示

設定終了後、display コマンドを実行すると、PTP 機能の設定内容や状態を確認できます。

表1-9 PTP 機能の状態表示

操作	コマンド
PTP機能の設定情報を表示する	**display ptp default**
ポートステータス情報を表示する	**display ptp port-status**
PTPフレームの送受信カウンタを表示する	**display ptp port-statistics**

1.4 PTPの設定例

PTP 機能の設定例を下記に示します。

1) モードの詳細設定をします。
2) GigabitEthernet ポート 2 を有効に設定します。

#モードの詳細設定をする(Onestep,E2E,Ethernet)

[QX-S708GT-2X-PW]ptp mode e2etransparent onestep ethernet

#Ethernet port view に入り、GigabitEthernet ポート 2 を有効にする

[QX-S708GT-2X-PW-GigabitEthernet1/1]interface GigabitEthernet 1/2

[QX-S708GT-2X-PW-GigabitEthernet1/2]ptp enable

[QX-S708GT-2X-PW-GigabitEthernet1/2]quit

[QX-S708GT-2X-PW]

QX-S700G シリーズ Ethernet PoE スイッチ

オペレーションマニュアル

9.セキュリティ

本マニュアルは以下に示す章で構成されています。

01-AAA、RADIUS および TACACS+プロトコルの設定

02-802.1X の設定

目次

このセクションのページは **9-x-x** です。

1 章 AAA、RADIUS および TACACS+プロトコルの設定 1-1

1.1 AAA と RADIUS および TACACS+プロトコルの概要 1-1

1.1.1 AAA の概要 1-1

1.1.2 RADIUS プロトコルの概要 1-1

1.1.3 TACACS+プロトコルの概要 1-2

1.2 AAA の設定 1-2

1.2.1 認証方式の設定 1-2

1.2.2 TACACS+アカウンティングの設定 1-3

1.2.3 TACACS+認可の設定 1-3

1.3 RADIUS プロトコルの設定 1-5

1.3.1 NAS ID の設定 1-5

1.3.2 NAS IP アドレスの設定 1-6

1.3.3 デッドタイムの設定 1-6

1.3.4 RADIUS サーバの設定 1-6

1.3.5 RADIUS コミュニケーションのキーの設定 1-7

1.3.6 リトライ回数の設定 1-7

1.3.7 タイムアウト時間の設定 1-7

1.4 TACACS+プロトコルの設定 1-8

1.4.1 デッドタイムの設定 1-8

1.4.2 TACACS+サーバの設定 1-8

1.4.3 TACACS+コミュニケーションのキーの設定 1-9

1.4.4 タイムアウト時間の設定 1-9

1.5 AAA、RADIUS および TACACS+プロトコルの表示 1-10

1章 AAA、RADIUS および TACACS+プロトコルの設定

1.1 AAAとRADIUSおよびTACACS+プロトコルの概要

1.1.1 AAAの概要

認証(Authentication)、認可(Authorization)、および課金(Accounting)という 3 つのセキュリティ機能を使用して、全般的なフレームワークを提供するのが AAA です。AAA を設定することは、ネットワークセキュリティを管理することと同義です。

ネットワークセキュリティとは、アクセス制御を示し、以下の項目が含まれます。

- ネットワークサーバにアクセス可能なユーザ
- アクセス認可を受けているユーザが提供されるサービス
- ネットワークリソースを使用するユーザの課金

AAA では、以下のサービスを実現します。

- ユーザがアクセスの権利を持つかどうかを認証する(認証)
- ユーザに一定のタイプのサービスを認可する(認可)
- ユーザのネットワークリソース使用についての情報を記録する(課金)

1.1.2 RADIUSプロトコルの概要

I. RADIUS とは

RADIUS(Remote Authentication Dial-In User Service)とは、クライアント/サーバアーキテクチャでの分散情報スイッチングプロトコルの一種です。RADIUS は、ネットワークへの無認可のアクセスを防ぎ、高いセキュリティとリモートユーザアクセスの両方が必要なネットワーク環境でよく使用されます。たとえば、シリアルポートとモデムを使用して各地に散らばっている多数のダイアルインユーザを管理するために使用されることがあります。RADIUS システムは、ネットワークアクセスサーバ(NAS)の重要な付属要素です。

ユーザが、ほかのネットワークにアクセスする権利、または NAS(PSTN 環境ではダイアルインアクセスサーバ、Ethernet 環境ではアクセス機能のある装置)への接続を通じてネットワークリソースを利用する権利を要求すると、NAS（つまり RADIUS クライアントエンド）はユーザ AAA 要求を RADIUS サーバに送信します。RADIUS サーバには、ユーザ認証とネットワークサービスへのアクセスのす

べての情報を記録するユーザデータベースがあります。NAS からユーザの要求を受信したときに、RADIUS サーバは、このユーザデータベースを照会して AAA を実行し、設定情報と課金データを更新し、NAS に返します。ここで、NAS はユーザおよびそのコネクションを制御し、RADIUS プロトコルは NAS と RADIUS 間で設定情報と課金情報を送信する方法を制御します。

NAS と RADIUS サーバは、UDP パケットで情報を交換します。どちらもユーザ設定情報(パスワードなど)をアップロードする前にパケットを暗号化して、妨害または傍受を防ぎます。

II.　RADIUS の動作

RADIUS サーバはアクセスサーバのようなデバイスのプロキシ機能を使用して、ユーザ認証を実行します。はじめに、ユーザが、クライアントユーザ名と暗号化パスワードを含む要求メッセージを RADIUS サーバに送信します。次に、ユーザは RADIUS サーバから各種の応答メッセージを受信します。ACCEPT メッセージはユーザが認証にパスしたことを示し、REJECT メッセージはユーザが認証にパスせず、ユーザ名とパスワードを再度入力しなければ、アクセスを拒否されることを示します。

1.1.3 TACACS+プロトコルの概要

TACACS+(Terminal Access Controller Access Control System Plus)は、スイッチにアクセスしようとするユーザの検証を集中的に行うセキュリティアプリケーションです。独立したモジュラ型の認証、認可、アカウンティング機能が提供されます。各サービスを固有のデータベースに結合し、デーモンの機能に応じてそのサーバまたはネットワークで使用できる他のサービスを使用できます。

1.2 AAAの設定

AAA の設定では、以下の設定を行います。

- 認証方式の設定
- TACACS+アカウンティングの設定
- TACACS+認可の設定

1.2.1 認証方式の設定

認証方式を設定するには、System view で以下のコマンドを実行します。

表1-1 認証方式の設定

操作	コマンド
指定した認証方式を設定する	**aaa authentication login { console | telnet | ssh | http } { { local | radius | tacacs } [{ local | radius | tacacs } [{ local | radius | tacacs }]] }**
指定した認証方式をデフォルトに戻す	undo **aaa authentication login { console | telnet | ssh | http }**

デフォルト：local

1.2.2 TACACS+アカウンティングの設定

TACACS+アカウンティングを設定するには、System view で、以下のコマンドを実行します。

表1-2 TACACS+アカウンティングの有効/無効の設定

操作	コマンド
TACACS+アカウンティングを設定する	**aaa accounting { console | telnet | ssh } tacacs { [commands] [exec] }**
TACACS+アカウンティングをデフォルトに戻す	**undo aaa accounting { console | telnet | ssh }**

デフォルト：undo, commands disabled, exec disabled

1.2.3 TACACS+認可の設定

TACACS+認可を設定にするには、System view で以下のコマンドを実行します。

表1-3 認証方式の有効/無効の設定

操作	コマンド
TACACS+認可を有効にする	**aaa authorization { console | telnet | ssh } tacacs commands**
TACACS+認可をデフォルトに戻す	**undo aaa authorization { console | telnet | ssh }**

デフォルト：undo, commands disabled

1.3 RADIUSプロトコルの設定

QX-S700G シリーズ GigabitEthernet スイッチでは、RADIUS プロトコルは RADIUS サーバグループごとに設定します。実際のネットワーク環境では、RADIUS サーバグループは独立した RADIUS サーバまたは設定が同じで 2 つの異なる IP アドレスを有するプライマリ/セカンダリ RADIUS サーバのセットにすることができます。したがって、すべての RADIUS サーバグループの属性には、プライマリサーバとセカンダリサーバの IP アドレス、共有キー、およびアクセスブロックタイムなどがあります。

実際には、RADIUS プロトコルの設定では、NAS と RADIUS サーバ間の情報交換に使用する一部の必要なパラメータのみを定義します。これらのパラメータを有効にするには、その view で RADIUS サーバグループを使用する ISP ドメインを設定し、RADIUS AAA スキームを使用するように指定する必要があります。設定コマンドの詳細については、セクション 9 セキュリティ “AAA の設定”を参照してください。

RADIUS プロトコルの設定では、以下の設定を行います。

- NAS ID の設定
- NAS IP アドレスの設定
- デッドタイムの設定
- RADIUS サーバの設定
- RADIUS コミュニケーションキーの設定
- RADIUS 要求パケットのリトライ回数の設定
- タイムアウト時間の設定

上記の設定のうち、RADIUS サーバの IP アドレスの設定は必須です。その他の設定はオプションです。

1.3.1 NAS IDの設定

attribute 32 の NAS ID を設定にするには、System view で以下のコマンドを実行します。

表1-4 NAS ID の設定

操作	コマンド
attribute32のNAS IDを設定する	**radius attribute 32** *id*
attribute32のNAS IDをデフォルトに戻す	**undo radius attribute 32**

デフォルト：設定なし

1.3.2 NAS IPアドレスの設定

attribute 4 の NAS ID アドレスを設定にするには、System view で以下のコマンドを実行します。

表1-5 NAS IP アドレスの設定

操作	コマンド
NAS IPアドレスを設定する	**radius attribute 4** *ipv4*
NAS IPアドレスをデフォルトに戻す	**undo radius attribute 4**

デフォルト：設定なし

1.3.3 デッドタイムの設定

デッドタイムを設定にするには、System view で以下のコマンドを実行します。

表1-6 デッドタイムの設定

操作	コマンド
デッドタイムを設定する	**radius deadtime** *minutes*
デッドタイムをデフォルトに戻す	**undo radius deadtime**

デフォルト：0

1.3.4 RADIUSサーバの設定

RADIUS サーバのパラメータを設定にするには、System view で以下のコマンドを実行します。

表1-7 RADIUS サーバのパラメータの設定

操作	コマンド
RADIUSサーバのパラメータを設定する	**radius host** *host_name* **[auth-port** *auth_port* **] [acct-port** *acct_port* **] [timeout** *seconds* **] [retransmit** *retries* **] [key**

	{ [unencrypted] *unencrypted_key* **| encrypted** *encrypted_key* **}]**
RADIUSサーバのパラメータを削除する	**undo radius host** *host_name* **[auth-port** *auth_port* **] [acct-port** *acct_port* **]**

1.3.5 RADIUSコミュニケーションのキーの設定

RADIUS コミュニケーションのキーを設定にするには、System view で以下のコマンドを実行します。

表1-8 RADIUS コミュニケーションのキーの設定

操作	コマンド
RADIUSコミュニケーションのキーを設定する	**radius key { [unencrypted]** *unencrypted_key* **| encrypted** *encrypted_key* **}**
RADIUSコミュニケーションのキーを削除する	**undo radius key**

デフォルト：設定なし

1.3.6 リトライ回数の設定

アクティブサーバへのリトライ回数を設定にするには、System view で以下のコマンドを実行します。

表1-9 アクティブサーバへのリトライ回数の設定

操作	コマンド
リトライ回数を設定する	**radius retransmit** *retries*
リトライ回数をデフォルトに戻す	**undo radius retransmit**

デフォルト：3

1.3.7 タイムアウト時間の設定

RADIUS サーバへの応答待機時間を設定にするには、System view で以下のコマンドを実行します。

表1-10 アクティブサーバへのリトライ回数の設定

操作	コマンド
応答待機時間を設定する	**radius timeout** *seconds*
応答待機時間をデフォルトに戻す	**undo radius timeout**

デフォルト：5

1.4 TACACS+プロトコルの設定

TACACS+プロトコルの設定では、以下の設定を行います。

- デッドタイムの設定
- TACACS+サーバの設定
- TACACS+コミュニケーションキーの設定
- タイムアウト時間の設定

1.4.1 デッドタイムの設定

デッドタイムを設定にするには、System view で以下のコマンドを実行します。

表1-11 アクティブサーバへのリトライ回数の設定

操作	コマンド
デッドタイムを設定する	**tacacs-server deadtime** *minutes*
デッドタイムをデフォルトに戻す	**undo tacacs-server deadtime**

デフォルト：0

1.4.2 TACACS+サーバの設定

TACACS+サーバのパラメータを設定にするには、System view で以下のコマンドを実行します。

表1-12 TACACS+サーバのパラメータの設定

操作	コマンド
TACACS+サーバのパラメータを設定する	**tacacs-server host** *host_name* **[port** *port* **]**

	[timeout *seconds* **] [key { [unencrypted]** *unencrypted_key* **| encrypted** *encrypted_key* **}]**
TACACS+サーバのパラメータを削除する	**undo tacacs-server host** *host_name* **[port** *port* **]**

デフォルト：0

1.4.3 TACACS+コミュニケーションのキーの設定

TACACS+コミュニケーションのキーを設定するには、System view で以下のコマンドを実行します。

表1-13 TACACS+コミュニケーションのキーの設定

操作	コマンド
TACACS+コミュニケーションのキーを設定する	**tacacs-server key { [unencrypted]** ***unencrypted_key*** **| encrypted** ***encrypted_key*** **}**
TACACS+コミュニケーションのキーを削除する	**undo tacacs-server key**

デフォルト：設定なし

1.4.4 タイムアウト時間の設定

タイムアウト時間を設定するには、System view で以下のコマンドを実行します。

表1-14 タイムアウト時間の設定

操作	コマンド
タイムアウト時間を設定する	**tacacs-server timeout** *seconds*
タイムアウト時間をデフォルトに戻す	undo **tacacs-server timeout**

デフォルト：5

1.5 AAA、RADIUSおよびTACACS+プロトコルの表示

display コマンドを実行して、AAA、RADIUS および TACACS+の設定の実行状態を表示します。

表1-15 AAA の設定情報の表示

操作	コマンド
AAAの設定情報を表示する	**display aaa**
RADIUSの設定情報を表示する	**display radius [statistics]**
TACACS+の設定情報を表示する	**display tacacs-server**

目次

このセクションのページは **9-x-x** です。

2 章 802.1X の設定 2-1

2.1 802.1X の概要 2-1

2.2 802.1X の設定 2-1

2.2.1 802.1x 対応ポートと再認証のパラメータ設定 2-1

2.2.2 フィーチャーの設定 2-2

2.2.3 ゲスト VLAN の設定 2-2

2.2.4 RADIUS-assigned QoS の有効/無効の設定 2-3

2.2.5 RADIUS-assigned VLAN の有効/無効の設定 2-3

2.2.6 再認証リクエストの最大回数の設定 2-4

2.2.7 ポートの許可状態の設定 2-4

2.2.8 定期的な再認証機能の有効/無効の設定 2-4

2.2.9 802.1X タイマの設定 2-5

2.2.10 ポートの再認証 2-5

2.3 802.1X 設定の表示 2-5

2.4 ポートの初期化 2-6

2章 802.1X の設定

2.1 802.1Xの概要

802.1X は、ポートベースのネットワークアクセスコントロールプロトコルです。

802.1X が有効になっているポートに接続された装置を、認証サーバ(RADIUS サーバなど)で認証し、不正なアクセスから保護します。

802.1X 認証には以下の構成要素があります。

- クライアント（サプリカント）
- アクセス装置（オーセンティケータ）
- 認証サーバ

2.2 802.1Xの設定

802.1X の設定では、以下の設定を行います。

- 802.1x 対応ポートと再認証のパラメータを設定
- グローバルでフィーチャーの有効/無効の設定
- ゲスト VLAN の設定
- RADIUS-assigned QoS の有効/無効の設定
- RADIUS-assigned VLAN の有効/無効の設定
- 再認証リクエストの最大回数の設定
- ポートの許可状態の設定
- 定期的な再認証機能の有効/無効の設定
- ポートの再認証

2.2.1 802.1x対応ポートと再認証のパラメータ設定

802.1x 対応ポートと再認証のパラメータを設定するには、System view で以下のコマンドを実行します。

表2-1 再認証のパラメータ設定

操作	コマンド
802.1x対応ポートと再認証のパラメータを設	**dot1x authentication timer** { **inactivty**

定する	*inactivity_time* | **re-authenticate** *re-authenticate_time* }
802.1x対応ポートと再認証のパラメータをデフォルトに戻す	undo **dot1x authentication timer** { **inactivty | re-authenticate** }

デフォルト：re-authenticate 3600

2.2.2 フィーチャーの設定

グローバルでフィーチャーの有効/無効を設定するには、System view で以下のコマンドを実行します。

表2-2 再認証のパラメータ設定

操作	コマンド
グローバルでゲストVLAN/ RADIUS-assigned QoS/ RADIUS-assigned VLANを有効にする	**dot1x feature** { **guest-vlan** | **radius-qos** | **radius-vlan** }*
グローバルでゲストVLAN/ RADIUS-assigned QoS/ RADIUS-assigned VLANを無効する	**undo dot1x feature** { **guest-vlan** | **radius-qos** | **radius-vlan** }*

デフォルト：無効

2.2.3 ゲストVLANの設定

ゲスト VLAN の ID やポートのゲスト VLAN の有効/無効を設定するには、System view および Ethernet port view で以下の手順でコマンドを実行します。

表2-3 ゲスト VLAN の設定

操作	コマンド	備考
1. System-viewに移行する	**system-view**	-
2. スイッチでゲストVLANを有効にする	**dot1x guest-vlan supplicant**	デフォルト：無効
3. ゲストVLANのIDを設定する	**dot1x guest-vlan** *vlan_id*	デフォルト：設定なし
4. Ethernet port viewに移行する	**interface** *interface-type*	-

	interface-number	
5. ポートのゲストVLANを有効にする	**dot1x guest-vlan**	デフォルト：無効

2.2.4 RADIUS-assigned QoSの有効/無効の設定

ポートで RADIUS-assigned QoS の有効/無効を設定するには、Ethernet port view で以下のコマンドを実行します。

表2-4 RADIUS-assigned QoS の有効/無効の設定

操作	コマンド
ポートでRADIUS-assigned QoSを有効に設定する	**dot1x radius-qos**
ポートでRADIUS-assigned QoSを無効に設定する	**undo dot1x radius-qos**

デフォルト：無効

2.2.5 RADIUS-assigned VLANの有効/無効の設定

ポートで RADIUS-assigned VLAN の有効/無効を設定するには、Ethernet port view で以下のコマンドを実行します。

表2-5 RADIUS-assigned VLAN の有効/無効の設定

操作	コマンド
ポートでRADIUS-assigned VLANを有効に設定する	**dot1x radius-vlan**
ポートでRADIUS-assigned VLANを無効に設定する	**undo dot1x radius-vlan**

デフォルト：無効

2.2.6 再認証リクエストの最大回数の設定

再認証リクエストの最大回数を設定するには、System view で以下のコマンドを実行します。

表2-6 再認証リクエストの最大回数の設定

操作	コマンド
再認証リクエストの最大回数を設定する	**dot1x max-reauth-req** *times*
再認証リクエストの最大回数をデフォルトに戻す	**undo dot1x max-reauth-req**

デフォルト：2

2.2.7 ポートの許可状態の設定

ポートの許可状態を設定するには、Ethernet port view で以下のコマンドを実行します。

表2-7 ポートの許可状態の設定

操作	コマンド
ポートの許可状態を設定する	**dot1x port-control** { **force-authorized** | **force-unauthorized** | **auto** | **single** | **multi** | **mac-based** }
ポートの許可状態をデフォルトに戻す	**undo dot1x port-control**

デフォルト：force-authorized

2.2.8 定期的な再認証機能の有効/無効の設定

定期的な再認証機能の有効/無効を設定するには、System view で以下のコマンドを実行します。

表2-8 定期的な再認証機能の有効/無効の設定

操作	コマンド
定期的な再認証機能を有効に設定する	**dot1x re-authentication**

定期的な再認証機能を無効に設定する	**undo dot1x re-authentication**

デフォルト：無効

2.2.9 802.1Xタイマの設定

802.1X タイマを設定するには、System view で以下のコマンドを実行します。

表2-9 802.1X タイマの設定

操作	コマンド
802.1Xタイマを設定する	**dot1x timeout { quiet-period** *quiet_seconds* **| tx-period** *tx_seconds* **}**
802.1Xタイマをデフォルトに戻す	**undo dot1x re-authentication**

デフォルト：quiet-period 60、tx-period 5

2.2.10 ポートの再認証

ポートを再認証するには、Ethernet port view で以下のコマンドを実行します。

表2-10 ポートの再認証

操作	コマンド
ポートの許可状態を設定する	**dot1x re-authenticate**

2.3 802.1X設定の表示

display コマンドを実行して、802.1X の設定の状態を表示します。

表2-11 802.1X の設定情報の表示

操作	コマンド
ステータスを表示する	**display dot1x status**
統計情報を表示する	**display dot1x statistics** { **all** | **eapol** | **radius** } [**interface** *interface-type*

	interface-number]
統計情報をリセットする	**reset dot1x statistics [interface** *interface-type interface-number* **]**

2.4 ポートの初期化

ポートを初期化するには、User view で以下のコマンドを実行します。

表2-12 ポートの初期化

操作	コマンド
ポートを初期化する	**dot1x initialize [interface** *interface_num* **]**